Panda Systems Management

Guía de administración de Panda Systems Management

Versión: 11.3.00-01

Autor: Panda Security

Fecha: 08/08/2023

panda

pandasecurity.com

Aviso legal.

Marcas registradas.

Información de contacto.

Oficinas centrales:

Panda Security
Calle Santiago de Compostela 12
Bilbao (Bizkaia) 48003 España.
https://www.pandasecurity.com/spain/about/contact/

Acerca de la Guía de administración

- Para obtener la versión más reciente de esta guía consulta la dirección web:

https://www.pandasecurity.com/rfiles/enterprise/documentation/pcsm/docswebpage/SYSTEMSMANAGEMENT-Manual-ES.pdf

Información sobre las novedades de la versión

Para conocer las novedades de la última versión de Panda Systems Management consulta la siguiente URL:

https://www.pandasecurity.com/spain/support/card?id=300121

Soporte técnico

Panda Security ofrece un soporte técnico global cuyo objetivo principal es responder a cuestiones específicas sobre el funcionamiento de sus productos. El equipo de soporte técnico también genera documentación sobre detalles técnicos del producto, que ofrece a través de su portal eKnowledge Base.

- Para acceder a información específica del producto consulta la siguiente URL:

https://www.pandasecurity.com/spain/support/cloud-systems-management.htm

- Para acceder al portal eKnowledge Base consulta la siguiente URL:

https://www.pandasecurity.com/spain/support/#enterprise

Encuesta sobre la Guía de administración

Evalúa esta guía para administradores y enviamos sugerencias y peticiones para próximas versiones de la documentación en:

https://www.pandasecurity.com/spain/support/#enterprise

Tabla de contenidos

Parte 1: Introducción a Panda Systems Management

Parte 2: Instalación y organización de dispositivos

Parte 4: Visibilidad de dispositivos

Parte 5: Resolución de incidencias y soporte técnico

Parte 1

Introducción a Panda Systems Management

Capítulo 1

Prólogo

La Guía de administración de Panda Systems Management contiene información básica y procedimientos de uso para obtener el máximo beneficio del producto.

CONTENIDO DEL CAPÍTULO

¿A quién está dirigida esta guía?

El objetivo de esta guía es ofrecer información técnica sobre el producto al departamento de IT de las empresas que mantienen y gestionan sus equipos y dispositivos informáticos desde dos posibles configuraciones:

- 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.

Iconos

En esta guía se utilizan los siguientes 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.

Capítulo 2

Información básica de Panda Systems Management

Panda Systems Management es una solución basada en la nube destinada a departamentos de IT que quieren ofrecer un servicio profesional de monitorización y administración remota de dispositivos, minimizando 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 usuario se ven reducidos debido a los beneficios mostrados a continuación:

- Es un servicio alojado en la nube, por lo que requiere nula infraestructura adicional tanto en la empresa o departamento proveedor del servicio como en el parque informático administrado.
- 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 instantánea 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.

CONTENIDO DEL CAPÍTULO

Características 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 PCSM (impresoras, routers, switches, scanners, centralitas, etc.). Gestión de servidores VMware ESXi (VMware vSphere Hypervisor 4.1, 5.0, 5.1, 5.5, 6.0 y 6.5), Gestión de servidores Microsoft Hyper-V en Windows 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.
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.
Visualización de la seguridad del equipo	Muestra el estado del antivirus instalado en el equipo.
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, tales como Exchange, SQL y IIS, 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 descarga scripts previamente configurados de la ComStore y lánzalos de forma programada, o como respuesta automática a una alerta.
Gestión de parches	Automatiza el despliegue de actualizaciones y parches para los sistemas operativos Windows instalados.
Despliegue de software	Despliega de forma centralizada el software en equipos Windows, Linux, macOS e iOS de la red.

Tabla 2.1: listado de características de Panda Systems Management

Característica	Descripción
Gestión del software	Comprueba que los dispositivos administrados cumplen con las directrices de instalación de software establecidas por la empresa y actualiza las últimas versiones de los programas publicados por los proveedores del software.
Políticas	Establece configuraciones comunes en los dispositivos gestionados. Disponibles 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 impacte en el trabajo de los usuarios. Panda Systems Management soporta el intérprete de comandos PowerShell para solucionar problemas y configurar dispositivos Windows de forma avanzada. El administrador podrá conectarse a una interfaz completa de Powershell en dispositivos remotos desde cualquier lugar. La versión requerida en el dispositivo del administrador es PowerShell 5.1. La versión requerida en el dispositivo del cliente es PowerShell 2.0.
Control remoto	Acceso compartido al escritorio del usuario o control total a través del agente PCSM o directamente desde la consola web de administración. Compatible con cortafuegos y Network Address Translation (NAT).
Chat	El técnico puede invitar al usuario del dispositivo y a otros técnicos a una sesión de chat para facilitar la comunicación y la colaboración a la hora de localizar y solucionar las incidencias.
Gestión remota de dispositivos de red	Acceso a las herramientas de administración incorporadas en los dispositivos de red, impresoras y otros equipos que no admiten la instalación del agente PCSM. El administrador podrá 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	Sistema de informes flexible en formato PDF y CSV. Soporte de varios idiomas y alcance configurable hasta abarcar todo el parque informático mediante la agregación de informes.
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.
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.

Tabla 2.1: listado de características de Panda Systems Management

Perfil de usuario de Panda Systems Management

Los usuarios de Panda Systems Management son profesionales de las tecnologías de la información con un perfil técnico medio-alto, concentrándose en dos grandes grupos:

- **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.

Componentes de Panda Systems Management

- **Consola de administración Panda Systems Management**

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.

La consola de administración es un recurso accesible únicamente por los técnicos encargados de ofrecer soporte.

- **Agente PCSM**

Es un pequeño programa de tamaño menor a 10 megabytes en su versión Windows, que se instala en cada uno de los dispositivos compatibles a administrar. Una vez desplegado, el técnico de soporte podrá acceder al dispositivo a través de la consola de administración.

> *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 el apartado "***Integración de dispositivos de red***" en la página* ***54****.*

El agente admite dos modos de ejecución:

- **Modo usuario / monitor**: es la forma de ejecución normal del agente PCSM y está diseñada para pasar inadvertido 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 Panda Systems Management**

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, los 365 días del año.

La información de estado que fluye desde cada uno de los dispositivos administrados hacia el servidor Panda 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.

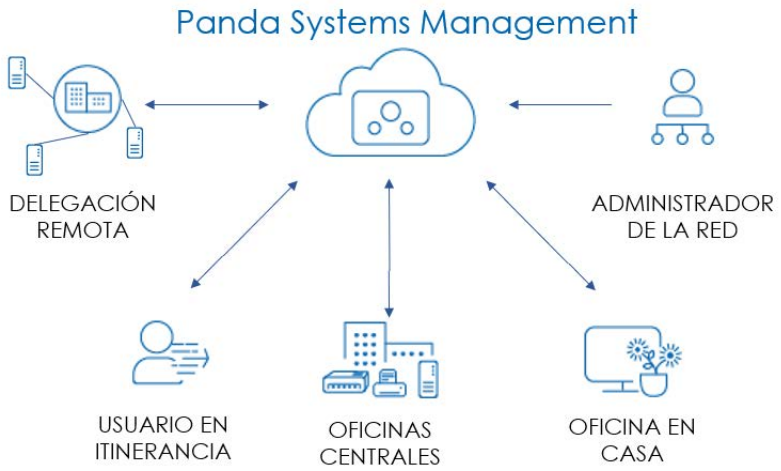


Figura 2.1: esquema básico de funcionamiento Panda Systems Management

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 adquiere el producto Panda Systems Management se le entrega una cuenta de administración principal con los máximos privilegios, capaz de gestionar todos los recursos del producto.

*Consulta el capítulo "**Cuentas de usuario y roles**" en la página **297** para crear nuevos usuarios y roles que delimiten el acceso de los técnicos de sistemas a recursos clave de Panda Systems Management.*

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. En esta guía el usuario de la consola de administración recibe el nombre de "administrador" para diferenciarlo del usuario del dispositivo gestionado.

- **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.

Capítulo 3

Elementos básicos de la consola de administración

La consola se estructura de forma intuitiva y visual distribuyendo los recursos de administración a pocos clics de distancia para minimizar 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. De esta forma tanto MSPs como administradores podrán entregar valor a sus clientes desde el primer minuto.

La consola de administración se estructura en varios bloques mostrados a continuación:

- Menú general.
- Barra de pestañas.
- Barra de iconos.
- Menú desplegable.
- Paneles de control.
- Panel de agrupaciones.
- Controles de selección.
- Listados.
- Secciones

CONTENIDO DEL CAPÍTULO

Elementos de la consola de administración

Menú general

Es el menú situado en la parte superior de la ventana, accesible desde cualquier punto de la consola, y que agrupa toda la funcionalidad de Panda Systems Management en 8 secciones o áreas mostradas a continuación.

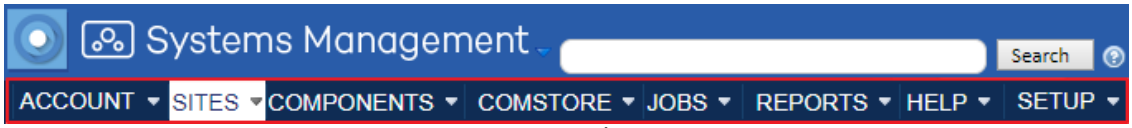


Figura 3.1: Menú general

Al pasar el ratón por cada uno de las áreas del menú general se mostrará una ventana desplegable que permite acceder de forma rápida a las pestañas que dividen la funcionalidad de cada área, mostradas en el punto siguiente.

Menú	Descripción
Cuenta	Acceso al Nivel cuenta. Para obtener más información sobre los distintos niveles implementados en Panda Systems Management consulta el apartado "**Jerarquía de niveles**".
Zonas	Acceso al Nivel cuenta y al listado de zonas. Para obtener más información sobre los distintos niveles implementados en Panda Systems Management consulta el apartado "**Jerarquía de niveles**".
Componentes	Acceso a los componentes ya descargados y disponibles para el administrador. Para obtener más información consulta el capítulo "**Componentes y ComStore**" en la página **139**.
ComStore	Repositorio de componentes creados por Panda Security que extienden la funcionalidad de Panda Systems Management. Para obtener más información consulta el capítulo "**Componentes y ComStore**" en la página **139**.
Tareas	Acceso al sistema de programación de tareas. Para obtener más información consulta el capítulo "**Tareas**" en la página **129**.
Informes	Acceso al sistema de generación de informes. Para obtener más información consulta el capítulo "**Informes**" en la página **195**.
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 "**Cuentas de usuario y roles**" en la página **297**.

Tabla 3.1: entradas del menú general

Barra de pestañas

La barra de pestañas permite el acceso a las herramientas de la consola que generan listados consolidados en pantalla. La barra de pestañas también permite acceder a herramientas para crear y visualizar configuraciones.

Dependiendo del área del menú general seleccionada, la barra de pestañas se ajustará para representar las opciones apropiadas.

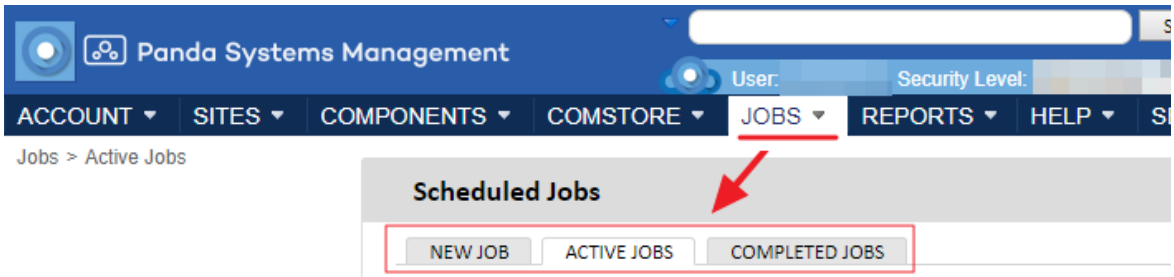


Figura 3.2: barra de pestañas del menú general Trabajos

Barra de iconos

La barra de iconos permite el acceso a operaciones que modifican el estado de los elementos seleccionados en el listado de dispositivos asociado. La barra de iconos varía tanto en el número de opciones como en su aspecto dependiendo del punto de acceso a la misma y a los elementos que afecta.

Barra de iconos que afecta a varios elementos

Haz clic en las casillas de selección **(1)** para determinar los elementos que se verán afectados por la acción, y haz clic en el icono apropiado **(2)**, situado debajo de la barra de pestañas.

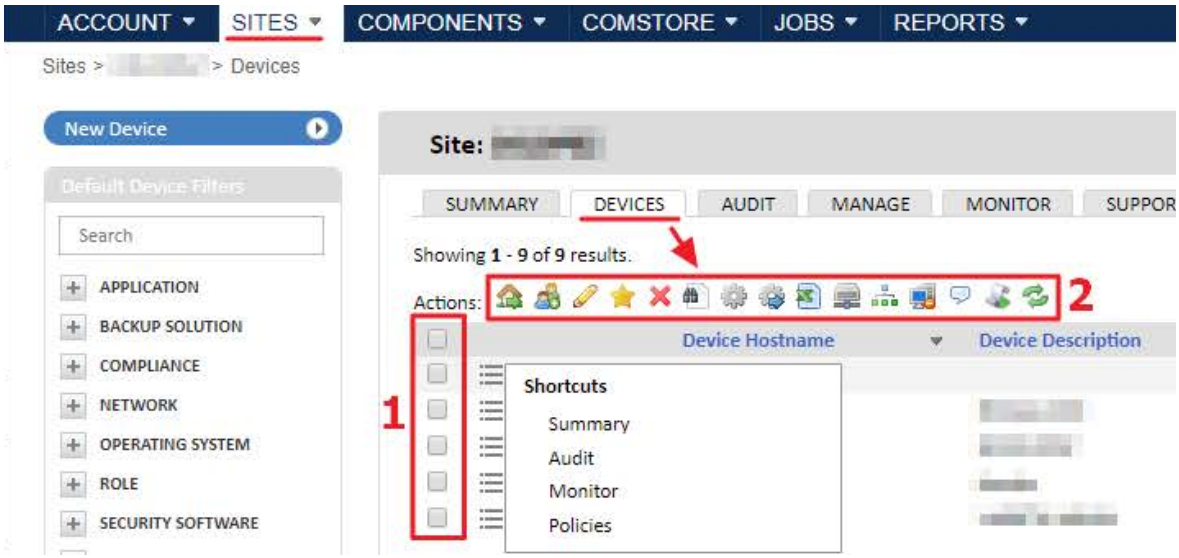


Figura 3.3: barra de iconos del menú general Zonas, menú de pestañas Dispositivos

Barra de iconos que afecta a un elemento

El aspecto visual de la barra de iconos puede variar, desde su posición, asociada al elemento que afecta, hasta su forma, en formato menú de contexto o barra de iconos estándar.

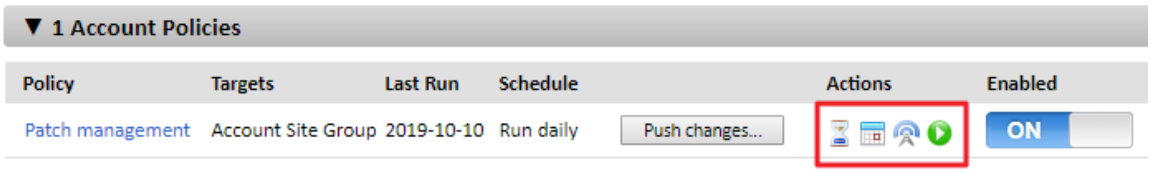


Figura 3.4: barra de iconos de formato estándar asociada a un elemento

Menú Desplegable

En algunos de los listados de la consola, junto a las casillas de selección de dispositivos, está situado el icono menú desplegable. Este icono da acceso a distintas funciones y herramientas dependiendo de la pantalla en la que se encuentre:

- En el listado de Zonas de una Cuenta, muestra los elementos de la Barra de pestañas.
- Dentro de la Zona, cuando se encuentra situado en la línea de un dispositivo, muestra la Barra de pestañas del dispositivo **(1)** y si este está online muestra las herramientas remotas disponibles **(2)**.

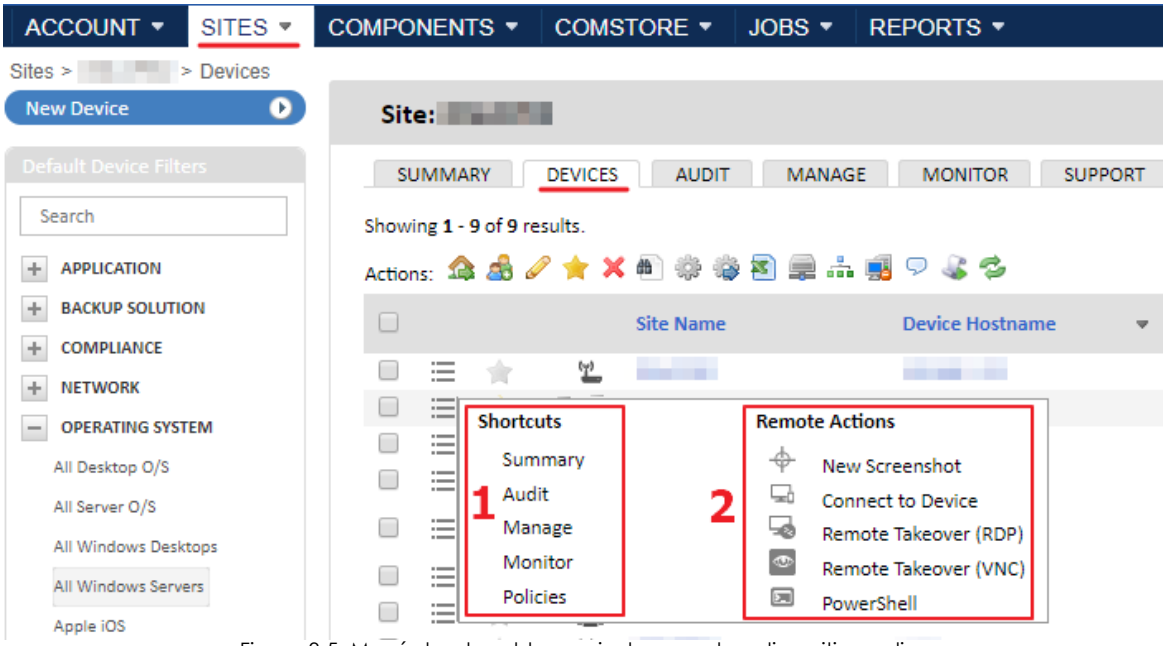


Figura 3.5: Menú desplegable en nivel zona sobre dispositivo online

Panel de agrupaciones

> *Consulta el Capítulo "**Agrupaciones de dispositivos**" en la página **69** para obtener una descripción de las diferentes agrupaciones de dispositivos disponibles en Panda Systems Management.*

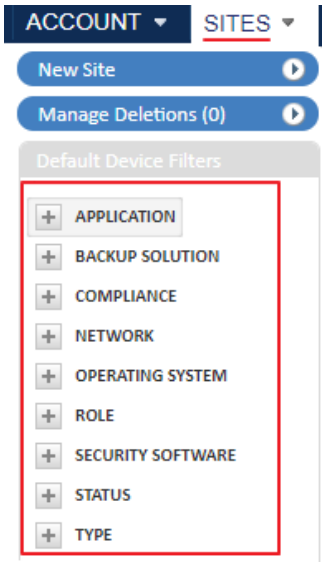


Figura 3.6: panel lateral en el menú general Zonas

En la parte izquierda de la consola se encuentran varios paneles con las agrupaciones de elementos disponibles en Panda Systems Management dependiendo del área seleccionada en el menú general y de la pestaña en la barra de pestañas.

Paneles de control

Los paneles de control (Dashboards) muestran información con diferentes grados de detalle sobre un conjunto de dispositivos. Existen tres tipos:

- Panel de control del Nivel cuenta.
- Resumen del Nivel zona.
- Resumen del Nivel dispositivo.

> *Consulta el capítulo "**Visibilidad y estado de los de dispositivos**" en la página **175** para obtener más detalle sobre la información mostrada en los distintos paneles de control. Consulta el apartado "**Jerarquía de niveles**" en este mismo capítulo para obtener una explicación sobre los diferentes niveles en los que se divide la consola de administración.*

Panel de control del Nivel cuenta

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

Este panel reúne información general del estado del parque de dispositivos: notificaciones, tareas, alertas, etc.

Resumen del Nivel zona

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

Resumen del Nivel dispositivo

Refleja el estado del dispositivo y es accesible desde cada dispositivo particular integrado en Panda Systems Management. Para acceder al Resumen del Nivel dispositivo sigue los pasos mostrados a continuación:

- Desde el menú general **Zonas**, haz clic en la zona a la que pertenece el dispositivo
- En el menú de pestañas **Dispositivos**, haz clic en el dispositivo y en la pestaña **Resumen**.

Controles de selección

Una misma ventana puede agrupar varias pantallas de configuraciones distintas accesibles desde controles de selección situados en la zona superior derecha.

Figura 3.7: Control de selección en el menú de pestañas Auditoría.

Listados

Panda Systems Management muestra listados de elementos tales como tareas, dispositivos o configuraciones utilizando una serie de controles estándar que permiten su ordenación y configuración para ajustarse a las necesidades del administrador. Estos controles son:

- Contador de elementos mostrados.
- Configuración de columnas.
- Configuración de elementos por página.
- Información de paginación.
- Configuración de filtros y búsquedas.

Contador de elementos mostrados

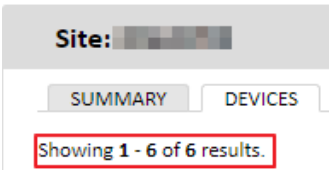


Figura 3.8: contador de elementos mostrados

Situado en la parte superior izquierda, debajo del menú de pestañas, muestra el número de elementos mostrados en el listado del total de elementos disponibles.

Configuración de columnas

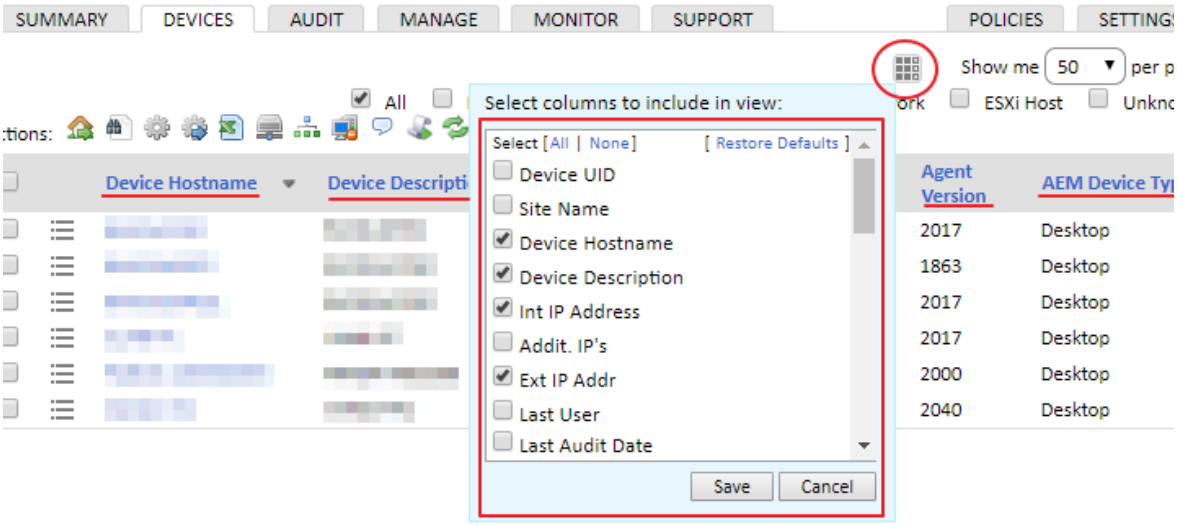


Figura 3.9: configuración de columnas en listados de dispositivos

Al hacer clic en el icono  situado en la parte superior derecha se muestra un desplegable con todas las columnas disponibles en el listado. De esta forma el administrador puede modificar la vista del listado seleccionando la información relevante que quiere visualizar.

Configuración de elementos por página

Situado en la parte superior derecha o izquierda de la ventana, permite establecer el número de elementos por página mostrados (10, 25, 50 o 100 elementos).

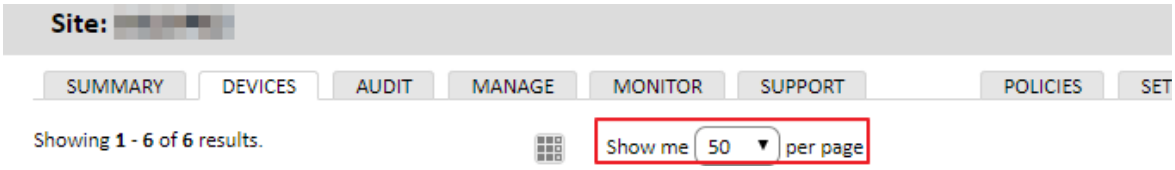


Figura 3.10: Elemento de paginación

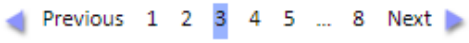


Figura 3.11: Control de paginación

Información de paginación

Situada en la parte inferior de la pantalla, indica el número de página actual y permite avanzar y retroceder de página mediante los iconos de las fechas y o saltar directamente al número de página indicado.

Configuración de filtros y búsquedas

En algunos listados especialmente largos se incluyen controles que facilitan el filtrado de resultados:

- **Desplegables**: permiten seleccionar una entre varias opciones de filtrado disponibles.
- **Búsquedas libres**: permiten búsquedas libres de texto.
- **Casillas de selección**: permite seleccionar varias opciones de búsqueda simultáneas.

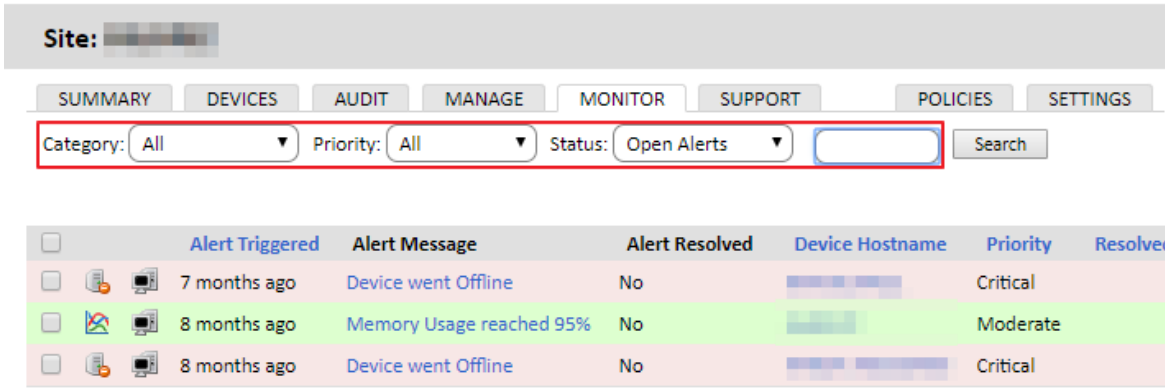


Figura 3.12: filtros y búsquedas en listados

Casillas de selección

Permiten seleccionar los elementos de los listados para actuar sobre ellos mediante la barra de iconos. Consulta la figura 3.13 **(1)**.

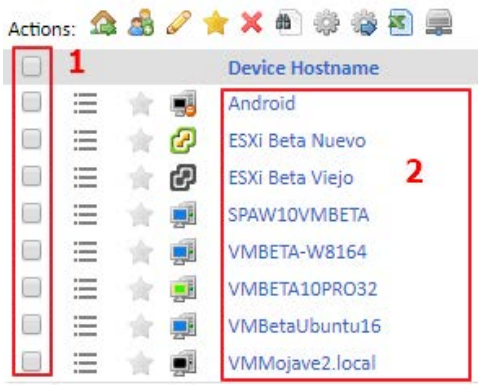


Figura 3.13: casillas de selección (1) y enlaces (2)

Enlaces

Muchos de los elementos que aparecen en listados tienen asociados un enlace **(2)** que permite cambiar de Nivel para ampliar la información mostrada (consulta el apartado "**Jerarquía de niveles**" para una aclaración sobre el concepto de Nivel y su utilización en la consola Panda Systems Management). De esta manera, los listados reúnen información resumen de los elementos y al hacer clic en un elemento concreto se mostrará información más específica sobre ese elemento.

Al trabajar con listados se distinguen dos tipos de acciones fundamentales: seleccionar uno o varios elementos para actuar sobre ellos a través de la barra de iconos, y cambiar de nivel de la consola haciendo clic en su enlace asociado. Para distinguir las dos acciones, en este manual se utiliza el verbo "seleccionar" (por ejemplo, "selecciona uno o más dispositivos del listado"), y el verbo "haz clic" (por ejemplo "haz clic en el dispositivo) para cambiar de nivel a uno inferior.

Secciones

En toda la interface de Panda Systems Management, y sobre todo en las pantallas de configuración (menú general **Ajustes** y menú de pestañas **Configuración**) la información se distribuye a lo largo de secciones que agrupan funcionalidades relacionadas.

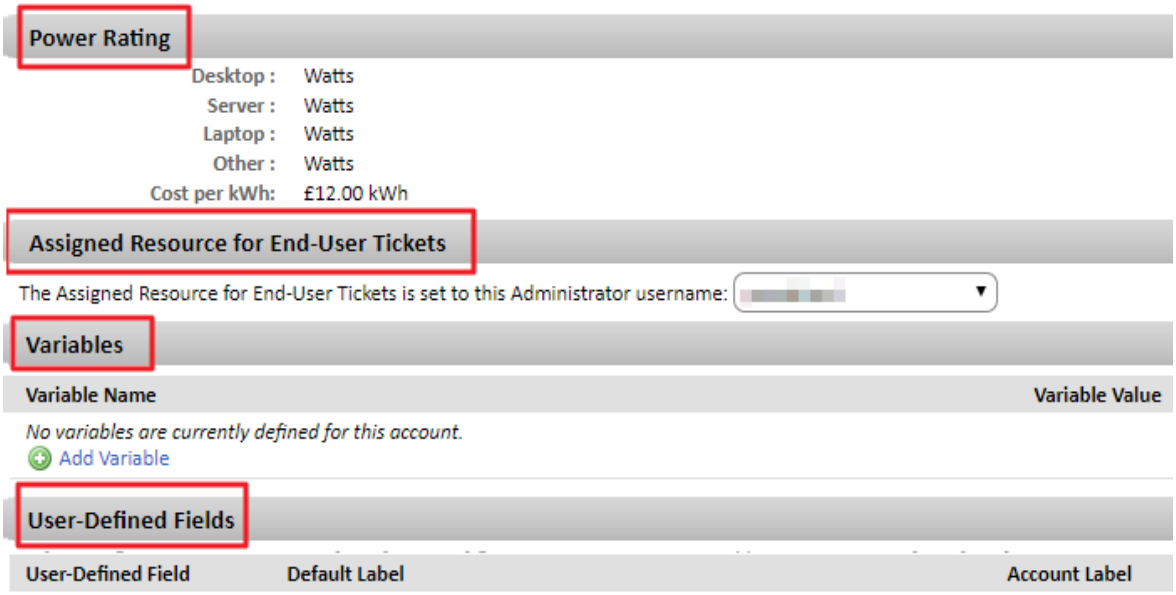


Figura 3.14: distribución de las configuraciones en secciones

Jerarquía de niveles

Panda Systems Management organiza la consola de administración en tres entidades / niveles con el objeto de simplificar su manejo y facilitar la reutilización de procedimientos establecidos por el personal técnico en la consola. Del nivel más general al más particular son las siguientes:

- Nivel cuenta.
- Nivel zona.
- Nivel dispositivo.

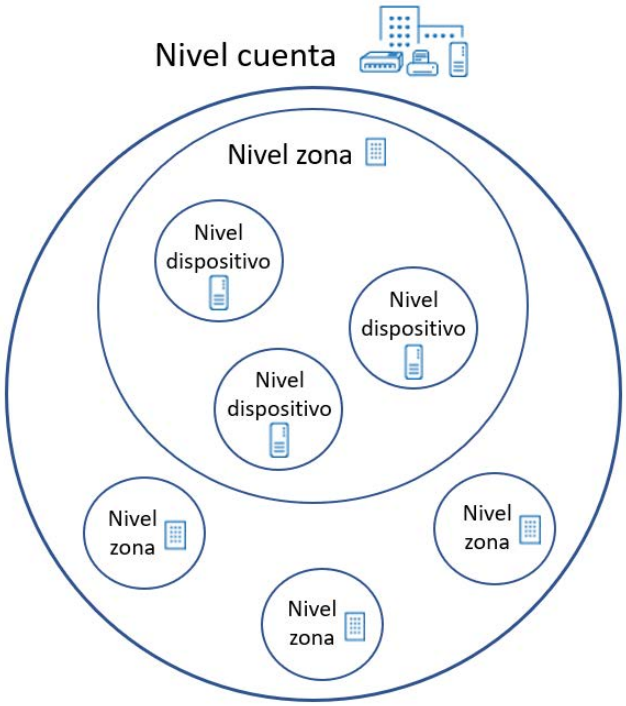


Figura 3.15: jerarquía de niveles

Nivel cuenta

¿Qué es?

El Nivel cuenta es la entidad de agrupación más general, siendo además única por cada cliente. Reúne automáticamente todos los dispositivos administrados por el MSP / departamento de IT pertenecientes a sus 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 "**Agrupaciones de dispositivos**" en la página **69**.

Acceso

Los recursos del Nivel cuenta se encuentran distribuidos en el menú general **Cuenta** y menú general **Zona**.

Figura 3.16: recursos del Nivel cuenta accesibles desde el menú general Cuenta

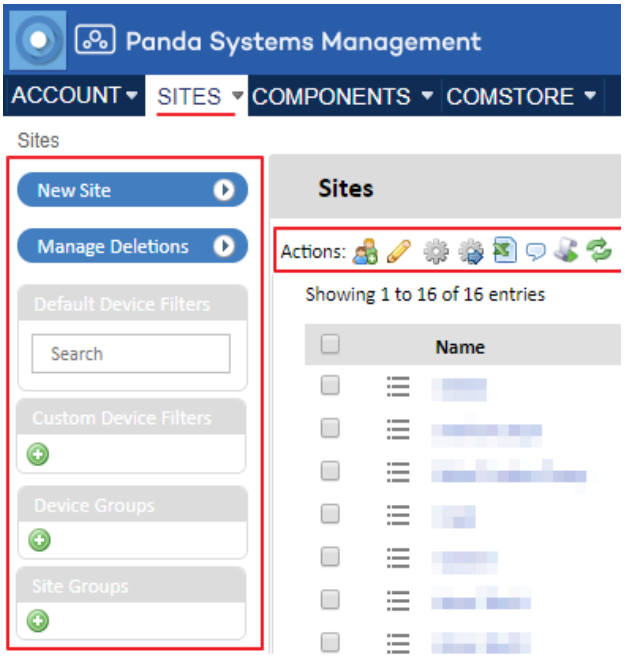


Figura 3.17: Recursos del Nivel Cuenta accesibles desde el menú general Zonas

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

Para acceder a la configuración del Nivel cuenta haz clic en el menú general **Ajustes**, **Configuración de cuenta**.

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

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 una de estas zonas agrupará 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 el menú general **Zonas**, haciendo clic en una zona y en su barra de pestañas **Configuración**. Esta configuración se añade al agente Panda Systems Management que el usuario del dispositivo instala en su equipo, aplicándose de forma automática y sin intervención del administrador.

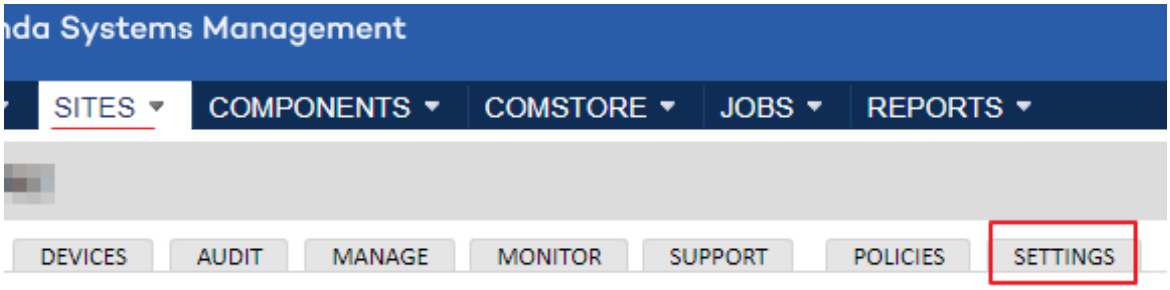


Figura 3.18: Acceso a la configuración de una zona

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 "**Agrupaciones de dispositivos**" en la página **69**.

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

Pertenencia

La pertenencia de un dispositivo administrado a una zona u otra, queda determinada por la instalación del agente PCSM, aunque desde la consola es posible mover equipos entre zonas, una vez instalado en el dispositivo del usuario. Consulta el apartado "**Mover equipos entre zonas**" en la página **71**.

> *Descarga el agente PCSM directamente desde la página de la zona elegida de forma que, al instalarse en el dispositivo del usuario, éste se agregará automáticamente a la zona en cuestión en la consola. Para más información, consulta el capítulo "**Despliegue e instalación de dispositivos**" en la página **45**.*

> *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 PCSM 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.

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

Nivel dispositivo

¿Qué es?

Es la representación lógica en la consola para un dispositivo concreto gestionado. Los Niveles dispositivo se crean automáticamente, añadiéndose uno por cada equipo del cliente con un agente PCSM 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.

Capítulo 4

Primeros pasos en Panda Systems Management

Este capítulo muestra en forma de ejemplo las tareas típicas que deberá de afrontar un administrador para desplegar, integrar y gestionar los dispositivos de la red. Así mismo se presentan de forma simplificada muchos conceptos necesarios para utilizar Panda Systems Management, aunque una explicación más profunda de los mismos se trata en capítulos posteriores, de tipo monográfico. Se recomienda seguir paso a paso las instrucciones iniciadas para familiarizarse con el producto.

A modo de resumen, las tareas para integrar y gestionar un equipo Windows en Panda Systems Management son las siguientes:

- Creación y configuración de la primera zona.
- Instalación manual del agente Panda Systems Management en un dispositivo Windows.
- Localización rápida de dispositivos mediante filtros.
- Visualización de dispositivos.
- Auditoria de hardware, software y licencias.
- Monitorización.
- Gestión de parches.
- Distribución de software.
- Resolución remota de incidencias.

En el desarrollo cada uno de estas tareas se incluye un enlace al capítulo que trata en profundidad ese aspecto de Panda Systems Management.

CONTENIDO DEL CAPÍTULO

Creación y configuración de la primera zona

*Consulta el capítulo "**Agrupaciones de dispositivos**" en la página **69** para obtener más información sobre los distintos tipos de agrupaciones soportadas por Panda Systems Management.*

Las zonas son un tipo de agrupación básica que permite separar los dispositivos integrados en la plataforma Panda Systems Management de forma que su gestión sea más eficiente para el administrador de la red.

Desde un punto de vista administrativo, la división en zonas permite ordenar en la consola Panda Systems Management los dispositivos del parque informático. Desde un punto de vista técnico, una zona lleva asociada la configuración de conectividad a Internet de los dispositivos que forman parte de ella. Como normal general, si dos dispositivos tienen la misma configuración de proxy para acceder a recursos externos a la red local no será necesaria la creación de varias zonas, pero si la configuración de acceso es distinta, se recomienda crear zonas independientes, cada una con su propia configuración de acceso.

Crear una zona y configurar la conexión a Internet

- En el menú general **Zonas** haz clic en el botón **Nueva zona** del panel lateral izquierdo.
- Rellena el campo **Nombre** y **Descripción**.
- Si los dispositivos que se integrarán en la zona tiene acceso directo a Internet elige **Tipo de proxy Ninguno**. Si acceden a través de un proxy elige el tipo adecuado y las credenciales.
- Haz clic en el botón **Guardar**.

Todos los dispositivos que se integren en la Todos los dispositivos que se integren en la zona creada heredarán de forma automática la configuración de conexión definida

Cambiar la configuración de la conexión a Internet de una zona

- En el menú general **Zonas** haz clic en la zona a modificar.
- Haz clic en el menú de pestañas **Configuración**.
- En la sección **Proxy** haz clic en el link **Editar** situado a la derecha de la ventana y rellena los datos del proxy y las credenciales necesarias.

> *La configuración de proxy en los equipos ya desplegados no cambia al actualizar dicha configuración en la zona asociada al dispositivo. Es necesario volver a descargar el agente PCSM o modificar manualmente la configuración en el agente instalado en el equipo. Consulta el apartado "Información de conexión" en la página 47.*

Instalación manual del agente en un equipo Windows

> *Consulta el capítulo "Despliegue e instalación de dispositivos" en la página 45 para obtener más información acerca de los distintos métodos de despliegue implementados en Panda Systems Management y de los requisitos que tienen que cumplir los dispositivos.*

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

- La zona en la consola de administración a la que va a pertenecer.
- La información mínima para poder acceder a Internet desde el dispositivo y conectarse con el servidor Panda Systems Management.

Al generar el paquete de instalación desde la zona, Panda Systems Management incorpora de forma automática esta información en el instalador, de forma que no es necesaria ninguna configuración posterior en el equipo del usuario.

Descarga del agente PCSM para Windows

- En el menú general **Zonas**, haz clic en la zona recién creada.
- Haz clic en el botón **Nuevo dispositivo** situado en el panel lateral izquierdo. Se mostrará una ventana con las plataformas soportadas. Selecciona la plataforma Windows.

Figura 4.1: ventana de selección de plataforma para descargar el agente PCSM

Figura 4.2: Agente PCSM en la barra de notificaciones de Windows

- El paquete de instalación se descargará en el equipo del administrador. Copia el instalador en un dispositivo USB, compártelo en la red o envíaselo al usuario por correo electrónico.
- Una vez recibido el agente en el equipo Windows a integrar, haz doble clic sobre el instalador. La instalación es silenciosa y al poco tiempo se mostrará el icono de Panda Systems Management en el área de notificaciones de la barra de tareas.

Comprueba que el equipo está correctamente integrado

- Haz clic en el menú general **Zonas** y en la zona creada en el paso anterior.
- Haz clic en el menú de pestañas **Dispositivos**. Se mostrará un listado con todos los dispositivos integrados en la zona junto a información sobre el hardware y su estado.

Localización rápida de dispositivos mediante filtros

*Consulta el capítulo "**Agrupaciones de dispositivos**" en la página **69** para obtener más información sobre los distintos tipos de agrupaciones soportados por Panda Systems Management.*

Para agilizar la gestión de los dispositivos integrados en Panda Systems Management se ofrecen varios tipos de agrupaciones, algunas de tipo estático y otras de tipo dinámico. En este momento ya hemos utilizado una agrupación de tipo estático, las zonas, y ahora utilizaremos otro tipo de agrupación dinámica: los filtros.

Panda Systems Management incorpora de serie una gran cantidad de filtros predefinidos que permiten localizar de forma rápida los dispositivos gestionados.

Panel lateral de filtros

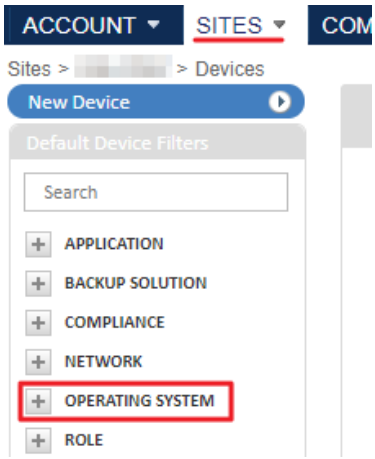


Figura 4.3: panel lateral Filtros

Para utilizar el sistema de filtros sigue los pasos mostrados a continuación:

- Haz clic en el menú general **Zonas** y en la zona creada en el primer paso.
- El panel de la izquierda **Filtro de dispositivos** agrupa los filtros predefinidos en varias categorías. Haz clic en el botón + para desplegar la agrupación **Sistema operativo** y localiza el filtro que se corresponda con la versión del sistema operativo instalado en el dispositivo integrado.
- Al hacer clic en el filtro, el listado del panel de la derecha se actualiza para reflejar únicamente los dispositivos que concuerden con los criterios definidos en el filtro. Si se cambia la versión del sistema operativo del dispositivo, éste se integrará en el filtro apropiado de forma automática. Por esta razón los filtros son agrupaciones dinámicas.

Visualización de dispositivos

*Consulta el capítulo "**Visibilidad y estado de los de dispositivos**" en la página **175** para obtener más información sobre los recursos implementados en Panda Systems Management para visualizar el estado de los dispositivos gestionados.*

Panda Systems Management incorpora varias vistas que facilitan la presentación de información sobre los dispositivos gestionados con distintos grados de detalle.

Vista general de los dispositivos de la zona

Para obtener un resumen del estado de los dispositivos integrados en una zona sigue los pasos mostrados a continuación:

- Haz clic en el menú general **Zonas** y en la zona creada anteriormente.
- Haz clic en el menú de pestañas **Resumen** para visualizar un dashboard que consolida la información obtenida de los dispositivos integrados en la zona.
- En esta ventana se muestra información sobre el estado de los dispositivos (online, offline), consumos energéticos, antivirus y estado del parcheo del sistema operativo.

Vista detalle de los dispositivos de la zona

- Haz clic en el menú general **Zonas** y en la zona creada anteriormente.
- Haz clic en el menú de pestañas **Dispositivos** para visualizar un listado de los dispositivos integrados en la zona. Cada línea contiene una serie de columnas con información particular del dispositivo

- Para configurar el listado añadiendo o eliminando columnas haz clic en el icono de seleccionar columnas **(1)**.
- Filtra el listado según el tipo dispositivo a mostrar con las casillas de selección situadas encima de la barra de iconos **(2)**.

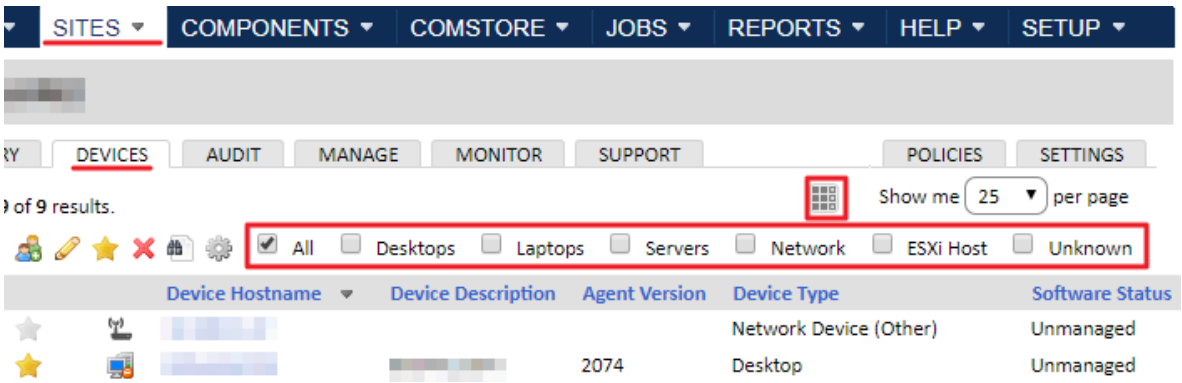


Figura 4.4: herramientas de filtrado y visualización de información de los dispositivos

Vista detalle de un dispositivo particular

- Haz clic en el menú general **Zonas** y en la zona creada anteriormente.
- Haz clic en el menú de pestañas **Dispositivos** y en el nombre del dispositivo creado.
- Haz clic en el menú de pestañas **Resumen**. Se mostrará una ventana con información más detallada del dispositivo: información del sistema operativo, estado del dispositivo, captura de pantalla del escritorio y gráficas de rendimiento de la CPU, consumo de disco duro y memoria.

Auditoria de hardware, software y licencias

*Consulta el capítulo "**Auditoria de activos**" en la página **159** para obtener más información acerca del recurso de auditorías de hardware, software y licencias.*

La funcionalidad de auditoria muestra una gran cantidad de información útil de los dispositivos administrados y de la red de la empresa.

Acceso al recurso de auditoría

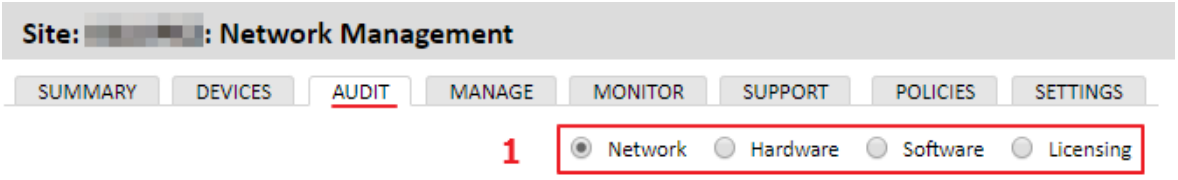


Figura 4.5: tipos de información recogidos por la herramienta Auditoría

- Haz clic en el menú general **Zonas** y en la zona creada. Se mostrará el listado de dispositivos integrados en la zona.

- Haz clic en el dispositivo integrado y en el menú de pestañas **Auditoría**.
- Haz clic en el control de selección **(1)** para mostrar el tipo de información requerido:
  - **Hardware**: información sobre el hardware instalado en el dispositivo.
  - **Software**: información sobre el software instalado en el dispositivo.
  - **Servicios:** información sobre los servicios instalados en el sistema operativo y su estado.
  - **Registro de cambios:** información sobre los cambios hardware, software y relativos al sistema efectuados en el dispositivo.
  - **Actividad:** listado de las acciones efectuadas en el dispositivo, tanto las promovidas por Panda Systems Management como por el administrador de la red.

Monitorización de dispositivos Windows

*Consulta el capítulo "**Monitorización**" en la página **111** para obtener más información acerca de los recursos de monitorización implementados en Panda Systems Management. Consulta el capítulo "**Alertas y tickets**" en la página **259** para obtener más información sobre la alertas y tickets generados por los monitores.*

Panda Systems Management monitoriza el estado de los recursos de los dispositivos de forma automática y constante, generando alertas en el caso de que algún parámetro caiga fuera de los umbrales establecidos. El sistema de monitorización es flexible ya que permite su extensión mediante componentes de creación propia o diseñados por Panda Security y publicados en la tienda ComStore.

Monitorizar puestos de trabajo Windows

Las políticas de Windows: Workstation ofrecen métricas basadas en el estado general Windows, y generan alertas cuando la situación del sistema se acerca o sobrepasa los límites marcados para el correcto funcionamiento. Estas métricas se obtienen de Monitor de disco y Monitor de servicio.

Para acceder a los monitores predefinidos sigue los pasos mostrados a continuación:

- Haz clic en el menú general **ComStore**, la tienda de componentes gratuita de Panda Security.
- En el menú lateral elige el tipo de componentes que se van a mostrar: **Políticas de monitorización**.
- Haz clic en el botón **Añadir políticas de cuenta** en el componente **Windows: Workstation**. Se mostrará una ventana con el detalle de la política de monitorización a agregar: destino de la

política (todas las estaciones Windows) y los monitores que incluye la política.

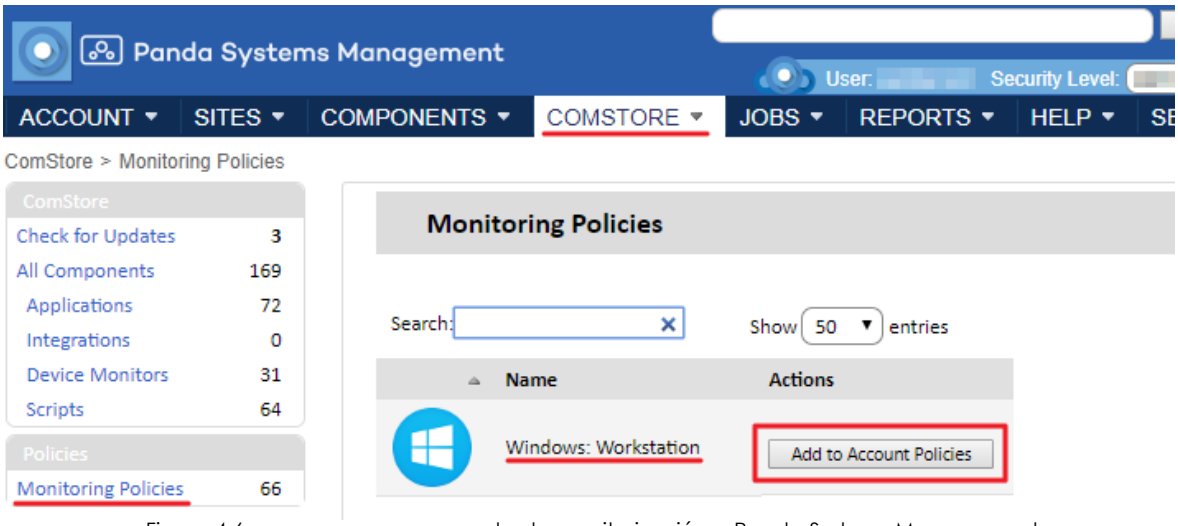


Figura 4.6: agregar un componente de monitorización a Panda Systems Management

- Haz clic en el botón **Guardar** y se mostrará la ventana de políticas asignadas. Para que la política se despliegue en los dispositivos haz clic en el botón **Desplegar cambios (1)** y espera unos minutos a que el icono **(2)** se vuelva azul. Comprueba también que el botón **ON (3)** está activado.

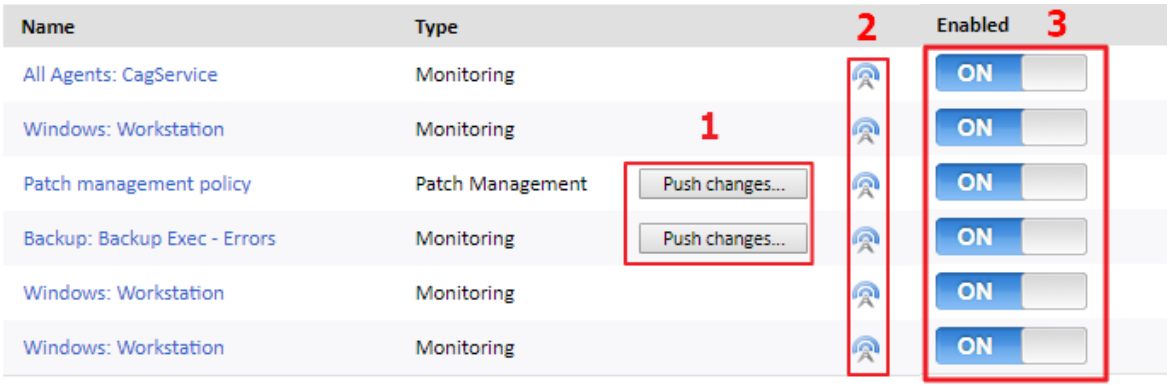


Figura 4.7: listado de políticas asignadas a la zona

Una vez desplegada la política de monitorización consulta las alertas que se generen siguiendo los pasos mostrados a continuación:

- Haz clic en el menú general **Zonas** y en la zona creada anteriormente.
- Haz clic en el menú de pestañas **Dispositivos** y en el dispositivo integrado anteriormente.
- Haz clic en el menú de pestañas **Monitorización** y en el control de selección **Alertas de monitorización** situado en la parte superior derecha de la ventana.
- Establece en el filtro de búsqueda el criterio **Estado**: **todas las alertas**, para mostrar tanto las alertas

que se han resuelto como las que todavía están abiertas.

> *Cuando se abra una nueva cuenta en Panda Systems Management se le aplicará de forma automática una política de monitorización Windows: Workstation y Windows: Server.*

Distribución de software mediante tareas inmediatas

> *Consulta el capítulo "**Distribución e instalación centralizada de software**" en la página **233** para obtener más información sobre las distintas estrategias que se pueden implementar con Panda Systems Management para distribuir software de forma centralizada.*

Panda Systems Management permite distribuir de forma remota y centralizada paquetes software publicados en la ComStore o creados por el administrador de la red sin necesidad de configurar servidores que actúen como repositorio en la oficina. En este ejemplo se distribuirá un paquete con el navegador web Firefox.

Distribución del navegador Firefox

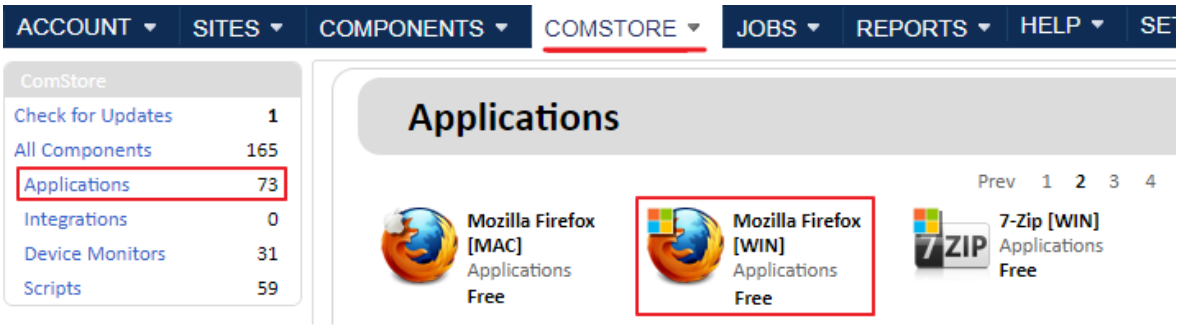


Figura 4.8: descarga del paquete Firefox de la tienda de componentes gratuitos ComStore

- Haz clic en el menú superior **ComStore**, la tienda gratuita de aplicaciones y componentes de Panda Security.
- En el panel lateral **ComStore** haz clic en **Aplicaciones**. El panel de la derecha se actualizará con un listado de las aplicaciones disponibles.
- Localiza la aplicación `Firefox Multi-lingual [WIN]` y haz clic sobre ella. Se mostrará una ventana con la descripción del componente.
- Al hacer clic en el botón **Añadir a mi biblioteca de componentes**, Panda Systems Management descargará el paquete en el repositorio de componentes del administrador, situado en el área **Componentes**. Este paso es necesario para poder utilizar cualquier componente publicado en la ComStore.
- Haz clic en el menú general **Componentes** para comprobar que se añadió `Firefox Multi-lingual [WIN]` al listado.

Una vez añadido el componente al repositorio del administrador es necesario crear una tarea para distribuir el paquete de instalación entre todos los dispositivos:

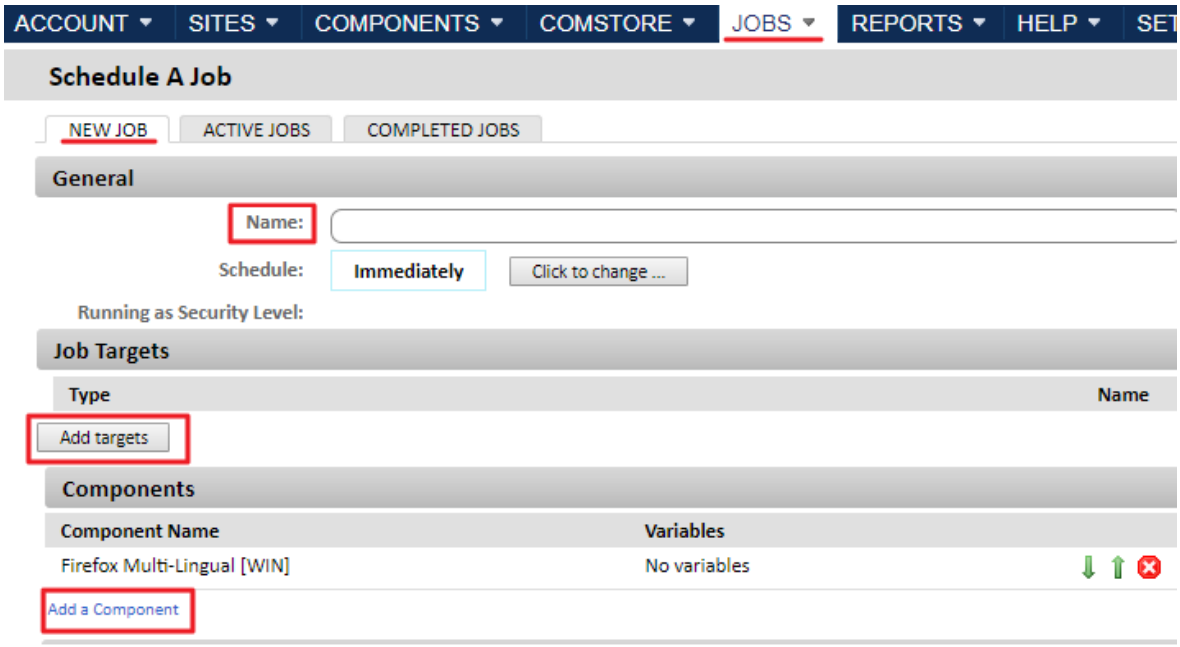


Figura 4.9: preparación de una tarea

- Haz clic en el menú general **Tareas**, menú de pestañas **Nueva tarea.**
- Introduce un nombre descriptivo para la tarea en el campo **Nombre** y añade un destino para la tarea en la sección **Destinatarios de la tarea** con el botón **Añadir dispositivos**. Se mostrará una ventana con el desplegable **Tipo de agrupación** donde aparecen todos los tipos de agrupaciones soportados por Panda Systems Management. Para instalar el componente en todos los dispositivos de una o varias zonas selecciona en el desplegable **Zonas**, elige la zona creada y haz clic en el botón **Añadir**.
- En la sección **Componentes** haz clic en el link **Añadir componente**. Se mostrará una ventana con todos los componentes de tipo aplicación almacenados en el repositorio del administrador. Selecciona el componente `Firefox Multi-lingual [WIN]` y haz clic en el botón **Guardar**.
- Haz clic en el botón **Guardar**.

Una vez creada la tarea, ésta se ejecutará de forma inmediata. Para comprobar el estado de la tarea haz clic en el menú general **Tareas**, menú de pestañas **Tareas activas**.

Gestión de parches

> *Consulta el capítulo "**Gestión de parches**" en la página **211** para obtener más información sobre la distintas estrategias implementadas en Panda Systems Management para mantener actualizados los sistemas operativos Windows de los equipos gestionados.*

Panda Systems Management mantiene actualizados los dispositivos de la red de forma centralizada a través de políticas de gestión de parches.

Configuración y despliegue de políticas Windows Update

- En el menú general **Zonas** elige la zona creada y haz clic en el menú de pestañas **Políticas.**
- Haz clic en el botón **Nueva política de zona**, elige el tipo **Windows Update** y haz clic en el botón **Siguiente**.
- Haz clic en el botón **Añadir dispositivos** y en el desplegable **Tipo de agrupación** selecciona **Filtro predeterminado de dispositivos**. Se mostrará el listado de filtros incluidos por defecto en la consola. Consulta el apartado "**Filtros de dispositivos**" en la página **76** para una descripción de los mismos. Selecciona el filtro **Todas las estaciones** para activar la funcionalidad de gestión de parches en todos los equipos de usuario.

> *Gestión de parches solo soporta dispositivos basados en Microsoft Windows.*

- En la sección **Opciones de política de Windows**, elige la política de parches **Descargar automáticamente las actualizaciones recomendadas para mi ordenador e instalarlas**.
- En la opción **Reinicio** marca la casilla **No hay reinicio automático con usuarios conectados para instalaciones de actualizaciones automáticas programadas** para evitar el reinicio incondicional del equipo de usuario.
- Haz clic en el botón **Guardar** y se mostrará la ventana de políticas asignadas. Para que la política se despliegue en los dispositivos haz clic en el botón **Desplegar cambios** y espera unos minutos a que el icono se vuelva azul. Comprueba también que el botón **ON** está activado.

Resolución remota de incidencias

*Consulta el capítulo "**Herramientas de acceso remoto a dispositivos**" en la página **271** para obtener más información sobre las herramientas remotas de acceso y resolución de problemas disponibles en Panda Systems Management.*

Panda Systems Management permite acceder remotamente a los dispositivos gestionados. Para ello es necesario que el equipo del administrador que accederá al equipo remoto tenga también instalado el agente PCSM.

De todas las herramientas de gestión remota de dispositivos que se incorporan solo unas pocas interfieren en las tareas del usuario; la mayor parte de ellas se ejecutarán en segundo plano pasando inadvertidas al usuario del dispositivo. Algunas de estas herramientas son directamente accesibles desde la consola de administración, otras sin embargo es necesario lanzarlas a través del agente PCSM.

Acceso al escritorio remoto con el protocolo VNC en dispositivos Windows

En este caso se utilizará una herramienta que permite acceder al escritorio remoto del equipo del usuario, con lo que se interrumpirá momentáneamente su trabajo. El acceso a la herramienta es a través de la consola de administración.

- En el menú general **Zonas** elige la zona creada y haz clic en el menú de pestañas **Dispositivos.**
- En el menú de contexto del dispositivo creado elige la opción **Control remoto VNC**. Se abrirá el agente Panda Systems Management con las credenciales correctas y se conectará al dispositivo de forma automática.

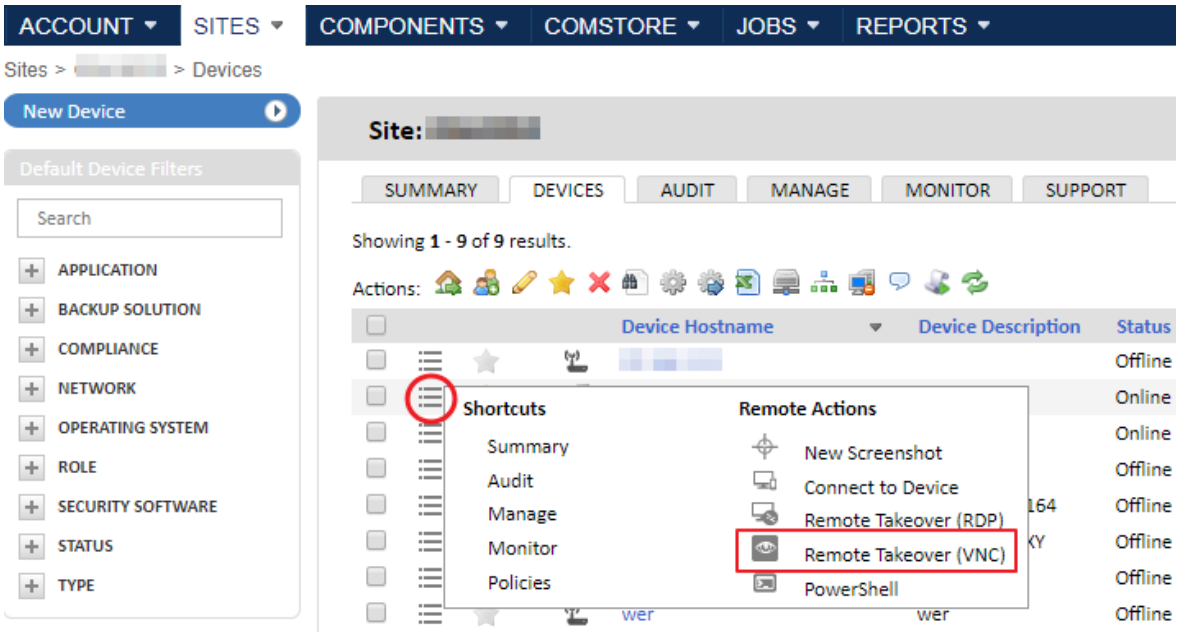


Figura 4.10: acceso a la herramienta de escritorio remoto desde la consola de administración

Monitor de recursos y línea de comandos remota

En este caso se accederá remotamente al gestor de tareas del dispositivo Windows y se abrirá una línea de comandos para hacer "troubleshooting", sin interferir con el trabajo del usuario.

Figura 4.11: Agente PCSM y herramientas disponibles

- En el menú general **Zonas** elige la zona creada y haz clic en el menú de pestañas **Dispositivos.**
- En el menú de contexto del dispositivo creado elige la opción **Conectar con dispositivo.** Se mostrará en primer plano el agente PCSM con las credenciales del administrador ya introducidas y conectado al equipo seleccionado.
- Haz clic en la barra de botones del panel izquierdo para lanzar las herramientas de resolución de problemas indicadas en la figura **4.11**.

Parte 2

Instalación y organización de dispositivos

Capítulo 5: Despliegue e instalación de dispositivos

Capítulo 6: Agrupaciones de dispositivos

Capítulo 5

Despliegue e instalación de dispositivos

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 PCSM recoge, cataloga y muestra en tiempo real y de forma ordenada en la consola.

El servidor Panda Systems Management y los dispositivos se comunican de tres maneras posibles:

- De forma directa instalando el agente PCSM en plataformas compatibles. En este escenario los agentes tienen salida a Internet para comunicarse con el servidor sin intermediarios.
- De forma indirecta a través de un proxy en dispositivos compatibles con el agente PCSM que no tengan acceso a Internet de forma directa.
- De forma indirecta a través del protocolo SNMP o de otros protocolos propietarios (ESXi) en dispositivos no compatibles con la instalación del agente PCSM.
- 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 PCSM 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 Panda Systems Management.

Por razones de seguridad se ha suprimido la posibilidad de asignar a un dispositivo el rol de nodo caché, aunque esta funcionalidad puede decir apareciendo en la consola de administración.

CONTENIDO DEL CAPÍTULO

Preparativos para integrar dispositivos al servicio

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

- Comprobar la compatibilidad del dispositivo con PCSM.
- Zona de pertenencia del agente.
- Información sobre la conexión del dispositivo a Internet.

Comprobar la compatibilidad del dispositivo con PCSM

El agente PCSM es compatible con los sistemas operativos Windows, Linux, macOS, Android e iOS, Consulta el capítulo "**Plataformas soportadas y requisitos**" en la página **317** para verificar que la versión del sistema operativo instalado en el dispositivo está soportada por Panda Systems Management. Si el dispositivo no lleva instalado un sistema operativo compatible o no admite la instalación de programas externos, como es el caso de routers, impresoras y otros dispositivos de red, consulta el apartado "**Integración de dispositivos de red**".

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**".

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 específica.

Los datos de configuración de proxy pueden ser introducidos de diversas maneras:

- **Manualmente en cada agente instalado**: en el propio dispositivo haz clic con el botón de la derecha del ratón 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**: en la consola de administración, desde el menú general **Zonas** haz clic en 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.

Distribución del agente PCSM por email

Este método de despliegue es compatible con:

- Equipos de escritorio, servidores o portátiles Windows, Linux y macOS.
- Teléfonos móviles y tablets iOS y Android.

Este método está indicado en las situaciones siguientes:

- Cuando no esté disponible una infraestructura de dominio que permita un despliegue centralizado a través de GPO u otras herramientas equivalentes de terceros.
- Cuando no haya ningún otro agente PCSM instalado en la red.
- Cuando el tamaño de la red es pequeño y no merece la pena configurar un despliegue centralizado.

Para enviar el paquete de instalación del agente PCSM por email:

- Desde el menú general **Zonas**, elige la zona donde residirán los equipos a integrar.
- Haz clic en barra de pestañas **Dispositivos** y en el botón **Añadir un dispositivo** situado en la parte superior izquierda de la pantalla. 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).

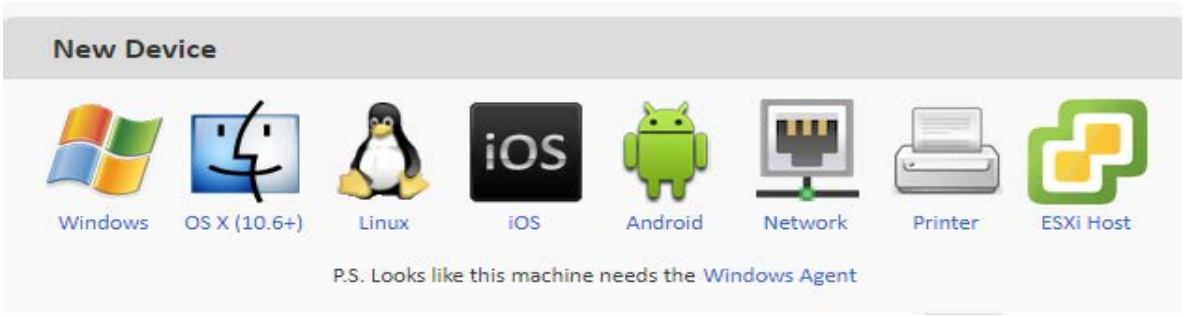


Figura 5.1: plataformas compatibles con Panda Systems Management

- Haz clic en la plataforma elegida e 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.

> *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.*

- 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** situado en la parte inferior de la ventana.

Distribución centralizada del agente PCSM

Este método de despliegue es compatible con:

- Equipos de escritorio, servidores o portátiles Windows, Linux y macOS.

Este método está indicado en las situaciones siguientes:

- Cuando se cuenta con una herramienta de distribución de software de terceros ya integrada en la infraestructura IT de la empresa.

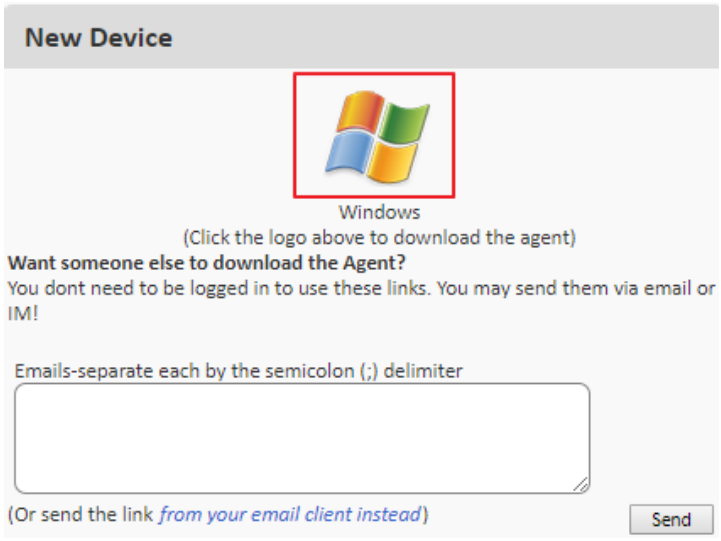


Figura 5.2: descarga directa del agente PCSM

El administrador puede descargar el agente PCSM desde la consola para luego distribuirlo de forma manual o con programas de instalación centralizada, como Active Directory. Para ello sigue el procedimiento del apartado "**Distribución del agente PCSM por email**", pero en vez de enviar un email, haz clic en el icono de la plataforma para descargar el agente PCSM en el equipo del administrador. Una vez descargado coloca el paquete de instalación en un recurso compartido accesible por los equipos de la red o configura una instalación de software mediante una GPO del directorio activo.

Distribución remota mediante el agente PCSM

Este método de despliegue es compatible con:

- Equipos de escritorio, servidores o portátiles Windows y macOS.

Este método está indicado en las situaciones siguientes:

- Cuando el número de dispositivos a integrar es alto y no se cuenta con una solución de distribución de software de terceros.

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`.

Procedimiento de distribución remota del agente PCSM

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).

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 Panda Systems Management instalado. Consulta el apartado "**Configuración de un nodo de red**" en este mismo capítulo para asignar el rol Nodo de red a un dispositivo.

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  .

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**.

3. Instala de forma remota los agentes desde la consola.

Transcurridos un máximo de 15 minutos desde el descubrimiento de la red, sigue los pasos mostrados a continuación:

- En el menú general **Zonas**, menú de pestañas **Auditoría**, selecciona **Red** en el control de selección situado en la parte superior derecha para mostrar los equipos descubiertos agrupados por su tipo.
- Selecciona los dispositivos a instalar y haz clic en el icono **Administrar equipos** en la barra de iconos.
- Elige el tipo de agente a instalar en la ventana mostrada.
- 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.
  - Haz clic en la pestaña **Configuración** de la zona a la que pertenecen los dispositivos a instalar o en el menú general **Ajustes**, **Configuración**.
  - En el apartado **Credenciales de despliegue de agentes**, haz clic en Editar y se abrirá un cuadro de texto donde indicar el nombre de usuario y la contraseña de administrador del dominio.
  - Con el botón de ON/ OFF puedes alternar en que nivel se aplican las credenciales introducidas. En ON (configuración por defecto) la plataforma utilizará las credenciales disponibles a nivel de **Cuenta** y **Zona**. En OFF, se utilizarán las introducidas a nivel de **Zona**.

> *Un agente PCSM instalado solo puede distribuir otros agentes 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 hará lo propio con dispositivos Apple.*

4. Descubrimiento de equipos en la red desde el agente PCSM (procedimiento alternativo).

En lugar de utilizar la consola de administración es posible iniciar el despliegue desde el agente PCSM de un equipo Windows. Para ello sigue los pasos mostrados a continuación:

- Haz clic en el menú general **Zonas** y en la zona donde reside el equipo descubridor.
- Haz clic en el menú de pestañas **Dispositivos y** en el menú de contexto asociado al dispositivo que distribuirá el agente PCSM haz clic en **Conectar con dispositivo**. Se abrirá el agente PCSM instalado en el equipo del administrador.
- En el menú **Herramientas** del agente PCSM haz clic en **Despliegue del agente** y en el botón **Descubrimiento de dispositivos** para mostrar todos los equipos conectados a la misma subred del

dispositivo e indicar si ya tienen un agente Panda Systems Management instalado y su versión.

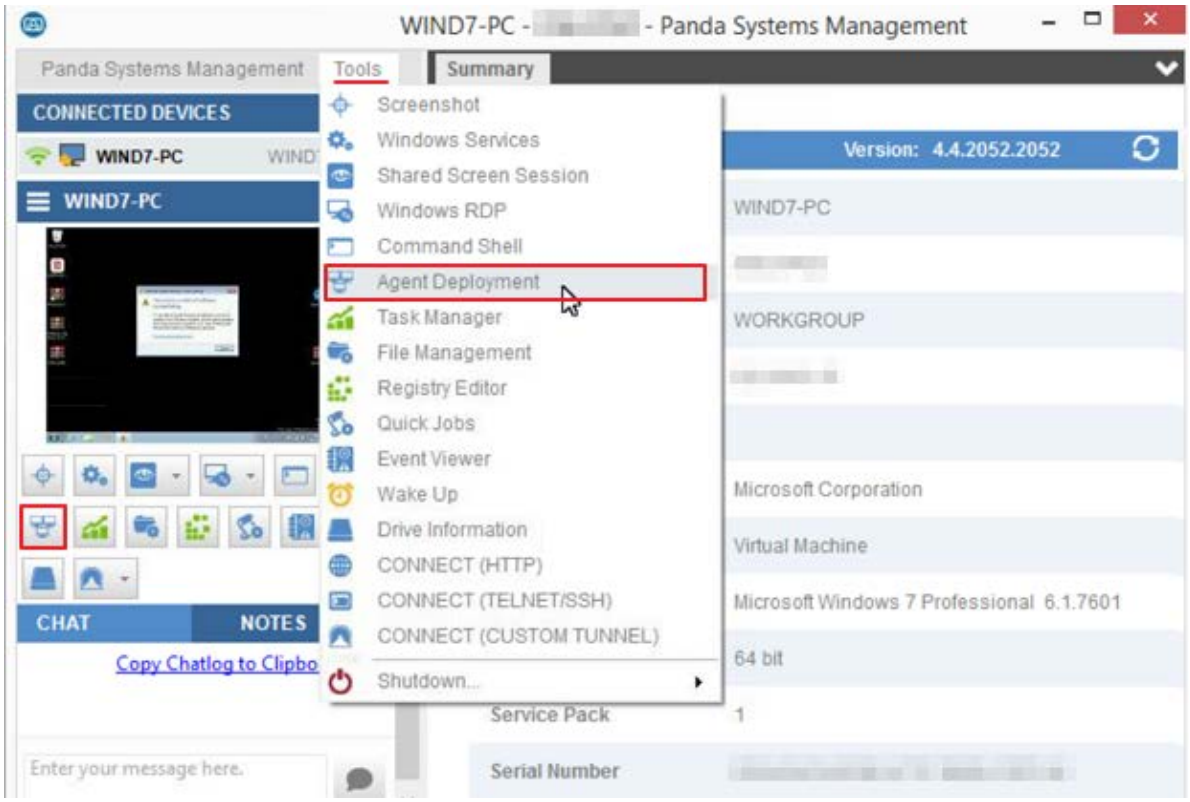


Figura 5.3: acceso a la herramienta de despliegue desde el agente PCSM

- Una vez que el proceso de descubrimiento 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 introducir las credenciales de usuario necesarias para poder instalar el agente y crear los servicios necesarios en los equipos de destino.

Distribución mediante clonación de imágenes

Cada agente PCSM instalado en un dispositivo genera un ID único que el servidor Panda Systems Management utiliza para identificarlo y que almacena en el registro de cada equipo.

En redes grandes de equipos que utilizan un hardware homogéneo, una de las estrategias básicas a la hora de acelerar el despliegue de nuevos equipos en la red consiste en clonar o realizar una imagen del sistema operativo completo junto a los programas instalados. En estos casos, para acelerar el despliegue del agente PCSM se procede a generar la imagen base desde un equipo con el agente ya instalado. Sin embargo, el identificador generado para ese dispositivo también se replicará en el resto de equipos que reciban la imagen, con lo que todos los dispositivos terminarán heredando el mismo ID. Para evitar este problema sigue los pasos mostrados a continuación en el equipo que servirá de base para generar la imagen:

Equipos Windows

- Desconecta el equipo de la red.
- Abre el editor del registro (`regedit.exe`) y navega hasta la rama `HKEY_LOCAL_MACHINE/Software/CentraStage`
- Borra la carpeta `CentraStage` incluyendo el identificador.
- Inicia el proceso de clonación.

Equipos macOS

- Desconecta el equipo de la red.
- Abre una ventana de terminal y ejecuta los comandos siguientes:

```
sudo su

cd /var/root/.mono/CurrentUser/software/centrastage

rm -f values.xml
```

- Inicia el proceso de clonación.

Instalación del agente en equipos de usuario y servidores

Instalación del agente PCSM en equipos Windows

- Para instalar el agente PCSM en un equipo Windows distinto de la versión Windows Core haz doble clic en el paquete de instalación. El agente PCSM se instalará en modo silencioso y se conectará automáticamente al servidor Panda Systems Management sin requerir ningún tipo de interacción con el usuario del dispositivo. El proceso de instalación se habrá completado cuando aparezca el icono de Panda Systems Management  en la barra de notificaciones de Windows en color azul (conectado).
- Para instalar el agente PCSM en un equipo Windows Core comprueba que el framework .NET esté instalado previamente y el equipo ha sido reiniciado. Accede mediante línea de comandos a la carpeta donde reside el fichero `agent.exe` y ejecútalo.

Instalación del agente PCSM en equipos macOS

- Descomprime el fichero `.Zip` y abre la carpeta `AgentSetup` creada.
- Haz doble clic en el fichero `CAG.pkg` y completa el asistente de instalación. Una vez terminado el proceso se mostrará el icono de PCSM en la barra de menú del dispositivo.

Instalación del agente PCSM en equipos Linux

- Abre un terminal Linux y accede a la carpeta donde reside el fichero `AgentSetup.sh`
- Teclea `sudo sh AgentSetup.sh` e introduce la contraseña de administrador cuando se requiera.

Instalación del agente en plataformas Android e iOS

Este método de despliegue es compatible con:

- Dispositivos móviles tales como teléfonos móviles y tablets basados en sistemas operativos Android e iOS.

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

- Importar el certificado en la consola (solo dispositivos iOS).
- Enviar por email la URL de descarga del agente PCSM.
- Asociar el dispositivo a la zona.

Integración de dispositivos de red

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.

Este método de despliegue es compatible con:

- Dispositivos que no admiten la instalación de software 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.

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 mostrará una ventana donde es necesario introducir la información relevante del dispositivo.

Agrega varios dispositivos de red a la vez:

- En el menú general **Zonas** haz clic en la zona donde residen los dispositivos a gestionar.
- En la pestaña **Auditoría**, haz clic en **Red** con el control de selección situado en la parte superior derecha de la ventana. 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.

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

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 Panda Systems Management y el propio dispositivo a administrar. Este equipo requiere la asignación del rol Nodo de red.

Para asignar un dispositivo a un Nodo de red consulta el apartado "**Configuración de un nodo de red**".

Integración 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 Panda Systems Management 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 máquina física.*

Asignar 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 Panda 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 apartado "**Configuración de un nodo de red**" en este mismo capítulo.

Definición de credenciales

Las credenciales del servidor ESXi se pueden definir de forma particular para cada servidor ESXi a integrar o se pueden heredar de la configuración general establecida en el Nivel cuenta o zona.

Para definir credenciales en el Nivel cuenta:

- Haz clic en el menú general **Ajustes** y en el menú de pestañas **Configuración de cuenta**.
- En la sección **Credenciales ESXi** haz clic en el link **Editar**.
- Indica el **Nombre**, **Puerto CIM** y el **Nombre del usuario**, **Puerto** y **Contraseña** utilizados en la herramienta de administración vSphere.

Para definir credenciales en el Nivel zona:

- Haz clic en el menú general **Zonas** y en la zona donde se definirán las credenciales ESXi.
- Haz clic en la pestaña **Configuración**, sección **Credenciales ESXi** y haz clic en el link **Editar**.
- Indica si las contraseñas a definir se heredarán del Nivel cuenta mediante el botón **Utilizar credenciales de nivel Cuenta para hosts ESXi**.
- Si las contraseñas no se heredarán del Nivel cuenta indica el **Nombre**, **Puerto CIM** y el **Nombre del usuario**, **Puerto** y **Contraseña** utilizados en la herramienta de administración vSphere.

Agregar 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 un diálogo con las plataformas admitidas.

- Haz clic en el icono ESXi.
- Introduce los datos necesarios para la comunicación 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**.

Agregar varios servidores ESXi a la vez

- En el menú general **Zonas** haz clic en la zona donde se integrarán los servidores ESXi.
- En el menú de pestañas **Auditoría** elige **Red** en el control de selección situado en la parte superior derecha de la pantalla. Se mostrarán todos los dispositivos descubiertos en la red.
- Haz clic en el grupo ESXi para listar todos los servidores ESXi encontrados en la red.
- Haz clic en el icono de **Administrar dispositivos**  de la barra de iconos 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.

Integración 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 "**Instalación del agente en equipos de usuario y servidores**". Una vez instalado el agente PCSM, se podrá auditar el servidor Hyper-V y las máquinas virtuales que albergue.

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).

Activar la aprobación manual de dispositivos

- En el menú general **Ajustes** haz clic en el menú de pestañas **Configuración de cuenta.**
- En el apartado **Control de acceso** activa el botón **Exigir aprobación para dispositivos nuevos**.

Comprobar los dispositivos pendientes de aprobación

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

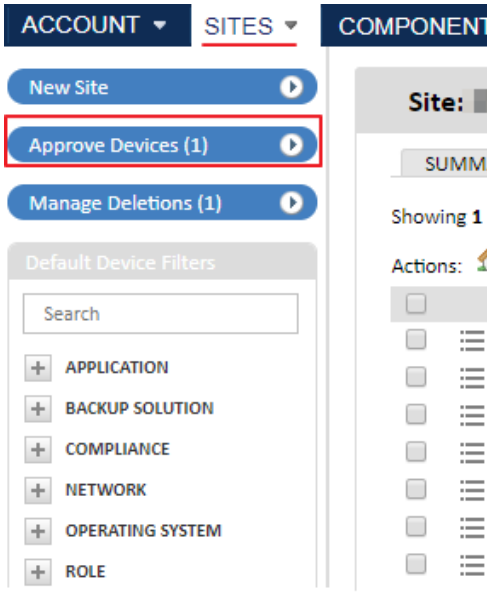


Figura 5.4: Aprobar dispositivos

• En el menú general **Zonas** haz clic en el botón **Aprobar dispositivos** del panel lateral izquierdo. Selecciona los dispositivos a aprobar y haz clic en el icono de la barra de iconos.

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

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

Desinstalación y borrado de dispositivos

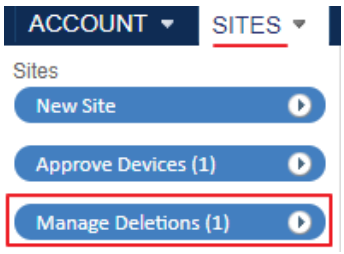


Figura 5.5: dispositivos borrados

Cuando un dispositivo deja de estar soportado por el departamento IT o ya no existe dentro del entorno administrado por la empresa, es necesario retirarlo de la plataforma Panda Systems Management para así recuperar la licencia asignada y poder utilizarla en otro dispositivo.

Panda Systems Management desinstala automáticamente el agente PCSM de los dispositivos eliminados desde la consola de administración si éstos estaban conectados al servidor en ese momento. En caso de no ser así, los dispositivos se moverán a la zona **Dispositivos eliminados** y el borrado se producirá cuando el agente PCSM vuelva a conectarse.

Para acceder a los dispositivos borrados haz clic en el menú general **Zonas** y en el panel lateral **Dispositivos borrados**.

Recuperar dispositivos borrados

Si cuando se inicia la acción de borrado el dispositivo no está conectado al servidor Panda Systems Management, el dispositivo se moverá al área **Dispositivos borrados**. Una vez allí es posible recuperarlo para que la próxima vez que el dispositivo se conecte no se inicie el proceso de desinstalación automática del agente PCSM. Para ello sigue los pasos mostrados a continuación:

- En la zona **Dispositivos borrados** selecciona los equipos a recuperar y haz clic en el icono  . Las entradas seleccionadas desaparecerán.
- Los equipos recuperados volverán a aparecer en la zona donde fueron integrados originalmente en el momento en que vuelvan a conectarse al servidor.

Desinstalación de dispositivos desde la consola de administración

Para borrar uno o varios dispositivos sigue los pasos mostrados a continuación:

- Desde el menú general **Zonas** haz clic en la zona donde residen los dispositivos a borrar y en el menú de pestañas **Dispositivos**.
- Con las casillas de selección indica los dispositivos a borrar y haz clic en el icono  .

Desinstalación del agente PCSM desde el dispositivo

Desinstalación del agente PCSM en dispositivos Windows

- Haz clic en el botón Iniciar situado en la esquina inferior izquierda del escritorio de Windows, Configuración y Aplicaciones.
- Haz clic en la entrada Panda Systems Management de la lista de programas instalados.
- Haz clic en el botón Desinstalar.

Desinstalación del agente PCSM en dispositivos macOS

- Abre una ventana de terminal y ejecuta el comando:

```
sudo bash /Applications/AEM\ Agent.app/Contents/Resources/uninstall.sh
```

Desinstalación del agente PCSM en dispositivos Linux

- Abre una ventana de terminal y ejecuta el comando:

```
sudo /bin/bash /opt/CentraStage/uninstall.sh
```

Configuración alternativa 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 personalizada de agente**, puedes configurar:

Campo	Descripción
Utilizar agente de conexión	Botón para activar o desactivar.
Utilizar configuración alternativa para el Agente	Permite introducir de forma manual los valores indicados para configurar un agente de conexión.
Dirección de canal de control	Uso restringido al departamento de Soporte de Panda Security.
Puerto del 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.
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 su segmento. 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 5.1: parámetros de configuración de las conexiones utilizadas por el agente PCSM

Configuración de un nodo de red

Un nodo de red es un dispositivo con un agente Panda 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 y ESXi.

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.
- Por el tipo de función adicional que desempeñará el equipo, es muy recomendable que éste permanezca siempre online. Consulta "**Monitor de estado online**" en la página **116** para obtener más información acerca de este monitor. Si el equipo permanece offline más de 5 minutos Panda Systems Management generara una alerta de tipo **Crítico** y enviará una notificación por correo a las cuentas configuradas por defecto.

> *Debido a que los equipos con el rol Nodo de red asignado ejecutan más tareas que las asignadas a un equipo normal, se recomienda crear un monitor adicional de CPU y de memoria para controlar el consumo de recursos de estos dispositivos. En situaciones de sobrecarga es posible que el dispositivo Nodo de red entre en modo offline, afectando a las conexiones con otros dispositivos gestionados.*

Requisitos para configurar un Nodo de red como monitor SNMP

Para que un agente con el rol Nodo de red monitorice dispositivos mediante el protocolo SNMP, es necesario la descarga e instalación del paquete .NET 4.0. Cuando los prerequisitos del sistema operativo se cumplen, el agente PCSM inicia de forma automática la descarga del paquete .NET 4.0.

> *El agente PCSM con el rol Nodo de red asignado no es compatible con la versión .NET Core 3.1 instalada de forma independiente. El propio agente PCSM se descargará una versión de .NET compatible cuando los requisitos del sistema operativo se cumplen. Cada 2 horas y al iniciarse, el agente PCSM comprueba si los requisitos se cumplen, y si es así, iniciará la descarga de forma automática y se reiniciará.*

A continuación se indican los sistemas operativos que soportan .NET 4.0 y los requisitos que son necesarios satisfacer:

- **Compatibilidad directa**:
  - Windows 10
  - Windows Server 2016
  - Windows Server 2019
- **Necesaria la instalación previa del parche KB2999226:**
  - Windows 8.1

- Windows Server 2012 R2

> *KB2999226 forma parte del paquete Microsoft Visual C++ 2015 Redistributable Update 3 y superiores, incluyendo a Microsoft Visual C++ 2017 Redistributable.*

- **macOS y Linux**: dado que es necesaria la instalación previa del paquete .NET 4.0 en estos sistemas operativos, los dispositivos pueden gestionar dispositivos SNMP directamente.

Tipos de nodo de red

Existen dos tipos de nodos de red:

- **Con escaneo 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 Panda Systems Management.

- **Sin escaneo de la red**

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

Asignar el rol Nodo de red a un equipo

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 con escaneo de red** o **Nodo de red sin escaneo de red**.

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

Retirar el rol Nodo de red de un equipo

En el menú general **Zonas**, **Dispositivos** selecciona el dispositivo al que será retirado 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 **Eliminar como nodo de red**.

Asignar dispositivos a un nodo de red

Para asignar un Nodo de red a un único dispositivo no compatible con el agente PCSM:

- Haz clic en el menú general **Zonas**, en la zona a la que pertenece el dispositivo a administrar y 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**.

Para asignar un equipo Nodo de red a varios dispositivos

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

Búsqueda de dispositivos (escaneo de red)

Durante la fase de auditoría de dispositivos, los equipos con el rol Nodo de red asignado intentarán descubrir los dispositivos vecinos de forma automática. El descubrimiento se limita inicialmente a la subred donde reside el equipo aunque el ámbito del descubrimiento se puede ampliar.

Proceso de descubrimiento de dispositivos en la red

El proceso automático de descubrimiento de dispositivos ejecuta los pasos mostrados a continuación:

- Para los dispositivos que residen en la misma subred que el equipo con el rol Nodo de red asignado:
  - Ping a todo el rango de IPs perteneciente a la subred donde reside el dispositivo.
  - Creación de un registro por cada dispositivo descubierto con su dirección IP y MAC.
  - Conexión a cada dispositivo por SNMP para determinar si es un dispositivo de red o una impresora.
  - Conexión al puerto 902 para determinar si es un servidor ESXi.
  - Conexión por NetBIOS y comprobación del TTL para determinar si es un dispositivo Windows.
- Para los dispositivos que no residen en la misma subred que el equipo con el rol Nodo de red asignado:
  - Ping a todo el rango de IPs perteneciente a las subredes adicionales definidas. Consulta el apartado "**Ampliar el descubrimiento de dispositivos a otras redes**" en este mismo capítulo.
  - Creación de un registro por cada dispositivo que responde al Ping y permite una conexión TCP a uno de los puertos siguientes: 22, 80, 8080, 443.
  - Conexión a cada dispositivo por SNMP para determinar si es un dispositivo de red o una impresora.
  - Conexión al puerto 902 para determinar si es un servidor ESXi.
  - Conexión por NetBIOS y comprobación del TTL para determinar si es un dispositivo Windows.
- Retirar los dispositivos duplicados de la lista aplicando el proceso mostrado a continuación:

- Si el dispositivo a añadir a la lista tiene dirección MAC disponible mira primero si existe otro dispositivo con la misma MAC en toda la cuenta y luego en toda la zona a la que pertenece el dispositivo. Si se encuentra se rechaza el dispositivo nuevo.
- Si el dispositivo a añadir a la lista no tiene dirección MAC disponible por encontrarse en otro segmento de red mira si existe otro dispositivo con la misma IP en la zona a la que pertenece el dispositivo. Si se encuentra se rechaza el dispositivo nuevo.

Ampliar el descubrimiento de dispositivos a otras redes

Para añadir nuevas subredes a la configuración de escaneo de un Nodo de red sigue los pasos mostrados a continuación:

- En el menú general **Zonas** selecciona la zona donde reside el Nodo de red y haz clic en el menú de pestañas **Configuración**.
- En la sección **Subredes adicionales para el descubrimiento de redes** añade la dirección IP inicial y final que se incluirán en el escaneo de dispositivos.
- Haz clic en el botón **Guardar**.

Las subredes de descubrimiento adicionales solo se pueden añadir en el Nivel zona.

Limitar el descubrimiento de dispositivos dentro de una misma subred

Para limitar el número de dispositivos escaneados en un descubrimiento de red sigue los pasos mostrados a continuación:

- En el menú general **Ajustes** haz clic en **Utilizar configuración alternativa para el Agente** en la sección **Configuración personalizada del agente**.
- En el campo **Límite del escaneo de red** indica el número de dispositivos que el Nodo de red intentara descubrir.

Para desactivar el descubrimiento de dispositivos:

- En el menú general **Ajustes** haz clic en **Utilizar configuración alternativa para el Agente** en la sección **Configuración personalizada del agente**.
- En el campo **Límite de subred** introduce el número 0.

Mejorar el descubrimiento de dispositivos por SNMP

Por defecto el agente PCSM utiliza conexiones SNMP anónimas (protocolo SNMP v2c, comunidad: "public") para conectarse a los dispositivos y recuperar información que ayude a su identificación.

Para mejorar la fase de validación SNMP en el Nivel cuenta sigue los pasos mostrados a continuación:

- En el menú general **Ajustes** haz clic en el menú de pestañas **Configuración de cuenta**.
- En la sección **Credenciales SNMP** haz clic en el link **Añadir credenciales SNMP** y configura las credenciales de cada dispositivo SNMP.

Para mejorar la fase de validación SNMP en el Nivel zona sigue los pasos mostrados a continuación:

- En el menú general **Zonas** haz clic en la zona a definir la configuración y en el menú de pestañas **Configuración.**
- En la sección **Credenciales SNMP** haz clic en el link **Añadir credenciales SNMP** y configura las credenciales de cada dispositivo SNMP.

Panda Systems Management utiliza la lista de credenciales en orden definida en el Nivel cuenta con cada dispositivo hasta que un grupo de credenciales valide la conexión. Si ningún grupo es validado por el dispositivo se pasa a utilizar la lista de credenciales definida en el Nivel zona.

Capítulo 6

Agrupaciones de dispositivos

Para facilitar la gestión de parques informáticos de tamaño medio y grande, Panda Systems Management incorpora un sistema de agrupación de dispositivos flexible basado en los recursos mostrados a continuación:

- Zonas
- Grupos
- Filtros
- Favoritos

Estos recursos se diferencian entre sí según sus características:

- Carácter estático o dinámico de la pertenencia de los dispositivos que los componen.
- Ámbito de agrupación de los dispositivos.
- Facilidad para modificar las agrupaciones y utilizarlas junto a otros recursos de visualización y resolución, tales como monitores, tareas o informes de estado.

Por razones de seguridad se ha suprimido la posibilidad de asignar a un dispositivo el rol de nodo caché, aunque esta funcionalidad puede decir apareciendo en la consola de administración.

CONTENIDO DEL CAPÍTULO

Zonas

Los dispositivos que comparten una misma configuración de red son candidatos a agruparse dentro de una misma zona. En empresas con una organización distribuida formada por delegaciones remotas, cada uno de los centros de trabajo puede incorporar recursos de red, tales como proxys, que modifican los mecanismos de conexión de los equipos con Internet. Esta configuración de red es necesaria para que tanto el equipo como el agente PCSM instalado puedan conectarse a los recursos externos a la red local, entre ellos el servidor Panda Systems Management.

*Consulta el apartado "**Jerarquía de niveles**" en la página **24** para obtener más información sobre el Nivel zona.*

Crear una nueva zona

- En el menú general **Zonas** haz clic en el botón **Nueva zona** situado en el panel izquierdo.
- Asigna un nombre y descripción.
- Modifica el tipo de conexión que utilizarán los dispositivos para acceder a los recursos externos. El proxy elegido se configurará por defecto con los datos suministrados en la pestaña **Configuración**. Consulta el apartado "**Configurar la conectividad de una zona**" más adelante en este mismo capítulo.

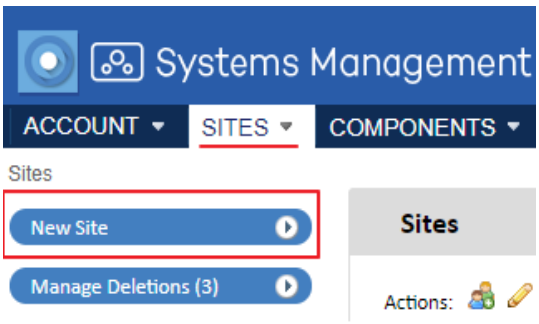


Figura 6.1: creación de una zona

- Elige los roles que podrán acceder a la zona. Consulta el capítulo "**Cuentas de usuario y roles**" en la página **297** para obtener más información sobre la estructura de usuarios y roles de Panda Systems Management.
- Selecciona los grupos de zonas a los que se añadirá la zona recién creada. Utiliza esta opción si existen dispositivos situados en distintas delegaciones que requieren procedimientos de administración similares.

Borrar una zona

En el menú general **Zonas** haz clic en el icono situado a la derecha de la zona al pasar el puntero del ratón por encima de ésta.

> *Al borrar una zona que contiene dispositivos, éstos serán eliminados de la consola de administración.*

Mover equipos entre zonas

- Haz clic en el menú general **Zonas** y selecciona la zona que contiene los dispositivos a mover.
- Selecciona los dispositivos con las casillas de selección y haz clic en el icono **Mover dispositivo(s) a otra zona**. Se mostrará una ventana con todas las zonas creadas en la cuenta y una caja de texto que permite filtrar las zonas para facilitar su búsqueda.
- Selecciona una zona y haz clic en el botón **Mover**.

Configurar la conectividad de una zona

Al configurar los parámetros de conexión de una zona, todos los equipos que pertenezcan a ésta heredarán la configuración de forma automática.

> *Los dispositivos que pertenecen a una zona no heredan los cambios de configuración de conectividad de forma automática si éstos se producen posteriormente a su integración.*

- En el menú general **Zonas** haz clic en la zona a configurar.
- Haz clic en la pestaña **Configuración**. En la sección **Proxy** configura el método de conexión y las credenciales necesarias para que los dispositivos puedan acceder a los recursos situados en el exterior de la red de la empresa.
- Haz clic en **Guardar**.

Listar las zonas creadas

Para obtener un listado de las zonas creadas haz clic en el menú general **Zonas**. Se mostrará un listado de las zonas con la información indicada a continuación:

Campo	Descripción
Nombre	Nombre de la zona. Haz clic en el enlace para mostrar el Nivel zona y todos sus recursos.
Descripción	Descripción de la zona introducida por el administrador de la red.
ID	Identificador interno de la zona utilizado por Panda Systems Management.
Dispositivos	Número de dispositivos que pertenecen a la zona. Haz clic en el enlace para mostrar el Nivel zona y todos sus recursos.
Offline	Número de dispositivos que tienen el agente PCSM instalado pero que no están conectados al servidor Panda Systems Management. Haz clic en el enlace para aplicar un filtro de dispositivos que muestre un listado de los dispositivos de la zona sin conexión.
Proxy	Configuración del proxy asignado a la zona.

Tabla 6.1: información del listado zonas.

Grupos

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

Se distinguen los tipos de grupos mostrados a continuación:

- **Grupos de dispositivos de zona**: son agrupaciones creadas dentro de una zona determinada y solo pueden contener dispositivos que pertenecen a la zona seleccionada.

- **Grupos de dispositivos**: 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 grupos son frecuentemente utilizados como destino en políticas, monitores y tareas. Si un grupo que está siendo utilizando por alguno de estos recursos es borrado, las políticas, monitores y tareas que lo estén utilizando no podrán resolver los dispositivos de destino y quedarán sin ejecución.*

Grupos de dispositivos de zona

Los grupos de dispositivos de zona contienen dispositivos que pertenecen a una misma zona.

Crear un grupo de dispositivos de zona

- En el menú general **Zonas** haz clic en la zona donde vas a crear el grupo de dispositivos de zona.
- En el panel lateral **Grupos de dispositivos de zona** haz clic en el icono  . Se mostrará una ventana donde introducir el nombre del grupo.
- Haz clic en el botón **Guardar**.

Asignar un dispositivo a un grupo de dispositivos de zona

- Haz clic en el menú general **Zonas** y en la zona a la que pertenece el dispositivo.
- Selecciona los dispositivos que formarán parte del grupo de dispositivos de zona con las casillas de selección.
- Haz clic en el icono  **Añadir dispositivo(s) a un grupo**. Se mostrará una ventana con los grupos disponibles creados anteriormente.

Borrar un grupo de dispositivos de zona

- Haz clic en el menú general **Zonas** y en la zona a la que pertenece el grupo de dispositivos de zona.
- En el panel lateral, sección **Grupos de dispositivos de zona**, haz clic en el icono  que aparece al pasar el puntero del ratón por encima del grupo.
- Haz clic en el botón **Aceptar**.

Editar un grupo de dispositivos de zona

- Haz clic en el menú general **Zonas** y en la zona a la que pertenece el grupo de dispositivos de zona.
- En el panel lateral, sección **Grupos de dispositivos de zona**, haz clic en el icono  que aparece al pasar el puntero del ratón por encima del grupo.

- Indica el nuevo nombre del grupo y sus miembros.
- Haz clic en el botón **Aceptar**.

Grupos de dispositivos

Los grupos de dispositivos contienen dispositivos que pertenecen a zonas distintas.

Crear un grupo de dispositivos

- En el menú general **Zonas** haz clic en el icono del panel lateral **Grupos de zonas**. Se mostrará una ventana donde introducir el nombre del grupo.
- Haz clic en el botón **Guardar**.

Asignar un dispositivo a un grupo de dispositivos

- Haz clic en el menú general **Zonas** y en la zona a la que pertenece el dispositivo.
- Selecciona los dispositivos que formarán parte del grupo de dispositivos con las casillas de selección.
- Haz clic en el icono **Añadir dispositivo(s) a un grupo**. Se mostrará una ventana con los grupos de dispositivos disponibles creados previamente.

Borrar un grupo de dispositivos

- Haz clic en el menú general **Zonas**.
- En el panel lateral, sección **Grupos de dispositivos**, haz clic en el icono que aparece al pasar el puntero del ratón por encima del grupo.
- Haz clic en el botón **Aceptar**.

Editar un grupo de dispositivos

- Haz clic en el menú general **Zonas**.
- En el panel lateral, sección **Grupos de dispositivos**, haz clic en el icono que aparece al pasar el puntero del ratón por encima del grupo.
- Indica el nuevo nombre del grupo y sus miembros.
- Haz clic en el botón **Aceptar**.

Grupos de zonas

Los grupos de zonas contienen todos los dispositivos que pertenecen a las zonas seleccionadas a agrupar.

Crear un grupo de zona

- En el menú general **Zonas** haz clic en el icono  del panel lateral **Grupo de zonas**. Se mostrará una ventana donde introducir el nombre del grupo.
- Haz clic en el botón **Guardar**.

Asignar una zona a un grupo de zona

- Haz clic en el menú general **Zonas** y selecciona con las casillas de selección las zonas a agrupar.
- Haz clic en el icono  **Añadir zona a grupo de zonas** en la barra de iconos. Se mostrará una ventana con los grupos disponibles creados anteriormente.

Borrar un grupo de zona

- Haz clic en el menú general **Zonas**.
- En el panel lateral, sección **Grupos de zonas**, haz clic en el icono  que aparece al pasar el puntero del ratón por encima del grupo.
- Haz clic en el botón **Aceptar**.

Editar un grupo de zona

- Haz clic en el menú general **Zonas**.
- En el panel lateral, sección **Grupos de zonas**, haz clic en el icono  que aparece al pasar el puntero del ratón por encima del grupo.
- Indica el nuevo nombre del grupo y sus miembros.
- Haz clic en el botón **Aceptar**.

Filtros

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

Se distinguen los tipos de filtros mostrados a continuación:

- **Filtros de zona**: son agrupaciones creadas dentro de una zona determinada y solo pueden contener dispositivos que pertenecen a esa zona.
- **Filtros de cuenta**: son agrupaciones creadas en el Nivel cuenta y pueden contener dispositivos que pertenecen a una, varias o todas las zonas.

- **Filtros de dispositivos**: son agrupaciones predefinidas disponibles tanto en el Nivel cuenta como en el Nivel zona.

> *Los filtros son frecuentemente utilizados como destino en políticas, monitores y tareas. Si un filtro que está siendo utilizando por alguno de estos recursos va a ser borrado, la consola de administración mostrará una ventana de advertencia. Si el filtro finalmente es borrado, las políticas, monitores y tareas que lo estén utilizando no podrán resolver los dispositivos de destino y quedarán sin ejecución.*

Filtros de dispositivos

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 las siguientes categorías:

Grupo	Descripción
Aplicación	Muestra los dispositivos que tienen instaladas aplicaciones como por ejemplo Adobe Flash, Java, Microsoft Office y otros.
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.
Red	Contiene filtros que muestran los dispositivos de red (routers, switches, cortafuegos, equipos NAS y SAN etc.) de los fabricantes más populares.
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 mostrar 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.).

Tabla 6.2: tipos de filtros predefinidos

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.
	Microsoft Office	Muestra los dispositivos que tienen la suite de ofimática Microsoft Office instalada.
	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.
	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.

Tabla 6.3: listado de filtros predefinidos

Categoría	Nombre del filtro	Uso
Atención	< .NET 4.0.3	Muestra los dispositivos Windows que tienen instalado el framework .NET con las versiones 1.x, 2.x, 3.x, 4.0.0, 4.0.1 y 4.0.2.
	< 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 no ejecutándose	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.
Red	Firewalls	Muestra los dispositivos de tipo cortafuegos de los fabricantes Fortigate, SonicWall y pfSense.
	Dispositivos NAS	Muestra los dispositivos de almacenamiento conectados a la red de los fabricantes QNAP y Synology.
	Routers	Muestra los dispositivos de tipo enrutador de los fabricantes Cisco, Huawei, Juniper, Netgear y ZyXEL.
	Dispositivos SAN	Muestra las redes de almacenamiento de los fabricantes Dell, EMC, HP y NetApp.
	Servidores	Muestra los equipos de tipo servidor conectados a la red de los fabricantes Dell, Fujitsu y HP.
	Switches	Muestra los dispositivos de tipo conmutador conectados a la red de los fabricantes Cisco, HP y Juniper.
	Dispositivos UPS	Muestra los sistemas de alimentación ininterrumpida conectados a la red del fabricante APC.

Tabla 6.3: listado de filtros predefinidos

Categoría	Nombre del filtro	Uso
Sistema Operativo	Todas las estaciones	Muestra los dispositivos de tipo sobremesa.
	Todos los servidores	Muestra todos los dispositivos de tipo servidor.
	Todas las estaciones Windows	Muestra los dispositivos de tipo sobremesa con sistema operativo Windows.
	Todos los servidores Windows	Muestra todos los dispositivos de tipo servidor con sistema operativo Windows.
	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 11	Muestra los dispositivos con sistema operativo Microsoft Windows 11.
	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.
	MS Win Server 2019	Muestra los dispositivos con sistema operativo Microsoft Windows 2019.
	MS Win Server 2022	Muestra los dispositivos con sistema operativo Microsoft Windows Server 2022.
	MS Win Vista	Muestra los dispositivos con sistema operativo Microsoft Windows Vista.
	MS Win XP	Muestra los dispositivos con sistema operativo Microsoft Windows XP.
	mac OS	Muestra los dispositivos con sistema operativo macOS.

Tabla 6.3: listado de filtros predefinidos

Categoría	Nombre del filtro	Uso
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 AVG instalado.
	Avira	Muestra los equipos con software de seguridad Avira instalado.
	ESET	Muestra los equipos con software de seguridad ESET instalado.
	Kaspersky	Muestra los equipos con software de seguridad Kaspersky instalado.
	McAfee	Muestra los equipos con software de seguridad McAfee instalado.
	Panda	Muestra los equipos con software de seguridad Panda Security instalado.
	Sophos	Muestra los equipos con software de seguridad Sophos instalado.
	Symantec	Muestra los equipos con software de seguridad Symantec instalado.
	Trend Micro	Muestra los equipos con software de seguridad Trend Micro instalado.
	Webroot	Muestra los equipos con software de seguridad Webroot instalado.

Tabla 6.3: listado de filtros predefinidos

Categoría	Nombre del filtro	Uso
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 apartado "Configuración de un nodo de red" en la página 63 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 escritorio 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.

Tabla 6.3: listado de filtros predefinidos

Categoría	Nombre del filtro	Uso
Tipo	**Todos los dispositivos**	Muestra todos los dispositivos gestionados por PCSM.
	Todos los firewalls	Muestra todos los dispositivos de tipo cortafuegos 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 NAS	Muestra todos los dispositivos de almacenamiento de red gestionados por PCSM.
	Todos los dispositivos de red	Muestra todos los dispositivos de red gestionados por PCSM.
	Todas las impresoras de red	Muestra todas las impresoras instaladas en la red y gestionados por PCSM.
	Todos los routers	Muestra todos los routers instalados en la red y gestionados por Panda Systems Management.
	Todos los dispositivos SAN	Muestra todos los dispositivos que forman parte de una red de área de almacenamiento (Storage Area Network) y gestionados por PCSM.
	Todos los switches	Muestra todos los dispositivos de tipo conmutador gestionados por PCSM.
	ESXi	Muestra los servidores ESXi gestionados por PCSM.
	Servidores físicos	Muestra todos los servidores físicos (no virtualizados).
	Máquinas virtuales	Muestra todos los servidores virtualizados gestionados por Panda Systems Management.

Tabla 6.3: listado de filtros predefinidos

Los filtros predefinidos no son editables.

Filtros de cuenta

Los filtros de cuenta pueden contener dispositivos de cualquier zona.

Crear un filtro de cuenta

- En el menú general **Zonas** haz clic en el icono  del panel lateral **Filtros de cuenta**. Se mostrará una ventana donde introducir los datos siguientes:
  - Nombre del filtro.

- Definición del filtro. Consulta el apartado "**Construcción de filtros**" más adelante.
- Selecciona la opción **Solo seleccionar dispositivos en las siguientes zonas** para limitar la aplicación del filtro a los dispositivos de zonas concretas, o elige todas las zonas con la opción **Seleccionar dispositivos en todas mis zonas**.
- Para especificar los usuarios de la consola de administración que tendrán acceso al filtro activa la opción **Compartir este filtro con usuarios con los siguientes roles.**

> *Los usuarios de la consola pueden ver los criterios de todos los filtros compartidos con ellos. Solo el usuario de la consola que creó el filtro podrá editarlo y eliminarlo.*

- Haz clic en el botón **Guardar**.

Borrar un filtro de cuenta

- Haz clic en el menú general **Zonas**.
- En el panel lateral, sección **Filtros de cuenta**, haz clic en el icono que aparece al pasar el puntero del ratón por encima del filtro.
- Haz clic en el botón **Aceptar**.

Editar un filtro de cuenta

- Haz clic en el menú general **Zonas**.
- En el panel lateral, sección **Filtros de cuenta**, haz clic en el icono que aparece al pasar el puntero del ratón por encima del filtro.
- Modifica la configuración del filtro y haz clic en el botón **Guardar**.

Filtros de zona

Los filtros de zona contienen dispositivos que pertenecen a una única zona.

Crear un filtro de zona

- En el menú general **Zonas**, haz clic en la zona donde se creará el filtro y haz clic en el icono del panel lateral **Filtros de zona**. Se mostrará una ventana donde introducir los datos siguientes:
  - Nombre del filtro.
  - Definición del filtro. Consulta el apartado "**Construcción de filtros**".
  - Para especificar los usuarios de la consola de administración que tendrán acceso al filtro activa la

opción **Compartir este filtro con usuarios con los siguientes roles.**

> *Los usuarios pueden ver los criterios de todos los filtros compartidos con ellos. Los administradores, por su parte, pueden editar y eliminar cualquier filtro compartido con ellos.*

- Haz clic en el botón **Guardar**.

Borrar un filtro de zona

- En el menú general **Zonas**, haz clic en la zona donde se borrará el filtro.
- En el panel lateral, sección **Filtros de zona**, haz clic en el icono que aparece al pasar el puntero del ratón por encima del filtro.
- Haz clic en el botón **Aceptar**.

Editar un filtro de zona

- En el menú general **Zonas**, haz clic en la zona donde se editará el filtro.
- En el panel lateral, sección **Filtros de zona**, haz clic en el icono que aparece al pasar el puntero del ratón por encima del filtro.
- Modifica la configuración del filtro y haz clic en el botón **Guardar**.

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	• Igual – No es igual • Está vacío – No está vacío • Contiene – No contiene • Comienza con – No comienza con • Termina con – No termina con	Cadena de caracteres. Utiliza el símbolo "%" 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	• Si / No • Activado / Desactivado • Online / Offline	
Date	• Antes – Después de, • Anterior a 7/14/30/60/90 días	Intervalo de fechas
Selección	• Es miembro de - No es miembro de	Grupos disponibles
Estado	• El estado es - El estado no es	Estados disponibles

Tabla 6.4: 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.

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.
Modo de privacidad	Filtra los dispositivos con el Modo de privacidad activado. Consulta el apartado "**Opciones del modo privacidad**" en la página **102**
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.
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 "**Auditoria de activos**" en la página **159**.
Arquitectura	Filtra dispositivos con arquitectura 32 bits o 64 bits.
CPU	Filtra por la marca y modelo de la CPU instalada en el dispositivo.
Campo personalizado	Filtra por el contenido del campo personalizado referido (del 1 al 30). Para más información, consulta el apartado "**Campos personalizados**" en la página **190** para establecer su contenido de forma manual y el apartado "**Etiquetas y campos personalizados**" en la página **153** para llevarlo a cabo de forma automática.
Capacidad de disco	Filtra por el tamaño del disco duro conectado.
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 "**Auditoria de activos**" en la página **159**.
Descripción	Filtra por el campo **Descripción** del dispositivo.
Descripción SNMP	Filtra por el campo descripción de la configuración SNMP establecida en el dispositivo.
Descripción de la zona	Filtra por el campo **Descripción** de la zona a la que pertenece el dispositivo.
Descripción del disco	Filtra por la cadena de descripción de los dispositivos de almacenamiento interno conectados al equipo.
Dirección IP	Filtro por dirección IP asignada al interface de red principal del dispositivo.
Dirección IP adicional	Filtra por alias de IP.

Tabla 6.5: listado de atributos disponibles en filtro

Atributo	Descripción
Dirección IP externa	Filtra por la dirección IP con la que se conecta el dispositivo al servidor. Generalmente se trata de la dirección pública del router que implementa los procesos de proxy y/o NATeo de tráfico,
Dirección MAC	Filtro por la dirección física de la interface de red principal del dispositivo.
Dispositivo administrado	Sin uso.
Dispositivos bajo demanda	Sin uso.
Dominio	Filtra por el dominio en redes Microsoft al que pertenece el dispositivo.
Esta zona es bajo demanda	Sin uso.
Estado – Online/Offline	Filtra los dispositivos que están conectados al servidor Panda Systems Management.
Estado – Puerto de red OK	Sin uso.
Estado – Suspendido	Filtra los dispositivos que han entrado en estado de ahorro de energía.
Estado de parcheo	Filtra los dispositivos por su estado relativo a la instalación de parches: **Sin política**, **Sin información**, **Es necesario reiniciar**, **Error de instalación**, **Parches pendientes aprobados**, **Completamente parcheado**.
Estado del antivirus	Filtra los dispositivos por el estado del producto antivirus instalado: **Ejecutándose y actualizado**, **Ejecutándose y no actualizado**, **No ejecutándose**, **No detectado**.
Fabricante	Filtra por el nombre de la empresa que ensambló el dispositivo.
Fabricante NIC	Filtra por el nombre del proveedor de la interface de red del 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 "**Auditoria de activos**" en la página **159**.
Favorito	Filtra por los dispositivos marcados como favoritos. Consulta el apartado "**Favoritos**" más adelante en este mismo capítulo.
Fecha de caducidad de la garantía	Filtra los dispositivos por la fecha de caducidad introducida.
Fecha de lanzamiento de BIOS	Filtra los dispositivos por la fecha de publicación de la BIOS.
Fecha de la última visualización	Muestra los dispositivos que han sido vistos por el servidor Panda Systems Management en la fecha indicada.
Firewall de Windows	Filtra los dispositivos que tienen el cortafuegos activado o desactivado.

Tabla 6.5: listado de atributos disponibles en filtro

Atributo	Descripción
Grupo de dispositivos	Filtra por el nombre del grupo de dispositivos al que pertenece el dispositivo.
Grupo de dispositivos de la zona	Filtra por el nombre del grupo de dispositivo de zona al que pertenece el dispositivo.
Grupo de zonas	Filtra los dispositivos que pertenecen al grupo de zonas indicado.
Memoria	Filtra por la cantidad de memoria instalada en el dispositivo.
Modelo	
Fecha de creación	Filtra los dispositivos por la fecha en la que se añadieron al sistema.
Monitor / pantalla	Filtra por el nombre del fabricante del monitor conectado al dispositivo.
Necesita reinicio	Filtra por los dispositivos que tengan pendiente un reinicio para completar tareas de instalación de programas, parches, actualización de componentes u otros.
Nodo de red	Muestra los dispositivos con el rol nodo de red asignado. Consulta el apartado "**Configuración de un nodo de red**" en la página **63**.
Nombre de BIOS	Filtra los dispositivos por el nombre del fabricante de la BIOS.
Nombre de la zona	Filtra por el nombre de la zona a la que pertenece el dispositivo.
Nombre del servicio mostrado al usuario	Filtra por el campo descripción del servicio instalado en el dispositivo.
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 "**Auditoria de activos**" en la página **159**.
Nombre del dispositivo conectado	Filtra por el campo **Nombre** de los dispositivos USB externos conectados al equipo. Para más información, consulta el capítulo "**Auditoria de activos**" en la página **159**.
Nombre del host	Filtra los dispositivos por el nombre asignado en el sistema operativo.
Nombre del parche (aprobado y pendiente)	Filtra los dispositivos por el nombre de parches que han sido aprobados pero todavía no se han instalado.
Nombre del parche (instalado)	Filtra los dispositivos por el nombre de parches que han sido instalados.
Nombre del parche (no aprobado)	Filtra los dispositivos por el nombre de parches que han sido excluidos.
Nombre del producto antivirus	Filtra por el nombre comercial del producto antivirus instalado en el dispositivo.
Nombre del servicio	Filtra por el nombre del servicio instalado en el dispositivo.

Tabla 6.5: listado de atributos disponibles en filtro

Atributo	Descripción
Nombre/versión 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 "**Auditoria de activos**" en la página **159**.
Núcleos físicos	Filtra por el número de núcleos que implementa el microprocesador del dispositivo.
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	Filtra los dispositivos que tienen instalado el paquete de software y versión indicadas.
Parches aprobados pendientes	Filtra los dispositivos que tienen el número especificado de parches aprobados pendientes de instalación.
Parches instalados	Filtra los dispositivos que tienen el número especificado de parches instalados.
Parches no aprobados	Filtra los dispositivos que tienen el número especificado de parches excluidos.
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 "**Auditoria de activos**" en la página **159**.
Service Pack	Filtra por la versión del Service Pack instalado en los equipos Windows.
Sistema Operativo	Filtra por el nombre y la versión del sistema operativo instalado en los dispositivos.
Tipo de dispositivo	Filtra por el tipo de dispositivo: **Desconocido**, **Escritorio**, **Portátil**, **Servidor**, **Smartphone**, **Tablet**, **Impresora**, **Dispositivo de red**, **Host ESXi**.
Tipo de dispositivo conectado	
Ubicación SNMP	Filtra según el contenido del campo Ubicación de la configuración SNMP establecida en el dispositivo.
Versión de .NET	Filtra por la versión del framework .NET instalado en los dispositivos.
Versión de BIOS	Filtra por el número de versión de la BIOS instalada en los dispositivos.
Versión de software	Filtra por la versión de un paquete de software instalado en el equipo.
Versión del agente	Filtra por la versión del agente PCSM instalado en el dispositivo.
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 "**Auditoria de activos**" en la página **159**.

Tabla 6.5: listado de atributos disponibles en filtro

Atributo	Descripción
Última auditoría	Filtra los dispositivos según la fecha en la que se realizó la última auditoría de hardware / software.
Ultimo reinicio	Filtra los dispositivos cuyo último reinicio ocurrió en periodos de tiempo determinados.
Último usuario	Filtra los dispositivos cuyo último usuario que inicio sesión coincide con el especificado.

Tabla 6.5: listado de atributos disponibles en filtro

Favoritos

Los favoritos es un recurso de agrupación que permite acceder de forma rápida a aquellos dispositivos que requieren una atención especial y constante. Este tipo de agrupación no puede ser utilizada en tareas, políticas, monitores ni informes.

Añadir y eliminar un dispositivo al grupo de favoritos

Utiliza el icono de la barra de iconos para marcar o retirar uno o varios equipos como favoritos desde:

- Una zona concreta en la pestaña **Dispositivos**.
- Desde un grupo de zona, un filtro de zona o un filtro de dispositivos.

Acceder a los dispositivos Favoritos

La sección favoritos se crea en el panel de control del Nivel zona:

- Haz clic en el menú general **Zonas** y en la zona donde residen los dispositivos favoritos.
- Haz clic en el menú de pestañas **Resumen**. En la parte inferior del panel de control se muestran los dispositivos favoritos junto a una barra de iconos para poder lanzar tareas, solicitar auditorias, o generar informes entre otras acciones.

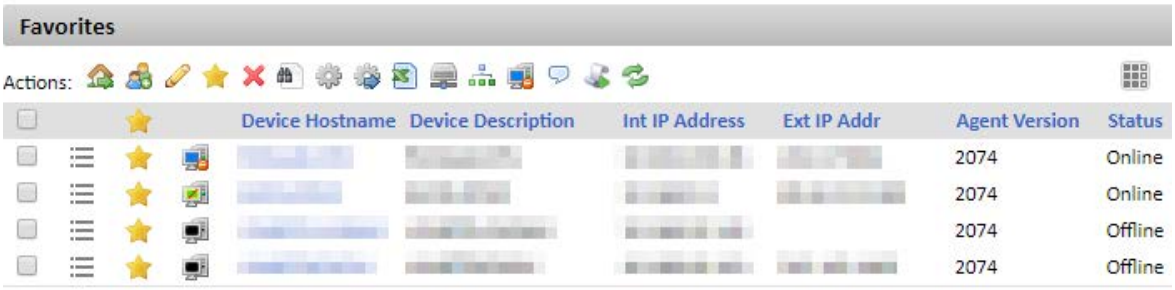


Figura 6.2: acceso a la sección favoritos

> *En la consola puede seguir apareciendo la posibilidad de asignar el rol de Nodo Caché a un dispositivo, aunque por motivos de seguridad esta funcionalidad ha dejado de ser soportada por Panda Security.*

Distribución eficiente de dispositivos

La distribución de los dispositivos en la consola administrados por 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.

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

Zonas

Ventajas

- Asocian una misma configuración de salida a Internet para el agente PCMS 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.

Grupos y filtros

Ventajas

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

Inconvenientes

- Los grupos / filtros tienen funcionalidad algo más 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 sin la configuración de proxy asociada y con un acceso limitado a la barra de pestañas.*

Organización general de dispositivos

Para obtener una estructura organizativa de dispositivos que facilite la gestión de los activos puedes aplicar las siguientes reglas 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 "**Cuentas de usuario y roles**" en la página **297**.

- **Marca los dispositivos más frecuentemente accedidos como Favoritos**

Los dispositivos problemáticos que requieren vigilancia constante son firmes candidatos a pertenecer al grupo **Favoritos**. Una vez que los problemas hayan sido resueltos retíralos de la sección **Favoritos** para mantenerla lo más ordenada posible y así acelerar el acceso a los dispositivos que todavía presenten problemas.

Parte 3

Configuración de procesos automáticos en dispositivos

Capítulo 7: Políticas

Capítulo 8: Monitorización

Capítulo 9: Tareas

Capítulo 10: Componentes y ComStore

Capítulo 7

Políticas

Las políticas son procesos específicos de gestión o resolución de incidencias que afectan a uno o varios dispositivos administrados y que se repiten a intervalos regulares durante un tiempo determinado, o que actúan al detectarse determinadas condiciones en el propio dispositivo.

Las políticas son 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 PCSM ejecutará ciertas acciones en cada dispositivo.

Las políticas pueden crearse en los tres niveles disponibles dependiendo de si los dispositivos pertenecen o no a una misma zona (cliente / delegación) 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.

*Consulta el capítulo "**Agrupaciones de dispositivos**" en la página **69** para obtener más información acerca de los distintos tipos de agrupaciones soportadas por Panda Systems Management.*

CONTENIDO DEL CAPÍTULO

Gestión de políticas

Crear políticas

Para crear una política sigue los pasos mostrados a continuación:

- 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** y en la zona apropiada, 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** y en la zona donde reside el dispositivo. Haz clic en el dispositivo al que se asignará la política y en la pestaña **Monitorizar.** Finalmente pulsa el botón **Añadir** situado en la parte inferior de la ventana.

*En el nivel de dispositivo solo es posible añadir políticas de tipo monitor. Consulta el capítulo "**Monitorización**" en la página **111** para más información sobre cómo crear una política 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 elegido. Consulta el apartado "**Tipos de políticas**" 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).
- Para terminar el proceso de creación de una política, haz clic en **Guardar y desplegar cambios** para guardar y ejecutar la política.

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, e incluso si se están produciendo problemas de solapamiento entre varias políticas creadas en distintos niveles.

Gestión de políticas

- Para listar las políticas creadas en el Nivel cuenta haz clic en el menú general **Cuenta** y menú de pestañas **Políticas**.
- Para listar las políticas creadas en el Nivel zona y en el Nivel zona agrupadas por su nivel sigue los pasos mostrados a continuación:
  - Haz clic en el menú general **Zona** y en la zona a gestionar sus políticas.
  - Haz clic en el menú de pestañas **Políticas**.
- Para listar los monitores asignados al dispositivo y creados en el Nivel cuenta, zona y dispositivo sigue los pasos mostrados a continuación:
  - Haz clic en el menú general **Zona** y en la zona donde reside el dispositivo.
  - Haz clic en el dispositivo a gestionar sus políticas de tipo monitorización.
  - Haz clic en el menú de pestañas **Monitorizar** y en el control de selección **Monitores** situado en la parte superior derecha de la ventana.

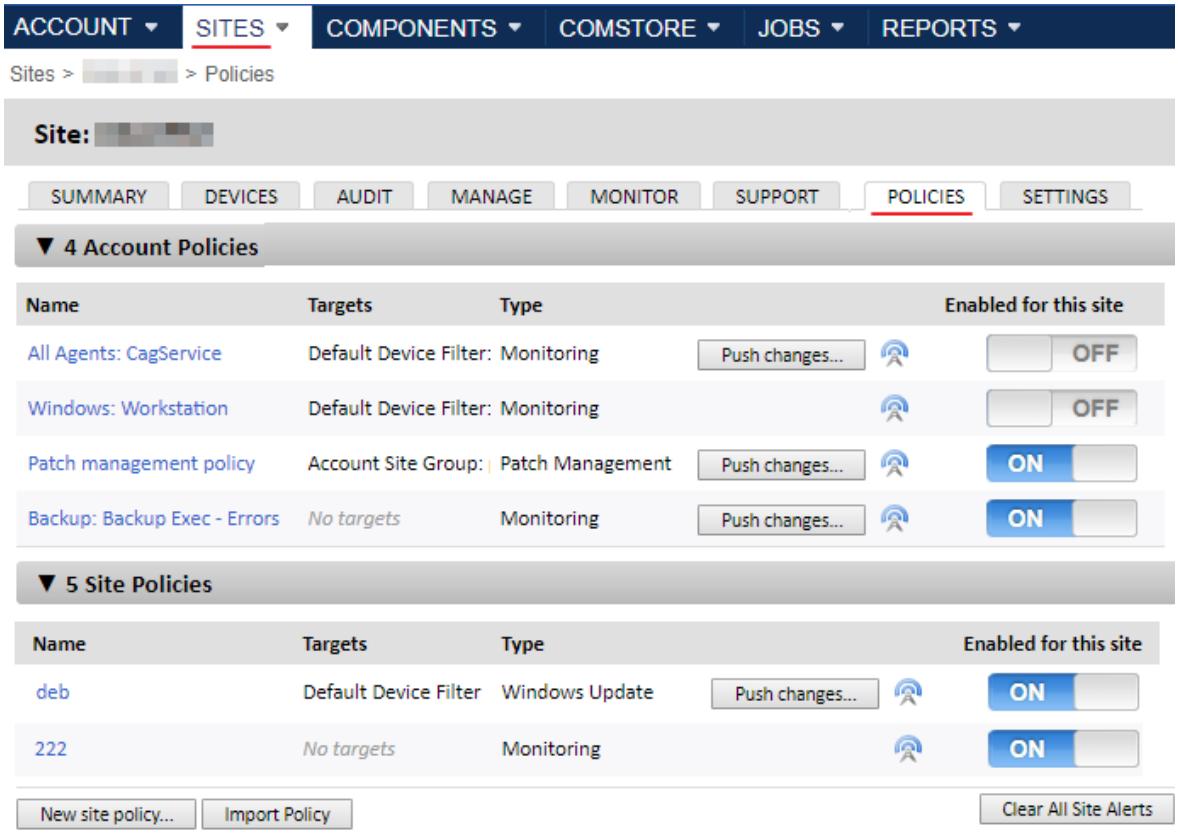


Figura 7.1: Listado de políticas asignadas en el Nivel zona

El listado de políticas en el Nivel cuenta y Nivel zona incluyen los campos mostrados en la tabla 7.1. Para ver los campos mostrados en el listado monitores del Nivel dispositivo consulta el apartado "**Gestión de monitores**" en la página **126**.

Campo	Descripción
Icono 	La política de Patch Management definida en el Nivel cuenta esta modificada en el Nivel zona actual. Solo se muestra en políticas de tipo Patch Management definidas en el Nivel cuenta y gestionadas en el nivel zona. Consulta el apartado "**Redefinición de políticas definidas en el nivel Cuenta**" en la página **225** para conocer más sobre la herencia de políticas.
Nombre	Nombre de la política.
Dispositivos	Agrupaciones de dispositivos destinatarios de la política.
Tipo	Clase de política, consulta más adelante el apartado "**Tipos de políticas**" en la página **101** en este capítulo.
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 apartado "**Redefinición de políticas definidas en el nivel Cuenta**" en la página **225** para conocer más sobre la herencia de políticas.
Desplegar cambios	Despliega la política a todos los dispositivos marcados como destino.
Icono 	Permite visualizar los dispositivos que recibirán la política.
Activado (para esta zona)	Activa o desactiva la política en toda la zona o cuenta.
Borrar 	Pasa el puntero del ratón por el nombre de la política para mostrar el icono a la derecha de la ventana. Elimina la política.
	Activa o desactiva la política.

Tabla 7.1: campos descriptivos de una política

Listar los dispositivos afectados por la política

Haz clic sobre el icono  para mostrar la pantalla **Asociaciones de la política.** Haz clic en el control de selección situado a la derecha de la ventana para filtrar los dispositivos mostrados en el listado:

Filtro	Descripción
Exclusiones de zonas	Zonas excluidas de la aplicación de la política.
Zonas activadas manualmente	Zonas incluidas de forma manual en la política.

Tabla 7.2: dispositivos afectados por la política

Filtro	Descripción
Todos los dispositivos	Dispositivos asociados a la política.
Dispositivos incluidos	Dispositivos que tienen actualmente aplicada la política.
Dispositivos excluido	Dispositivos actualmente excluidos de la aplicación de la política.

Tabla 7.2: dispositivos afectados por la política

Excluir e incluir zonas en una política de cuenta

Las políticas de cuenta pueden utilizar como destino grupos de zonas para distribuirse en todos los dispositivos integrados en zonas distintas dentro de la cuenta.

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 **Guardar y desplegar cambios**. Con esta acción, la política se guardará y se distribuirá de forma inmediata en todos los dispositivos afectados, comenzando su ejecución.

Tipos de políticas

Panda Systems Management soporta ocho tipos de políticas que se resumen a continuación:

Política	Descripción
Agente	Determina la apariencia del agente PCSM, así como las opciones de funcionalidad que son accesibles para el usuario.
ESXi	Vigila el rendimiento, almacén de datos y la temperatura de servidores ESXi.
Ventana de mantenimiento de la monitorización	Define un intervalo de tiempo en el cual no se producen notificaciones de email ni tickets.
Administración de dispositivos móviles	Establece condiciones de uso de dispositivos basados en la plataforma iOS.
Monitorización	Añade procesos de monitorización de los recursos de los dispositivos.
Gestión de parches	Descarga y aplica parches de software.
Energía	Configura las opciones de ahorro de energía de los dispositivos que las soporten.

Tabla 7.3: políticas disponibles y descripción

Política	Descripción
Gestión de software	Comprueba que los dispositivos administrados cumplen con las directrices de instalación de software establecidas por la empresa y actualiza las últimas versiones de los programas publicados por los proveedores del software.
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.

Tabla 7.3: políticas disponibles y descripción

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, capturas de pantalla, línea de comandos remota, gestión de servicios etc.) requerirán la confirmación del usuario antes de poder ser utilizadas con éxito.

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

- **Permitir conexiones cuando no hay ningún usuario que haya iniciado la sesión**: con el modo de privacidad activado, permite al administrador conectar con aquellos dispositivos donde el usuario no esté presente para autorizar 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 capturas de pantalla. El resto de herramientas de gestión remota no requieren la confirmación del usuario.

Opciones del servicio

- **Instalar servicio únicamente**: oculta el icono en el área de notificaciones (situada en la esquina inferior derecha del escritorio en los equipos Windows 

) de forma que el usuario no pueda 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 PCSM.

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

- **Desactivar menú de configuraciones**: el usuario no puede acceder al menú contextual del agente.
- Desactivar opción de salir: el usuario no puede cerrar el agente PCSM.
- **Desactivar la pestaña Tickets**: desactiva la pestaña de tickets en el agente PCSM. El usuario no puede añadir tickets de forman manual. Consulta el apartado "**Tickets**" en la página **265**.
- **Modo de navegación Agente**: permite establecer el modo de ejecución del agente PCSM.
  - **Desactivado**.
  - **Usuario**: el agente no muestra la ventana de Soporte y por tanto impide el inicio de sesión para entrar en el modo administrador. Este es el modo de ejecución normal del agente PCSM para gestionar dispositivos en la red.
  - **Admin**: el agente se ejecuta de forma completa. Este es el modo de ejecución destinado al administrador de la red que utiliza el agente PCSM para resolver problemas mediante las herramientas de acceso remoto. Consulta el capítulo "**Herramientas de acceso remoto a dispositivos**" en la página **271** para obtener más información.

ESXi

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

*Consulta el capítulo "**Monitorización**" en la página **111** para obtener más información.*

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 a políticas de tipo monitorización. Estos quedarán suprimidos 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 deberá ser tenido en cuenta.

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.

> *Solo se permite la activación de una política de administración de dispositivos móviles en un momento concreto.*

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.

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.
- **Wifi**: 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 de caracteres mínimo que el usuario deberá de utilizar al definir su código 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	Número de minutos que el dispositivo puede permanecer sin actividad antes de bloquear la pantalla. Elegir un valor entre 2 y 5 minutos para aplicar la política tanto en dispositivos Android como iOS.
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	Número de intentos de introducción del código de acceso antes de borrar todos los datos del dispositivo.

Tabla 7.4: configuración de las características 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.

Tabla 7.5: configuración de las restricciones de uso de un dispositivo iOS

Campo	Descripción
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.
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.

Tabla 7.5: configuración de las restricciones de uso de un dispositivo iOS

Campo	Descripción
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.
Permitir la instalación de zonas para la configuración de la interfaz de usuario	
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.

Tabla 7.5: configuración de las restricciones de uso de un dispositivo iOS

Campo	Descripción
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 7.5: configuración de las restricciones de uso de un dispositivo iOS

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 7.6: 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.
Tipo de proxy	Configura el proxy a utilizar con la conexión Wifi.

Tabla 7.7: configuración de la conexión Wifl

Monitorización

Añade procesos de monitorización de los recursos de los dispositivos.

*Consulta el capítulo "**Monitorización**" en la página **111** para obtener más información.*

Gestión de parches

Descarga y aplica parches de software.

*Consulta el capítulo "**Gestión de parches**" en la página **211** para obtener más información.*

Energía

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

- **Apagar el disco después de**: especifica el número de minutos de inactividad antes de que el disco duro entre en estado de reposo.
- **Apagar la pantalla después de**: especifica el número de minutos de inactividad antes de que la pantalla se apague.
- **Modo de espera después de**: especifica el número de minutos de inactividad antes de que el equipo entre en modo de suspensión.
- **Programación**: permite establecer un horario para forzar un estado de ahorro de energía en el equipo: suspensión, hibernación o apagado.

Gestión de software

Permite al administrador definir las aplicaciones qué se instalarán y se actualizarán en los equipos de la red para cumplir con las directivas de software establecidas en la empresa.

*Consulta el capítulo "**Gestión del software**" en la página **247** para más información.*

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 "**Gestión de parches**" en la página **211** para obtener más información.*

Capítulo 8

Monitorización

La monitorización es un tipo de política que detecta de forma desatendida el mal funcionamiento de los dispositivos de los usuarios. 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 comandos para resolverlas, todo ello sin intervención humana.

CONTENIDO DEL CAPÍTULO

Configuración manual de monitores

Políticas, monitores y acceso a la funcionalidad

En la mayor parte de los casos los monitores se crean en el marco de una política de tipo monitorización, que puede contener uno o más monitores. Cada monitor vigila un aspecto concreto del dispositivo y se permite su agrupación en una misma política para minimizar el número de elementos configurables por el administrador de la red y simplificar la gestión.

Como se indica en el capítulo "**Políticas**" en la página **97**, las políticas definen una serie de servicios o tareas que se ejecutan de forma repetitiva en el dispositivo (en este caso el servicio a ejecutar será un monitor) y los dispositivos que recibirán estas tareas. No obstante, es posible crear monitores fuera del marco de una política en el Nivel dispositivo, por lo tanto 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 **Monitorizar** haz clic en el control de selección **Monitores**.

Composición de un monitor

Un monitor se compone de cuatro grupos de configuraciones:

- **Tipo del monitor**: indica su funcionalidad.
- **Configuración de activación**: 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 "**Alertas y tickets**" en la página **259**).

Pasos para crear un monitor

1. Elige el tipo de política

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

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 dependiendo de los recursos objeto de monitorización en el dispositivo del usuario.

4. Configura el monitor

Dependiendo de 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 (**Crítico**, **Alto**, **Moderado**, **Bajo**, **Información**).
- **Resolución automática**: indica el tiempo que tiene que transcurrir para que una alerta se considere resuelta de forma automática, siempre que el origen de la causa que la provocó haya desaparecido.

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.

Monitorización de equipos Windows, Linux y macOS

Los monitores disponibles para equipos de sobremesa, portátiles y servidores son:

Nombre del monitor	Función	Disponible en
Componente de monitorización	Lanza un componente de monitorización de la **ComStore** o uno diseñado por el administrador.	Windows, macOS, Linux
Monitor WMI	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
Monitor de CPU	Controla el consumo de CPU.	Windows, macOS, Linux
Monitor de estado online	Comprueba cada 90 segundos si el dispositivo tiene un agente PCSM instalado y que funciona correctamente.	Windows, macOS, Linux, ESXi, Dispositivos de red
Monitor de memoria	Controla el consumo de memoria.	Windows, macOS, Linux
Monitor de parches	Controla la instalación de las actualizaciones programadas con el módulo Patch Management.	Windows
Monitor de procesos	Controla el estado de un proceso concreto.	Windows, macOS, Linux
Monitor de rendimiento de Windows	Monitoriza ciertos contadores del sistema operativo asociados a procesos en ejecución para generar alertas si caen por debajo de los umbrales establecidos.	Windows
Monitor de servicios	Controla el estado de un servicio concreto.	Windows
Monitor de Software	Supervisa el software que se instala o desinstala del dispositivo.	Windows

Tabla 8.1: listado de monitores disponibles

Nombre del monitor	Función	Disponible en
Monitor de uso del disco	Controla el consumo de disco duro.	Windows
Monitor del estado del antivirus	Monitoriza la presencia de un antivirus en el equipo y si está actualizado.	Windows, macOS, Linux
Monitor de registro de eventos	Supervisa la aparición de determinados registros en el visor de sucesos.	Windows
Monitor del tamaño de archivos / carpetas	Controla el tamaño de ficheros y carpetas.	Windows, macOS, Linux
Monitor vía ping	Monitoriza la conectividad de dispositivos mediante el protocolo ICMP y comprueba el buen funcionamiento de la red.	Windows

Tabla 8.1: listado de monitores disponibles

A continuación se indican los parámetros que se definen en cada tipo de monitor.

Componente de monitorización

Consulta el apartado "**Monitorización de dispositivos mediante componentes**" en la página **118**.

Monitor WMI

- **Espacio de nombres WMI**. Ejecuta el comando `Get-WMIObject -namespace "root" -class "__Namespace" | Select Name` en una ventana de Powershell para listar todos los espacios de nombres disponibles en Windows.
- **Consulta WMI en formato WQL.**Consulta el enlace **https://docs.microsoft.com/en-us/windows/desktop/wmisdk/querying-with-wql** para obtener información sobre el lenguaje WQL utilizado en las consultas WMI.
- **Propiedad WMI a recuperar**.
- **Cálculo del resultado (Valores numéricos)**: construye una ecuación que modifica el valor numérico obtenido. Utiliza los operadores matemáticos básicos (`+ - * /`) junto a una constante. Por ejemplo, para multiplicar el valor obtenido de la consulta por 5 introduce `*5`.
- **Traducción del resultado (Valores de texto)**: traduce los valores numéricos obtenidos a cadenas de caracteres que facilitan su comprensión. Utiliza el carácter "`,`" para separar varias traducciones y el carácter "`=`" para establecer la equivalencias. Por ejemplo `1=OK, 0=NoOK`.
- **Nombre para mostrar**: se utiliza como descripción del monitor en los listados de monitores.
- **Formato de datos**: indica la unidad de medida de los datos para ganar claridad en su visualización.
- **Configuración de las alertas**: especifica los valores y el período de tiempo que se tienen que producir para desencadenar alertas. En las expresiones de comparación se toma el valor original, no el producido como resultado de la ecuación introducida en **Cálculo del resultado**. La misma regla se aplica con las cadenas de caracteres configuradas en **Traducción del resultado**.

Monitor de CPU

- Límite de consumo de CPU en porcentaje.
- Tiempo que deberá de permanecer el consumo de CPU por encima del límite para activar el monitor en minutos.
- Intervalo de monitorización en minutos.

Monitor de estado online

- Establece la activación del monitor cuando el dispositivo no está accesible o cuando sí lo está.
- Tiempo que el dispositivo deberá de permanecer en el estado indicado anteriormente para generar una alerta.

Monitor de memoria

- Porcentaje de memoria utilizada por el sistema operativo y los programas durante el intervalo de tiempo establecido.
- Intervalo de comprobación medido en minutos.

Monitor de parches

El monitor se activará cuando se produzca una instalación fallida de un parche. Consulta el capítulo "**Gestión de parches** en la página **211**.

Monitor de procesos

- Nombre del proceso con o sin extensión.
- El proceso está en ejecución o se ha descargado de la memoria.
- El proceso ha alcanzado un porcentaje de consumo de CPU o de memoria durante un periodo medido en minutos.
- Intentar eliminar el proceso si se genera una alerta.

Monitor de rendimiento de Windows

- Contador con el formato `\Categoría\Contador`. Por ejemplo `\TCPv6\Conexiones activas`.

Ejecuta el comando TypePerf.exe -q en una ventana de línea de comandos para obtener un listado de todos los contadores disponibles en el equipo.

- Instancia.
- **Configuración de las alertas**: especifica los valores que desencadenarán una alerta y el periodo de tiempo que se tiene que mantener el valor.

Monitor de servicios

- Nombre del servicio.
- **Estado del proceso**: en ejecución o detenido.
- **Consumo del proceso**: porcentaje de CPU y de memoria.
- Periodo de tiempo medido en minutos que se debe de cumplir para generar una alerta.
- Retraso del comienzo de la monitorización con respecto al inicio del equipo medido en minutos.
- **Intentar iniciar acciones correctoras**: iniciar un servicio parado o parar un servicio en ejecución.
- No alertar en el caso de que el servicio se deshabilite de forma manual.

Monitor de software

- Nombre del paquete de software a comprobar. Consulta el apartado "**Auditoría de licencias** en la página **171**.
- **Estado del software**: instalado, no instalado, cambio de versión.

Monitor de uso del disco

- Unidad de disco a monitorizar.
- Uso de la unidad o espacio libre en porcentaje o en Gigabytes que servirá de límite.
- **Tipo de unidades a monitorizar**: unidades fijas y/o unidades mayores de un determinado tamaño.
- Tiempo en minutos que deberá de permanecer la condición configurada para que se genere una alerta.

Monitor del estado del antivirus

- **Estado del antivirus a monitorizar**: indica el estado del antivirus que activará el monitor (**No detectado**, **No ejecutándose**, **Ejecutándose y no actualizado**).
- Duración en minutos del estado del antivirus monitorizado para generar una alerta.

Monitor de registro de eventos

- **Nombre de registro de evento (obligatorio):** nombre de la rama del visor de eventos donde se almacena el evento (Aplicación, Seguridad, Sistema, Instalación, Eventos reenviados).
- **Nombre del origen de los eventos (obligatorio):** contenido del campo Origen del visor de eventos del dispositivo. Utiliza el carácter "`%`" de comodín para agrupar subcadenas. La comparación no tiene en cuenta mayúsculas y minúsculas.
- **Códigos de evento:** introduce uno o más códigos separados por espacios. Utiliza el carácter "–" delante de un código de evento para invertir la selección. Por ejemplo `-56` alertará de todos los códigos menos del `56`.
- **Tipo de evento**: **Crítico**, **Error**, **Aviso**, **Información** y/o **Detallado**.

- **Descripción de evento**: utiliza las reglas siguientes para buscar cadenas en la pestaña General del visor de sucesos:
  - Palabras independientes.
  - Frases entre comillas para buscar literales
  - Carácter de negación "–" para excluir de los resultados aquellos que contentan las palabras negadas.
  - El espacio separando las palabras aplica una operación `OR` entre ellas a la búsqueda.
  - Para buscar el carácter comillas utiliza dobles comillas.
- Frecuencia de aparición o no aparición en el intervalo de tiempo especificado para que el monitor genere una alerta.
- **Resolución automática**: especifica si la alerta se resolverá al detectar un evento distinto al definido en el punto anterior.

> *Para evitar la generación de un número de alertas exageradamente alto, Panda Systems Management desactiva su generación a partir de la 5º alerta dentro del intervalo de 12 horas. Si un monitor genera un número anormalmente alto de alertas (más de 1000 en 12 horas) éste se desactivará automáticamente para ese dispositivo concreto.*

Monitor del tamaño de archivos / carpetas

- **Tipo de monitorización**: fichero o carpeta.
- Ruta absoluta del elemento a monitorizar.
- **Tipo de comprobación**: mínimo o máximo.
- Tamaño límite.
- Tiempo que deberá de permanecer el elemento fuera de los parámetros establecidos para generar una alerta.

Monitor vía ping

- Dirección IP del dispositivo que se quiere monitorizar.
- Número de paquetes que se enviarán.
- Intervalo de tiempo en el cual se enviarán los paquetes.

Monitorización de dispositivos mediante componentes

Panda Systems Management permite utilizar componentes desarrollados por el administrador o por Panda Security para expandir las posibilidades del producto, y así abarcar virtualmente cualquier aspecto del dispositivo.

Para añadir un componente a una política de tipo monitorización sigue los pasos mostrados a continuación:

- Haz clic en el menú general **Comstore**, panel de la izquierda **Monitores** para listar todos los componentes que realizan tareas de monitorización. Consulta el capítulo "**Componentes y ComStore**" en la página **139** para obtener más información sobre la ComStore.
- Selecciona un componente y haz clic en el botón **Añadir a mi biblioteca de componentes**. El componente se descargará y se añadirá al repositorio particular del administrador.
- Haz clic en el menú general **Componentes**, panel lateral **Mis componentes**, **Monitores** para obtener un listado de todos los componentes ya incorporados en el repositorio del administrador.
- Sigue los pasos mostrados en el apartado "**Pasos para crear un monitor**" y en el paso 3 elige un monitor de tipo **Componente de monitorización**.
- Selecciona el componente de tipo monitor del desplegable **Ejecutar el Componente Monitor**.
- Indica cada cuantas horas y minutos se ejecutará el monitor.

Monitorización de impresoras

Panda Systems Management agrega de forma automática monitores pre configurados en el momento en que dispositivos de tipo impresora se incorporan a la plataforma de administración. El monitor se añadirá en la zona a la que pertenezca la impresora.

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.

Monitorización de dispositivos de red mediante 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.

Parámetros a monitorizar

La gran mayoría de dispositivos compatibles con SNMP publican en su MIB una cantidad de información detallando su estado, mediante la cual es posible recuperar muchos parámetros del funcionamiento interno 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 ha sufrido o sufrirá un fallo inminente y requerirá atención por parte del departamento técnico.

Monitor de tasa de transferencia SNMP

Este monitor sirve exclusivamente para monitorizar el volumen de datos enviados y recibidos por los dispositivos administrados. No es necesario ningún tipo configuración de la MIB ya que los dispositivos publican esta información en un OID fijo (1.3.6.1.2.1.2) que recibe el nombre de IF-MIB. Para ello indica los parámetros del monitor mostrados a continuación:

- **Intervalo de comprobación**: cada cuantos minutos se comprobaran los valores del OID.
- **Número de interface (opcional)**: número de la interface a monitorizar.
- **Tipo de trafico**: **Tráfico entrante**, **Tráfico saliente**, **Total**.
- **Condición de generación de alerta**: indica el valor medio necesario para generar una alerta y el tamaño de la muestra.

Pasos para la creación de monitores SNMP

Para monitorizar un dispositivo SNMP sigue los pasos mostrados a continuación:

1. Prepara 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 Panda 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 gratuito Mibble (**https://www.mibble.org**) o un software equivalente.

2. Designa un dispositivo con un agente instalado como Nodo de red

Consulta el apartado "**Configuración de un nodo de red**" en la página **63** para obtener información acerca de cómo designar a un agente PCSM el rol de Nodo de red y los requisitos que es necesario satisfacer.

> *Se recomienda comprobar la comunicación en el puerto 161 para los protocolos TCP y UDP entre el agente PCSM 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 apartado "**Integración de dispositivos de red**" en la página **57** para más información sobre como añadir a la consola de administración dispositivos no compatibles con la instalación del agente Panda Systems Management.

4. Configura 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.

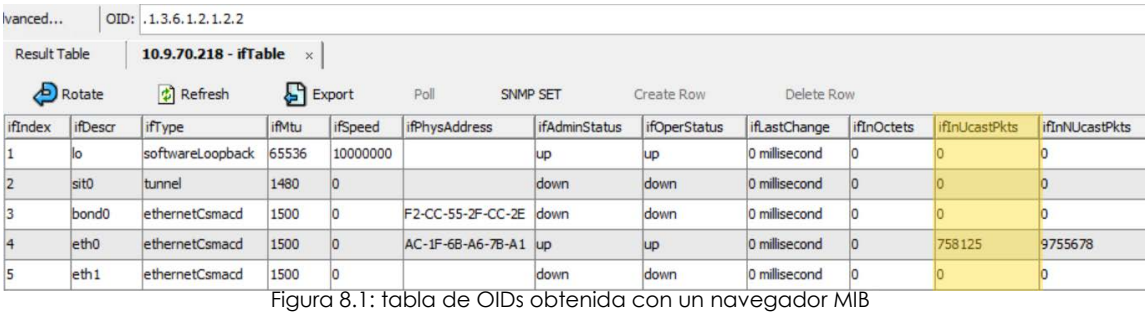
Para crear una política de monitorización SNMP sigue los pasos mostrados en el apartado "**Pasos para crear un monitor**" en la página **113** y configura los parámetros mostrados a continuación:

- **OID SNMP del objeto a monitorizar:** cadena OID que se corresponde al parámetro del dispositivo a monitorizar.
- **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**.
  - Para controlar mensajes de error devueltos por el dispositivo al enviar una petición SNMP, activa la casilla **Generar alerta cuando el OID devuelva Nulo, No existe el objeto o No existe la instancia**.
- **Intervalo de comprobación**: indica cada cuantos minutos el monitor leerá la OID configurada.
- **Transformar resultado:** establece correspondencias entre los valores que envía el dispositivo al servidor Panda Systems Management y cadenas de texto o datos numéricos que se mostrarán en la consola de administración. Las alertas se generan tomando como referencia los valores originales, pero en la consola PCSM se muestran 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**.

5. Configura una política de monitorización SNMP para grupos de dispositivos (opcional)

Para evitar crear un monitor independiente por cada valor de un dispositivo a monitorizar, se permite la monitorización de agrupaciones de OIDs. Por ejemplo, un caso de uso frecuente es la monitorización del espacio de varios discos duros de un mismo equipo.

En la práctica, monitorizar varios dispositivos a la vez implica monitorizar un OID que contiene toda la información a monitorizar en formato tabla. Para seleccionar las celdas de la tabla que interesan, es necesario especificar la fila y la columna de la tabla. Para ello sigue los pasos mostrados a continuación:



ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange	ifInOctets	ifInUcastPkts	ifInNUcastPkts
1	lo	softwareLoopback	65536	10000000		up	up	0 millisecond	0	0	0
2	sit0	tunnel	1480	0		down	down	0 millisecond	0	0	0
3	bond0	ethernetCsmacd	1500	0	F2-CC-55-2F-CC-2E	down	down	0 millisecond	0	0	0
4	eth0	ethernetCsmacd	1500	0	AC-1F-6B-A6-7B-A1	up	up	0 millisecond	0	758125	9755678
5	eth1	ethernetCsmacd	1500	0		down	down	0 millisecond	0	0	0

Figura 8.1: tabla de OIDs obtenida con un navegador MIB

- **OID SNMP del objeto a monitorizar:** cadena OID que representa la tabla que contiene los valores de los dispositivos a monitorizar.
- **Tabla SNMP**: activa esta opción si el OID indicado contiene una tabla de valores que reflejan el estado de uno o más dispositivos. Desactiva esta opción si el OID indicado contiene un único valor.
- **Columna identificación**: índice de la columna que contiene los identificadores de los dispositivos a monitorizar. La primera columna tiene el índice 0. Los identificadores de dispositivo son cadenas de caracteres que identifican los dispositivos a monitorizar, y que se incluirán en la salida del proceso de monitorización.
- **Columna valor**: número de la columna entre corchetes que contiene el estado del dispositivo a monitorizar. La primera columna tiene el indice 0. Se admiten operaciones aritméticas sencillas entre columnas; por ejemplo si la columna 10 contiene el espacio total de los discos duros y la columna 11 el espacio consumido, se puede indicar {10} - {11}/1048576 para calcular los gigas libres de los discos duros monitorizados.

Monitorización de servidores ESXi

Los monitores disponibles para servidores ESXi son visibles únicamente desde el Nivel dispositivo asociado al servidor. Consulta el apartado "**Políticas, monitores y acceso a la funcionalidad**" en la página **112**. A continuación se muestran los monitores para servidores ESXi:

Nombre del Monitor	Función
Monitor de CPU ESXi	Controla el consumo de CPU del servidor ESXi.
Monitor de memoria ESXi	Controla el consumo de memoria del servidor ESXi.
Monitor de almacén de datos ESXi	Controla el consumo de espacio en los diferentes almacenes de datos del servidor ESXi.
Monitor de sensor de temperatura ESXi	Controla la temperatura del servidor ESXi.
Monitor de ventilador ESXi	Controla el correcto funcionamiento de los ventiladores del servidor.
Monitor de estado del disco 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 8.2: listado de monitores compatibles con servidores ESXi

A continuación se indican los parámetros que definen cada tipo de monitor.

Monitor de CPU ESXi

- Límite de consumo de CPU en porcentaje.
- Tiempo que deberá de registrarse el consumo de CPU por encima del límite para activar el monitor en minutos.
- Intervalo de monitorización en minutos.

Monitor de memoria ESXi

- Porcentaje de memoria utilizado por el sistema operativo y los programas durante el intervalo de tiempo establecido.
- Intervalo de comprobación medido en minutos.

Monitor de almacén de datos ESXi

- Uso del almacén de datos en porcentaje que servirá de límite.

- Tiempo en minutos que deberá de registrarse la condición configurada para que se genere una alerta.

Monitor de sensor de temperatura ESXi

- Temperatura del servidor en grados Celsius.
- Tiempo en minutos que deberá de registrarse la condición configurada para que se genere una alerta.

Monitor de ventilador ESXi

Genera una alerta si el sensor del ventilador del servidor registra algún valor fuera de lo normal.

Monitor de estado del disco ESXi

Genera una alerta cuando un proveedor CIM (Common Information Model) detecta un fallo en la unidad de almacenamiento. Si no existen proveedores CIM activados el monitor no generará ninguna alerta.

> *Consulta https://code.vmware.com/vmware-ready-programs/management/cim para obtener más información acerca del estándar CIM en los productos VMWare.*

Monitor de fuente de alimentación de ESXi

Genera una alerta si el sensor de la fuente de alimentación del servidor registra algún valor fuera de lo normal.

Monitor de estado online

Consulta "**Monitor de estado online**".

Configuración automática de monitores

> *Con la creación de una nueva cuenta, Panda Systems Management añade de forma automática las políticas de monitorización Windows: Workstation y Windows: Server.*

Para acelerar la tarea de configurar monitores 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 dispositivos** para agregar grupos o filtros de dispositivos que recibirán la política.
- Haz clic en el botón **Guardar**.
- Si quieres que la política se aplique de forma inmediata, haz clic en el botón **Desplegar cambios**.

Monitor de Windows: Workstation

El objetivo de este monitor es ofrecer una visión rápida del estado del sistema operativo Windows instalado en el dispositivo. Este monitor solo ofrece métricas de Windows y alerta cuando éstas se acercan a los límites marcados.

Con esta política de monitor se recoge el estado de los siguientes parámetros:

- Monitor de uso del disco.
- Monitor de servicios.

El Monitor de Windows: Workstation ahorra tiempo a los técnicos de mantenimiento ya que es capaz de resolver automáticamente ciertos tipos de incidencias muy frecuentes sin generar alertas.

Monitor de Windows: Server

Este monitor ofrece una visión general del estado del servidor mediante un conjunto de gráficas.

Este monitor no genera una alerta de rendimiento cuando los dispositivos gestionados sobrepasan o se acercan a los límites establecidos en su configuración. Para generar alertas se puede aplicar conjuntamente otra política con ese objetivo.

Este monitor detectar las siguientes condiciones:

- Registro de eventos.
- Reinicio requerido.
- Reinicio por pantallazo azul.
- Estado del disco.
- Servidor fuera de línea.
- Conflictos de IP.
- Estado de parcheo.
- Monitor de memoria y CPU.

Importar y exportar una política de monitorización

Importar políticas de monitorización

- Para importar una política en el Nivel cuenta haz clic en el menú general **Cuenta**, pestaña **Políticas.**

- Para importar una política en el Nivel zona haz clic en el menú general **Zonas** y en la zona apropiada, y haz clic en el menú de pestañas.
- 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.

Exportar políticas de monitorización

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

- Haz clic en el nombre de la política para poder editarla.
- 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.

Gestión de monitores

Una vez creados y asignados los monitores, el administrador puede comprobar su estado y resultados en el Nivel dispositivo asociado a cada equipo monitorizado.

Acceso al listado de monitores

- Haz clic en el menú general **Zonas** y en la zona donde reside el dispositivo.
- En el menú de pestañas **Monitorizar** haz clic en el control de selección **Monitores** situado en la parte superior derecha de la ventana para listar todos los monitores asignados al dispositivo y su estado.

Descripción de los campos del listado de monitores

El listado muestra los monitores agrupados por política **(1)** dado que una política puede estar formada por uno o más monitores. **(2)**. Haz clic en los iconos ▶ y ▼ para ocultar o desplegar los monitores que pertenecen a una política. Los monitores que no tienen una política asociada aparecerán bajo el grupo **Sin políticas**.

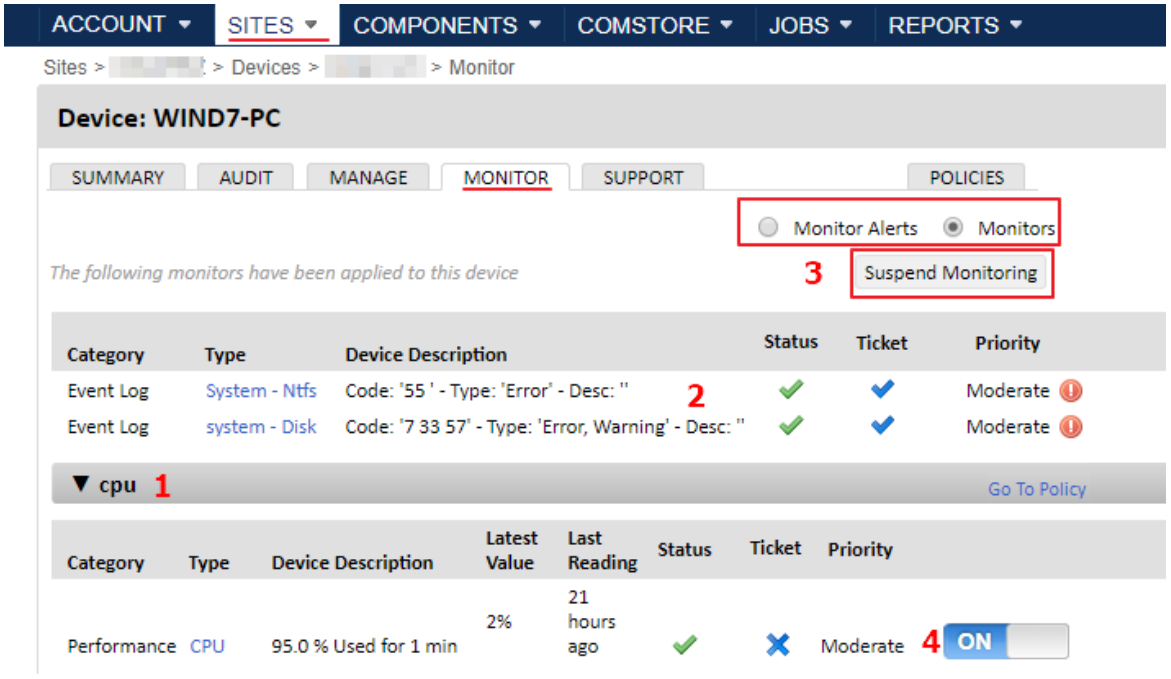


Figura 8.2: listado de monitores asociado al Nivel dispositivo del equipo

Además, el administrador puede suspender la monitorización completa del dispositivo **(3)** o cada monitor de forma individual **(4)**.

Campo	Descripción
Categoría	Muestra el tipo de monitor asignado.
Tipo	Dependiendo del tipo de monitor y de su configuración asociada muestra los parámetros principales, que describen el subtipo de monitor asignado.
Descripción del dispositivo	Describe los parámetros secundarios que forman la configuración del monitor.
Último valor	Muestra el último valor recibido en el servidor Panda Systems Management.
Última lectura	Muestra la fecha en la que se recibió la última lectura del monitor.
Últimas 30 métricas	En los monitores que devuelven datos de tipo numérico se forma una gráfica de líneas con las 30 últimas mediciones recibidas por el servidor Panda Systems Management. Pasa el puntero de ratón por encima de la gráfica para ampliar detalles.
Estado	Indica si el monitor no ha registrado ninguna lectura fuera de los parámetros establecidos.
Responder	Indica si el monitor tiene configurado algún tipo de respuesta al generar avisos.

Tabla 8.3: atributos de un monitor

Campo	Descripción
Ticket	Indica si el monitor tiene configurada la generación de tickets.
Prioridad	Indica la prioridad de las alertas generadas por el monitor y establecidas en su configuración.
Barra de iconos	Para los monitores que no tienen asociada una política se incluye una barra de iconos que permite su edición y borrado. • Borra todas las alertas generadas por el monitor. • Editar el monitor. • Borra el monitor. Para editar o borrar un monitor asociado a una política es necesario editar la política. Consulta el apartado "**Gestión de políticas**" en la página **98**.
	Activa o desactiva temporalmente el monitor.
	Indica que la política de la que depende el monitor está deshabilitada en el Nivel zona.

Tabla 8.3: atributos de un monitor

Capítulo 9

Tareas

Las tareas son grupos de operaciones que se ejecutan en los dispositivos con un agente PCSM instalado y que permiten realizar procesos de forma puntual o repetitiva según un calendario configurado. Dependiendo del ciclo de repeticiones existen dos tipos de tareas:

- **Tareas programadas**: son las tareas que se ejecutan bajo un patrón de repetición programado.
- **Tareas rápidas**: son las tareas que se ejecutan puntualmente bajo demanda por parte del administrador de la red.

Las tareas pueden definirse en el Nivel cuenta, zona o dispositivo dependiendo del conjunto de dispositivos afectado.

CONTENIDO DEL CAPÍTULO

Elementos de las tareas

Una tarea está formada por los elementos detallados a continuación:

Elemento	Descripción
Componente asociado	Contiene el proceso o procesos que se desplegarán en los dispositivos afectados por la tarea y se ejecutarán.

Tabla 9.1: elementos de una tarea

Elemento	Descripción
Destino	Conjunto de dispositivos que recibirán la tarea. Puede ser un filtro, grupo, zona o dispositivo particular.
Resultado	En cada ejecución la tarea devuelve un código indicando si se ejecutó con éxito o no, así como otro tipo de información asociada al proceso desplegado en los equipos.
Programación	Las tareas pueden ser rápidas si no requieren ningún tipo de configuración adicional, o programadas si se repiten a intervalos de tiempo regulares.
Otras configuraciones	Dependiendo del tipo de tarea y desde dónde se ejecute se permiten definir opciones avanzadas, tales como el tiempo máximo de ejecución de la tarea, los destinatarios de los resultados y de las alertas en caso de haberlas etc.

Tabla 9.1: elementos de una tarea

Por defecto las tareas se ejecutan bajo la cuenta Local System del sistema operativo del dispositivo.

Cambios involuntarios en los destinatarios de una tarea

Debido a que el tiempo transcurrido desde que una tarea se programa hasta que se ejecuta puede ser muy variable, es posible que en ese intervalo los destinatarios de la tarea varíen de forma arbitraria. Tal es el caso de una tarea que tiene como destino un grupo o filtro de equipos cuyos dispositivos integrantes varían a lo largo del tiempo de duración de la tarea (entrando o saliendo de la agrupación), o de una tarea que utiliza un recurso de agrupación (zona, grupo o filtro) que deja de existir antes de iniciar la ejecución de la tarea o en su transcurso.

De forma general, los miembros de un grupo de dispositivos que reciben una tarea se resuelven justo antes de iniciar la ejecución de la misma. De esta forma, una tarea que ya ha iniciado su ejecución no se verá afectada por el borrado o cambio en la definición de los grupos o filtros que utiliza como destino. Sin embargo, si antes de su ejecución algún grupo o filtro es borrado, la tarea intentará resolver los destinatarios momentos antes de su ejecución y no encontrará los grupos configurados, de modo que no se ejecutará.

Lanzar tareas rápidas

El lanzamiento de tareas rápidas despliega componentes de forma puntual y bajo demanda, sin pasar por el proceso de configuración del programador de tareas. Puede ejecutarse desde la barra de iconos (forma abreviada) del Nivel donde se encuentren los dispositivos afectados o desde el menú general **Tareas**, menú de pestañas **Nueva tarea** (forma completa).

Configuración de componentes para su uso en tareas

Para lanzar una tarea que ejecute un componente hay que habilitarlo previamente:

- Haz clic en el menú general **ComStore** y en el panel lateral **Aplicaciones** o **Scripts**.
- Haz clic sobre el componente a ejecutar. Se abrirá una ventana con su descripción y características. Haz clic en el botón **Añadir a mi biblioteca de componentes**.
- Haz clic en el menú general **Componentes**.
- Haz clic en el icono de favorito en los componentes que podrán ser lanzados por una tarea.

> *Solo los componentes de tipo script y aplicación incorporan el icono favoritos. Los componentes de tipo monitor solo pueden ser ejecutados por una política de tipo monitorización.*

Lanzar tareas rápidas desde el menú de acciones (forma abreviada)

Para ejecutar una tarea rápida de forma abreviada sigue los pasos mostrados a continuación:

- Define los destinatarios de la tarea:
  - Si los destinatarios son todos los dispositivos pertenecientes a una o varias zonas, haz clic en el menú general **Zonas** y selecciona con las casillas de selección las zonas que recibirán la tarea.
  - Si los destinatarios son filtros o grupos del Nivel cuenta o Nivel zona haz clic en una agrupación del panel de la izquierda y selecciona los dispositivos que recibirán la tarea.
- Haz clic en el icono de tarea rápida de la barra de iconos. Se mostrará un desplegable con todos los componentes configurados como favoritos.
- Utiliza el control **Búsqueda** para localizar un componente concreto de la lista, o el control **Grupos** para mostrar los componentes de un determinado grupo.

> *En este método solo es posible asignar un único componente a una tarea. Si quieres asignar dos o más componentes a una tarea rápida consulta el apartado "***Lanzar tareas programadas***".*

- Selecciona el componente a ejecutar y haz clic en **Guardar**. Si la tarea requiere variables de entrada se mostrará una caja de texto donde introducir la información necesaria.

Figura 9.1: componente con variables de entrada

- La tarea se ejecutará de forma inmediata. Si la casilla de selección **Ir a la página de la lista de tareas tras hacer el envío** está activada se mostrará la ventana de **Tareas activas**.
- El nombre de la tarea rápida será asignado de forma automática con el formato "`Tarea rápida ejecutando el componente`" [Nombre del componente] "`en el dispositivo`" [Nombre del dispositivo]

Lanzar tareas desde el menú general Tareas (forma completa)

En el menú general **Tareas**, menú de pestañas **Nueva tarea** se puede configurar de forma completa una tarea rápida. El procedimiento es equivalente al mostrado en el apartado "**Lanzar tareas rápidas desde el menú de acciones (forma abreviada)**" si bien en este caso se especifican de forma explicita todas las opciones de la tarea rápida:

Campo	Descripción
Nombre	Permite introducir un nombre que ayudará a localizarla posteriormente en el listado de tareas ejecutadas.
Programación	Tipo de programación, inmediata para las tareas rápidas.
Destinatarios de la tarea	Elige los grupos, filtros o zonas que recibirán la tarea.
Componentes	Elige uno o varios componentes y establece el orden de ejecución con las flechas verdes situadas a su derecha.
Tarea desactivada	Especifica si quieres desactivar la tarea para impedir su ejecución sin tener que borrarla.
Hacer que la tarea expire después de	Establece la duración de la tarea de forma relativa. Indica el intervalo de tiempo a partir del momento de su lanzamiento tras el cual la tarea quedará interrumpida.
Duración	Establece la duración de la tarea de forma absoluta indicando la fecha en la que terminará su ejecución.
Ejecución	Especifica las condiciones que se requieren para ejecutar el componente en el dispositivo del usuario: • **Ejecutar esta tarea sólo cuando el usuario haya iniciado sesión**: requiere que el usuario haya iniciado sesión en el dispositivo para ejecutar la tarea. • **El usuario que haya iniciado sesión debe tener derechos de administrador**. • **Ejecutar cuando el usuario haya iniciado sesión**: ejecuta el componente de forma automática cuando el usuario inicia la sesión en el dispositivo. • **Avisar al usuario pero no ejecutar**: el componente no se ejecuta de forma automática. Se presenta un mensaje emergente al usuario pidiendo una confirmación de ejecución.
Alertas	Define cuando se generará una alerta: si la tarea termina con éxito, fracaso, si genera un aviso o ha caducado por vencer el tiempo máximo de ejecución asignado. Para mostrar las alertas generadas haz clic en el menú general **Cuenta**, menú de pestañas **Monitorizar**.

Tabla 9.2: configuración de una tarea completa

Campo	Descripción
Enviar automáticamente por correo electrónico opciones de STDOUT/ STDERR	Copia en un mensaje de correo la salida estándar (`STDOUT`) o la salida de error (`STDERR`) que generó el componente terminada su ejecución.
Destinatarios de la tarea	Establece si las alertas se recibirán adicionalmente por correo en las cuentas configuradas. • **Para configurar las cuentas de correo predeterminadas a nivel de cuenta**: en el menú general **Ajustes**, menú de pestañas **Configuración de cuenta**, **Destinatarios de correo**, activa la casilla de selección **Alertas** e introduce las direcciones de correo haciendo clic en el icono **Editar destinatario**. • **Para configurar las cuentas de correo predeterminadas a nivel de zona**: en el menú general **Zonas** elige la zona, menú de pestañas **Configuración**, **Destinatarios de correo**, activa la casilla de selección **Alertas** e introduce las direcciones de correo haciendo clic en el icono **Editar destinatario.**

Tabla 9.2: configuración de una tarea completa

Lanzar tareas programadas

El lanzamiento de tareas programadas permite ejecutar componentes de forma repetitiva configurando el programador de tareas. El procedimiento puede iniciarse desde la barra de acciones haciendo clic en el icono  o desde el menú general **Tareas**, menú de pestañas **Nueva tarea**. En ambos casos se mostrará la pantalla de configuración para especificar cada una de las opciones de la tarea. El procedimiento es el mismo que el descrito en el apartado "**Lanzar tareas desde el menú general Tareas (forma completa)**" si bien es necesario indicar la programación de la tarea haciendo clic en el botón **Haga clic para cambiar** en el apartado **General**, **Programación**.

Programador de tareas

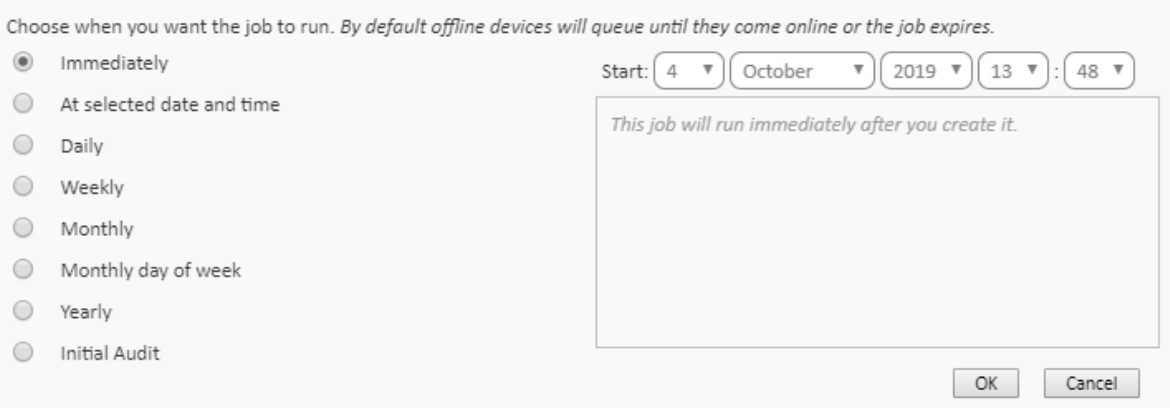


Figura 9.2: programador de tareas

El programador de tareas permite establecer la repetición de la tarea en función de los parámetros mostrados a continuación:

Campo	Descripción
Inmediatamente	Es el caso de una tarea rápida que se ejecuta en el momento de su configuración.
En la fecha y hora seleccionadas	La tarea se ejecuta una única vez en la fecha y hora establecidas.
Diariamente	La tarea se ejecuta todos los días a partir de la fecha y hora establecidas.
Semanalmente	La tarea se ejecuta todos los días de la semana establecidos a partir de la fecha y hora indicadas.
Mensualmente	La tarea se ejecuta los meses y días del mes indicados a partir de la fecha y hora establecidas.
Mensualmente, un día concreto de la semana	La tarea se ejecuta un día de la semana todos los meses. Se indica el día de la semana que se ejecutará la tarea y la fecha de inicio.
Anualmente	La tarea se ejecuta una vez al año en el día indicado a partir de la fecha y hora establecidas.
Auditoria Inicial	La tarea se ejecuta una vez que el dispositivo haya completado la primera auditoria después de la fecha de inicio establecida.

Tabla 9.3: configuración del programador de tareas

Gestión de tareas activas y completadas

Listado de tareas activas

Una tarea está activa cuando ha sido creada y está esperando su inicio según su programación configurada, o ya se ha iniciado pero todavía no ha terminado su ejecución.

Para mostrar un listado de las tareas activas haz clic en el menú general **Tareas**, menú de pestañas **Tareas activas**.

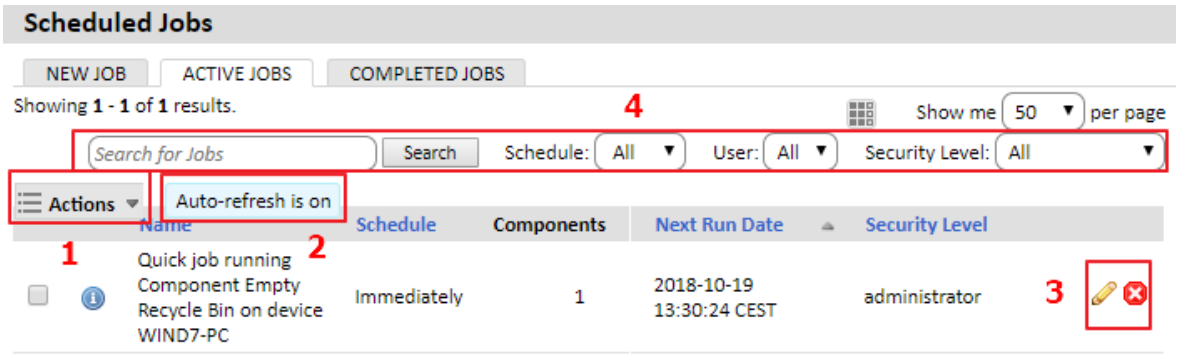


Figura 9.3: Ventana de tareas activas

La ventana de gestión de tareas activas contiene recursos para verificar el estado de las tareas y operar con ellas:

Campo	Descripción
Nombre	Nombre de la tarea. Si la tarea es rápida y se generó desde la barra de iconos el sistema le asigna un nombre automáticamente.
Programación	Inmediata o programada.
Componentes	Número de componentes que contiene la tarea.
Tareas ejecutadas	Número de veces que se ejecutó la tarea.
Próxima ejecución	Fecha de la próxima ejecución. Si la fecha aparece tachada la tarea no se volverá a ejecutar.
Última ejecución	Fecha de la última ejecución de la tarea.
Usuario	Usuario de la consola de administración que creó la tarea.
Rol	Rol del usuario de la consola de administración que creó la tarea.
Menú desplegable (1)	Permite exportar el listado de tareas activas, eliminar una tarea activa o recargar el listado de tareas.
Actualización automática (2)	El listado se recarga cada cierto tiempo para reflejar los cambios de estado de las tareas activas.
Acciones (3)	Borra o modifica la tarea.
Herramientas de búsqueda (4)	Incluye varios controles para filtrar el listado de tareas y facilitar la localización de una tarea particular.

Tabla 9.4: campos del listado de tareas activas

Listado de tareas completadas

Una tarea está completada cuando ha terminado su ejecución, tanto si ha tenido éxito como si ha dado algún tipo de error.

Para mostrar un listado de las tareas completadas haz clic en el menú general **Tareas**, menú de pestañas **Tareas completadas**. Los campos incluidos en el listado son los mismos que en Tareas Activas, descritos en el apartado "**Listado de tareas activas**".

Estado de una tarea

Para conocer el estado de una tarea haz clic sobre ella en los listados de tareas activas y completadas (menú general **Tareas**). Se abrirá la vista de tareas con toda la información relevante:

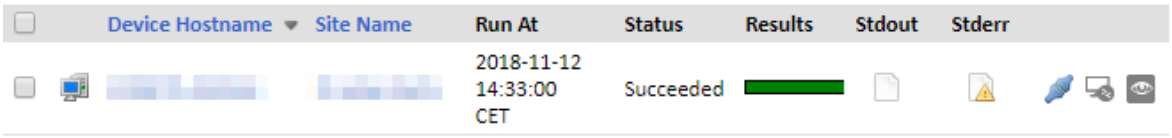


Figura 9.4: detalle de una tarea completada

Campo	Descripción
Nombre de host del dispositivo	Nombre del dispositivo que recibió la tarea.
Nombre de la zona	Agrupación de tipo zona a la que pertenece el dispositivo.
Ejecutado el	Fecha en la que se ejecutó la tarea.
Estado	Con éxito, error, vencido.
Resultados	Indica mediante un color el resultado de la ejecución de la tarea: • **Verde**: la tarea se ejecutó con éxito. • **Naranja**: la tarea se ejecutó pero se han encontrado algunos valores en la salida estándar (STDOUT). • **Rojo**: la tarea falló.
Stdout	Copia de la salida estándar del componente.
Stderr	Copia de la salida de error del componente.
Conectar con dispositivo	Consulta el capítulo "**Herramientas de acceso remoto a dispositivos**" en la página **271**.
Control remoto (RDP)	Consulta el capítulo "**Herramientas de acceso remoto a dispositivos**" en la página **271**.
Control remoto (VNC)	Consulta el capítulo "**Herramientas de acceso remoto a dispositivos**" en la página **271**.

Tabla 9.5: campos del estado de una tarea

Acciones sobre una tarea activa o completada

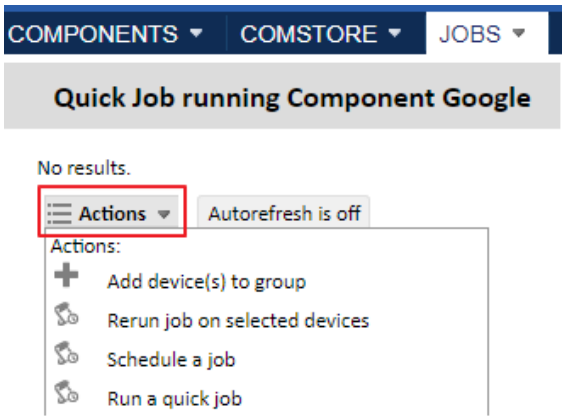


Figura 9.5: menú desplegable de acciones

Al hacer clic sobre una tarea activa o completada Panda Systems Management muestra una barra de iconos en forma de menú desplegable con varias opciones específicas para la gestión de tareas:

- **Volver a ejecutar la tarea en los dispositivos seleccionados**: vuelve a ejecutar la tarea en los dispositivos seleccionados, generalmente en aquellos donde se hayan dado errores en una ejecución previa.
- **Programar una tarea**: programa una tarea. Consulta el apartado "**Lanzar tareas programadas**".
- **Ejecutar una tarea rápida**: prepara la ejecución de una tarea rápida. Consulta el apartado "**Lanzar tareas rápidas**".
- **Descargar mensaje de error / salida seleccionado**: muestra una ventana donde permite preparar la descarga de la salida estándar o de error (`STDIN` / `STDOUT`) de la tarea.

Capítulo 10

Componentes y ComStore

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

CONTENIDO DEL CAPÍTULO

Tipos de componentes

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.

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 "**Distribución e instalación centralizada de software**" en la página **233**.

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 apartado que no esté cubierto inicialmente por la plataforma. En este caso será necesario añadir un componente de tipo monitor a la política. Consulta el capítulo "**Monitorización**" en la página **111** para obtener más información acerca de los monitores implementados en Panda Systems Management.

- **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.
Monitores	Política de cuenta, Política de zona o independiente.	Cada 60 segundos o configurable en la mayor parte de los monitores.	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 10.1: listado de tipos de componentes

> *Monitores, aplicaciones y scripts son prácticamente idénticos en lo que se refiere a su estructura interna. 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.*

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.*

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 (1)** en la figura 10.1 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 al repositorio del administrador:

- 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 **Añadir a mi Biblioteca de componentes** y el componente se descargará y se añadirá al repositorio.

Para listar los componentes ya añadidos al repositorio:

- Haz clic en el menú general **Componentes (2)**. En el panel lateral **Mis componentes (3)** se muestran los componentes agregados y agrupados según su categoría.
- Para buscar un componente concreto utiliza la caja de texto **Buscar (4)** situado a la derecha de la

ventana.

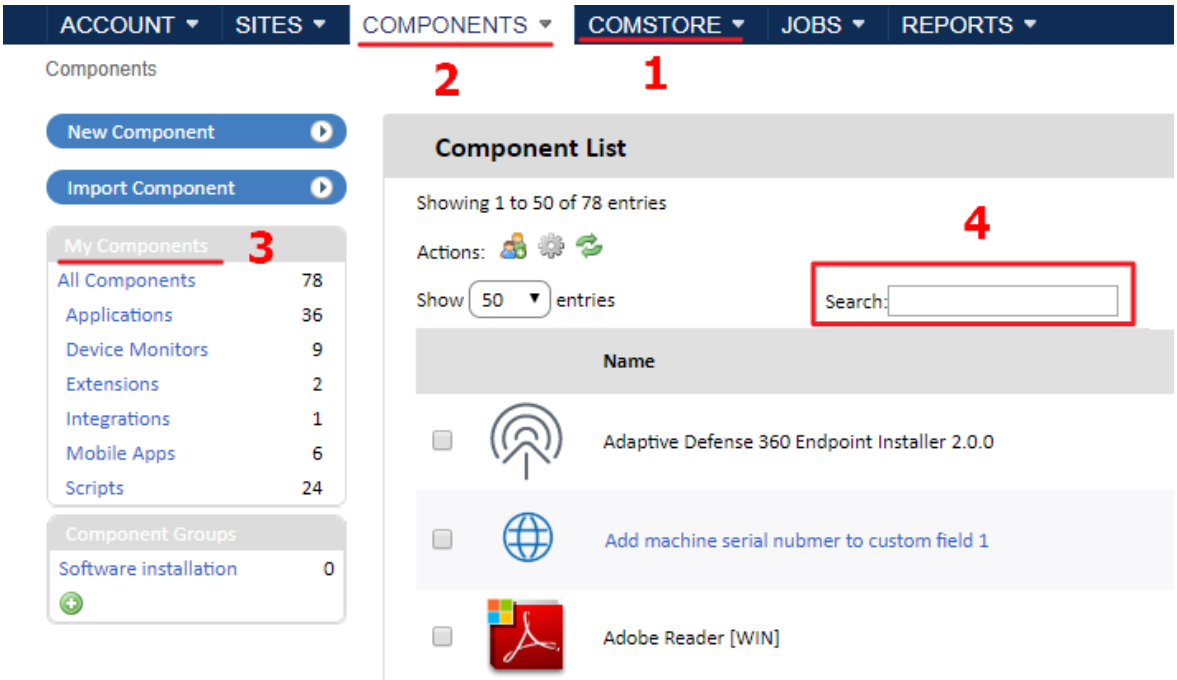


Figura 10.1: ventana de gestión de componentes

Agrupación de componentes en la ComStore

Los componentes publicados por Panda Security se agrupan 5 categorías en el panel lateral:

- Todos los componentes
- Aplicaciones
- Integraciones
- Monitores
- Scripts

Importar y descargar componentes

Para exportar un componente:

- En el menú general **Componentes** haz clic en el panel lateral **Importar componentes**. Únicamente se admiten componentes exportados previamente por la consola PCSM.

Para exportar un componente:

- En el menú general **Componentes** haz clic en el icono de la flecha del listado de componentes .

  Si el componente a descargar no tiene icono asociado, haz clic en el icono para copiar el componente. El componente copiado tendrá el icono asociado para su descarga.

Copia y retirada de componentes

- Para copiar un componente haz clic en el icono asociado al componente.

- Para retirar un componente del área **Componentes** haz clic en el icono asociado al componente. Las tareas que tengan ese componente asignado serán desactivadas pero no se borrarán. Un componente borrado sigue estando disponible en el área **ComStore** para su integración en el repositorio personal del administrador.

Clasificación y agrupación de los componentes integrados

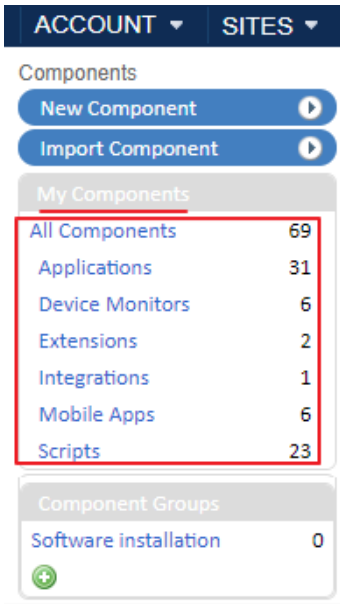


Figura 10.2: panel lateral mis filtros

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 **Grupos de componentes** accesible desde el panel lateral.

Para crear un grupo de componentes:

- Haz clic en el menú general **Componentes**.

- Haz clic en el icono en el panel lateral **Grupos de componentes** para dar un nombre al grupo.

- Selecciona los componentes que quieres agrupar con las casillas de selección del listado de componentes y haz clic en el icono de la barra de iconos. Se mostrará una ventana donde se listan los grupos de componentes creados previamente. Elige un grupo para añadir los

componentes seleccionados.

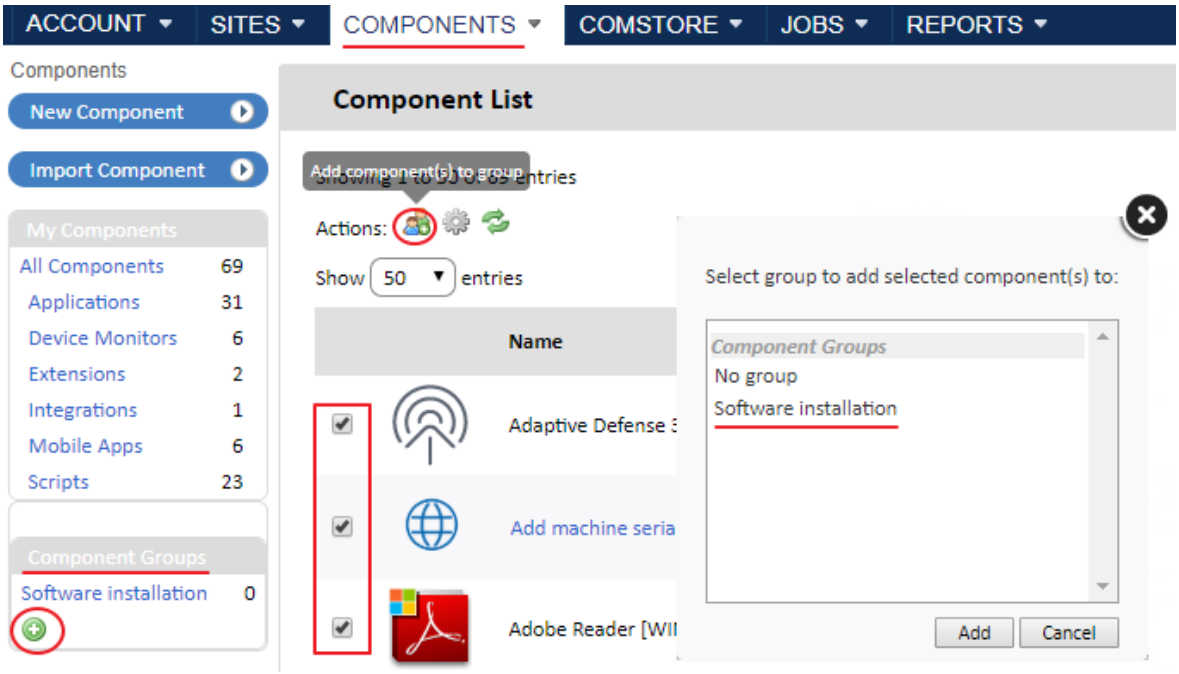


Figura 10.3: añadir un componente a un grupo de componentes

Actualización de componentes.

Periódicamente, Panda Security distribuye actualizaciones de los componentes publicados en la ComStore. Estas actualizaciones se muestran en el panel lateral **Buscar Actualizaciones** del menú general **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**.

> *La opción **Buscar Actualizaciones**, libera al administrador de la tarea de localizar 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.*

Si no deseas actualizar todos los componentes a la vez, puedes hacer clic en el botón **Get Update** de cada componente individual.

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

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**.

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 Panda Systems Management.

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 10.2: 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. Consulta el capítulo "**Distribución e instalación centralizada de software**" en la página **233**.*

Creación de un componente de tipo monitor

Presentación y objetivo del componente

A modo de ejemplo se detallan los pasos necesarios para crear un monitor desde cero y distribuirlo en los dispositivos de una zona concreta.

> *Consulta el apartado "**Distribución de documentos mediante lenguajes de script**" en la página **236** para ver otro ejemplo complementario de desarrollo de componentes.*

El objetivo del componente de ejemplo 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 si ha habido un incremento en el número de elementos almacenado en la cuarentena de los dispositivos administrados. 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 se incrementó el número de elementos en la cuarentena.
Acciones de Panda Systems Management	Envío de correo con el resultado de la monitorización al administrador. Generación de alerta automática.

Tabla 10.3: características del componente a desarrollar

Elementos necesarios

Para seguir el ejemplo completo, es necesaria una licencia trial o de pago de Panda Endpoint Protection o Panda Adaptive Defense / 360 y el agente de protección instalado en un dispositivo. Ya que los elementos introducidos en cuarentena por Panda Endpoint Protection / Panda Adaptive

Defense 360 son ficheros que almacena en un directorio, en este ejemplo puede probarse con cualquier otra carpeta del dispositivo a monitorizar.

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.

*El código fuente completo del componente se encuentra en el apartado "***Quarantine monitor***" en la página* **321**. *Será necesario copiar y pegar el código fuente más adelante.*

Protocolo de comunicación entre el componente y el servidor PCSM

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 script el que cree variables de entorno de forma manual para enviar respuestas al servidor, que las recogerá e incorporará a la consola.

En este caso se requerirán tres variables de entorno

Nombre Variable	Dirección	Objetivo
EP_PATH	**Lectura**	El script recupera del servidor PCSM 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 PCSM interpreta la monitorización como correcta. Si es 1 Panda Systems Management interpreta la monitorización como errónea.

Tabla 10.4: variables de entorno requeridas

La configuración de entrada 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 ha habido algún error en la ejecución del script:

- El código `0` indica que la ejecución se completó con éxito
  - La variable `Result` contendrá el número de ficheros nuevos detectados en el directorio. Si el número de ficheros es menor debido a un vaciado de la cuarentena o no ha variado, la variable `Result` contendrá el valor `0`.

- Si el número de ficheros en cuarentena es mayor, la variable `Result` contendrá la resta de los ficheros encontrados en el momento de la ejecución menos el número de la ejecución anterior.

- El código `1` indica que la ejecución no se completó. En este ejemplo se devuelve un código de error cuando el directorio de destino en el dispositivo del usuario no existe.

```
Set WshShell=WScript.CreateObject ("WScript.Shell")
Set objFSO=CreateObject ("Scrpting.FilesSystemObject")

'access to environment variable and quarantine path
On error resume Next
   Set WshSysenv=WshShell.Enviroment("PROCESS")
   Set objFolder=objFSO.GetFclder(WshSysEnv("EP_PATH"))

   if err.number<>0 then
      'PCSM didn't send the environment variable
     err.clear
     WScript.Echo"<-StartResult->"
     WScript.Echo"Result=PCOP_PATH variable not defined on PCSM console or path
not found"
     WScript.Echo"<-EndResult->"
     Set WshShell=nothing
     Set WsSysEnvy=nothing
     Set objFolder=nothing
     WScript.Quit(1)
   end if
On error goto 0
```

Para que el servidor interprete correctamente la salida estándar y pueda extraer el contenido de la variable `Result` del componente, es necesario adaptarse al siguiente formato:

```
Línea 1: <-Start Result->

Línea 2: Result=(datos a enviar)

Línea 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. La cadena de caracteres que quede a la derecha del "=" es el contenido que el servidor PCSM almacenará y procesará.

Resumen del diagnóstico

En aquellos monitores que requieran devolver varias líneas de información es necesario seguir el siguiente formato:

```
Línea 1: <-Start Diagnostic->

Línea 2: Información de diagnóstico 1
```

```
Línea 3: Información de diagnóstico 2

Línea 4: Información de diagnóstico 3

Línea 5: <-End Diagnostic->
```

La información relativa al diagnóstico de un monitor se visualiza en el detalle de la alerta, en el campo **Resumen del diagnóstico.** Consulta el apartado "**Visualizar el detalle de una alerta**" en la página **262**.

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 el panel lateral **Añadir Componente,** selecciona **Monitores** en la categoría del script y haz clic en el botón **Guardar**.
- Establece el nivel del componente. Este campo se utiliza para permitir o denegar el uso del componente a usuarios de la consola que no tengan establecido el nivel suficiente. Consulta el apartado "**Añadir una cuenta de usuario**" en la página **300**.
- Selecciona en la sección **Comandos** el lenguaje de scripting a utilizar, en este ejemplo VBScript.
- Introduce el código fuente del script en la caja de texto. Consulta el apartado "**Quarantine monitor**" en la página **321** para obtener el script completo de este ejemplo.
- 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.*

- Con el icono establece las **Variables de entrada** y **Variables de salida.**
  - En este ejemplo `EP_PATH` será una variable de entrada al script establecida por el administrador en la configuración del monitor, y contendrá la ruta donde se encuentra la carpeta de cuarentena de Panda Endpoint Protection. Elige el tipo de variable **Valor** ya que la variable contendrá una cadena de caracteres. Si la ruta de la cuarentena se encuentra en el mismo lugar para la mayoría de los equipos de usuario indícalo en el campo **Predeterminado**. Si deseas que se muestre una descripción para orientar al administrador sobre el tipo de dato que tiene que introducir en la creación del monitor indícalo en el campo **Descripción**.
  - `Result` será una variable de salida y contendrá el resultado del script.
- Haz clic en el botón **Guardar** para agregar el componente al repositorio. El nuevo componente se mostrará en el listado.

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

- En el caso del desarrollo de un monitor, es necesario crear una política de zona o política de

cuenta de tipo **Monitorización**.

- Añade como destino equipos Windows 7 y un monitor de tipo **Componente de monitorización**.
- En el desplegable selecciona el componente recién creado. Se mostrarán las variables de entrada configuradas en la creación del script, en este caso será `EP_Path`. Se mostrará la caja de texto asociada a la variable de entrada con el valor por defecto indicado en la creación del monitor (campo **Predeterminado**) y el icono si se indicó una descripción de la variable (campo **Descripción**). Pasa el ratón por encima del icono para mostrar el contenido de la descripción.

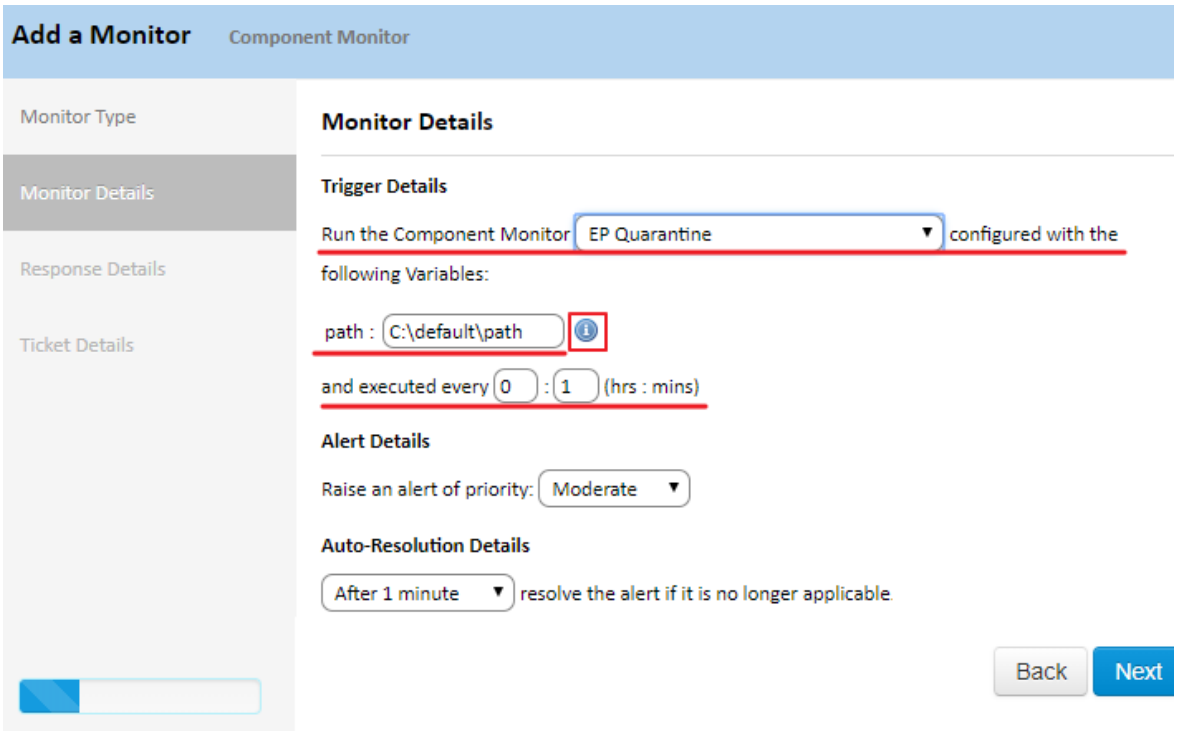


Figura 10.4: Configuración de ejemplo un monitor de tipo componente

- Indica cada cuanto tiempo se ejecutará el script (en este ejemplo cada 10 minutos), 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.
- 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.
- Haz clic en el botón **Desplegar cambios** para distribuir la política entre los dispositivos asignados y comenzar su ejecución.

3. Ejecución del componente

Una vez distribuido el monitor en los dispositivos, éste se ejecutará cada 10 minutos. Para ello, se invoca el intérprete de script asociado, se leen las variables de entorno necesarias y se escribe la respuesta adecuada.

En la línea 21 se lee la variable de entorno `EP_PATH` y se obtiene un objeto de tipo `FileSystemObject` que apunta a la carpeta de la cuarentena.

```
Set WshShell=WScript.CreateObject ("WScript.Shell")
Set objFSO=CreateObject ("Scrpting.FilesSystemObject")

'access to environment variable and quarantine path
On error resume Next
   Set WshSysenv=WshShell.Enviroment("PROCESS")
   Set objFolder=objFSO.GetFclder(WshSysEnv("EP_PATH"))

   if err.number<>0 then
      'PCSM didn't send the environment variable
     err.clear
     WScript.Echo"<-StartResult->"
     WScript.Echo"Result=PCOP_PATH variable not defined on PCSM console or path
not found"
     WScript.Echo"<-EndResult->"
     Set WshShell=nothing
     Set WsSysEnvy=nothing
     Set objFolder=nothing
     WScript.Quit(1)
   end if
On error goto 0
```

Las líneas 23 a 34 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 32).

Dado que el objetivo del monitor es comprobar si hay un incremento de ficheros en un directorio, y que cada ejecución calcula el número de ficheros una única vez, será necesario lanzar un mínimo de dos veces el script para poder comparar el número obtenido en dos momentos del tiempo distintos (cada 10 minutos según la configuración del monitor). Esto crea la necesidad de algún mecanismo de comunicación entre dos ejecuciones continuas del script, de manera que podamos recuperar el recuento de la ejecución inmediatamente anterior y compararlo con la actual. Dado que cada ejecución de un monitor es independiente del resto, el método idóneo para intercambiar datos entre ejecuciones es utilizar los recursos del propio dispositivo. Se recomienda utilizar el registro de Windows para este fin, aunque también pueden utilizarse ficheros temporales.

En la línea 42 se lee el recuento de ficheros almacenado en la ejecución anterior. Si no existe por ser la primera ejecución del componente se establece a 0 (línea 45). Posteriormente se almacena el recuento actual en el registro en la línea 49.

```
'access to registry for saving the count
On error resume Next
    'get previous file count
    iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor"))
   if Err.Number<>0 then
      'if error set to 0
       iCountPast=0
   end if
   iCountNow=colFiles.count
   'save the count
   WshShell.RegWrite "HKLM\Software\Panda Security\Monitor", iCountNow, "REG_SZ"
```

4. Envío de la información y procesamiento en la plataforma

Al terminar la ejecución del script, el servidor PCSM comprueba si el código de retorno es `0` o `1`. Si es `0` el script se da por correcto y el servidor PCSM 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. Si el código de retorno es `1` la ejecución se da por fallida.

```
if iCountPast < ICountNow then
  'there are more items in the folder, it sends data
  WScript.Echo "<-Start Result->"
  WScript.Echo "Result=" & ICountNow - iCountPast & "new items in PCOP quarantine"
  WScript.Echo "<-End Result->"
  Wscript.Quit (1)
else
  WScript.Quit (0)
```

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.

Definición de variables globales

- Haz clic en el menú general **Ajustes**, menú de pestañas **Configuración de cuenta** o menú general **Zona**, menú de pestañas **Configuración** dependiendo del nivel donde se crearán las variables. Las

variables creadas en el Nivel zona sobrescriben a las variables creadas en el Nivel cuenta si tienen el mismo nombre.

- En la sección **Nombre** de la variable haz clic en el link **Añadir variable**.
- Haz clic en la casilla **Enmascarar mis datos de entrada** si la información a almacenar es sensible, como usuarios y contraseñas.

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.

Etiquetas y campos personalizados

Al margen de generar alertas y correos al administrador cuando los parámetros de un monitor quedan fuera de la configuración establecida, es posible actualizar los **Campos personalizados** de forma automática.

*Consulta el apartado "**Campos personalizados**" en la página **190** para obtener información de cómo acceder a la funcionalidad de Campos personalizados y cuáles pueden ser sus usos.*

La actualización de los **Campos personalizados** de forma automática desde un monitor permite reflejar en la consola el estado de uno o varios parámetros no soportados directamente por el agente PCSM.

Escribir información de Campos personalizados en dispositivos Windows

El contenido de los campos personalizados se toma de las rama del registro `HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\CustomX` de cada dispositivo, siendo X un número del 1 al 30. Cada una de las ramas indicadas puede contener una cadena de caracteres de hasta 65534 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.

Si el lenguaje de script utilizado para desarrollar el componente de tipo monitor no tiene acceso a la API de escritura en el registro utiliza la siguiente línea de comandos para añadir valores:

REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage /v CustomField /t REG_SZ /d "Value" /f

donde:

***CustomField** es el nombre del campo (Custom1, Custom2, Custom3, etc.)*

***Value**: es el contenido del campo*

Acceso al contenido de los campos personalizados

Dentro del script, Panda Systems Management asigna de forma automática el contenido definido en los campos personalizados a las variables UDF_X, siendo X el número del campo.

Escribir información de Campos personalizados en dispositivos Linux y macOS

La información de los **Campos personalizados** en sistemas Linux y macOS se encuentra en un fichero llamado `values.xml` almacenado en las siguientes rutas.

- **En macOS**

```
/var/root/.mono/registry/LocalMachine/software/Centrastage/values.xml
```

o

```
/var/root/.mono/registry/CurrentUser/software/Centrastage/values.xml
```

- **En linux**

```
/root/.mono/registry/LocalMachine/software/Centrastage/values.xml
```

o

```
/root/.mono/registry/CurrentUser/software/Centrastage/values.xml
```

El formato del fichero `values.xml` es el siguiente:

```
<values>

<value name="DeviceID" type="string">YourDeviceID</value>

<value name="Custom1" type="string">CustomValue</value>
```

```
</values>
```

donde:

- **YourDeviceID**: es el identificador interno del dispositivo. Se corresponde con el campo ID que se encuentra en el menú de pestañas **Auditoría**, control de selección hardware, sección **Datos del dispositivo**.
- **CustomValue**: valor del campo **Custom** indicado en el atributo de la rama `Value` (en el ejemplo Custom1)

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.
- 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.

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 informático a administrar:

- En el menú general **Componentes**, haz clic en el icono  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.

Parte 4

Visibilidad de dispositivos

Capítulo 11: Auditoria de activos

Capítulo 12: Visibilidad y estado de los de dispositivos

Capítulo 13: Informes

Capítulo 11

Auditoria de activos

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.

CONTENIDO DEL CAPÍTULO

Acceso y disponibilidad del servicio de auditoria

La pestaña **Auditoria** está disponible en los tres niveles soportados (Cuenta, Zona y Dispositivo) mostrando información con un nivel de detalle variable desde lo más genérico hasta lo más preciso, 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**, en la zona apropiada y en el menú de pestañas **Auditoría**.
- Para acceder a las funcionalidades de auditoría en el Nivel dispositivo haz clic en el menú general **Zonas**, en la zona donde reside el dispositivo, en el dispositivo y 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 , en la barra de iconos.*

La información suministrada se agrupa en varias secciones dependiendo del Nivel y accesibles desde la parte superior derecha de la ventana **Auditoria**, haciendo clic en el control de selección apropiado **(1)**:

- **Red:** la auditoria de red es el proceso por el cual Panda Systems Management descubre dispositivos en la red y es ejecutada por los equipos que tienen el rol Nodo de red asignado.
- **Hardware**: inventario hardware instalado en los dispositivos.
- **Software**: inventario software instalado en los dispositivos.
- **Licencias**: información de las licencias de software consumidas.
- **Servicios**: servicios instalados en los equipos Windows y su estado de ejecución.
- **Registro de cambios:** registro de cambios de software, hardware y del sistema. El registro de la actividad se considera una funcionalidad de seguridad y se trata en el capítulo "**Registro de actividad" en la página 311**.

- **Actividad**: registra las tareas ejecutadas en el dispositivo, sea cual sea su origen.

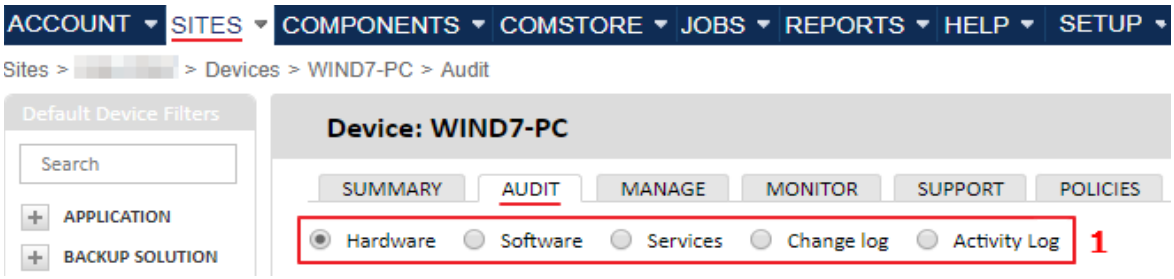


Figura 11.1: pantalla de auditoría

Disponibilidad de la información según el nivel seleccionado

Según el Nivel seleccionado (cuenta, zona o dispositivo) se acceden a diferentes tipos de información. A continuación se muestra una tabla con los tipos de información disponibles según el nivel seleccionado.

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

Tabla 11.1: funcionalidad de auditoria según el nivel seleccionado

Auditorias completas y deltas

Panda Systems Management soporta varios tipos de auditoria según el volumen y el momento en que se ejecutan:

- **Automáticas**: se ejecuta una auditoria automática en el momento de instalación del agente PCSM en el dispositivo y cada cierto tiempo. Consulta el apartado "**Frecuencia de ejecución de las auditorias**".

- **Manuales**: cada vez que se hace clic en el icono de la barra de iconos el agente PCSM ejecuta una auditoria manual.

- **Completas**: son auditorias que contienen toda la información de inventariado del dispositivo.

- **Parciales**: son auditorias diferenciales (deltas), que contienen únicamente los últimos cambios

producidos en el dispositivo.

> *Las auditorías parciales no están disponibles en dispositivos móviles (teléfonos y tablets)*

Frecuencia de ejecución de las auditorias

Tipo de dispositivo	Auditoria completa	Auditorias delta
Compatible con el agente PCSM	• Después de la instalación del agente PCSM. • Al hacer clic en el icono de la barra de iconos si solo se ha seleccionado un dispositivo.	• Cada 24 horas. • Cada vez que se completa con éxito una tarea. • Tras terminar completamente la instalación de todos los parches programados, incluyendo el reinicio si lo hubiera. • Al hacer clic en el icono de la barra de iconos si se han seleccionado varios dispositivos.
Dispositivos de red	• Cuando un dispositivo de red es asignado a un equipo con el rol Nodo de red. • Cuando se cambia el tipo del dispositivo. • Al hacer clic en el icono de la barra de iconos. • Cada 24 horas.	No aplica

Tabla 11.2: frecuencia de ejecución de los procesos de auditoria

Auditoria de red

Nivel cuenta

Muestra un recuento de los dispositivos descubiertos en toda la cuenta agrupados por su tipo. Los campos del listado se describen a continuación:

Campo	Descripción
Nombre	Nombre de la zona. Solo se muestran aquellas zonas que contienen dispositivos descubiertos y no integrados en Panda Systems Management.

Tabla 11.3: auditoría de red en el Nivel cuenta

Campo	Descripción
Descripción	Descripción de la zona.
Windows	Número de dispositivos descubiertos e identificados como Windows.
Mac	Número de dispositivos descubiertos e identificados como macOS.
Red	Número de dispositivos descubiertos e identificados como dispositivos de red.
Impresora	Número de dispositivos descubiertos e identificados como impresoras.
ESXi	Número de dispositivos descubiertos e identificados como servidores ESXi.
Desconocido	Número de dispositivos descubiertos sin identificar.

Tabla 11.3: auditoría de red en el Nivel cuenta

Nivel zona

La auditoría del Nivel zona muestra todos los dispositivos descubiertos dentro de la zona, con la posibilidad de iniciar una instalación remota del agente PCSM.

> *Consulta el apartado "**Búsqueda de dispositivos (escaneo de red)**" en la página **66** para obtener información sobre el procedimiento de descubrimiento e integración remota de dispositivos en Panda Systems Management.*

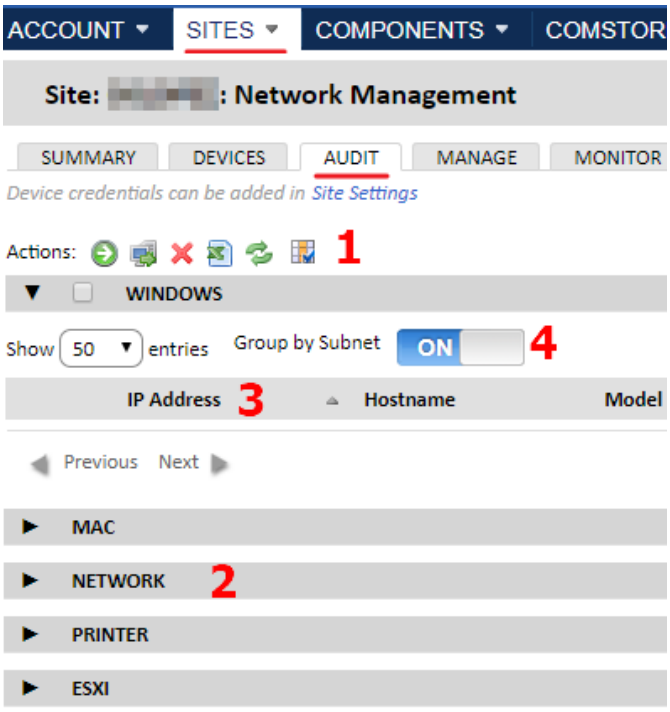


Figura 11.2: auditoría de red en el Nivel zona

La pantalla de auditoría de red se divide en varias secciones:

- **Barra de iconos (1)**: permite operar sobre los dispositivos encontrados.
- **Grupos de dispositivos (2)**: los dispositivos se muestran agrupados en función de las funcionalidades que Panda Systems Management soporta para el tipo de dispositivo. Si la agrupación no está vacía se indica el número total de dispositivos descubiertos de ese tipo. Una vez desplegada la agrupación se mostrará una casilla de selección para poder elegir a todos los dispositivos del grupo a la vez.
- **Campos del listado (3)**: muestran información del dispositivo. Para añadir o eliminar columnas haz clic en el icono .
- **Agrupar por subred (4)**: en el caso de que haya dispositivos que pertenezcan a distintas subredes, permite agruparlos mediante la subred a la que pertenecen para facilitar la lectura del listado.

Los campos incluidos por defecto que describen a los dispositivos encontrados son:

Campo	Descripción
Tipo de dispositivo	Icono que indica el tipo de dispositivo encontrado.
Dirección IP	Dirección IP de la interface de red del dispositivo.
Nombre de host de dispositivo	Nombre del dispositivo.
Descripción	Descripción del dispositivo establecida en el Nivel dispositivo, menú de pestañas **Resumen**.
Proveedor de NIC	Fabricante de la tarjeta de red.
Modelo	Modelo del dispositivo.
SNMP V1/V2 público	Indica si las credenciales del dispositivo con v1/v2c y si la comunidad es "public".

Tabla 11.4: listado de dispositivos en una auditoría de red del Nivel zona

La barra de iconos permite las acciones siguientes:

Acción	Descripción
Administrar dispositivos	Despliega e instala el agente PCSM en el dispositivo si éste es compatible, o integra el dispositivo de red en la plataforma. Consulta el apartado "**Procedimiento de distribución remota del agente PCSM**" en la página **50**.
Mover dispositivos	Mueve los dispositivos seleccionados a otra agrupación en caso de que Panda Systems Management no haya detectado correctamente su tipo.
Eliminar dispositivos	Retira el dispositivo de la lista de descubiertos. El dispositivo volverá a mostrarse en la siguiente auditoría de red.

Tabla 11.5: listado de dispositivos en una auditoría de red del Nivel zona

Auditoria de hardware

Nivel cuenta

Muestra el modelo de los dispositivos gestionados en toda la cuenta. El modelo 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 el modelo.

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

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 mantenida 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  de la barra de iconos para introducir la información relevante del equipo no administrado.

Nivel dispositivo

Las auditorias del Nivel dispositivo son las más precisas, mostrando toda información relevante del dispositivo elegido. Algunos tipos de dispositivos tienen campos editables señalados desde la pestaña de **Resumen**.

Dependiendo del tipo de dispositivo, el contenido de la pestaña **Auditoría** cambia, mostrando la información indicada en las tablas presentadas a continuación:

General

Campo	Descripción	Disponible en
Nombre del host	Nombre del dispositivo.	Todos
Descripción	Cadena de caracteres que identifica al dispositivo.	Todos
Sistema operativo	Sistema operativo instalado en el dispositivo y versión interna.	Todos
Service Pack		Equipos de sobremesa, portátiles y servidores.
Arquitectura	Arquitectura hardware del dispositivo (32 bits o 64 bits).	Equipos de sobremesa, portátiles y servidores.
Versión Hyper-V	Versión del motor de virtualización Hyper-V.	Servidores Hyper-V

Tabla 11.6: información general del dispositivo

Campo	Descripción	Disponible en
Versión de .NET	Versión del framework .NET instalado.	Equipos de sobremesa, portátiles y servidores.
Dominio	Dominio Windows al que pertenece el equipo.	Equipos de sobremesa, portátiles y servidores.
Último reinicio	Fecha en la que el equipo se reinició por última vez.	Equipos de sobremesa, portátiles y servidores.
IMEI	Código de identificación del terminal móvil.	Dispositivo móvil

Tabla 11.6: información general del dispositivo

Almacenamiento

Campo	Descripción	Disponible en
Unidad de disco	Punto de montaje de la unidad.	Equipos de sobremesa, portátiles y servidores.
Tipo de unidad	Tipo de medio de almacenamiento (interno, extraíble, óptico...)	Equipos de sobremesa, portátiles y servidores.
Tamaño	Tamaño de la unidad de almacenamiento.	Equipos de sobremesa, portátiles y servidores.
Libre	Espacio libre de la unidad de almacenamiento.	Equipos de sobremesa, portátiles y servidores.
Descripción		Equipos de sobremesa, portátiles y servidores.
Almacén de datos	Nombre del almacén de datos conectado al servidor ESXi.	Servidores ESXi
Almacenamiento	Cadena de caracteres que identifica al hardware del almacén de datos.	Servidores ESXi
Sistema de ficheros	Sistema de ficheros utilizado por el servidor ESXi en el almacén de datos.	Servidores ESXi
Capacidad	Espacio total del almacén de datos.	Servidores ESXi
Libre	Espacio libre del almacén de datos.	Servidores ESXi
Suscripción	Porcentaje máximo de ocupación potencial de las máquinas virtuales que residen en el almacén de datos. Al hacer clic se muestran las unidades lógicas creadas con el porcentaje de ocupación individual asignado.	Servidores ESXi
Estado	Estado del sistema de almacenamiento (Ok, No Ok).	Servidores ESXi

Tabla 11.7: información del sistema de almacenamiento

Datos del dispositivo

Campo	Descripción	Disponible en
Versión del agente	Versión interna del agente PCSM.	Equipos de sobremesa, portátiles y servidores.
ID	Identificador interno del dispositivo.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Visto por última vez	Última vez que el agente PCSM contactó con el servidor PCSM.	Todos
Fecha de creación	Fecha en la que el Nivel dispositivo fue creado para el dispositivo en particular.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Fecha de creación	Fecha en la que el dispositivo móvil se integró en la plataforma PCSM.	Dispositivos móviles
Fecha de la última auditoría	Fecha en la que se ejecutó la última auditoría completa en el dispositivo.	Todos

Tabla 11.8: datos del agente PCSM instalado en el dispositivo

Hardware

Campo	Descripción	Disponible en
Fabricante	Nombre del fabricante del equipo o del sistema operativo si es un dispositivo virtual.	Todos
Modelo	Modelo del equipo o cadena "Virtual machine".	Todos
Número de serie	Número de serie del equipo asignado de forma manual.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Placa madre	Modelo de la placa madre del dispositivo.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Procesador	Marca y modelo del microprocesador instalado.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Núcleos físicos	Número de núcleos instalados en el microprocesador.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Memoria	Cantidad de memoria instalada en el dispositivo.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.

Tabla 11.9: información del hardware instalado en el dispositivo

Campo	Descripción	Disponible en
Adaptador de pantalla	Fabricante y modelo de la tarjeta de vídeo instalada.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Monitores	Marca y modelo del monitor conectado al dispositivo.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Nombre de BIOS	Fabricante de la BIOS del dispositivo.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Versión de BIOS	Versión de la BIOS del equipo.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Fecha de lanzamiento de BIOS	Fecha de publicación de la BIOS. Este valor se utiliza en los informes para determinar la obsolescencia del dispositivo.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Potencia nominal		Equipos de sobremesa, portátiles y servidores, servidores ESXi.
ICCID	Identificador de la tarjeta SIM.	Dispositivo móvil
Operador	Compañía que suministra el servicio de telefonía.	Dispositivo móvil
Número	Número de teléfono móvil.	Dispositivo móvil

Tabla 11.9: información del hardware instalado en el dispositivo

Adaptadores de red

Campo	Descripción	Disponible en
Adaptador	Nombre de la tarjeta de red instalada.	Todos
Dirección MAC	Dirección física de la tarjeta de red.	Todos
Velocidad	Megabits por segundo y modo dúplex negociado por la tarjeta de red.	Servidores ESXi y dispositivos móviles.

Tabla 11.10: información de las tarjetas de red

Procesadores

Campo	Descripción	Disponible en
Nombre	Marca y modelo del procesador físico instalado.	Servidores ESXi
Velocidad	Megahercios de los microprocesadores instalados.	Servidores ESXi
Núcleos totales	Número de núcleos físicos disponibles en el servidor ESXi	Servidores ESXi

Tabla 11.11: información del microprocesador del dispositivo

Información del invitado

Campo	Descripción	Disponible en
Nombre del host	Nombre del servidor ESXi que aloja al sistema virtualizado.	Servidor ESXi
Nombre del invitado	Nombre del dispositivo virtualizado.	Servidor ESXi
Sistema operativo	Sistema operativo instalado en el equipo virtualizado.	Servidor ESXi
Almacén de datos	Almacén de datos asignado al equipo virtualizado.	Servidor ESXi
CPU	CPU virtual asignada al equipo virtualizado.	Servidor ESXi
RAM	Tamaño de la memoria RAM asignada al equipo virtualizado.	Servidor ESXi
Imágenes	Numero de snapshots (puntos de restauración) tomados de la máquina virtual.	Servidor ESXi

Tabla 11.12: información de las máquinas virtualizadas

Información de IP

Campo	Descripción	Disponible en
Dirección IP	Dirección IP asignada al adaptador de red.	Equipos de sobremesa, portátiles y servidores, servidores ESXi
Ext. de dirección IP	Dirección IP con la que el dispositivo accede a los recursos situados en el exterior de su red interna.	Equipos de sobremesa, portátiles y servidores, servidores ESXi
IP(s) adicionales	Alias de red.	Equipos de sobremesa, portátiles y servidores.

Tabla 11.13: información de conexión TCP/IP

Memoria

Campo	Descripción	Disponible en
Módulo	Identificador del chip de memoria formado por el banco al que está conectado y tecnología de implementación de la memoria.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Tipo	Tecnología de implementación de la memoria.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.

Tabla 11.14: información sobre la memoria instalada en el dispositivo

Campo	Descripción	Disponible en
Número de pieza	"Part number" del chip de memoria.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Número de serie	Número de serie del chip de memoria.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Capacidad	Tamaño del chip de memoria.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.
Velocidad	Frecuencia interna de funcionamiento del chip de memoria.	Equipos de sobremesa, portátiles y servidores, servidores ESXi.

Tabla 11.14: información sobre la memoria instalada en el dispositivo

Dispositivos conectados

Campo	Descripción	Disponible en
Tipo	Tipo del dispositivo externo conectado al equipo.	Equipos de sobremesa, portátiles y servidores.
Nombre	Nombre del volumen del dispositivo conectado.	Equipos de sobremesa, portátiles y servidores.
Nombre del controlador	Nombre interno del controlador.	Equipos de sobremesa, portátiles y servidores.
Fabricante del controlador	Empresa que desarrolló el controlador.	Equipos de sobremesa, portátiles y servidores.
Versión del controlador	Versión interna del controlador.	Equipos de sobremesa, portátiles y servidores.
Archivo del controlador	Nombre del archivo que contiene el controlador.	Equipos de sobremesa, portátiles y servidores.
Última modificación del archivo del controlador	Fecha de la última actualización del controlador.	Equipos de sobremesa, portátiles y servidores.
Nombre del puerto	Nombre del puerto físico al que se conecta el dispositivo.	Equipos de sobremesa, portátiles y servidores.

Tabla 11.15: información de los controladores que gestionan los dispositivos de almacenamiento externo

Auditoría de software

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.

Nivel zona

Los programas mostrados 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.

Nivel dispositivo

Los programas mostrados 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.

Auditoría de licencias

Nivel cuenta

El objetivo de la auditoría de licencias es determinar el número de instalaciones producidas de cada programa, con el objetivo de 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 está compuesto 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 administradas 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.

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.*

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.

Auditoría de servicios

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 que se muestra en la lista de servicios instalados en el equipo.
- **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**).

Auditoría de cambios

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.

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.

Auditoría de actividad

Nivel cuenta

Muestra los dispositivos que se movieron entre zonas:

Campo	Descripción
Tipo	Movimiento de dispositivo entre zonas.
Dispositivo	Nombre del dispositivo movido.
Nombre	Descripción de la operación indicando la zona origen, la zona destino y el usuario de la consola de administración que lo efectuó.
Iniciado	Fecha en la que se ha producido la operación.

Tabla 11.16: significado de los campos que describen el movimiento de dispositivos entre zonas

Nivel dispositivo

Muestra toda la actividad asociada con un dispositivo concreto sin importar su origen:

Campo	Descripción
Tipo	Tipo de actividad registrada representado por su icono.
Nombre	Nombre de la actividad.
Iniciado	Fecha en la que inició la actividad.
Finalizado	Fecha en la que finalizó la actividad.
Política	Si la actividad está vinculada a la activación de una política muestra el nombre de ésta.
Estado	Estado de la actividad (**En ejecución**, **Completado**, **Error** etc.).
Resultados	Código de resultado devuelto por la actividad. En algunos casos se muestra un icono que permite ampliar la información.
Progreso	Barra de color verde, rojo o naranja con el resultado de la ejecución de la actividad (**Correcto**, **Error**, **Precaución** respectivamente).
Stdout	Copia de la salida estándar de la actividad.
Stderr	Copia de la salida de error de la actividad.

Tabla 11.17: significado de los campos que describen las actividades registradas en los dispositivos

Capítulo 12

Visibilidad y estado de los de dispositivos

Panda Systems Management ofrece varios recursos para visualizar el estado de los dispositivos. Dependiendo de la herramienta elegida, la información se muestra de forma resumida y consolidada para las agrupaciones de dispositivos soportadas (grupo, filtro, zona y cuenta) o de forma detallada e individual para cada dispositivo integrado en la plataforma.

CONTENIDO DEL CAPÍTULO

Acceso al estado de los dispositivos

Las herramientas disponibles para visualizar el estado de los dispositivos se muestran a continuación:

- **Panel de control general**: accesibles en el Nivel cuenta y Nivel zona.
- **Paneles de control de zona**: accesible desde la barra de pestañas **Resumen** dentro de una zona.
- **Listados de dispositivos y zonas**: accesibles desde el Nivel cuenta.
- **Detalle de dispositivo**: accesible desde la pestaña **Detalle** dentro de un dispositivo.

Panel de control general

Objetivo

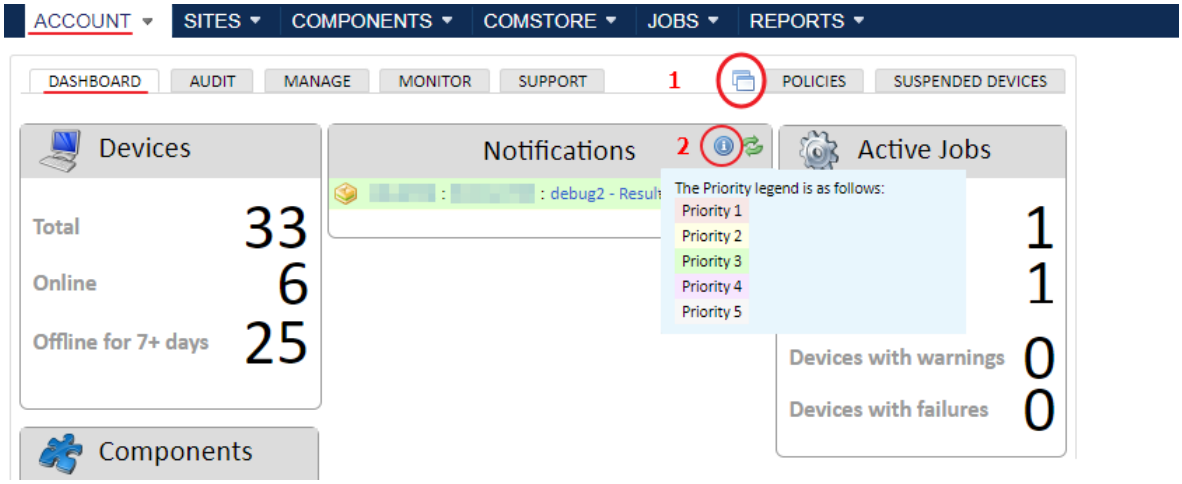


Figura 12.1: acceso al modo kiosco del panel de control general

Muestra un resumen de todos los dispositivos integrados en la plataforma Panda Systems Management para poder valorar de un solo vistazo el estado del parque informático de la empresa.

Para mostrar el panel de control en modo kiosco / pantalla completa haz clic en el icono **(1)**.

Acceso

En el menú general **Cuenta** haz clic en la barra de pestañas **Panel de control**.

Información mostrada

La información se estructura en los bloques siguientes:

- **Dispositivos**: muestra un recuento de los dispositivos integrados en la plataforma agrupado por su estado de conexión.
- **Componentes**: muestra un recuento de los componentes integrados en la cuenta y en la ComStore.
- **Tareas activas**: muestra un recuento de las tareas creadas agrupadas por su estado.
- **Alertas abiertas**: muestra un recuento de las alertas generadas agrupadas por su prioridad.
- **Notificaciones**: muestra las alertas generadas por los dispositivos de la cuenta.

Dispositivos

Campo	Descripción
Total	Número total de dispositivos integrados en Panda Systems Management.
Online	Número total de dispositivos conectados en este momento.
Offline durante más de 7 días	Número total de dispositivos que no han conectado con el servidor Panda Systems Management en más de una semana.

Tabla 12.1: recuento de los dispositivos integrados en Panda Systems Management

Componentes

Campo	Descripción
Total	Número de componentes añadidos al repositorio de la cuenta y accesibles en el menú general **Componentes**.
ComStore	Número de componentes publicados por Panda Security en la ComStore.
Actualizaciones	Número de componentes que tienen actualizaciones publicadas pendientes de aplicar en el repositorio de la cuenta.

Tabla 12.2: recuento de los componentes integrados en la cuenta

Notificaciones

Campo	Descripción
Icono	Tipo de notificación.
Zona	Zona a la que pertenece el dispositivo que generó la alerta.
Nombre del dispositivo	Nombre del dispositivo que generó la alerta.
Información de la alerta	Resumen de la alerta.
Marca de tiempo	Intervalo de tiempo desde que se generó la alerta hasta el presente.
Color	Cada notificación tiene un color de fondo según su prioridad. Para obtener una leyenda de los colores y prioridades pasa el puntero del ratón por encima del icono situado en el encabezado de la tabla notificaciones. **(2)** (Figura 12.1)

Tabla 12.3: listado de notificaciones de la cuenta

Tareas activas

Campo	Descripción
Dispositivos programados	Número de dispositivos que tienen una tarea programada asignada. Si un dispositivo tiene varias tareas solo se cuenta una vez.
Dispositivos en ejecución	Número de dispositivos que tienen una tarea programada en ejecución.
Dispositivos con avisos	Número de dispositivos que han enviado una cadena de post-condición anunciando un aviso.
Dispositivos con fallos	Número de dispositivos que han devuelto un error al ejecutar una tarea.

Tabla 12.4: información de los avisos generados por las tareas

Alertas abiertas

Contiene el número de dispositivos con alertas pendientes, agrupadas por su importancia.

Paneles de control de zona

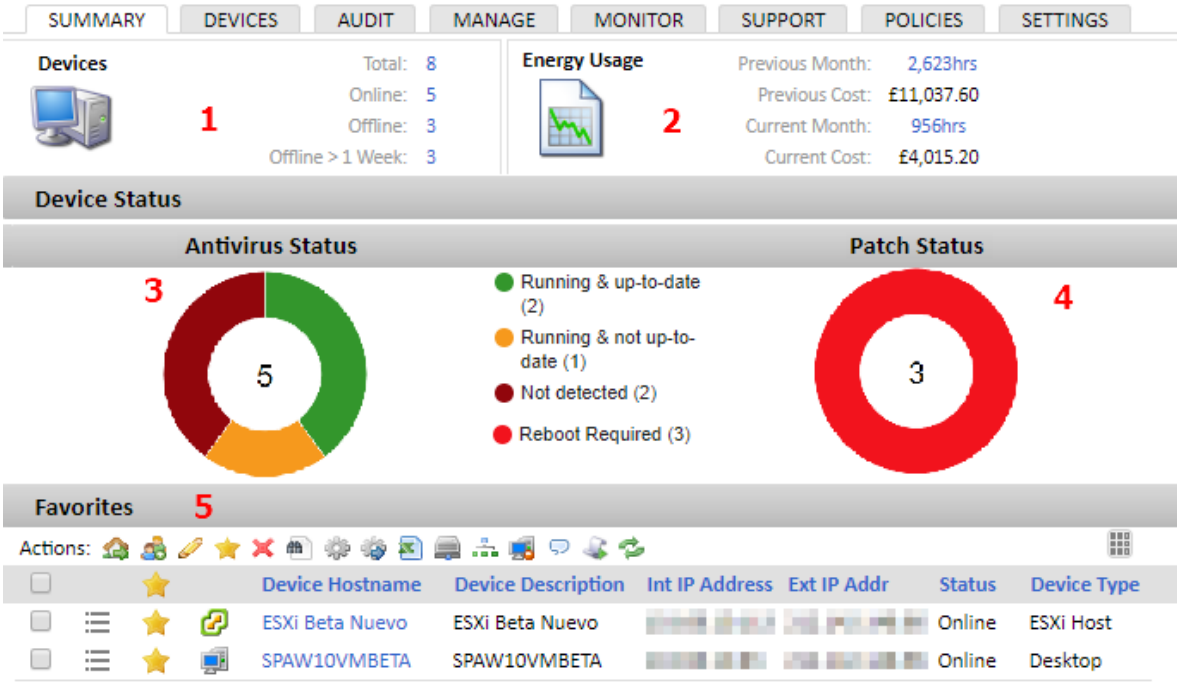


Figura 12.2: Panel de control de zona

Objetivo

Muestra información estadística y de estado de los dispositivos que forman parte de la zona elegida. En el panel de control de zona se indican los consumos de energía de los dispositivos, así como el estado del antivirus y el nivel de parcheo de los equipos.

Utiliza el panel de control de zona para acceder de forma rápida a aquellos equipos marcados como **Favoritos**, que requieren una atención especial, y a la herramienta de **Notas**, que permite intercambiar mensajes entre los distintos administradores o establecer recordatorios.

Acceso

Desde el menú general **Zonas**, selecciona la zona y haz clic en el menú de pestañas **Resumen**.

Información mostrada

Cada bloque de información mostrara está referido a la figura 12.2 de la página 179.

Dispositivos (1)

Campo	Descripción
Total	Número total de dispositivos integrados en la zona.
Offline	Número total de dispositivos integrados en la zona que no están conectados al servidor PCSM en este momento.
Online	Número total de dispositivos integrados en la zona que están conectados al servidor PCSM en este momento.
Offline más de una semana	Número total de dispositivos integrados en la zona que no se han conectado al servidor PCSM desde hace una semana.

Tabla 12.5: recuento resumen de los dispositivos integrados en Panda Systems Management y su estado

Uso de energía (2)

Campo	Descripción
Mes anterior	Suma del número total de horas que los dispositivos de la zona han estado encendidos el mes pasado.
Coste anterior	Coste derivado del número de horas que los dispositivos de la zona han estado encendidos el mes pasado y precio por Kw/h especificado en libras.
Mes actual	Suma del número total de horas que los dispositivos de la zona han estado encendidos este mes.
Coste actual	Coste derivado del número de horas que los dispositivos de la zona han estado encendidos y el precio por Kw/h especificado en libras.

Tabla 12.6: coste de la energía consumida por los dispositivos de la zona

Estado del antivirus (3)

*Consulta el apartado "**Auditoría del antivirus instalado**" en la página **192** para configurar Panda Systems Management y recuperar correctamente la información del antivirus instalado en el dispositivo.*

Campo	Descripción
Gráfico de tarta	Distribución gráfica de todas las series representadas relativas a la presencia de antivirus en los dispositivos de la zona, su estado y el estado del fichero de firmas.
Ejecutándose y actualizado	Número de dispositivos en la zona que tienen un antivirus instalado, en ejecución y con el fichero de firmas actualizado.
Ejecutándose y no actualizado	Número de dispositivos en la zona que tienen un antivirus instalado, en ejecución pero con un fichero de firmas de más de tres días de antigüedad.

Tabla 12.7: información del antivirus

Campo	Descripción
No ejecutándose	Número de dispositivos en la zona que tienen un antivirus instalado pero sin ejecutar.
No detectado	Número de dispositivos en la zona que no tienen un antivirus instalado o no es compatible. Consulta el apartado "**Auditoría del antivirus instalado**".

Tabla 12.7: información del antivirus

Estado de parcheo (4)

Campo	Descripción
Gráfico de tarta	Distribución gráfica de todas las series representadas relativas al parcheo de los sistemas operativos de los dispositivos de la zona.
Sin política	Número de equipos en la zona que no tienen asignada una política de parcheo.
Sin información	Número de equipos en la zona que no han enviado al servidor Panda Systems Management información de parcheo.
Necesita reinicio	Número de equipos en la zona que requieren un reinicio para completar la tarea de parcheo.
Error de instalación	Número de equipos en la zona que tienen uno o más errores en la última operación de parcheo realizada.
Aprobación pendiente	Número de equipos en la zona que tienen parches publicados pendientes de aprobar.
Actualizado	Número de equipos en la zona actualizados.

Tabla 12.8: estado del parcheo

Favoritos (5)

Mediante la zona de **Favoritos** los equipos especialmente problemáticos o en observación pueden ser accedidos de forma más rápida que navegando por el menú general. Consulta el apartado "**Favoritos**" en la página **90** para marcar un equipo como favorito.

La zona **Favoritos** incluye una barra de iconos completa para poder operar sobre los dispositivos seleccionados así como del selector de columnas mostrado en el apartado "**Listados de dispositivos**".

Notas

Introduce recordatorios o mensajes destinados a otros administradores en la sección **Notas** del panel de control de zona.

Listado de zonas

Objetivo

Muestra la distribución por zonas de los dispositivos integrados en Panda Systems Management e información básica de la configuración de cada zona.

Acceso

Haz clic en el menú general **Zonas**.

Información mostrada

Campo	Descripción
Nombre	Nombre de la zona.
Descripción	Descripción de la zona.
ID	Identificador interno utilizado por Panda Systems Management.
Dispositivos	Número de dispositivos integrados en la zona.
Offline	Número de dispositivos integrados en la zona que no está conectado.
Proxy	Configuración de acceso a Internet a través de proxy asignada a la zona.

Tabla 12.9: información de las zonas creadas en la cuenta

Listados de dispositivos

Objetivo

Muestra los datos más relevantes de los dispositivos que pertenecen a una agrupación concreta y permite efectuar acciones sobre los mismos.

Acceso

Dependiendo del ámbito de la agrupación sigue los pasos mostrados a continuación:

- Para acceder al listado de dispositivos de una agrupación creada en el Nivel cuenta haz clic en el menú general **Zonas** y en la agrupación seleccionada del panel lateral de agrupaciones.
- Para acceder al listado de dispositivos de una agrupación creada en el Nivel zona haz clic en el menú general **Zonas**, después en la zona seleccionada y finalmente en la agrupación seleccionada del panel lateral de agrupaciones.
- Para acceder al listado de dispositivos de una zona haz clic en el menú general **Zonas**, en la zona seleccionada y en el menú de pestañas **Dispositivos**.

Información mostrada

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
Casilla de selección	Selecciona los dispositivos que recibirán las acciones de la barra de iconos.
Accesos directos	Desplegable con el menú de pestañas del dispositivo y el menú de acciones.
Favorito	Marca el dispositivo como favorito para su acceso directo. Consulta "**Acceder a los dispositivos Favoritos**" en la página **90**.
Estado del dispositivo	Icono representativo del rol y del estado de conexión del dispositivo.
ID	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.
IPs adición.	Alias de IP.
Dirección IP ext.	Dirección IP del router o dispositivo que conecta a Internet al dispositivo.
Último usuario	Último usuario que se conectó al dispositivo.
Grupo	Grupos de dispositivos de zona a los que pertenece el dispositivo.
Fecha de creación	Fecha de alta del dispositivo en el sistema.
Última actualización	Fecha de la última vez que el servidor accedió al dispositivo.
Última auditoría	Fecha de la última vez que se realizó una auditoria de software y hardware. Para más información, consulta capítulo "**Auditoria de activos**" en la página **159**.
Nombre de la sesión	Sin uso actualmente.
Favorito	Marca el dispositivo como favorito para un acceso rápido en los dashboards del sistema.
Modo privacidad	Modo de privacidad del dispositivo.

Tabla 12.10: atributos de los dispositivos

Campo	Descripción
Versión del agente	Número de versión del agente PCSM.
Puerto web ok	• **True**: El agente se conecta correctamente con el servidor y puede enviar y recibir datos. • **False**: El agente no se ha podido conectar con el servidor.
Nodo de red	El agente tiene el rol Nodo de red activado.
Estado	Estado (**Online**, **Offline**). El estado **Online** indica que el agente PCSM 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	
Placa madre	Marca y modelo de la placa madre del dispositivo.
CPU	Marca, modelo y velocidad de la CPU.
Núcleos físicos	Número de núcleos del microprocesador.
Memoria	Cantidad de memoria instalada.
Direcciones MAC	Dirección física de la tarjeta de red.
Personalizar el campo 1-30	Contenido de los campos personalizados definidos. Para más información consulta el apartado "**Campos personalizados**" para establecer su contenido de forma manual y el apartado "**Etiquetas y campos personalizados**" en la página **153** desde un script.
Tipo de dispositivo	Tipo del dispositivo (**Estación de trabajo**, **Portátil**, **Tablet**, **Teléfono móvil**, **Impresora**, **Dispositivo de red**, **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.
Tiempo Online (horas)	Tiempo que el agente PCSM ha permanecido conectado con el servidor Panda Systems Management.
Coste	Coste asociado al dispositivo según su consumo.
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	Fecha en la que se publicó la BIOS del dispositivo. Esta fecha se toma como base para calcular la obsolescencia de los equipos en los informes. Consulta el apartado "**Hardware Lifecycle**".
Versión de BIOS	

Tabla 12.10: atributos de los dispositivos

Campo	Descripción
Último reinicio	Fecha del último reinicio del dispositivo.
Necesita reinicio	Indica si el equipo requiere un reinicio para completar el proceso de instalación
Versión de .NET	Versión del framework .NET instalado en el equipo.
Parches aprobados pendientes	Número de parches publicados pendientes de aprobación.
Parches no aprobados	Número de parches publicados y no aprobados.
Parches instalados	Número de parches instalados.
Estado del parcheo	Estado de la actualización del equipo.
Asignación de nodos	Nombre del equipo Nodo de red asignado al dispositivo.
Descripción SNMP	Campo Descripción de la configuración SNMP del dispositivo.
Ubicación SNMP	Campo Ubicación de la configuración SNMP del dispositivo.
Fabricante NIC	Nombre del fabricante de la tarjeta de red.
Fabricante	Nombre del fabricante del dispositivo.
Producto antivirus	Nombre del antivirus.
Estado del Antivirus	Estado del antivirus: Ejecutándose y actualizado, Ejecutándose y no actualizado, No ejecutándose, No detectado.
Fecha de caducidad de la garantía	Fecha en la que expira la garantía.

Tabla 12.10: atributos de los dispositivos

Herramientas de búsqueda y filtrado

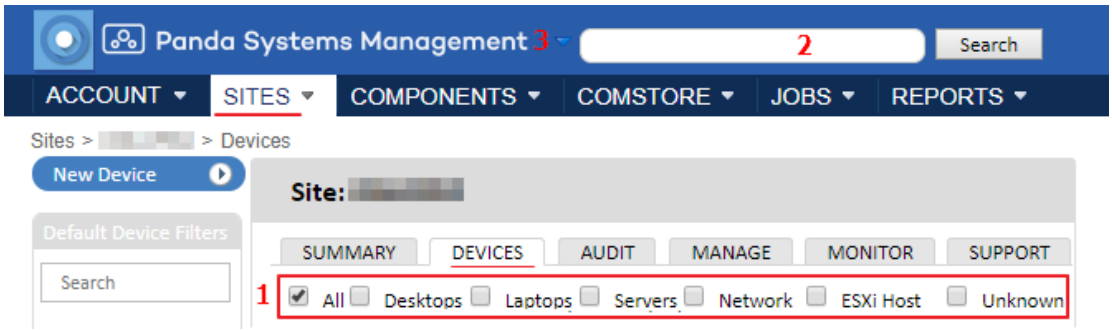


Figura 12.3: herramientas de búsqueda y filtrado de dispositivos

Los listados permiten buscar y filtrar los dispositivos mostrados mediante dos herramientas:

- **Filtrado por tipo de dispositivo (1)**: utiliza las casillas de selección situadas a la derecha de la barra de acciones para filtrar los listados por el tipo de dispositivo (**Todos**, **Escritorios**, **Portátiles**, **Servidores**, **Red**, **Host ESXi**, **Desconocido**)
- **Búsqueda textual (2)**: utiliza la barra de búsqueda situada en la parte superior de la ventana para buscar por el contenido de los campos que describen a los dispositivos. Haz clic en el icono ▾ **(3)**

para especificar el campo en el que se buscará:

- **Hostname**: campo **Nombre del host** del dispositivo.
- **desc**: campo **Descripción** del dispositivo.
- **Serial**: campo **Número de serie** del dispositivo.
- **Ip**: campo **Dirección IP ext.** del dispositivo.
- **Lastuser**: campo **Último usuario** del dispositivo.
- **Sitename**: nombre de la zona a la que pertenece el dispositivo.
- **Sitedesc**: descripción de la zona a la que pertenece el dispositivo.

Detalle de dispositivo

Objetivo

Muestra datos detallados del hardware instalado en el dispositivo seleccionado, así como su estado de conectividad, estado del antivirus, estado de la monitorización en tiempo real, ejecución de tareas y consumo de recursos entre otra información.

*Para obtener información extendida del estado del dispositivo haz clic en el link **more...** o en la barra de pestañas **Auditoría**. Consulta el capítulo "**Auditoria de activos**" en la página **159** para obtener más información.*

Acceso

Desde el menú general **Zonas**, selecciona la zona a la que pertenece el dispositivo y haz clic en el mismo. Se mostrará la vista del Nivel dispositivo con la pestaña **Resumen** seleccionada.

Información mostrada

Información del dispositivo

Campo	Descripción	Disponible en
Icono estado	Muestra el rol de equipo y el estado de la conexión.	Todos
Nombre del host	Nombre del dispositivo e icono representando su tipo.	Todos
Descripción	Descripción del dispositivo. Haz clic en el link **Editar** para cambiar la descripción.	Todos

Tabla 12.11: sección Información del dispositivo

Campo	Descripción	Disponible en
ID	Identificador interno.	Dispositivos de red.
Proveedor de NIC	Fabricante de la tarjeta de red.	Dispositivos de red.
Nombre SNMP	Campo Nombre del protocolo SNMP configurado en el dispositivo.	Dispositivos de red.
Descripción SNMP	Campo Descripción del protocolo SNMP configurado en el dispositivo.	Dispositivos de red.
Ubicación SNMP	Campo Ubicación del protocolo SNMP configurado en el dispositivo.	Dispositivos de red.
Contacto SNMP	Campo Contacto del protocolo SNMP configurado en el dispositivo.	Dispositivos de red.
Tiempo de actividad SNMP	Campo Tiempo de actividad del protocolo SNMP establecido por el dispositivo.	Dispositivos de red.
Fecha de creación	Fecha en la que el dispositivo se integró en Panda Systems Management.	Dispositivos de red.
Último usuario	Nombre de la última cuenta que hizo login en el equipo.	Equipos de sobremesa, portátiles y servidores.
Sistema operativo	Sistema operativo instalado en el dispositivo.	Equipos de sobremesa, portátiles y servidores, servidores ESXi, dispositivos móviles.
Dominio	Dominio Windows al que pertenece el dispositivo.	Equipos de sobremesa, portátiles y servidores.
Último reinicio	Fecha de la última vez que el equipo se inició.	Equipos de sobremesa, portátiles y servidores.
Fecha de la última auditoría	Fecha en la que Panda Systems Management recogió información de auditoria del dispositivo.	Dispositivos de red.
Dirección IP interna	Dirección IP asignada a la tarjeta de red del dispositivo.	Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi, dispositivos móviles.
Ext. de dirección IP	Dirección IP utilizada por el dispositivo para conectarse a recursos externos a la red local de la empresa.	Dispositivos de red, servidores ESXi.
Dirección MAC	Dirección física de la tarjeta de red del dispositivo.	Dispositivos de red.
Campos personalizados 1-30	Contenido de los campos personalizados definidos. Para más información consulta el apartado "**Campos personalizados**" para establecer su contenido de forma manual y el apartado "**Etiquetas y campos personalizados**" en la página **153** desde un script.	Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi.

Tabla 12.11: sección Información del dispositivo

Campo	Descripción	Disponible en
Credenciales ESXi	Credenciales de conexión asignadas al servidor ESXi y definidas en la pestaña configuración del Nivel zona o Ajustes en el menú general.	Servidores ESXi.
Credenciales SNMP	Credenciales de conexión asignadas al dispositivo SNMP y definidas en la pestaña configuración del Nivel zona o Ajustes en el menú general. Consulta el apartado "**Mejorar el descubrimiento de dispositivos por SNMP**" en la página **67**.	Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi.
Nodo de red	Dispositivo con el nodo de red asignado al equipo.	Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi.
Visto por última vez	Fecha de la última vez que el dispositivo móvil conectó con el servidor Panda Systems Management.	Dispositivos móviles.
Fecha de inscripción	Fecha en la que el dispositivo móvil se integró en Panda Systems Management.	Dispositivos móviles.
Grupos	Grupos a lo que pertenece el dispositivo.	Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi, dispositivos móviles.
Tipo de dispositivo	• Escritorio • Portátil • Servidor • Smartphone • Tablet	Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi, dispositivos móviles.
Fabricante	Nombre del fabricante del dispositivo.	Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi, dispositivos móviles.
Modelo		Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi, dispositivos móviles.
Número de serie		Equipos de sobremesa, portátiles y servidores, dispositivos de red.
Potencia nominal	Consumo asignado al dispositivo.	Dispositivos de red, servidores ESXi.

Tabla 12.11: sección Información del dispositivo

Campo	Descripción	Disponible en
Etiqueta Servicio/ Recurso	Cadena de texto para la identificación del servidor.	Servidores ESXi.
Imágenes	Numero de imágenes tomadas de las máquinas virtuales albergadas en el servidor ESXi.	Servidores ESXi.
ID de objeto		Dispositivos de red.
Contador de páginas impresas	Contador con el número de páginas imprimidas.	Dispositivos de red (impresoras).
Latitud de GPS	Si el dispositivo implementa hardware de geolocalización, indica la latitud registrada.	Dispositivos móviles.
Longitud de GPS	Si el dispositivo implementa hardware de geolocalización, indica la longitud registrada.	Dispositivos móviles.
Última actualización de GPS	Si el dispositivo implementa hardware de geolocalización, fecha con la última actualización de la posición del dispositivo móvil.	Dispositivos móviles.

Tabla 12.11: sección Información del dispositivo

Estado

Campo	Descripción	Disponible en
Estado del dispositivo	Estado de la conexión del dispositivo: **Online**, **Offline**.	Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi, dispositivos móviles.
Alertas abiertas	Número de alertas abiertas en el dispositivo.	Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi, dispositivos móviles.
Tickets abiertos	Número de tickets abiertos asignados al dispositivo.	Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi, dispositivos móviles.
Fecha de garantía	Fecha en la que expira la garantía del dispositivo. Para introducir una fecha haz clic en el enlace **Editar**.	Equipos de sobremesa, portátiles y servidores, dispositivos de red, servidores ESXi, dispositivos móviles.

Tabla 12.12: sección Estado

Campo	Descripción	Disponible en
Estado de parcheo	Estado del parcheo: • Sin política. • Sin información. • Necesita reinicio. • Error de instalación. • Aprobación pendiente. • Totalmente parcheado.	Equipos de sobremesa, portátiles y servidores Windows .
Producto antivirus	Fabricante y nombre del antivirus.	Equipos de sobremesa, portátiles y servidores.
Estado del antivirus	Estado del motor antivirus: • Ejecutándose y actualizado. • Ejecutándose y no actualizado. • No ejecutándose. • No detectado.	Equipos de sobremesa, portátiles y servidores.
Firewall de Windows	Estado del cortafuegos nativo de Windows (**Activado**, **Desactivado**).	Equipos de sobremesa, portátiles y servidores Windows.
Windows Updates	Estado del servicio Windows Update del dispositivo (**Activado**, **Desactivado**).	Equipos de sobremesa, portátiles y servidores Windows.

Tabla 12.12: sección Estado

Captura de pantalla

Muestra una captura de pantalla del dispositivo solo si es un equipo de sobremesa, portátil o servidor y si está encendido.

Haz clic en el icono  para actualizar la captura de pantalla.

Notas

Introduce recordatorios o mensajes destinados a otros administradores relativos al dispositivo concreto en la sección **Notas**. Se guardará una marca de tiempo de forma automática.

Consumibles

Muestra el estado de los consumibles en dispositivos de tipo impresora de red.

Campos personalizados

Los campos personalizados muestran información específica del dispositivo no soportada de forma nativa por Panda Systems Management. Esta información puede utilizarse para agrupar dispositivos mediante filtros de cuenta o filtros de zona (consulta el apartado "**Filtros**" en la página **75**) y también

puede reflejar el resultado de un componente de monitorización ejecutado en el dispositivo (consulta el apartado "**Etiquetas y campos personalizados** en la página **153**).

Para definir el contenido de un campo personalizado:

- Haz clic en el icono  y rellena una o varias cajas de texto correspondientes a los 30 campos personalizados disponibles.
- Haz clic el link **Borrar** y **Borrar campos personalizados** para eliminar el contenido de las cajas de texto.
- Haz clic en el botón **Guardar** para salvar el contenido de los campos personalizados.

La información contenida en los campos personalizados se muestra con el formato "`Campo personalizado X: #######`", donde `X` es el número del campo (de 1 a 30) y `#######` su contenido. Para mostrar campos personalizados autoexplicativos, Panda Systems Management permite cambiar en el Nivel cuenta la cadena "`Campo personalizado X`" por otra que describa mejor el tipo de dato que albergará el campo. Para ello sigue los pasos mostrados a continuación:

- Haz clic en el menú general **Ajustes**, menú de pestañas **Configuración de cuentas**.
- En la sección **Campos personalizados** haz clic en los iconos  y  para asignar, borrar y editar respectivamente las cadenas **Campos personalizados X** por otras que describan su contenido.

El procedimiento mostrado también es aplicable en el Nivel zona.

Información del invitado

Esta sección únicamente se muestra cuando el dispositivo es un servidor ESXi o Hyper-V y tiene máquinas virtuales alojadas.

Campo	Descripción
Nombre del host	Nombre del servidor ESXi o Hyper-V que alberga la máquina virtual.
Nombre del invitado	Nombre del equipo virtualizado.
Sistema operativo	Sistema operativo instalado en el equipo virtualizado.
Estado	Estado de la máquina virtual. (**Online**, **Offline**).

Tabla 12.13: sección Información del invitado

Estado de la monitorización en tiempo real

Muestra la información generada por los monitores asignados al dispositivo que envían datos en tiempo real para comprobar que su funcionamiento es correcto. Esta sección se incluye en equipos de sobremesa, portátiles y servidores, dispositivos de red y servidores ESXi.

Campos	Descripción
Monitorizar	Nombre del monitor y su descripción.
Prioridad	Prioridad establecida en el monitor.
Último valor	Último valor devuelto por el monitor.
Última lectura	Fecha en la que se recogió el último valor devuelto por el monitor.
Últimas 30 métricas	Gráfica de líneas con los 30 últimos valores devueltos por el monitor.
Estado	Indica si los parámetros monitorizados se encuentra en el rango definido por el monitor, o por el contrario hay alguna desviación y el monitor ha generado una alerta.

Tabla 12.14: sección estado de la monitorización en tiempo real

Actividad reciente

Consulta el apartado "**Auditoría de actividad**" en la página **174** para obtener información sobre la actividad de un equipo.

Auditoría del antivirus instalado

Soporte nativo

Panda Systems Management detecta automáticamente el estado del antivirus instalado en el equipo y del fichero de firmas descargado. La detección nativa de antivirus comprueba si los productos basados en Aether están actualizados o no. Los antivirus en sistemas Windows y macOS detectados de forma nativa son:

Antivirus	Windows	macOS
Avast Antivirus	**SI**	
Avast Business Antivirus	**SI**	
Bitdefender Endpoint Security	**SI**	
ESET Endpoint Antivirus	**SI**	
Kaspersky Endpoint Security	**SI**	**SI**
Kaspersky Security for Windows Server	**SI**	
McAfee Endpoint Security	**SI**	

Tabla 12.15: listado de antivirus detectados

Antivirus	Windows	macOS
McAfee VirsuScan Enterprise	SI	
Panda Endpoint Protection	SI	
Sophos Antivirus	SI	
Symantec Endpoint Protection	SI	
System Center Endpoint Protection	SI	
Trend Mico Worry-Free Business Security	SI	
Webroot Secure Anywhere	SI	SI
Windows Defender Antivirus	SI	
Windows System Center Endpoint Protection	SI	

Tabla 12.15: listado de antivirus detectados

Estado de la protección

Panda Systems Management distingue varios estados de protección dependiendo de si existe o no un antivirus instalado, si está activado y si el fichero de firmas es reciente o tiene más de 3 días de antigüedad.

Detectado	En ejecución	Actualizado	Estado del antivirus
SI	SI	SI	Ejecutándose y actualizado
SI	SI	NO	Ejecutándose y no actualizado
NO	NO	SI	No ejecutándose
SI			No ejecutándose
NO			No detectado

Tabla 12.16: estados detectados del antivirus instalado

Ampliación de los antivirus soportados

Para los productos de antivirus no soportados de forma nativa o para cualquier antivirus en sistemas macOS o Linux, es necesario enviar la información en el servidor a través de un fichero `.json` con el formato descrito a continuación:

```
{"product":"Override Antivirus","running":true,"upToDate":true}
```

Campo	Descripción
product	Nombre del antivirus que se mostrará en la consola Panda Systems Management.

Tabla 12.17: significado de los campos incluidos en el json para extender el soporte de antivirus

Campo	Descripción
running	Estado del antivirus: • "true": en ejecución • "false": detenido
upToDate	Estado del fichero de firmas: • "true": actualizado recientemente • "false": no actualizado recientemente

Tabla 12.17: significado de los campos incluidos en el json para extender el soporte de antivirus

El fichero `.json` debe ser almacenado en:

Sistema operativo	Ruta y nombre del fichero
Windows	`%ProgramData%\CentraStage\AEMAgent\antivirus.json`
macOS	`/usr/local/share/CentraStage/AEMAgent/antivirus.json`
Linux	`/usr/local/share/CentraStage/AEMAgent/antivirus.json`

Tabla 12.18: ruta de almacenamiento del fichero .json

*Puedes desarrollar un componente y distribuirlo en todo el parque de equipos de forma automática para que compruebe el estado del antivirus en los dispositivos y escriba el fichero .json cada cierto tiempo. Si el fichero .json no ha sido modificado en más de 7 días, el agente PCSM lo borrará. Consulta el capítulo "***Componentes y ComStore***" en la página* **139** *para desarrollar componentes compatibles con Panda Systems Management.*

Capítulo 13

Informes

El sistema de informes de Panda Systems Management muestra el estado de los dispositivos administrados en varios formatos (pdf y csv), altamente configurables en lo relativo a contenidos, y adaptables según el tipo de público objetivo al que va destinado. Las características principales del sistema de informes son:

- Soporte de informes programados e inmediatos.
- Soporte de varios idiomas.
- Flexibilidad en la elección de los dispositivos que aportarán datos a cada informe.
- Configuración del contenido de cada tipo de informe.
- Capacidad para consolidad informes de varias zonas en un único documento que ofrece una perspectiva global del parque informático.

CONTENIDO DEL CAPÍTULO

Acceso a la funcionalidad de informes

Toda la funcionalidad de informes es accesible desde el menú general **Informes**, siendo posible generar desde esta área cualquier tipo de informe de cualquier ámbito. Sin embargo, para acelerar la selección de los dispositivos que abarcará el informe, es posible invocar la herramienta de informes desde los tres niveles (Cuenta, Zona y Dispositivo) disponibles en Panda Systems Management. Dependiendo del nivel en el que se genere el informe, el alcance del documento variará. A continuación se indican los puntos de la consola de administración desde los que se puede generar informes y el alcance de los mismos.

Informes con datos de dispositivos de varias zonas

- Desde el menú general **Zonas**, selecciona una o varias zonas y haz clic en el icono  de la barra de iconos.
- Genera informes en formato pdf de todos los dispositivos incluidos en las zonas seleccionadas.

Informes con datos de dispositivos de una zona

- Haz clic en el menú general **Zonas** y en la zona a la cual pertenecen los dispositivos.
- Selecciona **Dispositivos** en la barra de pestañas y marca con las casillas de selección los dispositivos que formarán parte del informe.
- Haz clic en el icono  de la barra de iconos para generar un informe en formato pdf.

Informes con datos de un único dispositivo

- Haz clic en el menú general **Zonas** y en la zona a la cual pertenece el dispositivo. Selecciona **Dispositivos** en la barra de pestañas y haz clic en el dispositivo del cual se generará el informe. Haz clic en el icono  del menú de acciones para generar un informe en formato pdf.

Informes con alcance configurable

- Desde el menú general **Informes**, menú de pestañas **Nuevo informe** se accede a la configuración completa del sistema de informes. Al acceder de forma directa no se especifican de antemano los dispositivos que aportarán datos al informe, de forma que el administrador tiene que indicar de forma manual las agrupaciones o dispositivos individuales de los cuales se realizará el informe.

Creación de informes

Para crear un informe sigue los pasos mostrados a continuación:

- Determina el ámbito del informe y dependiendo del caso accede al sistema de informes mediante una de los procedimientos descritos en el punto "**Acceso a la funcionalidad de informes**".
- Rellena los campos de la plantilla del informe:

Campo	Descripción
Nombre	Indica un nombre para el informe. Si no se especifica se añade `Scheduled Report for [Username]`
Programación	Especifica si el informe se ejecutará de forma inmediata, una única vez o varias veces a lo largo del tiempo. Consulta el apartado "**Programador de tareas**" en la página **134** para una descripción del programador de tareas. Los informes programados para ejecutarse inmediatamente se pueden descargar desde la consola para que el administrador no tenga que esperar a que llegue el correo electrónico. Se mostrará una ventana emergente en la esquina superior derecha para descargar el informe.
Informe global	Permite consolidar los informes generados sobre dispositivos pertenecientes a distintas zonas en un único informe.
Informes individuales	Genera un informe por cada zona de destino.
Idioma	Selecciona el idioma del informe.
Activado	Por defecto los informes creados son introducidos en la cola de tareas del programador. Si el informe no está activado la plantilla de configuración se guarda pero el informe no se generará. Esto evita tener que borrar un informe cuando temporalmente no se quiere generar.
Seleccionar informe	Selecciona el tipo de informe, las secciones que lo formarán y los filtros de dispositivos necesarios. Consulta el apartado "**Tipos de informes disponibles y configuración**".
Dispositivos	Selecciona los dispositivos mostrados en el informe. Dependiendo del método de acceso al sistema de informes, este campo podrá estar ya predefinido o no.

Tabla 13.1: parámetros de configuración de un informe

Campo	Descripción
Destinatarios de correo	Indica las direcciones de correo y otros parámetros del mensaje de correo utilizado para entregar el informe: • **Asunto**: asunto del correo. Si no se especifica se añade uno automático. • **Cuerpo**: cuerpo del mensaje. Si no se especifica se añade información sobre la ejecución y las características del informe. • **Enviar a los destinatarios predeterminados de la cuenta**: envía el correo a las cuentas definidas en el menú general **Ajustes**, menú de pestañas **Configuración de cuenta**, sección **Destinatarios de correo** siempre que tengan activado el envío de informes. • **Enviar a los destinatarios predeterminados de la zona**: envía el correo a las cuentas definidas en el menú general **Zonas** haciendo clic en una zona, menú de pestañas **Configuración**, sección **Destinatarios de correo** siempre que tengan activado el envío de informes. • **Destinatarios adicionales**: especifica cuentas de correo adicionales para el informe a definir.

Tabla 13.1: parámetros de configuración de un informe

Los correos electrónicos que adjuntan un informe demasiado grande para procesarse contienen un enlace a la consola de administración para descargar el informe.

Estructura de los informes

Los informes se dividen de dos partes bien diferenciadas:

- Una primera hoja de introducción con datos del tipo de informe generado.
- Cuerpo del informe, de tamaño variable, que contiene la información propiamente dicha.

Introducción al informe

Figura 13.1: hoja de introducción con datos del tipo de informe generado

Dependiendo de si están definidos, los campos que se incluyen en la introducción del informe son:

- Logotipo del producto Panda Systems Management.
- Tipo de informe generado.
- Descripción del informe.
- Fecha de creación. Se utiliza el huso horario definido en el menú superior **Ajustes**, menú de pestañas **Información personal**.
- Zonas que abarca el informe.
- Filtros aplicados a los dispositivos incluidos en el informe.
- Nombre de los dispositivos incluidos en el informe.
- Grupos de dispositivos a los que pertenecen los dispositivos incluidos en el informe.
- Número total de dispositivos incluidos en el informe.

Cuerpo del informe

Los informes se dividen en secciones. Dependiendo el tipo de informe es posible configurar las secciones que se mostrarán.

Si un informe abarca varias zonas (ver el apartado "**Creación de informes**" para activar la funcionalidad **Informe global**), el informe presentará una sección independiente con los datos de cada zona.

Tipos de informes disponibles y configuración

Panda Systems Management soporta los tipos de informe mostrados a continuación:

- **Ejecutivo**: muestra el estado general del parque de dispositivos administrado.
- **Auditoria**: muestra información del estado de los recursos de los dispositivos.
- **Monitorización**: muestra el estado de los monitores asignados a los dispositivos y alertas abiertas.
- **Gestión de parches**: muestra el nivel de parcheo de los dispositivos Windows.
- **Actividad**: muestra la actividad desarrollada por los administradores en los dispositivos.
- **Exportar**: genera todos los tipos de informes con el máximo de detalle sustituyendo elementos gráficos por listados con la actividad registrada en la plataforma Panda Systems Management.

Ejecutivo

Resumen ejecutivo

- **Descripción**: muestra el estado de funcionamiento de los dispositivos gestionados.
- **Opciones**:
  - **Espacio libre**: establece el umbral en porcentaje de espacio libre en el disco duro para considerar al dispositivo como correcto.

- **Memoria Ram**: establece el umbral en valor absoluto de memoria RAM para considerar al dispositivo como correcto.

El informe contiene 6 secciones que se pueden incluir u ocultar:

- **Summary**: incluye una explicación sobre las distintas secciones del informe, como se realizan las mediciones y como afectan en la calificación final.
- **Asset Management:**
  - **Device type**: tabla con el número de dispositivos agrupados por su tipo en el parque.
  - **Device Health check**: tabla con el número de dispositivos que no superan los umbrales configurados. También se indican los dispositivos que tienen instalado un sistema operativo Windows no soportado por el fabricante. Consulta **https://www.pandasecurity.com/es/support/card?id=300102.**
- **Monitoring:**
  - Gráfico de tarta con el número de alertas producidas agrupadas según su prioridad.
  - Gráfico de tarta con el número de alertas producidas agrupadas por su estado.
  - Tabla con el número de alertas agrupadas por prioridad y su estado.
  - Tabla con el número de alertas agrupadas por tipo de dispositivo y su estado.
  - Tabla de los 5 servidores con más alertas.
  - Tabla de los 5 equipos no servidores con más alertas.
- **Patch management:**
  - Gráfico de tarta con el número de servidores agrupado por su estado de parcheo.
  - Gráfico de tarta con el número de equipos de sobremesa agrupado por su estado de parcheo.
  - Tabla con el total de servidores registrados y el número de ellos con todos los parches instalados.
  - Tabla con el total de equipos de sobremesa registrados y el número de ellos con todos los parches instalados.
- **Antivirus:**
  - Gráfico de tarta con el número de servidores agrupado por su estado de antivirus.
  - Gráfico de tarta con el número de equipos de sobremesa agrupado por su estado de antivirus.
  - Tabla con el número de servidores que tienen el antivirus actualizado, sin actualizar y sin ejecutar.
  - Tabla con el número de equipos de sobremesa que tienen el antivirus actualizado, sin actualizar y sin ejecutar.
- **Proactive Maintenance:**
  - Tabla con las tareas creadas para el mantenimiento automatizado.

Resumen del estado de los dispositivos

- **Descripción**: muestra el estado de funcionamiento de los dispositivos gestionados.

- **Opciones**:
  - **Espacio libre**: establece el umbral en porcentaje de espacio libre en el disco duro para considerar al dispositivo como correcto.
  - **Memoria RAM**: establece el umbral en valor absoluto de memoria RAM para considerar al dispositivo como correcto.

La información incluida se divide en varias secciones:

- **Summary**
  - Gráfico de tarta con el número de dispositivos total agrupados según superen o no los test realizados por la plataforma.
  - Gráfico de tarta con el número de dispositivos total agrupados según su tipo.
- **Tipo de dispositivo**: por cada tipo de dispositivo se incluye una tabla de detalle indicando los test que han pasado y han fallado:
  - **Device name**, **Device Description**, **Operating System**: campos para identificar al dispositivo.
  - **Sufficient disk space**: resultado del test de espacio mínimo libre disponible.
  - **Sufficient ram**: resultado del test de memoria RAM mínima disponible
  - **Software Compliant:** muestra si todas las aplicaciones del dispositivo qué estan gestionadas por el módulo de Gestión de software. En caso contrario, este campo se mostrará en blanco.
  - **Fully patched**: muestra si el equipo no tiene parches pendientes de instalar.
  - **Antivirus up to date**: muestra si el fichero de firmas del antivirus está actualizado antes de 3 días.
  - **Under warranty**: muestra el equipo se encuentra en garantía.
  - **Online within 30 days**: muestra si el equipo se ha conectado en los últimos 30 días.
  - **No open alerts**: muestra si el equipo no tiene alertas sin resolver.

Hardware Lifecycle

- **Descripción**: muestra los dispositivos gestionados en la red agrupados por la zona y ordenados según la fecha en la que se ensamblaron para ayudar al administrador a localizar los equipos más antiguos y proclives a fallar. La fecha de ensamblado del equipo se basa en la fecha de publicación de la BIOS.
- **Opciones**:
  - **Espacio libre**: establece el umbral en porcentaje de espacio libre en el disco duro para considerar al dispositivo como correcto.
  - **Memoria RAM**: establece el umbral en valor absoluto de memoria RAM para considerar al dispositivo como correcto.

Información contenida en el informe:

- **Hardware Replacement Recommendations**: gráfico de tarta que agrupa los dispositivos en 4 categorías:

- **Suitable for 24 months**: equipos con menos de 3 años de antigüedad.
- **Replacement recommended within 12-24 months**: equipos entre 3 y 4 años de antigüedad.
- **Replacement recommended within 12 months**: equipos con más de 4 años de antigüedad.
- **Unknown**: sin información de la antigüedad (dispositivos de red, impresoras y otros dispositivos sin acceso a la BIOS).

- **Operating System Support**: gráfico de tarta con los sistemas operativos soportados y no soportados por Microsoft. El resto de sistemas operativos cuentan como soportados por sus respectivos fabricantes. Consulta **https://www.pandasecurity.com/es/support/card?id=300102**.
  - **Operating system is supported**: el fabricante publica actualizaciones y ofrece servicio técnico.
  - **Operating system is unsupported unless manufacturer extended support has been arranged**: el fabricante dejó de publicar actualizaciones recientemente y ya no ofrece servicio técnico, a no ser que el cliente haya contratado un paquete de servicio de soporte extendido.
  - **Operating system is unsupported**: el fabricante dejó de publicar actualizaciones y ya no ofrece servicio técnico. Se recomienda actualizar el sistema operativo.
- **Agrupación:** por cada agrupación mostrada en el gráfico de tarta se listan los dispositivos que encajan en cada rango.
  - **Device name**, **Device Description**, **Operating System**: campos para identificar al dispositivo.
  - OS Support: estado del soporte del sistema operativo por parte del fabricante.
  - **Last User**: cuenta del usuario que inició sesión por última vez en el equipo.
  - **Serial Number**
  - **Sufficient Disk Space**: resultado del test de espacio mínimo libre disponible.
  - **Sufficient RAM**: resultado del test de memoria RAM mínima disponible
  - **Under Warranty**: muestra el equipo se encuentra en garantía.
  - **Online Within 30 days**: muestra si el equipo se ha conectado en los últimos 30 días.
  - **Build date**: fecha en la que fue ensamblado el equipo. Se toma de la fecha de fabricación de la BIOS, por lo que esta fecha puede no ser del todo exacta ya que el equipo puede haberse ensamblado bastante tiempo después.

Auditoría

Almacenamiento de los dispositivos

- **Descripción**: muestra el estado de los dispositivos de almacenamiento conectados a los dispositivos.
- **Opciones**:
  - **Seleccione el tipo de unidad**: muestra un desplegable con los tipos de dispositivos de almacenamiento que se incluirán en el informe.

Información contenida en el informe:

- **Tipo de dispositivo**: por cada tipo de dispositivo se incluye una tabla con los equipos y sus dispositivos conectados:
  - **Device name**, **Device Description**: campos para identificar al dispositivo.
  - **Drive**: letra o punto de montaje que identifica a la unidad.
  - **Drive Type**: tipo de dispositivo de almacenamiento (local, removible, óptico etc.).
  - **Size**: capacidad total del dispositivo de almacenamiento.
  - **Free**: espacio libre en Gbytes del dispositivo de almacenamiento.
  - **Used (%)**: gráfico de barra mostrando el porcentaje de espacio usado del dispositivo de almacenamiento.

Auditoría detallada de los equipos

- **Descripción**: muestra una auditoria completa de cada dispositivo administrado.
- **Opciones**:
  - **Seleccione un campo personalizado para este informe**: muestra un desplegable con campos personalizados que se incluirán en el informe.

La información contenida en este informe es una copia de la pestaña **Auditoria** en el Nivel dispositivo. Consulta el capítulo "**Auditoria de hardware**" en la página **164** para obtener información de cada uno de los campos incluidos en el informe.

Auditoría de red

- **Descripción**: muestra un listado completo de todos los dispositivos del parque informático, tanto los administrados como los encontrados pero todavía sin gestionar.
- **Opciones**:
  - **Agentes administrados**: el informe incluirá todos los dispositivos administrados por Panda Systems Management.
  - **Dispositivos descubiertos**: el informe incluirá todos los dispositivos descubiertos y no administrados por Panda Systems Management.

La información incluida se divide en varias secciones:

- **Summary**:
  - Gráfico de tarta con el total de dispositivos descubiertos en el parque informático agrupados por integración en Panda Systems Management.
- **Managed**: por cada tipo de dispositivo se incluye una tabla con la información mostrada a continuación:
  - **Device name**, **Device Description**: campos para identificar al dispositivo.
  - **IP Address:** dirección IP del dispositivo.

- **Vendor:** fabricante del dispositivo.
- **Created:** fecha en la que el dispositivo se integró en Panda Systems Management.

- **Unmanaged**: por cada tipo de dispositivo se incluye una tabla con la información mostrada a continuación:
  - **Device name**, **Device Description**: campos para identificar al dispositivo.
  - **SNMP Description**: campo **Descripción** del protocolo SNMP.
  - **IP Address:** dirección IP del dispositivo.
  - **Vendor:** fabricante del dispositivo.
  - **Discovered:** fecha en la que Panda Systems Management descubrió por primera vez el dispositivo en la red.

Software

- **Descripción**: muestra un listado completo del software instalado en los dispositivos del parque informático.
- **Opciones**: permite añadir reglas de filtrado de software o lista todo el software encontrado. Utiliza "%" como comodín para sustituir uno o varios caracteres al principio o final del nombre del paquete de software a filtrar.

La información incluida se divide en varias secciones:

- **Summary**: listado con todo el software encontrado y el número de ocurrencias de cada programa.
  - **Software**: nombre del programa encontrado.
  - **Instances found**: número de dispositivos que tienen instalado el programa.
- **Dispositivo**: listado con el software encontrado en cada dispositivo.
  - **Device name**, **Device Description**, **Operating System**: campos para identificar al dispositivo.
  - **Software**: nombre del programa encontrado.
  - **Version**: versión del programa encontrado.

Monitorización

Estado de los monitores de dispositivos

- **Descripción**: muestra los últimos valores de los monitores asignados a los dispositivos.
- **Opciones**:
  - **Seleccione el estado de los monitores**: filtra los monitores incluidos en el informe por su estado.
  - **Seleccione los tipos de monitor**: filtra los monitores incluidos en el informe según su categoría.

Información contenida en el informe:

- **Nombre del dispositivo**: por cada dispositivo me incluye una tabla con la siguiente información:

- **Device Name**, **Device Description**, **Operating System**: campos para identificar al dispositivo.
- **Monitor Type**: categoría del monitor.
- **Monitor Description.**
- **Priority.**
- **Lastest value**: último valor devuelto por el monitor.
- **Last reading**: fecha en la que se recibió el último valor del monitor.
- **Status:** estado del monitor (OK, Alerta, No responde).

Alertas de monitor abiertas

- **Descripción**: muestra el estado actual de las alertas abiertas por dispositivo.

La Información contenida en el informe una tabla con los siguientes campos:

- **Device Name**, **Device Description:** campos para identificar al dispositivo.
- **Total:** número total de alertas abiertas en el dispositivo.
- **Critical:** número total de alertas abiertas de importancia crítica en el dispositivo**.**
- **High:** número total de alertas abiertas de importancia alta en el dispositivo.
- **Moderate:** número total de alertas abiertas de importancia moderada en el dispositivo.
- **Low:** número total de alertas abiertas de importancia baja en el dispositivo.
- **Information:** número total de alertas de tipo informativo abiertas en el dispositivo.

Monitorización de rendimiento

- **Descripción**: muestra el rendimiento del dispositivo mediante las gráficas accesibles en el Nivel dispositivo de la consola de administración.
- **Opciones**:
  - **Seleccione las opciones de rendimiento de este informe**: selecciona los recursos del dispositivo que se mostrarán en el informe: **CPU**, **Memoria**, **Disco duro**.

La Información contenida en el informe es una tabla con los siguientes elementos:

- **Device Name**, **Device Description:** campos para identificar al dispositivo.
- Gráfica de líneas que representa el consumo de memoria registrado en forma de porcentaje durante último mes.
- Gráfica de líneas que representa el consumo de CPU en porcentaje durante último mes.
- Gráfica de líneas que representa el consumo de espacio en los dispositivos de almacenamiento interno en porcentaje durante último mes.

Gestión de parches

Actividad de gestión de parches

- **Descripción**: muestra la actividad de parcheo de Panda Systems Management en los dispositivos seleccionados y en el rango de fechas configurado.
- **Opciones**:
  - **Intervalo de fechas**: el informe mostrará información en el rango de fechas elegido (**Últimos 7 días**, **Últimos 30 días**, **Mes actual**, **Intervalo personalizado**).
  - **Estado de instalación**: incluye en el informe los parches instalados con éxito y/o los que dieron error.

El informe contiene una tabla con los siguientes elementos:

- **Device Name**, **Device Description**, **Operating System**: campos para identificar al dispositivo.
- **Last Reboot:** fecha en la que el equipo se reinició por última vez para finalizar la instalación de parches descargados o por otra causa.
- **Patch Name**: nombre del parche.
- **Type**: software.
- **Priority**: establecida por el proveedor del parche.
- **Published**: fecha en la que el proveedor publicó el parche.
- **Installed**: fecha en la que el parche se instaló en el dispositivo.
- **Install**: estado de la instalación del parche (**Installed** o **Failed**).

Información de gestión de parches

- **Descripción**: muestra una visión detallada del estado de cada parche instalado en los dispositivos.
- **Opciones**:
  - **Seleccionar parche**: el informe mostrará información de todos los parches publicados o únicamente de los indicados.
  - **Select Patch Details Options for this report**: filtra los parches mostrados en el informe por su estado (**Aprobado**, **No aprobado**, **Instalado**).

El informe contiene una tabla con los siguientes elementos:

- **Nombre del dispositivo:**
  - **Device Name**, **Device Description**, **Operating System**: campos para identificar al dispositivo.
  - **Patch Status**: indica si el equipo requiere un reinicio para completar la instalación de algún parche descargado.
  - **Patch title**: nombre del parche.
  - **Priority**: establecida por el proveedor del parche.

- **Status**: estado del parche (**Aprobado**, **Instalado**, **No aprobado**)

Resumen de gestión de parches

- **Descripción**: muestra una visión general del estado de parcheo de cada dispositivo.

El informe contiene varias secciones:

- **Resumen:**
  - Gráfico de tarta con el total de equipos agrupados por su estado de parcheo (**Actualizado**, **Aprobación pendiente**, **Error de instalación**, **Necesita reinicio**, **Sin información**, **Sin política**).
- **Servidores:**
  - **Device Name**, **Device Description:** campos para identificar al dispositivo.
  - **Last Reboot**: fecha en la que el equipo se reinició por última vez para finalizar la instalación de parches descargados o por otra causa.
  - **Installed:** número de parches instalados con éxito.
  - **Approved Pending**: número de parches publicados pendientes de aprobar por el administrador.
  - **Not Approved:** número de parches excluidos de la instalación.
  - **Patch Status**: estado del dispositivo con respecto a la actividad de parcheo (**Fully Patched**, **Install Error**, **Reboot Required**).

Actividad

Actividad del dispositivo

- **Descripción**: muestra las acciones realizadas por el administrador sobre los dispositivos gestionados.
- **Opciones**:
  - **Intervalo de fechas**: el informe mostrará información en el rango de fechas elegido (**Últimos 7 días**, **Últimos 30 días**, **Mes actual**, **Intervalo personalizado**).
  - **Filtro de actividad**: incluye en el informe los distintos tipos de acciones que Panda Systems Management ejecuta en los dispositivos.

El informe contiene una tabla con los siguientes elementos:

- **Device Name**, **Device Description**, **Operating System:** campos para identificar al dispositivo.
  - **Type:** icono que representa la acción ejecutada sobre el dispositivo.
  - **User Name**: nombre del usuario de la consola que inició la acción.
  - **Activity:** actividad realizada en el equipo.
  - **Started**: fecha de inicio de la acción.
  - **Ended**: fecha de finalización de la acción.
  - **Duration**: tiempo transcurrido en la ejecución de la acción.

- **Status**: indica si la acción fue completada.

Exportar

Los informes de esta categoría son ficheros en formato csv que registran los distintos tipos de actividades y acciones desarrolladas por Panda Systems Management. Este tipo de informes contiene una línea por cada actividad, acción o cambio producido en el producto y son especialmente útiles a la hora de tratarlos de forma automática con herramientas externas, como por ejemplo Microsoft Excel para filtrar, buscar y agrupar los eventos producidos.

Para limitar el alcance se soporta el filtrado por fecha y por el concepto principal que trata el informe.

El contenido es configurable mediante el botón **Seleccionar columnas** para mostrar más o menos información en cada línea.

A continuación se muestran los informes disponibles junto a una explicación de su cometido.

- **Actividad del administrador**: muestra cada actividad ejecutada en la fecha configurada. El listado de líneas se filtra por el usuario de la consola de administración configurado y no por los dispositivos elegidos como destino en el campo **Objetivos del informe**.
- **Registro de cambios del dispositivo**: muestra cada cambio registrado en el fichero de log del dispositivo. El listado de líneas se filtra por el tipo de cambio: **hardware**, **software**, **system**.
- **Información del dispositivo**: muestra toda la información disponible de cada dispositivo.
- **Actividad del dispositivo**: muestra las actividades indicadas en el filtro y que ejecutó el administrador sobre el dispositivo para el rango de fechas configurado.
- **Almacenamiento de los dispositivos**: muestra un listado de todos los discos disponibles en los dispositivos seleccionados, junto a su espacio disponible.
- **Auditoría de Microsoft**: muestra la información necesaria para licenciar los productos Microsoft instalados en los dispositivos auditados.
- **Alertas de monitorización**: muestra las alertas generadas por lo monitores en el rango de fechas indicado y según el filtrado configurado.
- **Software instalado**: muestra el software instalado en los dispositivos según el criterio configurado.
- **Información de los parches**: muestra todos los parches publicados por los proveedores del software instalado en los equipos filtrados por su estado.
- **Resumen de parcheo de los dispositivos**: muestra los dispositivos con parches pendientes de instalación.
- **Número de dispositivos de la zona:** muestra el total de dispositivos de una zona agrupados por tipo de dispositivo.

Parte 5

Resolución de incidencias y soporte técnico

Capítulo 14: Gestión de parches

Capítulo 15: Distribución e instalación centralizada de software

Capítulo 16: Gestión del software

Capítulo 17: Alertas y tickets

Capítulo 18: Herramientas de acceso remoto a dispositivos

Capítulo 14

Gestión de parches

La herramienta Gestión de parches está formada por un conjunto de recursos orientados a automatizar la distribución e instalación de parches y actualizaciones de software de forma centralizada. No solo facilita la actualización diaria del software de los dispositivos, sino que permite realizar auditorías, mostrando de forma sencilla y rápida aquellos equipos sin actualizar o con vulnerabilidades conocidas.

Con esta herramienta 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 herramienta Gestión de parches utiliza la API Windows Update existente en todos dispositivos Microsoft Windows compatibles con Panda Systems Management y por tanto solo es compatible con sistemas Microsoft Windows.

CONTENIDO DEL CAPÍTULO

¿Qué parches puedo distribuir / aplicar?

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

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

- 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…

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 la sección "***Desactivación de Windows Update para evitar interferencias***" en la página* **217**.
>
> *Los procedimientos aquí descritos pueden colisionar con otros procedimientos definidos por software de terceros, como, por ejemplo las políticas de Windows Update definidas en una GPO. Se recomienda desactivar políticas de terceros fabricantes que interfieran con las definidas en Panda Systems Management.*

Clasificación de los parches según el tipo de política utilizada

Dependiendo de si se utiliza una política de tipo Windows Update o Patch Management, Panda Systems Management asigna una clasificación diferente de los parches, aunque siempre basada en su importancia:

- **Política Windows Update**: utiliza la clasificación empleada por el motor de Windows Update (**Importantes**, **Recomendados**, **Opcionales**).
- **Política Patch Management**: utiliza la clasificación empleada en el Microsoft Security Response Center Priority (**Crítica**, **Importante**, **Moderada**, **Baja**, **Sin especificar**).

Orden de instalación de los parches

Panda Systems Management instala las actualizaciones en un orden que depende del tipo de parche y su importancia:

Orden	Categoría	Importancia
1	Actualizaciones de seguridad	Crítica
2	Actualizaciones de seguridad	Importante
3	Actualizaciones de seguridad	Moderada
4	Actualizaciones de seguridad	Baja
5	Actualizaciones de seguridad	Sin especificar
6	Service Packs	No aplica
7	Paquetes acumulativos de revisiones	No aplica
8	Actualizaciones críticas	No aplica
9	Actualizaciones	No aplica

Tabla 14.1: prioridad de instalación de parches

Orden	Categoría	Importancia
10	Otros	No aplica

Tabla 14.1: prioridad de instalación de parches

Frecuencia de auditoria de parches

El módulo de gestión de parches comprueba los equipos administrados para buscar nuevos parches. Esta búsqueda la realiza de forma automática en los siguientes casos:

- La política de administración de parches se ha ejecutado.
- Auditoría completa inicial (justo después de la instalación del Agente).
- Auditoría periódica cada 24 horas.
- Auditoría manual (cuando se selecciona un solo dispositivo o múltiples dispositivos).
- Los siguiente eventos no activan un escaneo de parches:
- Trabajos rápidos o programados.
- Trabajos de respuesta de alerta.
- Tareas del usuario.

Método I: Política Windows Update

Las políticas de tipo Windows Update establecen de forma centralizada la configuración del servicio Windows Update, accesible individualmente desde el panel de control de cada dispositivo Windows de la red.

De esta forma, el administrador controlará desde un único lugar 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.

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 del servicio Windows Update de todos los dispositivos afectados.

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.

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 desde Panda Systems Management utilizando otros métodos de gestión de parches.

Toda la configuración de la 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:

Campo	Campo
Actualización de Microsoft	• **Recibir actualizaciones para los productos de Microsoft y revisar nuevo software de Microsoft opcional al actualizar Windows:** además de las actualizaciones de Windows también se reciben de otros productos de Microsoft (Word, Excel, Powerpoint,...).
WSUS	• **Cambiar configuración del servidor WSUS:** permite establecer el servidor WSUS desde el que hacer la instalación. • **No permitir conexiones a Microsoft para la instalación o búsqueda de parches cuando se utilice un servidor WSUS**: las actualizaciones buscarán los archivos y ficheros en el servidor WSUS, evitando buscar los que falten en servidores externos. • **Nombre del grupo de destino del lado 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 de la empresa.Con este parámetro se permite especificar los grupos separados por punto y coma a los que pertenece el dispositivo sobre el que aplica la política.
Horas activas	• **Configurar horas activas**: establece el espacio de tiempo durante el cual que los equipos están en uso.

Tabla 14.2: opciones disponibles en la política Windows Update

Campo	Campo
Canal de actualización	• **Cambiar la configuración del canal de actualización para los dispositivos disponibles**: • **Implementación dirigida:** las actualizaciones se reciben inmediatamente después de su lanzamiento general. • **Implementación amplia:** las actualizaciones se reciben más tarde, tras recibir feedback de la comunidad (rama actual para empresas). • **Aplazar actualizaciones de funcionalidad:** permite postergar el momento de la instalación de las actualizaciones que introducen nuevas funcionalidades durante el máximo tiempo posible o estableciendo un periodo lo más cercano posible a un determinado número de días. • **Aplazar actualizaciones de calidad:** permite postergar el momento de la instalación de las actualizaciones que mejoran el rendimiento durante el máximo tiempo posible o estableciendo un periodo lo más cercano posible a un determinado número de días.
Compartir actualizaciones	• **Permitir que los dispositivos compartan actualizaciones dentro de la red local:** los dispositivos conectados a una misma red pueden buscar los ficheros de actualización en los equipos de la misma red. • **Permitir que los dispositivos compartan actualizaciones de Windows fuera de la red local:** los equipos pueden buscar los ficheros para la actualización en equipos con los que no comparten una red local.
Inicio rápido	• **Desactiva el inicio rápido de Windows;** permite que las actualizaciones se instalen durante el apagado y el encendido del dispositivo.
Configurar actualizaciones	• **Descargar automáticamente las actualizaciones recomendadas para mi ordenador e instalarlas** • **Descargar actualizaciones por mí, pero permitirme elegir cuándo instalarlas.** • **Notificarme, pero no descargarlas ni instalarlas automáticamente.** • **Desactivar actualizaciones automáticas**
Instalar nuevas actualizaciones	• Establece el día de la semana y la hora en las que se instalarán las nuevas actualizaciones.
Actualizaciones recomendadas	• **Recibir actualizaciones recomendadas del mismo modo que las actualizaciones importantes.**

Tabla 14.2: opciones disponibles en la política Windows Update

Campo	Campo
Quien puede instalar actualizaciones	• **Permitir a todos los usuarios instalar actualizaciones en este ordenador**: Permite que los usuario de los dispositivos instalen las actualizaciones sin que pasen por el administrador de la cuenta.
Reinicio	• **No hay reinicio automático con usuarios conectados paras instalaciones de actualizaciones automáticas programadas.** • **Reindicador para el reinicio con instalaciones programadas:** las notificaciones del sistema para realizar un reinicio del dispositivo. • **Demorar reinicio para instalaciones programas:** notifica que el reinicio se llevara a cabo en el lapso de tiempo indicado**.**

Tabla 14.2: opciones disponibles en la política Windows Update

Desactivación de Windows Update para evitar interferencias

Es posible que existan otros programas de terceros que establezcan configuraciones sobre el subsistema Windows Update y que provoquen interferencias con la herramienta de parcheo de Panda Systems Management. Un caso muy común es la existencia de una configuración local por defecto de Windows Update en cada dispositivo, que instale los parches importantes cada cierto tiempo. Para evitar la interferencia de políticas de parcheo definidas por productos de terceros o por el usuario sigue los pasos mostrados a continuación:

- Crea una política de tipo Windows Update con destino todos los dispositivos que recibirán actualizaciones a través de Panda Systems Management.
- En Política de parches elige **Desactivar actualizaciones automáticas**.
- Distribuye la política entre los 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.

Método II: Política Gestión de parches.

Las políticas de 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 importancia (**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.

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 **14.1** de la página **219** 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**" en la página **219** para configurar una política de Gestión de parches.

Redefinición de políticas en el Nivel Zona

Establece en el Nivel zona 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 en cada zona creada. De esta forma se elimina la necesidad de crear una nueva configuración completa en cada 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.

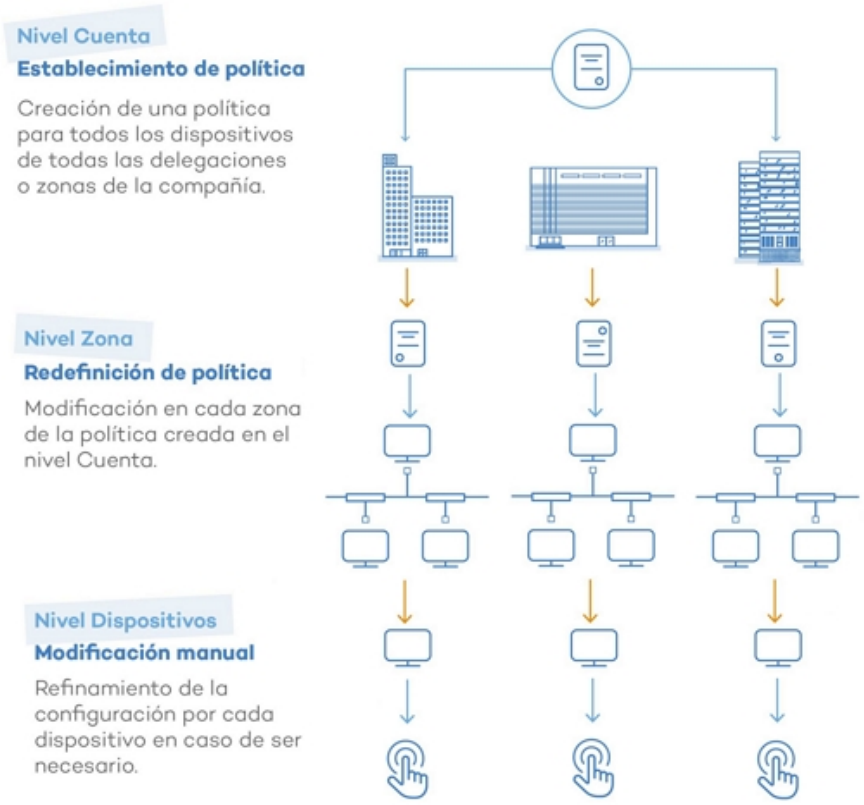


Figura 14.1: estrategia general para definir las políticas de parches

Modificaciones particulares por dispositivo

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

Creación de Políticas de Gestión de parches

> *Panda Systems Management asigna una política Gestión de parches en modo Auditar de forma automática a los dispositivos de la cuenta.*

Para crear una política de tipo Gestión de parches en el Nivel zona o Nivel cuenta haz clic en el menú de pestañas **Políticas** y selecciona el tipo de política **Gestión de parches**. Se mostrará una pantalla para configurar de forma centralizada el comportamiento de la gestión de parches para todos los dispositivos afectados por la política creada.

Aprobar 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 conjunto de dispositivos se lleva cabo mediante el proceso de aprobación de parches, configurado en la sección **Aprobación de parches** dentro 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:

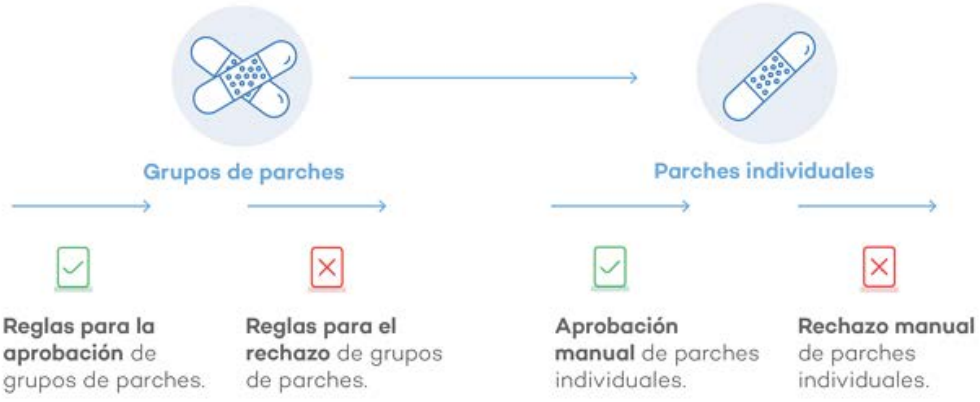


Figura 14.2: flujo de aprobación y denegación de parches

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.

Sección	Campo	Descripción
Opciones de política de gestión de parches	**Dispositivos**	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.
	Solo auditoría	Crea una política que no instala parches en los dispositivos, con el objetivo de que el administrador pueda valorar el estado de actualización del parque informático y detectar parches problemáticos antes de su descarga y aplicación.
	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. Consulta el apartado "**Programador de tareas**" en la página **134**.
	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.
Aprobación de los parches	**Criterios de instalación**	Consulta "**Criterios de aprobación y de exclusión de parches**" en la página **223**.
	No aprobar estos parches	Consulta "**Criterios de aprobación y de exclusión de parches**" en la página **223**.
	Disponibles	Consulta "**Configurar parches individuales**" en la página **224**.
	Aprobar	Consulta "**Configurar parches individuales**" en la página **224**.
	No aprobar	Consulta "**Configurar parches individuales**" en la página **224**.

Tabla 14.3: opciones de una política Patch Management

Sección	Campo	Descripción
Opciones de inicio / apagado	Inicio	Arranca los dispositivos apagados compatibles con Wake-On-Lan 10 minutos antes de la instalación de los parches
	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. 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. • **Permitir el reinicio cuando un dispositivo de almacenamiento esté conectado** para prevenir un posible arranque desde el sistema operativo almacenado en el USB. • **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. • **Mostrar recordatorio personalizado**: indicar el número de horas que transcurrirán para mostrar una nueva notificación al usuario. • **Permitir un número máximo de cancelaciones**: pasado el número definido la notificación queda fija en la pantalla del usuario.

Tabla 14.3: opciones de una política Patch Management

Aprobación de parches y creación de filtros

Para determinar los parches que se instalarán en los dispositivos y excluir aquellos que estén considerados como peligrosos o sin interés, utiliza la sección **Aprobación de parches** dentro de la configuración de una política de Gestión de parches. Para incluir o excluir un grupo de parches define en los apartados **Criterios de instalación** y **No aprobar estos parches** reglas similares a las empleadas al crear filtros de dispositivos, mostradas en el apartado "**Construcción de filtros**" en la página **84**. En este caso los atributos empleados describen las características de los parches a instalar o excluir. Adicionalmente, es posible especificar parches individuales para incluir o excluir de la instalación en la sección **Configurar parches individuales**.

Criterios de aprobación y de exclusión de parches

Los campos disponibles en la creación de un filtro tanto de aprobación como de no aprobación de parches se detallan a continuación:

Campo	Descripción
(Todos)	Selecciona todos los parches publicados.
Categoría	• **Aplicaciones**: Actualizaciones relacionas con aplicaciones que reciben novedades mediante Windows Update. • **Conectores**: Módulos que ayudan a comunicar dispositivos con servidores que ejecutan software Windows Server. • **Actualizaciones críticas**: Actualizaciones para el mantenimiento del sistema operativo no relacionadas con la seguridad. • **Actualizaciones de identificadores**: Nuevas definiciones de malware para Windows Defender. Se desactivan cuando el equipo utiliza otro antivirus. • **Drivers**: Actualizaciones de drivers. • **Packs de funcionalidades**: Actualizaciones diseñadas para unificar funcionalidades entre las versiones de Service Pack. • **Actualizaciones de seguridad**: Actualizaciones para el mantenimiento de la seguridad de los equipos. Estas actualizaciones deberían instalarse lo antes posible. • **Service packs**: Paquete con actualizaciones. • **Herramientas**: Actualizaciones de utilidades o características. • **Actualizaciones acumulativas**: Agrupación de actualizaciones individuales para componentes específicos de Windows. • **Actualizaciones**: Actualizaciones que resuelven un problema especifico que no sea de seguridad. • **Upgrades**: Actualizaciones de funcionalidades de Windows.
Descripción	Busca cadenas de texto en el campo descripción de los parches publicados.
Tamaño de la descarga	Especifica el tamaño en bytes de la descarga. Para otras medidas añadir G (gigabytes), M (megabytes) o K (kilobytes).
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	Fecha en la que Microsoft publicó el parche.

Tabla 14.4: atributos para la creación de filtros de parches

Campo	Descripción
Requiere información del usuario	Selecciona los parches que pueden requerir interacción por parte del usuario para completar su instalación (**Puede requerirla**) o no la requieren nunca (**No la requiere**).
Título	Nombre del parche.
Tipo	Selecciona el parche si es software o driver.

Tabla 14.4: atributos para la creación de filtros de parches

Configurar parches individuales

Para facilitar la búsqueda de parches individuales a incluir o excluir se muestra un listado dividido en tres grupos:

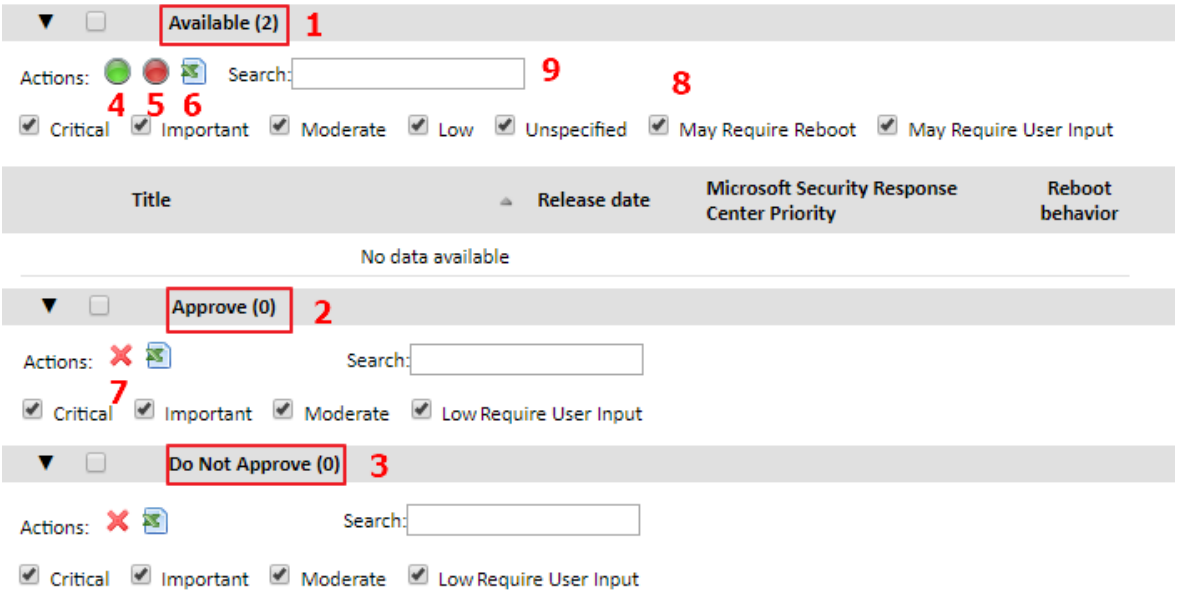


Figura 14.3: configuración de parches individuales

- **Disponibles (1)**: parches publicados sin aplicar sobre los que no se ha establecido ninguna acción todavía.
- **Aprobar (2)**: parches marcados para su instalación.
- **No aprobar (3)**: parches marcados para su exclusión.

Para marcar uno o más parches como aprobados o no aprobados utiliza la barra de iconos que se muestra al hacer clic en cada uno de los grupos disponibles.

- **Aprobar (4)**: incluye el parche para su instalación, lo elimina del grupo **Disponibles** y lo añade en el grupo **Aprobar**.
- **No aprobar (5)**: excluye el parche de su instalación, lo elimina del grupo **Disponibles** y lo añade al grupo **No Aprobar.**
- **Exportar todos los parches a csv (6)**: genera un listado de los parches seleccionados en formato CSV.

- **Quitar de la lista (7)**: en los grupos **Aprobar** y **No aprobar** este icono se utiliza para deshacer la aprobación o exclusión de parches.

Para facilitar la localización de un parche concreto se utiliza una barra de búsqueda **(8)**:

- **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 (9)**: búsqueda libre en los atributos del parche.

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. En la parte inferior de la ventana se listan las políticas de Gestión de parches creadas en el Nivel cuenta. Estas políticas incorporan el botón **Modificar**. Si la política ya ha sido modificada se mostrará un icono de color verde para reflejar el nuevo estado y el botón pasará a ser **Editar modificación**.

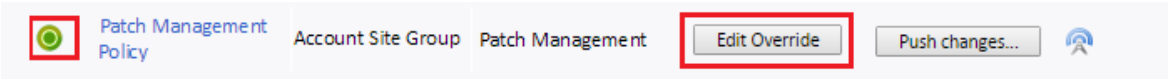


Figura 14.4: redefinición de políticas Patch Management

Al hacer clic en el botón **Modificar** o **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.

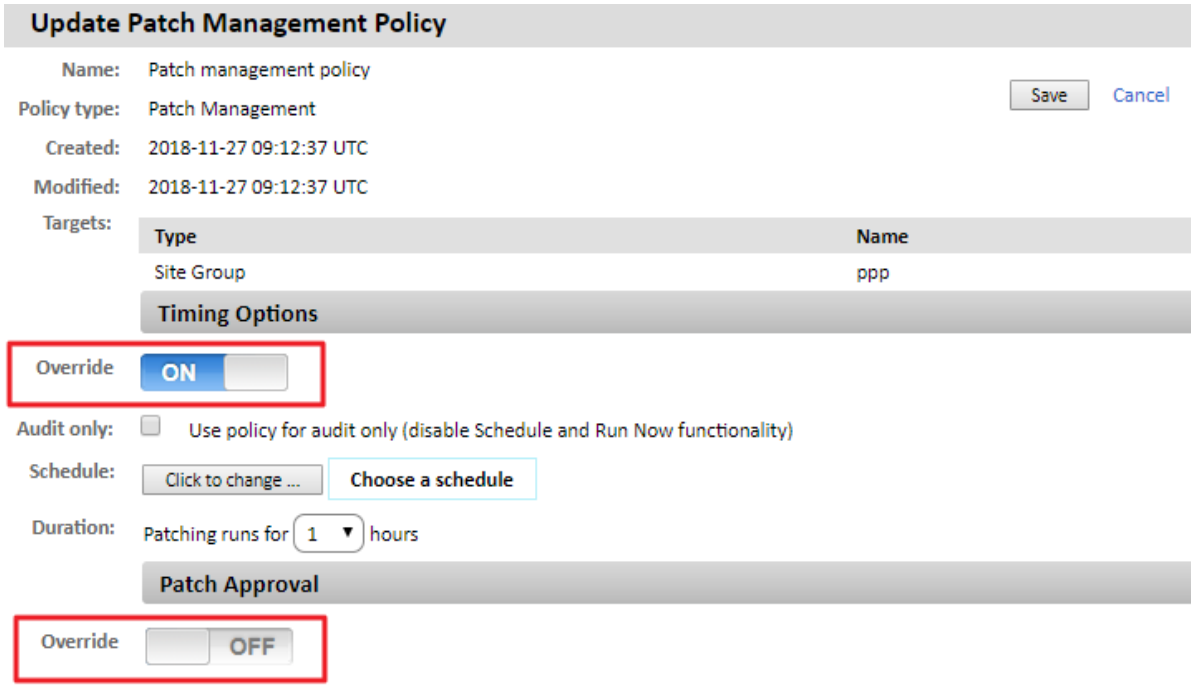


Figura 14.5: modificación en el Nivel zona de una política definida en el Nivel cuenta

Haz clic sobre los botones **Modificar** para habilitar la sobreescritura de los valores configurados originalmente.

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.

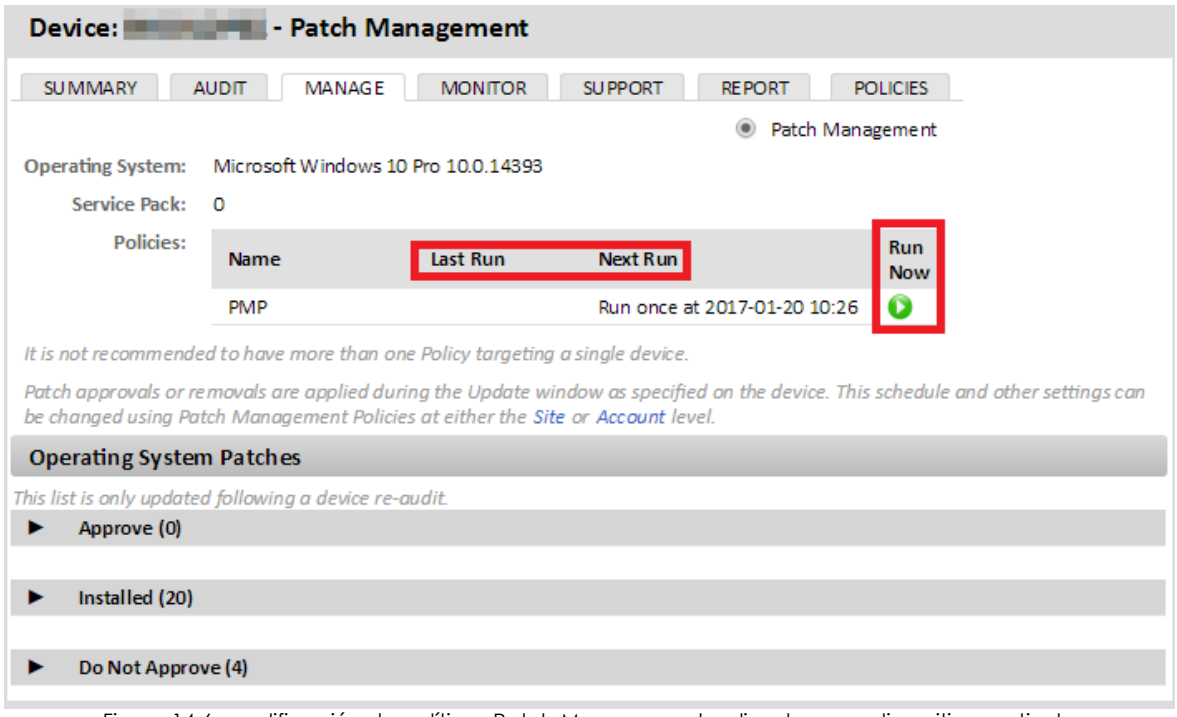


Figura 14.6: modificación de políticas Patch Management aplicadas a un dispositivo particular

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.
- **Programar**: 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.

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.

Estado de la actualización de los dispositivos

Para mostrar el estado de parcheo del parque informático, el administrador de la red tiene disponibles dos opciones:

- **Resumen**: muestra un gráfico de tarta con los porcentajes de equipos según su estado de parcheo. Para acceder al resumen haz clic en el menú superior **Zonas**, elige la zona y haz clic en el menú de pestañas **Resumen**.
- **Detalle**: muestra el mismo gráfico de tarta indicado en **Resumen** junto con un listado de los equipos administrados y su estado de parcheo, política asignada, parches instalados y otra información relevante. La información de detalle puede mostrarse en los Niveles cuenta y zona:

- Para acceder al detalle del estado de parcheo en el Nivel cuenta haz clic en el menú superior **Cuenta**, menú de pestañas **Administrar** y haz clic en el control de selección **Gestión de parches** situado en la parte superior derecha de la pantalla.
- Para acceder al detalle del estado de parcheo en el Nivel zona haz clic en el menú superior **Zonas**, elige la zona, haz clic en el menú de pestañas **Administrar** y haz clic en el control de selección **Gestión de parches** situado en la parte superior derecha de la pantalla.

Administrar el estado de la actualización de los dispositivos

La pantalla **administrar** se divide en tres zonas:

Figura 14.7: menú de pestañas Administrar con la información del estado del parcheo

- **Gráfico de tarta (1)**: indica en porcentajes los dispositivos actualizados y con parches pendientes de instalación.
- **Listado de dispositivos (2)**: muestra el estado de los equipos con respecto a su estado de parcheo.
- **Listado de políticas asignadas (3)**: ayuda a localizar las policías de tipo Gestión de parches asignadas a los dispositivos.

Gráfico de tarta Estado de parcheo (1)

Permite visualizar los porcentajes de equipos en sus diferentes estados a través de las series mostradas a continuación:

- **Sin política**: porcentaje y número de equipos que no tienen una política de gestión de parches

asignada.

- **Sin información**: no existen datos de auditoria de parches disponibles.
- **Necesita reinicio**: dispositivos con parches descargados pero que requieren un reinicio para completar su instalación.
- **Error de instalación**: dispositivos con errores en la instalación de parches.
- **Aprobación pendiente**: dispositivos con parches que no han sido instalados por estar pendiente su aprobación.
- **Actualizado**: dispositivos completamente actualizados.

Listado de dispositivos (2)

Muestra un listado de todos los dispositivos de la cuenta o de la zona elegida. Se incluye información del estado de parcheo, una barra de filtrado y otra de búsquedas para agilizar la localización de dispositivos con estados concretos. El listado permite configurar las columnas mostradas mediante el icono  . Los campos específicos de estado de parcheo se muestran a continuación:

- **Política**: nombre de la política Gestión de parches asignada al dispositivo.
- **Última ejecución**: última vez que la política Gestión de parches fue ejecutada en el dispositivo.
- **Programación:** frecuencia de ejecución de la política Gestión de parches asignada al dispositivo.
- **Estado de parcheo: Sin política**, **Sin información**, **Es necesario reiniciar**, **Error de instalación**, **Aprobación pendiente**, **Actualizado**.
- **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.
- **Parches instalados**: número de parches instalados en el equipo.
- **Parches no aprobados:** parches excluidos de la instalación por la política asignada.
- **Ultimo reinicio**: muestra la fecha en la que se reinició el equipo.
- **Necesita reinicio**: indica si el equipo está pendiente de un reinicio para completar la instalación.

La información mostrada en esta tabla se actualiza en cada auditoría ejecutada sobre los dispositivos. Para actualizar los datos mostrados selecciona los dispositivos a auditar y haz clic en el icono  *de la barra de iconos.*

La barra de búsqueda permite **(4)** filtrar los dispositivos según los criterios mostrados a continuación:

- **Política de cuenta / zona**: muestra los dispositivos asignados a la política seleccionada.
- **Tipo**: muestra los dispositivos según su tipo (**Todos**, **Estación Windows**, **Servidores Windows**).
- **Estado de parcheo**: **Todos**, **Sin política**, **Sin información**, **Es necesario reiniciar**, **Error de instalación**, **Parches pendientes aprobados**, **Completamente parcheado.**

- **Campo de búsqueda**: filtra los dispositivos según el contenido de sus atributos.

Listado de las políticas asignadas (3)

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 (5):** 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.
- **Programar**: frecuencia de ejecución de la política Gestión de parches asignada al dispositivo.
- **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.
- 

: activa o desactiva la política para la zona / cuenta.

Tabla comparativa de métodos de Patch Management

Método	Nivel de detalle de 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 14.5: comparativa de políticas de aplicación de parches disponibles en Panda Systems Management

Capítulo 15

Distribución e 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.

CONTENIDO DEL CAPÍTULO

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 macOS.

> *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 "**Componentes y ComStore**" en la página **139**, los componentes de tipo 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 es necesario crear un componente independiente.

Procedimiento para distribuir e instalar paquetes

El procedimiento general consta de varios pasos:

1. Determina 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 Panda Systems Management 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. Comprueba si el software a distribuir está publicado en la ComStore

- Haz clic en el menú general **ComStore**, la tienda gratuita de aplicaciones y componentes de Panda Security.
- En el panel lateral **ComStore** haz clic en **Aplicaciones**. El panel de la derecha se actualizará con un listado de las aplicaciones disponibles.
- Localiza la aplicación `Firefox Multi-lingual [WIN]` y haz clic sobre ella. Se mostrará una ventana con la descripción del componente.
- Al hacer clic en el botón añadir a mi **Biblioteca de componentes**, Panda Systems Management lo descargará en el repositorio de componentes del administrador, situado en el área **Componentes**. Este paso es necesario para poder utilizar cualquier componente publicado en la ComStore.
- Haz clic en el menú general **Componentes** para comprobar que aparece `Firefox Multi-lingual [WIN]` en el listado.

Una vez añadido el componente al repositorio del administrador es necesario crear una tarea para distribuir el paquete de instalación entre todos los dispositivos. Consulta el capítulo "**Tareas**" en la página **129** para obtener más información.

3. Genera un componente de instalación de software

Si el software a distribuir no está publicado en la ComStore es necesario crear un componente de distribución de software. Los pasos involucrados son los mismos que los descritos en el apartado "**Desarrollo de componentes**" en la página **145** para la creación de componentes de tipo script o monitor.

4. Lanza una tarea para enviar el componente de instalación al agente PCSM 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.

5. Recoge 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.

Ejemplos de despliegue

Para ilustrar la distribución de software se proponen varios 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 incluidos, así como las herramientas de terceros utilizadas y lenguajes de script se muestran a modo de ejemplo y pueden cambiar. Panda Systems Management está diseñado para ser flexible y adaptarse a las herramientas con las que el administrador se encuentre más cómodo.

Distribución de documentos mediante lenguajes de script

> *En este capítulo se utilizará el script Deploy_documents.vbs. El código fuente se encuentra disponible en el capítulo "**Código fuente**" en la página **321**.*

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. Determina los dispositivos sobre los que se distribuirán los ficheros

Panda Systems Management no tiene visibilidad sobre el contenido del sistema de ficheros de los dispositivos de los usuarios de modo que el paquete de instalación se distribuirá entre todos los dispositivos que potencialmente requieran los documentos y será el propio script (líneas 25-32) el que compruebe si la carpeta con los ficheros ya existía o no.

```
Set objFSO=CreateObject ("Scripting.FileSystemObject")
Set WshSysEnv=WshShell.Enviroment ("Process")
Set obj.Folder=objFSO.GetFolger(WshSysEnv("USERDESKTOP") & WshSysEnv("PCSM PATH")

If err.number<>0 Then
     WScript.Echo "Deploy unsuccesful: The folder already exist"
     WScript.Quit(1)
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). Si la carpeta ya existía se asume que los documentos ya han sido distribuidos y se termina el script con error.

```
'the folder will be create in the user's desktop
Set objFolder = objFSO.CreateFolder(WshSysEnv("USERDESKTOP")& WshSysEnv("PCSM
PATH")
'the documents will be moved to the folder
objFSO.MoveFile "docl.docs", objFolder.Path & "\docl.docx"
If Err.Number<> 0 Then
   'Wscript.Echo "Deploy unsuccessful: " & Err.Description
    WScript.Quit (1)
Else
    Wscript.Echo "Deploy OK: All files were copied"
    WScript.Quit (0)
End If
```

2. Genera un componente de distribución de ficheros mediante script

- En el menú general **Componentes** haz clic en el botón **Nuevo componente** situado en el panel lateral izquierdo:
- Selecciona la categoría **Aplicación** e introduce un nombre y descripción.
- Haz clic en el botón **Añadir archivo** y añade los tres ficheros que se van a distribuir.
- Añade en la sección **Comandos** el código fuente del apartado "**Deploy Files**" en la página **323** y selecciona en el desplegable **Comando de instalación** la opción **VBScript**.

- En la sección **Variables** haz clic en el icono e indica en el campo **Nombre** el nombre de la variable que contendrá la ruta de la carpeta a distribuir, en este caso `PCSM_PATH`. En el campo **Tipo** elige **Valor**, en **Predeterminado** la cadena que se utilizará en caso de que el administrador no indique nada en el proceso de lanzamiento del script, y en **Descripción** un texto explicativo del objetivo de la variable.
- Haz clic en el botón **Guardar.**

El componente configurado de esta forma ejecutará el script que será el encargado de comprobar si no existe la carpeta de documentos en el equipo del usuario, y en su caso la creará y moverá los tres documentos. Este proceso se ejecutará en todos los dispositivos que reciban el componente de distribución.

En la zona de **Condiciones posteriores** se indican cadenas de texto que son 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 unsuccessfull`, el resultado de la ejecución del script será considerado como aviso.

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

Consulta el capítulo "Tareas" en la página 129 para obtener más información sobre cómo crear tareas inmediatas y programadas.

- Haz clic en el menú general **Tareas** y en el menú de pestañas **Nueva tarea**.
- Haz clic en el botón **Añadir dispositivos** para seleccionar los destinatarios de la tarea.
- Haz clic en el link **Añadir componente**. Se mostrarán todos los componentes de tipo aplicación marcados como favoritos.
- Haz clic en **Guardar**.

4. Recoge 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 44-45). Se termina con un `Errorlevel 0`.
- **Error**: se produce algún error en la copia de ficheros. Se termina con un `Errorlevel 1` (línea 42).
- **Éxito - Advertencia**: la carpeta ya existe, de forma que los ficheros no se copian. Se termina con un `Errorlevel 1` (línea 31) 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.

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

Para ver el resultado del despliegue haz clic en el menú general **Tareas**, menú de pestañas **Tareas completadas**. Se mostrará una barra 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.

Distribución de documentos sin lenguajes de script.

El script de instalación se simplifica si no son necesarias comprobaciones previas ni generación de advertencias en la consola.

En este caso se distribuyen los tres 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:\documentacion`.
- Si la carpeta existe previamente se sobrescribe 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.

1. Determina los dispositivos sobre los que se distribuirán los ficheros

Sigue los pasos detallados en el punto 1 del apartado "**Distribución de documentos mediante lenguajes de script**".

2. Genera un componente de distribución de ficheros

Sigue los pasos detallados en el punto 2 del apartado "**Distribución de documentos mediante lenguajes de script**". En este caso, el componente necesitará una secuencia de comandos simple, de modo que en el campo **Comando de instalación** elige Batch e introduce la siguiente información.

```
@echo off

pushd %~dp0

nombre_del_fichero_autoextraible.exe
```

Tampoco es necesario definir variables de entrada o de salida ya que la ruta donde se copiarán los ficheros se define en el propio paquete extraíble.

Crea un fichero auto extraíble

Sigue los pasos mostrados a continuación para generar un fichero autoextraíble silencioso:

- **Prepara la carpeta con los documentos a distribuir**

Crea la carpeta raíz `c:\documentación`, y en su interior coloca todos los ficheros, carpetas y subcarpetas que se necesiten distribuir.

- **Genera el ejecutable**

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

- **Configura el comportamiento del ejecutable**

En este punto establecemos que el fichero se ejecutará en modo silencioso, por lo que no preguntará nada al usuario y sobrescribirá todos los ficheros en caso de que ya existan en el equipo.

- En la pestaña **Avanzado** haz clic en el botón **Autoextraíble**.
- En la pestaña **Modos**, sección **Mostrar**, elige la opción **Ocultar todo**.
- En la pestaña **Actualizar**, sección **Modo de actualización** elige **Extraer y reemplazar ficheros**.
- En la pestaña **Actualizar**, sección **Modo de sobreescritura** elige **Sobrescribir todos los ficheros**.
- Haz clic en **Aceptar**.
- En la pestaña **General** indica la ruta donde se descomprimirán los ficheros en **Carpeta de extracción.**

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

Sigue los pasos detallados en el punto 3 del apartado "**Distribución de documentos mediante lenguajes de script**".

4. Recoge el resultado del despliegue para determinar posibles fallos

Sigue los pasos detallados en el punto 4 del apartado "**Distribución de documentos mediante lenguajes de script**".

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**, control de selección **Software** en un dispositivo que ya tenga instalado el paquete.

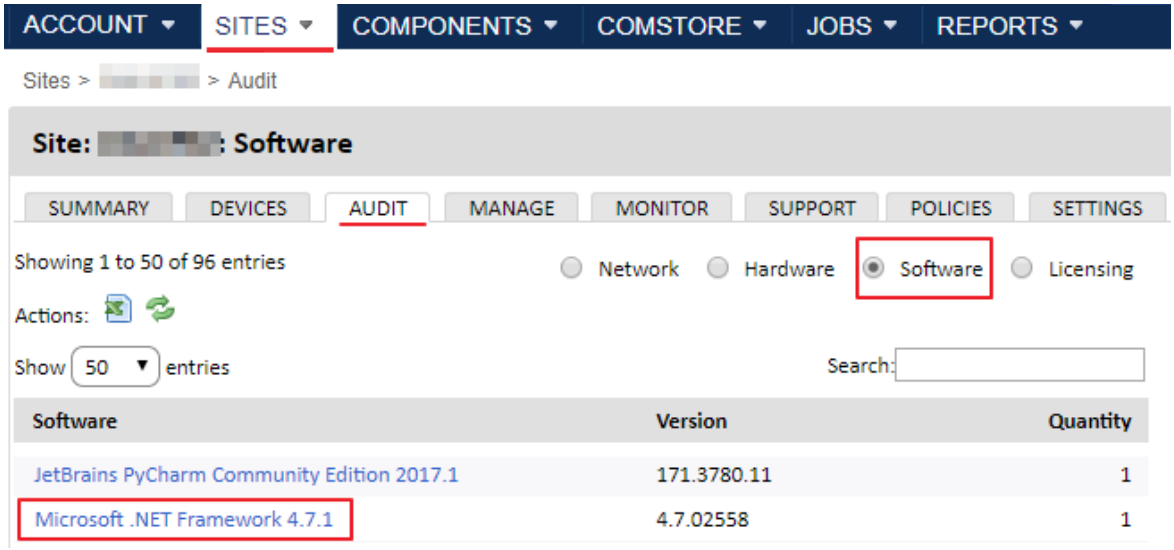


Figura 15.1: obtención de la cadena de identificación del paquete instalado

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

*Consulta el capítulo "**Crear un filtro de zona**" en la página **83** para obtener más información sobre la creación y gestión de filtros.*

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

2. Genera un componente de distribución de ficheros

Sigue los pasos detallados en el punto 2 del apartado "**Distribución de documentos mediante lenguajes de script**". Como en este caso el paquete software requiere parámetros para instalarse en modo quiet es necesario pasárselos en el campo **Comando de instalación**. En este caso elige como lenguaje de script **Batch**:

```
@echo off
```

```
pushd %~dp0

dotNetFx40_Full_x86_x64.exe /q /norestart
```

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 enviar el software al agente PCSM de los dispositivos

Sigue los pasos detallados en el punto 3 del apartado "**Distribución de documentos mediante lenguajes de script**" pero en el campo **Tipo de agrupación** selecciona **Filtros de cuenta** y elige el filtro creado en el paso 1.

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 iconos.*

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 Panda Systems Management generar una auditoria de programas instalados fiable.

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 `Eee to Msi Converter`, que en su versión gratuita nos permite generar instaladores MSI de forma simple.

> *Para descargar la versión gratuita de Exe to Msi Converter free visita la página: https://www.exemsi.com/*

Para generar el instalador sigue los siguientes pasos:

1. Determina los dispositivos sobre los que se distribuirán los ficheros

Sigue los pasos detalladas en el punto 1 de la sección "**Distribución de documentos mediante lenguajes de script**". En este caso la entrada que aparecerá en Añadir / Quitar programas será conocida de antemano, ya que el programa `Exe to Msi Converter Free` nos permite configurar el nombre del programa que aparecerá en esta sección, por lo que podremos indicarla directamente en el campo **Búsqueda** del filtro.

2. Genera un componente de distribución de ficheros mediante un instalador msi

Sigue los pasos detallados en el punto 2 de la sección "**Distribución de documentos mediante lenguajes de script**". Como en este caso el paquete software requiere parámetros para instalarse en modo silencioso es necesario indicarlos en el campo **Comando de instalación**. En este caso elige como lenguaje de script **Batch**:

```
@echo off

pushd %~dp0

MSIEXEC /I "my software.msi" /qn
```

Crea un fichero auto msi

Sigue los pasos mostrados a continuación para generar un fichero autoextraíble silencioso:

- Ejecuta el programa `Exe to Msi Converter Free` y haz clic en **Siguiente**.
- En la pantalla **Executable** Introduce el nombre del ejecutable en la caja de texto **Setup Executable Input file Name, i**ntroduce el nombre y la ruta del fichero `.msi` a generar en la caja de texto **MSI Output File Name** y haz clic en **Siguiente**.
- En la pantalla **Security and User Context** haz clic en el botón **Siguiente**.
- En la pantalla **Applications id** haz clic en el botón **Create new** y haz clic en **Siguiente**.
- En la pantalla **Properties** indica el **Product name Manufactuer** y **Version** en formato `x.x.x.x`. Estos datos son los que se mostrarán en el apartado Agregar / quitar programas de Windows.
- En la pantalla **More properties** haz clic en el botón **Siguiente**.
- En la pantalla **Parameters** haz clic en el botón **Siguiente**.
- en la pantalla **Actions** haz clic en el botón **Siguiente**.

- En la pantalla **Summary** haz clic en **Build**. El fichero `.msi` se generará en la ruta especificada.

3. Lanza una tarea para enviar el software al agente PCSM de los dispositivos

Sigue los pasos detallados en el punto 3 de la sección "**Distribución de documentos mediante lenguajes de script**" pero en el campo **Tipo de agrupación** selecciona **Filtros de cuenta** y elige el filtro creado en el paso 1.

4. Recoge el resultado del despliegue 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 iconos.*

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.*

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`.

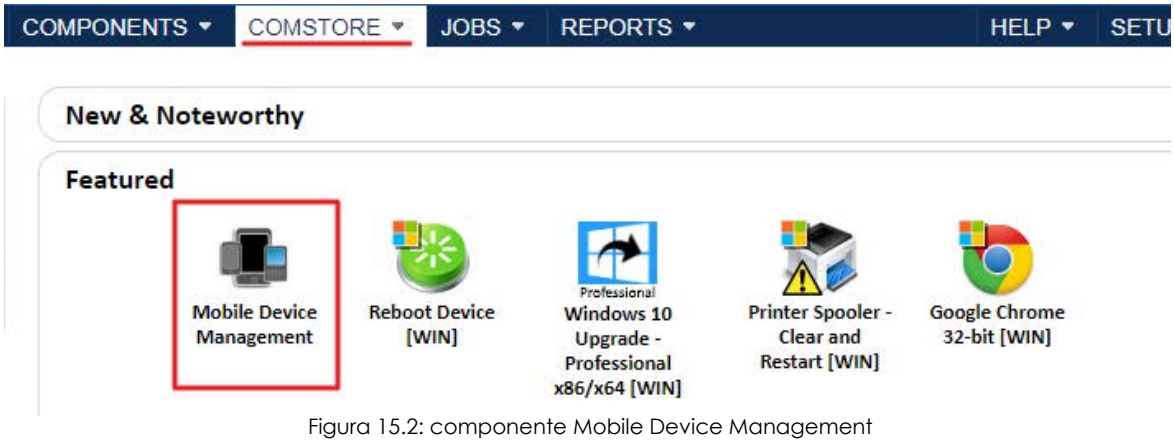


Figura 15.2: componente Mobile Device Management

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

Instalación de 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  .

Capítulo 16

Gestión del software

Mantener actualizadas las aplicaciones instaladas en los equipos de los usuarios es una de las tareas principales del departamento de IT en las empresas. Muchas aplicaciones y librerías de uso diario contienen fallos y vulnerabilidades utilizados por virus y amenazas, que los proveedores solucionan actualizándolas periódicamente.

Panda Systems Management permite mantener actualizadas las aplicaciones compatibles instaladas en los equipos gestionados de la red sin interacción por parte del usuario ni del administrador. Además, podrá localizar rápidamente dispositivos que no cumplan con la política de software definida y aprobar actualizaciones de software de forma inmediata.

El administrador no necesitará comprobar de forma manual el lanzamiento de nuevas versiones de los programas utilizados por los usuarios con el módulo de Gestión del software, ni crear o actualizar componentes para distribuirlas. Así mismo, obtendrá una instantánea del estado de los equipos, identificando de forma rápida aquellos que no cumplen con las políticas de software establecidas.

Gracias a estos beneficios se producirá un ahorro de tiempo y una simplificación en la gestión de la red de la empresa al tiempo que se mejora la seguridad de las aplicaciones instaladas.

CONTENIDO DEL CAPÍTULO

Flujo general de trabajo con Gestión de software

Para gestionar de manera sencilla y segura todo el catálogo de aplicaciones críticas de los equipos de la red, el flujo de trabajo del administrador será, a grandes rasgos, el siguiente:

- El administrador crea la política de gestión de software en base a la estrategia a seguir. Consulta el apartado "**Política Gestión de software**".
- Dependiendo del comportamiento seleccionado para la aprobación de actualizaciones, especificado en la tabla **16.3**:
  - Panda Systems Management aprobará e instalará las actualizaciones automáticamente.
  - Panda Systems Management requerirá la aprobación manual de las actualizaciones mediante el botón que aparece en el listado de aplicaciones del panel de gestión de software.
- El administrador comprobará la conformidad de los equipos de la red con respecto a las políticas de gestión de software configuradas. Consulta el apartado "**Visualización del estado de la gestión de software**" y el apartado "**Creación de informes de Gestión de Software**".

Funcionamiento del módulo gestión del software

Características

El módulo cumple con tres funciones principales:

- **Gestión de actualizaciones de software de terceros:** mantiene los equipos actualizados con las últimas versiones de frameworks y aplicaciones.
- **Aprobación de actualizaciones**: configura el modo de instalación para realizarlas de manera desatendida o manual.
- **Informes de cumplimiento integrados:** muestran si los equipos gestionados tienen las últimas versiones de aplicaciones y frameworks.

Funcionamiento

De forma autónoma Panda Systems Management busca las actualizaciones de las aplicaciones instaladas y permite establecer su aprobación de forma automática o manual. El módulo también permite instalar el software de manera desatendida de forma inmediata cuando se detecta una nueva versión, o programando su instalación en otro momento. Consulta "**Crear una política de Gestión de software**" para saber más.

Aplicaciones compatibles

El principal objetivo del módulo de Gestión de software es garantizar que los equipos de la red cuentan con la última versión disponible del software instalada.

Además, Panda Security monitoriza las aplicaciones e incorpora un proceso de calidad para asegurar su correcta instalación. Así, las aplicaciones estarán disponibles para su actualización en un intervalo máximo de 48 horas y en el idioma del equipo del usuario.

El módulo de Gestión de software es compatible con las siguientes aplicaciones:

Aplicaciones	Windows	macOS
7-Zip	SI	
Adobe Acrobat Reader DC	SI	SI
Adobe Air	SI	SI
Adobe Flash Player	SI	SI
Adobe Shockwave Player	SI	
Datto File Protection	SI	SI
Datto Workplace Classic	SI	SI
FilleZilla Client	SI	SI
Foxit Reader	SI	
Google Chrome	SI	SI
Java Runtime Enviroment	SI	SI
Microsoft Office 365	SI	
Mozilla Firefox	SI	SI
Notepad ++	SI	
Paint.NET	SI	
PUTTY	SI	
Skype	SI	SI
VLC Media Player	SI	SI
VMWare Tools	SI	
Zoom	SI	

Tabla 16.1: aplicaciones compatibles con el módulo Gestión de software

Esta lista está en continuo desarrollo. Si precisas algún programa nuevo ponte en contacto con Panda Security.

El funcionamiento del módulo Gestión de software es independiente de la Comstore. El administrador no deberá desplegar el software mediante componentes ni verificar la existencia de nuevas versiones que le obliguen a modificarlos.

Requisitos del módulo gestión del software

Configuración del firewall

Panda Systems Management busca las actualizaciones de los programas en las páginas web de los proveedores, por ello es necesario que el firewall corporativo y el instalado en el propio dispositivo permitan el acceso y la descarga de contenidos desde estas páginas, a fin de que no bloqueen la descarga de la actualización.

Aplicación	URL
Adobe Acrobat Reader DC	https://storage.centrastage.net
Deploy F-Secure Computer Protection	https://download.sp.f-secure.com
FileZilla Client	https://filezilla-project.org
Foxit Reader	https://www.foxitsoftware.com
Mozilla Firefox	https://download.mozilla.org
Notepad ++	https://notepad-plus-plus.org
Paint.NET	https://www.dotpdn.com
PuTTY	https://the.earth.li
Skype	https://get.skype.com
Trend Micro Worry-Free Services-Deployment	https://wfbs-svc-nabu-aal.trendmicro.com o https://wfbs-svc-emea-aal.trendmicro.com
VLC Media Player	https://www.mirrorservice.org
Windows 10 Upgrade - Professional x86/x64	Windows 10 Upgrade - Professional x86/x64 https://storage.centrastage.net

Tabla 16.2: URLS de actualización de las aplicaciones soportadas

Plataformas soportadas

Las plataformas compatibles con el módulo Gestión del software son:

- Windows (32 y 64 bits)

- macOS

> *Consulta el apartado "**Aplicaciones compatibles**" para obtener un listado de las aplicaciones soportadas por el módulo Gestión de software.*

Permisos

Dependiendo del nivel desde donde se ejecute la política de Gestión de Software, puede ser necesaria la creación de permisos. Consulta la sección "**Cuentas de usuario y roles**" en la página **297**.

Política Gestión de software

Al crear una cuenta nueva de Panda Systems Management, se genera una política de tipo Gestión de software de forma automática. Consulta "**Políticas**" en la página **97** para obtener más información sobre el sistema de políticas de Panda Systems Management.

Concepto de Equipo conforme y Equipo no conforme

Los dispositivos gestionados en una política del módulo de Gestión de software pueden tener tres estados diferentes:

- **No administrado**: cuando no se aplica ninguna política de Gestión de Software sobre el dispositivo.
- **No Conforme**: cuando una o más aplicaciones soportadas tiene el estado de No conforme. Esto sucede cuando el dispositivo no tiene instalada la última versión disponible.
- **Conforme**: cuando todas las aplicaciones gestionadas por la política tienen instalada la última versión disponible.

Crear una política de Gestión de software

Para crear una política de gestión de software sigue los pasos mostrados a continuación:

- 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** y en la zona donde se quiere aplicar, haz clic en el menú de pestañas **Políticas** y en el botón **Nueva política de zona** situado en la parte inferior de la ventana.
- Indica en la caja de texto **Nombre** el nombre de la política y en el desplegable **Tipo** selecciona **Gestión de Software**. Haz clic en el botón **Siguiente**.
- En la ventana de creación de políticas añade los **Dispositivos** sobre los que se aplicará y el **Momento de ejecución**. Elige si las actualizaciones se instalarán **inmediatamente** o **según lo programado**. Consulta "**Lanzar tareas programadas**" en la página **133** para obtener más información sobre el programador de tareas.

- En el listado de las aplicaciones administradas enumeradas en la tabla **16.1** selecciona cómo se actualizará cada una de ellas:

Acción	Descripción	Informe de cumplimiento
No administrada	Seleccionado por defecto. Panda Systems Management no instalará ni actualizará la aplicación.	La aplicación siempre se considera conforme.
Aprobación manual	El administrador debe aprobar manualmente las actualizaciones individuales para esta aplicación a medida que estén disponibles. Si la aplicación aún no está instalada, no se instalará.	La aplicación se considera conforme cuando está ausente o cuando está instalada y actualizada.
Aprobación e instalación manual si no está presente	El administrador debe aprobar manualmente las actualizaciones individuales para esta aplicación a medida que estén disponibles. Si la aplicación no está instalada, debe aprobar su instalación.	La aplicación se considera conforme solo cuando está presente y actualizada.
Aprobación automática	Panda Systems Management actualizará automáticamente la aplicación sin requerir aprobación. Si la aplicación aún no está instalada, no se instalará.	La aplicación se considera conforme cuando está ausente o cuando está instalada y actualizada.
Aprobación e instalación automática si no está presente	Panda Systems Management actualizará automáticamente la aplicación sin requerir aprobación. Si la aplicación no está instalada, se instalará automáticamente.	La aplicación se considera conforme solo cuando está presente y actualizada.

Tabla 16.3: opciones de aprobación de una política de Gestión de software

- Haz clic en **Guardar.** La política creada aparecerá en las listas de políticas de **Cuenta** o **Zona**, dependiendo de donde se haya creado.

- Para ejecutarla, selecciona la opción **Desplegar cambios**  , que se encuentra junto a ella.

Una vez aprobada la instalación de una actualización esta acción no puede revertirse. Para evitar la instalación de aplicaciones con aprobación es necesario editar la política.

Visualización del estado de la gestión de software

> *Aunque los cambios de estado del software se muestran inmediatamente en las páginas de Gestión de software, en las auditorías estos cambios pueden tardar hasta 24 horas en verse reflejados.*

Panel de visualización

Para acceder desde el Nivel cuenta:

- En el menú general selecciona **Cuenta** y después en la barra de pestañas **Administrar**. Con el control de selección accede al panel de **Gestión de software** para ver el estado de gestión de software.

Para acceder desde el Nivel zona:

- En el menú general **Zonas** elige la zona y haz clic en la barra de pestañas **Administrar**. Con el control de selección abre el panel de **Gestión de software (1).**

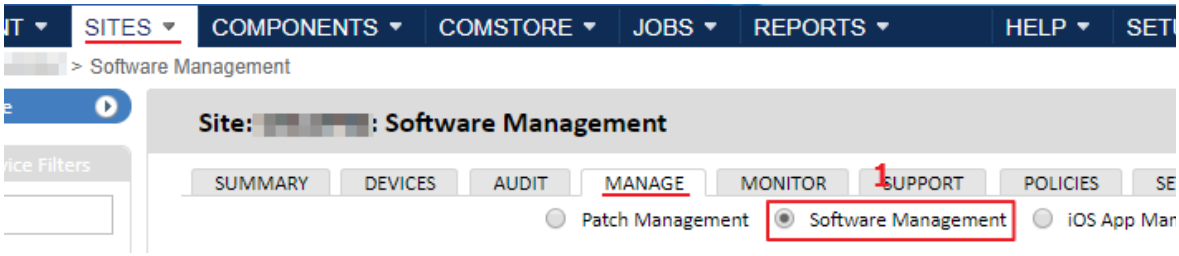


Figura 16.1: ruta de acceso a Gestión de software en nivel de Zona

El panel de visualización consta de los elementos siguientes:

- **Gráfico de tarta (1)**: muestra el número de conformes y no conformes de los dispositivos gestionados por la política.
  - **Total**: número de dispositivos recogidos en la política.
  - **Conforme**: número de las aplicaciones cuyo estado es conforme.
  - **No conforme**: número de aplicaciones cuyo estado es no conforme.
- **Barra de búsqueda (2):** permite filtrar y mostrar los dispositivos según los parámetros introducidos.
- **Listados de dispositivos (3):** listado de todos los dispositivos gestionados por la política.

- **Listados de aplicaciones (4):** listado de todas las aplicaciones gestionadas por la política.

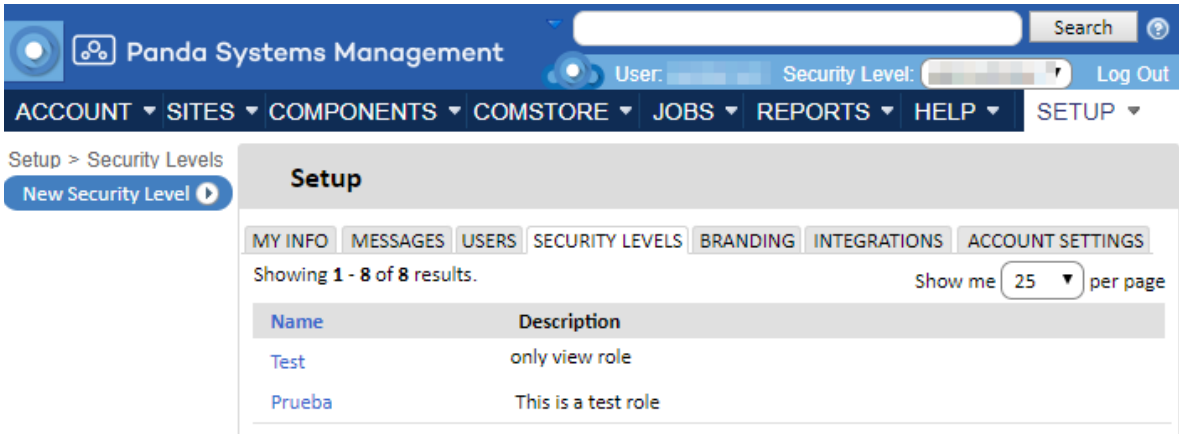


Figura 16.2: vista general del panel

Barra de búsqueda

Al utilizar diferentes criterios para realizar la búsqueda se pueden filtrar los resultados mostrados para obtener los equipos sobre los que se quiere trabajar.

Campo	Descripción
Política	Listado de políticas de gestión de software. Las políticas a nivel de cuenta se muestran tanto a nivel de cuenta como de zona, mientras que las políticas a nivel de zona solo se muestran a nivel de zona. Por defecto, no se selecciona ninguna política.
Tipo	• Todo • Todos los Windows • Todos los Mac • Todos los servidores de Windows • Todas las estaciones de trabajo de Windows
Estado del software	• Todo • No conforme • Conforme • No administrado
Buscar	Introduce el texto y haz clic en **Buscar** para filtrar los resultados.

Tabla 16.4: elementos de la barra de herramientas

Listado de los dispositivos

Muestra los dispositivos gestionados por la política y su estado.

Campo	Descripción
Nombre de la zona	Nombre de la zona al que está asociado el dispositivo.

Tabla 16.5: elementos mostrados sobre los dispositivos a nivel de cuenta y zona

Campo	Descripción
Nombre del dispositivo	Nombre del dispositivo.
Descripción del dispositivo	Descripción del dispositivo.
Política	El nombre de la política de Gestión de software que se asocia al dispositivo.
Última ejecución	Fecha y hora en la que se ejecutó por última vez la política.
Programación	Próxima ejecución de la política de gestión de software.
Estado del software	• No administrado • Conforme • No conforme Para más información sobre los estados del software consulta el apartado "**Concepto de Equipo conforme y Equipo no conforme**".

Tabla 16.5: elementos mostrados sobre los dispositivos a nivel de cuenta y zona

Listado de las aplicaciones (Nivel cuenta y Nivel zona)

Muestra un listado de las aplicaciones compatibles, indicando las últimas versiones publicadas y la acción establecida para su aplicación.

*Consulta "**Aplicaciones compatibles**" para saber más.*

Campo	Descripción
Nombre de la aplicación	Nombre de la aplicación compatible.
Última versión	La última versión disponible de la aplicación en los sistemas operativos: • Windows 32bits • Windows 64bits • macOS
No conforme	Número de dispositivos No conforme, cuando una o más de las aplicaciones no tienen la última versión disponible instalada.
Botón de aprobación	Permite aprobar una actualización de forma manual. La aplicación se instalará inmediatamente. El botón solo está disponible en los casos en los que se haya configurado la política como **Aprobación manual** o **Aprobación e instalación manual si no está presente** y el estado de la aplicación administrada **no es compatible**. Consulta la tabla **16.3**.

Tabla 16.6: elementos del listado de dispositivos

Listado de las aplicaciones (Nivel dispositivo)

Este panel informativo es accesible desde el Nivel dispositivo, en la pestaña de **Administrar** para gestionar cada dispositivo conectado de forma individual. En este caso, la configuración del módulo varía mostrando distintos campos de información y acciones.

Campo	Descripción
Nombre	Nombre de la aplicación compatible.
Versión instalada	Versión de la aplicación instalada en el equipo.
Última versión	Última versión disponible de la aplicación.
Acción	La acción de la política de gestión de software como se especifica en los detalles de la política. Consulta "**Crear una política de Gestión de software**" en la página **251**.
Estado	Se muestra alguno de los siguientes estados: • **Cumple**: la versión instalada coincide con la última versión publicada por el proveedor del software. • **No conforme**: la versión instalada no coincide con la última versión publicada por el proveedor del software. • **No administrado**: La acción de la política se establece en No administrada para todas las aplicaciones soportadas. • **Error de instalación**: la última instalación o actualización resultó en un error.
Stdout / Stderr	Haz clic para ver el mensaje Stdout (salida estándar) o Stderr (error estándar) para ver la última actividad del dispositivo.
Botón de aprobación	Aprueba la instalación de la aplicación de software. La aplicación se instalará al instante. El botón solo está presente si la acción de política es **Aprobación manual** o **Aprobación e instalación manual si no está presente** y el estado de la aplicación administrada es **no compatible**.

Tabla 16.7: elementos del panel desde el dispositivo

Creación de informes de Gestión de Software

El sistema de gestión de software es compatible con la creación de informes a través del **Resumen Ejecutivo** y **Resumen del estado de los dispositivos**. El contenido completo y las características de los informes se pueden consultar en el capítulo "**Informes**" en la página **195**.

Resumen ejecutivo

Recoge una visión general del estado del nivel sobre el que se ha ejecutado. En total reúne seis métricas:

- Asset management

- Monitoring
- Patch Management
- Software Management
- Antivirus
- Proactive Maintenance

Resumen del estado de los dispositivos

Muestra el estado del dispositivo y es accesible desde cada dispositivo integrado en el sistema. Ofrece una visión superficial de los dispositivos analizados:

- Espacio en disco
- Memoria
- Aprobación de software
- Parches
- Antivirus
- Garantía
- Estado de conexión los últimos 30 días
- Alertas abiertas

Capítulo 17

Alertas y tickets

Los monitores comprueban de forma constante ciertos parámetros de los dispositivos que tienen asignados. Cuando estos parámetros sobrepasan los valores establecidos como referencia, el monitor emitirá una alerta o ticket para reclamar la atención del administrador sobre el problema.

CONTENIDO DEL CAPÍTULO

Ciclo de gestión de alertas y tickets

Panda Systems Management utiliza las alertas para advertir al administrador de la red la existencia de un problema en los dispositivos gestionados. De esta forma, cuando un monitor comprueba que un parámetro en un dispositivo supera los límites establecidos en la configuración, generará una alerta siguiendo las reglas mostradas a continuación:

- Una alerta se corresponde con un único equipo de la red.
- Las alertas se generan con el estado **Abierto** para indicar al administrador que existe un problema

subyacente no resuelto.

- El estado de una alerta cambia de forma automática a **Cerrado** cuando el error subyacente ha desaparecido y ha transcurrido el tiempo indicado en la configuración del monitor, en el campo **Resolución automática**.
- Para evitar tener múltiples alertas abiertas ya corregidas el administrador puede cerrarlas manualmente.
- Si un dispositivo generó una alerta ya resuelta y la condición de error se vuelve a producir, Panda Systems Management generará una nueva alerta.

Una vez generada la alerta, el administrador de la red puede acceder a su descripción y detalle para determinar las acciones correctivas a realizar, conectándose al dispositivo remotamente o reconfigurando los parámetros del monitor si resultaron ser muy estrictos. Si se están generando muchas alertas del mismo tipo es posible silenciarlas temporalmente para evitar la generación de ruido.

Una vez solucionada la alerta, ésta se puede cerrar para eliminarla del listado de alertas abiertas y así centrar la atención en las alertas que todavía pueden requerir de la intervención del administrador.

El ciclo de gestión de alertas es el siguiente:

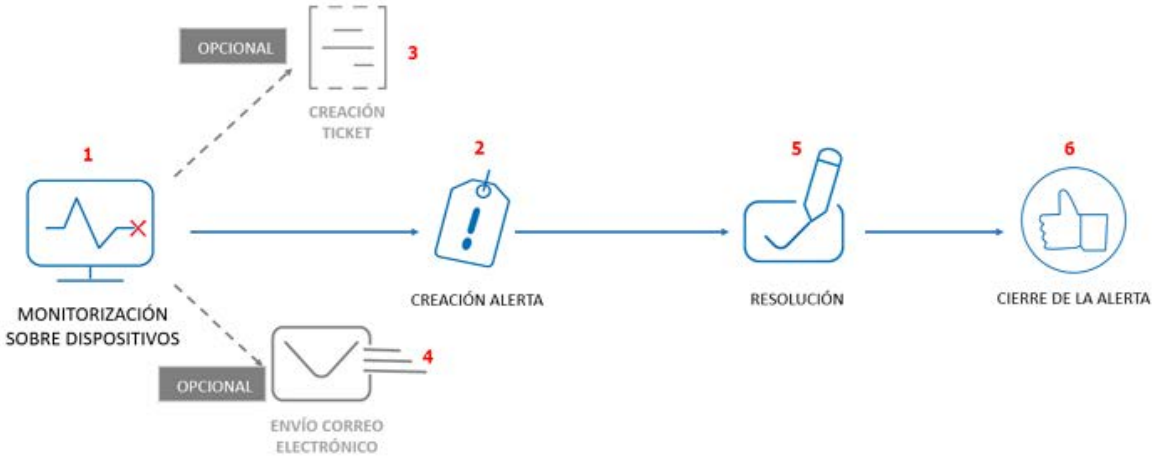


Figura 17.1: flujo de gestión de alertas en Panda Systems Management

- Un monitor detecta una condición excepcional en un dispositivo **(1)** y genera una entrada en el listado de alertas **(2)**. Dependiendo del tipo de monitor la alerta tendrá una categoría y se generará con una importancia establecida en la configuración del monitor.
- Si así está establecido en la configuración del monitor, el administrador recibe un correo **(4)** electrónico indicando la existencia de una nueva alerta y se genera un ticket **(3)**. Los correos electrónicos cuentan con un enlace al identificador de la alerta.
- El administrador accede a la consola para obtener el detalle de la alerta (importancia, tipo, dispositivos involucrados, monitor asociado y otra información adicional).
- Si se están generando múltiples alertas del mismo tipo el administrador puede evitar temporalmente el envío de correos silenciando la alerta. No obstante las alertas se seguirán añadiendo en el listado de alertas.

- El administrador ejecuta las medidas de resolución necesarias **(5)** (consulta el capítulo "**Herramientas de acceso remoto a dispositivos**" en la página **271**) o modifica el monitor para rebajar los límites configurados previamente.
- El administrador o el sistema cierra la alerta de forma manual **(6)** y reactiva el envío de correos por si la alerta se vuelva a producir en el futuro. El administrador puede haber configurado la generación de alertas en modo resolución automática, esto implica que una alerta se cerrará de forma automática cuando haya pasado el tiempo especificado en la configuración del monitor asociado.

Alertas

Configuración de alertas

Solo las políticas de tipo monitor pueden generar alertas y se configuran en el propio monitor. Consulta el apartado "**Configuración manual de monitores**" en la página **112** para iniciar la configuración de una política de tipo monitor.

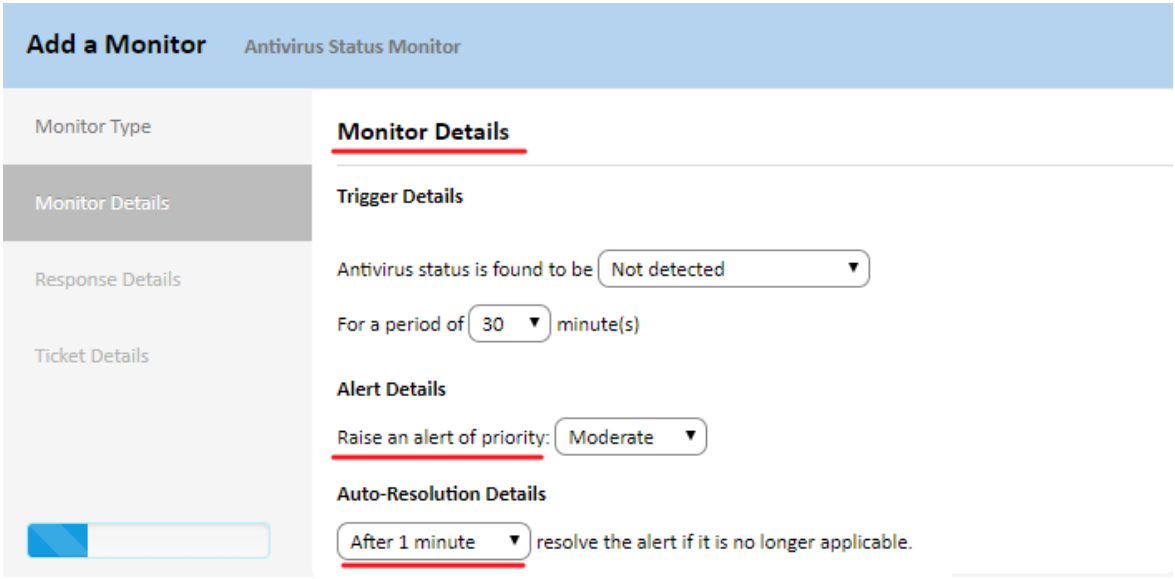


Figura 17.2: configuración de una alerta

En la pantalla **Información del monitor** especifica los parámetros siguientes:

- **Información de alertas. Generar alertas de prioridad**: indica la prioridad de las alertas generadas por el monitor. Esta prioridad podrá usarse posteriormente a la hora de ordenar y filtrar las alertas pendientes.
- **Resolución automática**: especifica el intervalo de tiempo que tiene que pasar para que la alerta se cierre de forma automática si la situación que la provocaba ha desaparecido.

Gestión de alertas

Límites en el envío de alertas

Para evitar la generación masiva de alertas, cada monitor configurado tiene establecido un límite de 10.000 alertas por dispositivo y día. Una vez alcanzado este límite, se ejecutan las acciones siguientes:

- El monitor se desactiva automáticamente para el dispositivo que ha superado el límite. Se configurará automáticamente en OFF el botón ON/OFF asociado al monitor visible en la barra de pestañas **Políticas**. Consulte "**Gestión de monitores**" en la página **126**.
- Se envía un correo electrónico de notificación a todos los administradores (máx. 50 usuarios) para informar del nuevo estado del monitor y la causa de su desactivación.

Visualizar las alertas generadas

Para mostrar un listado de las alertas generadas accede a la pestaña **Monitorizar** en los distintos niveles disponibles dependiendo del alcance de la información a obtener:

- Para mostrar un listado de las alertas generadas en toda la cuenta:
  - Haz clic en el menú general **Cuenta** y en el menú de pestañas **Monitorizar**.
  - En el control de selección situado en parte superior derecha de la ventana, haz clic en la opción **Alertas de monitorización**.
- Para mostrar un listado de las alertas generadas en una zona:
  - Haz clic en el menú general **Zonas,** y en la zona.
  - En el menú de pestañas haz clic en **Monitorizar**.
- Para mostrar un listado de las alertas generadas en un único dispositivo:
  - Haz clic en el menú general **Zonas** y en la zona.
  - Haz clic en el menú de pestañas **Dispositivos** y en el dispositivo mostrado en el listado.
  - Haz clic en el menú de pestañas **Monitorizar** y en el control de selección situado en la parte superior derecha de la ventana la opción **Alertas de monitorización**.

Visualizar el detalle de una alerta

Haz clic en una alerta para mostrar la ventana de detalle.

Las opciones disponibles son:

Sección	Campo	Descripción
Resumen del dispositivo	Nombre del host	Nombre del dispositivo que desencadenó la alerta.
	Zona	Zona a la que pertenece el dispositivo.
	Sistema operativo	Nombre y versión del sistema operativo instalado en el dispositivo.
	Marca/modelo	Proveedor y modelo del hardware.
	Último usuario	Nombre de la cuenta que inició sesión en el equipo por última vez.
	Campo personalizado 1-30	Contenido de los campos personalizados si el componente asociado al monitor hace uso de los mismos. Consulta el apartado "**Etiquetas y campos personalizados**" en la página **153** para obtener más información.
	Descripción	Descripción asociada al dispositivo.
	Dirección IP	Dirección IP de la interface de red del dispositivo.
	Arquitectura	32 bits o 64 bits.
	Número de serie	
	Dominio	Dominio Windows al que pertenece el equipo.
Resumen de la alerta	UID de la alerta	Identificador único de la alerta.
	Política	Nombre de la política que contiene el monitor que generó la alerta. Al hacer clic se mostrará la definición de la política y los monitores asociados a la misma.
	Resuelta	La alerta permanece abierta o ha sido cerrada por el administrador o por el sistema.
	Alerta generada	Fecha y hora en la que se generó la alerta.
	Mensaje	Descripción del motivo por el cual el monitor generó la alerta.
	Desencadenante	Regla que generó la alerta.
	Silenciada	El administrador recibe o no un correo electrónico con cada alerta generada.
	Alerta recibida	Fecha y hora en la que se el sistema mostró la alerta en la consola.
Resumen del diagnóstico	Resumen del diagnóstico	Muestra una ventana con la información de diagnóstico generada por el monitor. Consulta "**Resumen del diagnóstico**" en la página **148**.
Respuesta de la alerta	Acción	Acción ejecutada por Panda Systems Management al generar la alerta según la configuración del monitor (envío de correo y generación de ticket).

Tabla 17.1: atributos de una alerta

Sección	Campo	Descripción
	Mensaje	Asunto del correo electrónico enviado y mensaje incluido en el ticket creado.

Tabla 17.1: atributos de una alerta

Gestión de alertas

Las alertas se gestionan con la barra de iconos **(1)** situada debajo del menú de pestañas en los distintos niveles disponibles (Figura **17.3**).

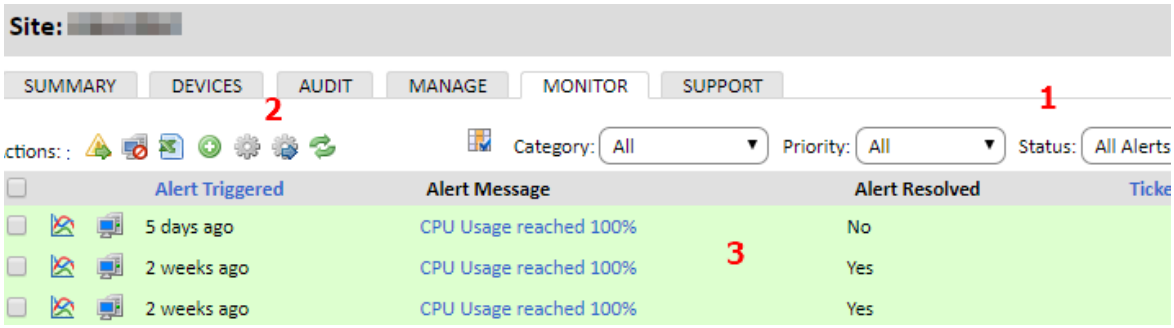


Figura 17.3: listado de alertas

Icono	Descripción
Resolver alertas seleccionadas	Marca como resueltas las alertas marcadas con la casilla de selección.
Desactivar monitores de Dispositivos	Impide el envío de correos generados por los monitores asignados al dispositivo.
Activar monitores para Dispositivos	Permite el envío de los correos generados por los monitores asignados al dispositivo.
Exportar a csv	Exporta el listado de alertas a un fichero csv.
Nuevo ticket	Asigna un nuevo ticket. Consulta "**Tickets**".
Programar una tarea	Asigna una tarea programada a los dispositivos que generaron las alertas seleccionadas.
Ejecutar una tarea rápida	Ejecuta una tarea inmediata sobre los dispositivos que generaron las alertas seleccionadas.
Actualizar vista actual	Recarga la página manualmente para visualizar los nuevos resultados.

Tabla 17.2: iconos de la barra de iconos del listado Alertas

Búsqueda y filtrado de alertas

Para localizar una determinada alerta Panda Systems Management cuenta con una barra de filtros **(2)** (Figura **17.3**). Las opciones disponibles son:

Filtro	Descripción
Categoría	Filtra por la categoría del monitor que generó la alerta.
Prioridad	Filtra por la prioridad de las alertas. La prioridad se especifica en la configuración del monitor que la genera.
Estado	Filtra las alertas abiertas, resueltas o silenciadas.
Búsqueda	Filtra por el contenido de algunos campos de las alertas.

Tabla 17.3: barra de filtros de alertas

Campos del listado de alertas

El listado alertas es configurable mediante el icono **(3)** (Figura **17.3**) para añadir más o menos columnas que describen las características del dispositivo que generó la alerta. A continuación se muestran las columnas específicas de la alerta.

Campo	Descripción
Tipo de alerta	Icono descriptivo con el tipo del monitor que generó la alerta.
Alerta generada	Tiempo transcurrido desde la creación de la alerta.
Mensaje de la alerta	Descripción del motivo por el cual el monitor generó la alerta.
Alerta resuelta	Indica si la alerta está marcada como cerrada.
Número de ticket	Identificador del ticket asociado a la alerta.
Alerta desactivada	Indica si el administrador silenció la alerta para impedir el envío de correos electrónicos.
Prioridad	Importancia de la alerta configurada en la definición del monitor que la generó.
Resuelta	Cuando la alerta ha sido resuelta indica el tiempo que permaneció abierta y quien la cerró (el agente si la condición establecida por el monitor ha desaparecido o el nombre de la cuenta del administrador que cerró la alerta de forma manual).

Tabla 17.4: campos del listado Alertas

Tickets

Los tickets extienden las capacidades de las alertas añadiendo las funcionalidades siguientes:

- Ofrecen a los técnicos la posibilidad de añadir información sobre el problema detectado, los trabajos realizados o las soluciones aplicadas.

- Pueden ser creados de forma automática por un monitor pero también de forma manual por un técnico o incluso por un usuario de la red.

Configuración de tickets

Crear un ticket automático en la configuración de un monitor

Los tickets creados automáticamente desde un monitor quedan asociados a la alerta generada por éste.

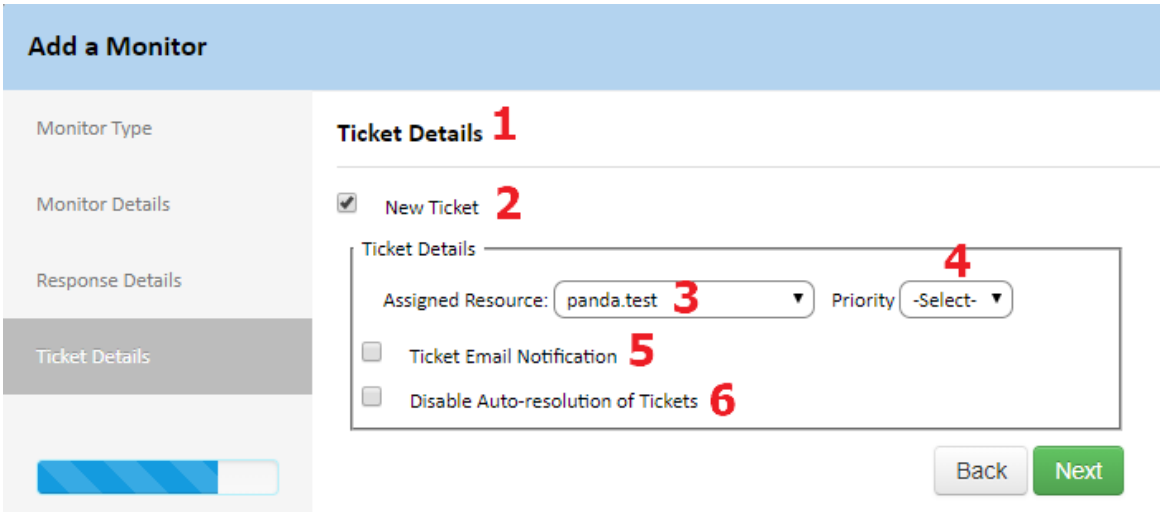


Figura 17.4: generación de tickets desde un monitor

- Consulta el apartado "**Configuración manual de monitores**" en la página **112** para iniciar la configuración de una monitor.
- En la sección **Información del ticket (1)** de la configuración del monitor, activa la opción **Crear ticket de soporte (2).**
- Mediante el campo **Usuario asignado (3)** indica el administrador de la red que es responsable del servicio que monitoriza el ticket.
- Indica la prioridad del ticket en el campo **Prioridad (4)**.
- Indica si el ticket se resolverá de forma automática **(5)** y si se notificará su creación mediante correo electrónico **(6).**

Crear un ticket desde la consola de administración

Los tickets generados desde la consola de administración no tienen alerta asociada ya que su creación es manual por parte del administrador de la red como respuesta a una situación que no ha sido controlada por el sistema de monitorización.

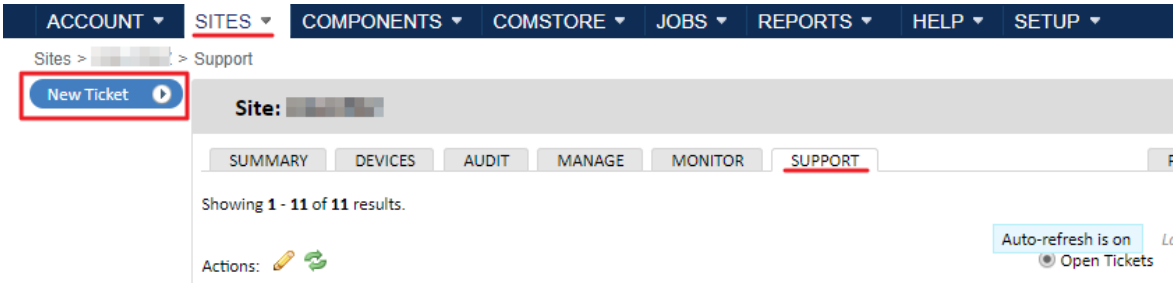


Figura 17.5: creación de un ticket desde la consola de administración

- En el menú superior **Zonas**, haz clic en la zona y en el menú de pestañas **Soporte**.
- Haz clic en el botón **Crear ticket de soporte** situado en la parte superior izquierda de la ventana
- Indica el resumen / título del ticket, descripción, prioridad y el administrador de la red al que será asignado.
- Haz clic en **Ok**. El nuevo ticket se añadirá a la lista de tickets con el estado **Nuevo**.

Crear un ticket desde el agente PCSM

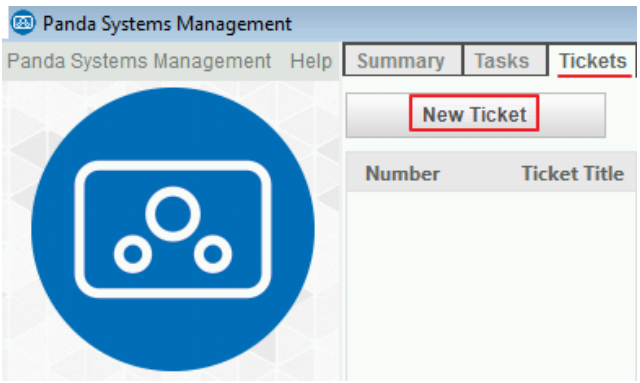


Figura 17.6: creación de un ticket desde el agente PCSM

Para los casos en los que el mal funcionamiento de un dispositivo no se traduzca en una alerta o generación de ticket automática, el propio usuario puede advertir la situación al equipo de IT. Para ello sigue los pasos mostrados a continuación:

- En el equipo del usuario haz clic en el icono del agente PCSM desde la barra de notificaciones situada en el escritorio, en la parte derecha de la barra de tareas.
- Haz clic en la pestaña **Tickets** y en el botón **Nuevo ticket**.
- Indica el título del ticket, la descripción con el problema y pulsa **Ok**.
- En la consola del administrador se mostrará de forma inmediata una nueva entrada en el menú de pestañas **Soporte** con el ticket generado.

Creación de tickets desde una alerta

En los casos en los que la configuración del monitor no establezca la creación de tickets pero el administrador quiera añadir información a la alerta generada, sigue los pasos mostrados a continuación:

- En el menú general **Zonas** haz clic en la zona apropiada y en el menú de pestañas **Monitorización.**
- Con las casillas de selección indica las alertas que serán asignadas al ticket. Un único ticket solo puede tener una alerta asignada de modo que si se han seleccionado varias alertas se generarán un número idéntico de tickets.
- En la barra de iconos haz clic en el icono  e indica la cuenta del administrador al que quedarán asignados los tickets, su importancia y si se generará o no un aviso por correo.
- Haz clic en **Guardar**. Los tickets serán visibles en la pestaña **Soporte** y el campo **Descripción** llevará el contenido del campo **Mensaje de alerta** de su alerta asociada.

Gestión de tickets

Visualizar los tickets generadas

Accede a la pestaña **Soporte** en los distintos niveles disponibles dependiendo del alcance de la información a obtener:

- Para mostrar un listado de los tickets generadas en toda la cuenta haz clic en el menú general **Cuenta** y en el menú de pestañas **Soporte**.
- Para mostrar un listado de los tickets generados en una zona haz clic en el menú general **Zonas,** haz clic en la zona y en **Soporte** dentro del menú de pestañas.
- Para mostrar un listado de las alertas generadas en un único dispositivo:
  - Haz clic en el menú general **Zonas,** elige la zona y haz clic en el menú de pestañas **Dispositivos**.
  - En el listado selecciona el dispositivo, haz clic en el menú de pestañas **Soporte** y en el control de selección situado en la parte superior derecha de la ventana la opción **Alertas de monitorización**.

Visualizar el detalle de un ticket

Haz clic en el campo **Número** de un ticket para mostrar la ventana de detalle.

La información disponible es:

Campo	Descripción
Creado por	Cuenta del usuario que creo el ticket desde la consola web o desde un monitor, o nombre del dispositivo si el ticket fue creado por un usuario.
Zona	Zona a la que pertenece el dispositivo referido por el ticket.
Fecha de creación	Fecha y hora en la que el ticket fue creado.
Estado	Estado del ticket. Los tickets se crean con el estado **Nuevo** y posteriormente el administrador podrá cambiarlo en función del progreso de la incidencia.
Prioridad	Importancia de 1 a 5 de la incidencia.

Tabla 17.5: detalle de un ticket

Campo	Descripción
Asignado a	Cuenta del técnico asignado a la resolución de la incidencia descrita por el ticket.
Resumen	Asunto del ticket.
Descripción	Desarrollo del ticket. Descripción completa del problema detectado. Si el ticket fue generado por un usuario o desde la consola de administración contiene las notas que se añaden de forma manual. Si el ticket fue generado por un monitor contiene una descripción automática del parámetro monitorizado que ha traspasado los márgenes configurados.

Tabla 17.5: detalle de un ticket

Modificación de tickets

- Para modificar el estado de un ticket selecciona los tickets y haz clic en la barra de iconos **Actualizar estado de los tickets seleccionados**.
- Para modificar el resto de campos de un ticket haz clic en el campo **Número**, edita el campo apropiado y haz clic en **Guardar**.

Filtrado de tickets

Utiliza los controles de **Tickets abiertos**, **Todos los tickets** y **Mis tickets** para filtrar el listado de tickets según su estado.

Campos del listado de tickets

Campo	Descripción
Número	Cadena de caracteres que identifica al ticket de forma única.
Zona	Zona a la que pertenece el dispositivo referido por el ticket.
Creado por	Cuenta del usuario que creó el ticket desde la consola web o desde un monitor, o nombre del dispositivo si el ticket fue creado por el usuario del dispositivo afectado.
Resumen	Asunto del ticket.
Descripción	Desarrollo del ticket. Descripción completa del problema detectado. Si el ticket fue generado por un usuario o desde la consola de administración contiene las notas que se hayan añadido de forma manual. Si el ticket fue generado por un monitor contiene una descripción automática del parámetro monitorizado que ha traspasado los márgenes configurados.
Prioridad	Importancia de 1 a 5 de la incidencia.
Estado	Estado del ticket. Los tickets se crean con el estado **Nuevo** y posteriormente el administrador podrá cambiar su estado en función del progreso de la incidencia.
Fecha de creación	Fecha y hora en la que el ticket fue creado.

Tabla 17.6: atributos de un ticket mostrados en el listado Tickets

Campo	Descripción
Asignado a	Cuenta del técnico asignado a la resolución de la incidencia descrita por el ticket.

Tabla 17.6: atributos de un ticket mostrados en el listado Tickets

Capítulo 18

Herramientas de acceso remoto a dispositivos

Panda Systems Management permite acceder de forma remota y transparente a los dispositivos del parque informático para resolver incidencias, reduce los desplazamientos del departamento técnico y evita las interrupciones en el trabajo diario del usuario.

CONTENIDO DEL CAPÍTULO

Herramientas de acceso remoto disponibles

Herramientas integradas en Panda Systems Management

Muchas de las herramientas de acceso remoto están diseñadas para poder ser ejecutadas en segundo plano, sin interrumpir el trabajo de los usuarios. En la tabla **18.1** se muestra un listado de todas las herramientas junto a su descripción y una indicación de su tipo (intrusiva o compatible con la actividad del usuario).

Herramienta	Descripción	Segundo plano
Captura de pantalla remota	Visualización rápida de mensajes de error.	SI
Pestaña de servicios de Windows	Acceso a parada, arranque y reinicio de servicios sin conectar con el escritorio remoto.	SI
Sesión de pantalla compartida	Acceso al escritorio remoto por VNC o Web Remote. Disponibles desde el agente PCSM y desde la consola de administración.	NO
RDP de Windows	Acceso al escritorio remoto por RDP. Implica el cierre de la sesión del usuario. Según la directiva de grupo establecida por el administrador (GPO), los usuarios deberán facilitar una contraseña adicional.	NO
Web Remote Chat	Web Remote Chat permite una conexión en tiempo real con técnicos de soporte mediante un navegador compatible.	SI
Shell de comandos	Línea de comandos remota DOS o Powershell.	SI
Apagado / Reinicio	Apagado o reinicio del equipo.	NO
Despliegue del agente	Instala de forma remota el agente en la red local.	SI
Administrador de tareas	Acceso al administrador de tareas sin conectar con el escritorio remoto.	SI

Tabla 18.1: herramientas de acceso remoto a dispositivos integradas en Panda Systems Management

Herramienta	Descripción	Segundo plano
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.	SI
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.	SI
Editor del registro	Acceso a la herramienta `Regedit` sin conectar con el escritorio remoto.	SI
Tareas rápidas	Lanza tareas en el dispositivo.	SI
Visor de eventos	Accede al visor de sucesos sin conectar con el escritorio remoto.	SI
Wake Up	Arranca de forma remota un dispositivo de la red mediante el envío de un "magic packet" por parte de un equipo que esté en la misma subred.	SI
Conexión con dispositivos de red	Permite conectarse de forma remota al interface de configuración de dispositivos de red.	N/A

Tabla 18.1: herramientas de acceso remoto a dispositivos integradas en Panda Systems Management

Disponibilidad de las herramientas del agente PCSM por plataforma

Dependiendo del sistema operativo instalado en el dispositivo, no estarán disponibles todas las herramientas en el agente PCSM. En la tabla **18.2** se indican las herramientas disponibles y su disponibilidad según la plataforma a la que se accede.

Herramienta	Windows	macOS	Linux
Captura de pantalla remota	**SI**	**SI**	
Pestaña de servicios de Windows	**SI**		
Sesión de pantalla compartida (VNC y Web Remote)	**SI**	**SI**	
RDP de Windows	**SI**		
Shell de comandos	**SI**	**SI**	**SI**
Apagado / Reinicio	**SI**	**SI**	**SI**
Despliegue del agente	**SI**	**SI**	
Administrador de tareas	**SI**		
Transferencia de archivos	**SI**	**SI**	**SI**
Información de unidad	**SI**		

Tabla 18.2: herramientas de acceso remoto a dispositivos integradas en Panda Systems Management

Herramienta	Windows	macOS	Linux
Editor del registro	SI		
Tareas rápidas	SI	SI	SI
Visor de eventos	SI		
Wake Up	SI	SI	SI
Conexión con dispositivos de red	SI	SI	SI

Tabla 18.2: herramientas de acceso remoto a dispositivos integradas en Panda Systems Management

Requisitos de acceso a las herramientas

Respecto al dispositivo gestionado, para poder acceder a los recursos de los dispositivos de forma remota, se requiere instalar un agente PCSM en el dispositivo, excepto en los casos descritos en el apartado "**Acceso a dispositivos no compatibles el agente PCSM**".

Respecto al dispositivo utilizado por el administrador de la red, se requiere un agente PCSM instalado, excepto para las siguientes herramientas, que solo necesitan un navegador compatible con Panda Systems Management:

- Captura de pantalla remota
- Sesión de pantalla compartida por Web Remote.

Para utilizar el resto de herramientas se requiere un agente PCSM instalado en el equipo del administrador.

Utiliza un equipo Windows para administrar los equipos de la red con el agente PCSM.

Acceso a las herramientas desde la consola

Para facilitar su uso, la consola de administración incorpora accesos directos a las herramientas incluidas en el agente PCSM. Las ventajas de utilizar los accesos directos de la consola son:

- La consola de administración invoca el agente PCSM con las credenciales apropiadas, lo que ahorra este paso al administrador.
- La consola de administración invoca el agente PCSM apuntando al dispositivo elegido. De este modo se evita el tener que navegar la estructura de equipos desde el panel de equipos del propio agente PCSM para buscar el dispositivo a gestionar.

Estos accesos directos se encuentran en los menús de contexto asociados a cada equipo en los listados de dispositivos y en la pestaña **Resumen** del dispositivo:

- Para acceder al menú de contexto desde los listados de dispositivos:
  - Haz clic en el menú superior **Zona**, selecciona la zona y haz clic en el menú de pestañas

Dispositivo. Se mostrará un listado de dispositivos con un menú de contexto asociado a cada línea.

- Desplaza el ratón por encima del icono de menú de contexto para mostrar los accesos directos disponibles en función del tipo de dispositivo.

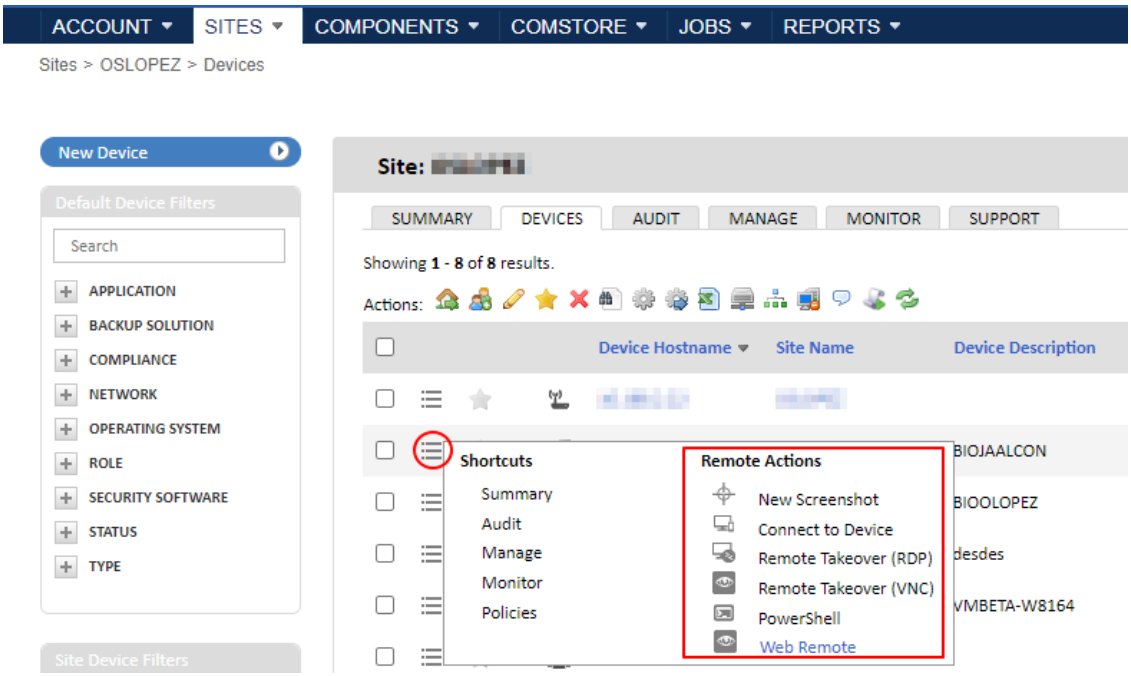


Figura 18.1: acceso al menú de contexto de acciones remotas desde el listado de dispositivos

- Para acceder a las herramientas de acceso remoto desde la pestaña **Resumen**:
  - Haz clic en el menú superior **Zona**, selecciona la zona y haz clic en el menú de pestañas **Dispositivo**. Haz clic en el dispositivo que deseas acceder.
  - En el menú de pestañas **Resumen**, desplaza el ratón por encima del menú de contexto **Acciones**

y **Acciones remotas** o haz clic en el icono .

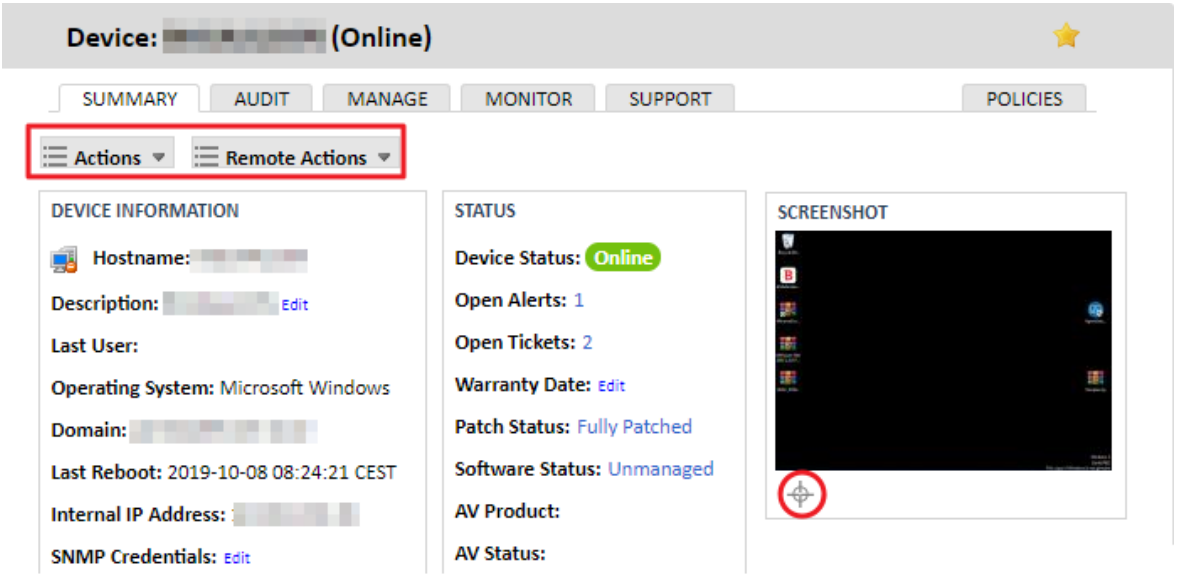


Figura 18.2: herramientas de acceso remoto desde el menú de pestañas Resumen

Los accesos directos a las herramientas del agente PCSM disponibles desde la consola web son:

Herramienta	Descripción
	Actualiza la captura de pantalla en miniatura del escritorio del dispositivo mostrada en la consola de administración.
Nueva captura de pantalla	Abre una ventana con una captura de pantalla del escritorio del dispositivo.
Conectar con dispositivo	Conecta el agente PCSM instalado en el equipo del administrador al dispositivo seleccionado para evitar introducir las credenciales de forma manual.
Control remoto (RDP)	Conexión remota al escritorio del dispositivo mediante el protocolo RDP.
Control remoto (VNC)	Conexión remota al escritorio del dispositivo mediante el protocolo VNC.
Conectar (HTTP)	Establece un túnel HTTP con el dispositivo de red. Consulta "**Acceso a dispositivos no compatibles el agente PCSM**".
Conectar (Telnet / SSH)	Establece un túnel Telnet / SSH con el dispositivo de red. Consulta "**Acceso a dispositivos no compatibles el agente PCSM**".
Conectar (personalizado)	Establece un túnel personalizado con el dispositivo de red. Consulta "**Acceso a dispositivos no compatibles el agente PCSM**".
Enviar un mensaje a los dispositivos seleccionados	Muestra un mensaje emergente en el escritorio del dispositivo del usuario.

Tabla 18.3: herramientas de acceso remoto disponibles desde la consola de administración

Herramienta	Descripción
Powershell	• Establece una o varias sesiones remotas simultáneas en el dispositivo con el intérprete PowerShell. • Requiere una versión de Powershell 5.1 o superior en el equipo que accede. • Requiere suministrar credenciales RDP. • Requiere habilitar el acceso remoto a Powershell desde el equipo con el comando `Enable-PSRemoting`.
Web Remote	Conexión remota al escritorio del dispositivo desde la consola de administración. En equipos donde hay varios usuarios con una sesión interactiva iniciada, Web Remote permite conectarse a cada sesión de forma individual.

Tabla 18.3: herramientas de acceso remoto disponibles desde la consola de administración

Acceso a las herramientas desde el agente PCSM

El acceso a las herramientas del agente PCSM desde la consola de administración es mucho más rápido, pero no todas están disponibles mediante este método. Por esta razón, el administrador puede utilizar el agente PCSM para tener un acceso completo.

Para acceder a las herramientas del agente PCSM, introduce las credenciales del administrador en el mismo. Este paso previo se puede hacer de forma directa utilizando el agente, o desde la propia consola web:

- Desde la consola web:
  - En el menú de contexto asociado al dispositivo (ver apartado "**Acceso a las herramientas desde la consola**" en la página **274**) haz clic en la opción **Conectar con dispositivo**. Se lanzará el agente PCSM instalado en el equipo del administrador con las credenciales apropiadas.
  - Accede a las herramientas de control situadas en la parte superior izquierda de la ventana.
- Desde el propio agente:
  - En la barra de notificaciones del escritorio de Windows, localiza el icono del agente PCSM y haz doble clic.
  - Introduce las credenciales y haz clic en el botón **Iniciar sesión**.
  - Haz clic en el icono  para desplegar todas las zonas configuradas en la cuenta. Selecciona la zona apropiada y haz en el dispositivo a conectar. En el panel de la derecha se mostrará la información asociada al dispositivo.
  - Haz clic nuevamente en el dispositivo para desplegar el panel de herramientas de administración.

Herramientas de control remoto

El administrador puede acceder al escritorio remoto de un equipo Windows o macOS mediante las herramientas:

- **Conectar remoto (VNC)**: conecta con el escritorio remoto en curso mediante el protocolo VNC.
- **Conectar remoto (RDP)**: crea una nueva sesión remota por RDP en equipos Windows
- **Web Remote**: conecta con una sesión interactiva directamente desde la consola de administración.

Control remoto mediante VNC

Comparte el escritorio, el ratón y el teclado del dispositivo remoto mediante el protocolo Virtual Network Computing (VNC). Si VNC no está permitido en el dispositivo de destino, la conexión VNC no será posible. Para permitir o denegar el uso de VNC en el dispositivo remoto, consulta "**Configuración de VNC para dispositivos Windows**".

VNC no permite el cambio de usuario y no puede conectarse a un dispositivo donde no hay ningún usuario conectado.

VNC no se instala por defecto en el dispositivo del usuario. Cuando el administrador activa el control remoto mediante VNC, el agente descargará e instalará el componente.

Operativa específica en dispositivos macOS

- Al conectar a un dispositivo macOS, se muestra al usuario una notificación emergente indicando que el programa PCSM Agent.app desea controlar este ordenador utilizando funciones de accesibilidad. Indica al usuario que haga clic en **Abrir Preferencias del Sistema** en el dispositivo, y que seleccione la aplicación en el panel de **Privacidad** para permitir la interacción entre su dispositivo y la sesión VNC del agente mediante Vine Server. Es necesario que Vine Server se instale durante el despliegue del agente PCSM y se ejecute como usuario (en lugar de como root) para que el permiso anterior pueda tener efecto.
- Para que VNC funcione correctamente en dispositivos macOS, es necesario que estas aplicaciones estén listadas y marcadas en **Preferencias del sistema**, **Seguridad y privacidad**, **Privacidad** en las siguientes secciones:
  - **Accesibilidad**: agente PCSM, Vine Server
  - **Acceso a todo el disco**: agente PCSM, Vine Server
- Si Vine Server se actualiza, es posible que sea necesario eliminar agente PCSM en **Preferencias del Sistema** > **Seguridad y Privacidad** > **Privacidad**. A continuación, en la siguiente conexión que requiera el agente PCSM, el sistema operativo le mostrará al usuario una notificación emergente

que le pedirá volver a añadir la aplicación.

Acceso en modo solo lectura

Para compartir unicamente el escritorio remoto de un dispositivo e impedir el acceso a su teclado y ratón, haz clic en la flecha situada al lado del icono de acceso por VNC y haz clic en **Conectarse en modo Solo ver**.

Configuración de VNC para dispositivos Windows

Para activar o desactivar a nivel de cuenta el acceso remoto VNC a los dispositivos:

- Haz clic en el menú general **Ajustes**, menú de pestañas **Configuración de cuenta**, sección **Configuración VNC**
- Activa o desactiva la opción **Permitir VNC**. Con el selector, indica si la configuración aplica a todas las zonas de la cuenta o únicamente a algunas de ellas:
  - Al desactivar el acceso por VPN se eliminará el servicio VNC de todos los dispositivos, así como todos los ficheros asociados al mismo.
  - Al activar el acceso por VPN, los dispositivos descargarán e instalarán de forma automática el servidor VNC.

Control remoto mediante RDP

Crea una sesión nueva e independiente de escritorio remoto mediante el protocolo Remote Desktop Protocol (RDP) en el dispositivo Windows del usuario.

Para ver lo que se muestra en la pantalla del dispositivo remoto mediante RDP, haz clic en la flecha que aparece junto al icono de RDP y haz clic en **Conectar con la sesión de la consola**.

Autenticación NLA

La autenticación a nivel de red (NLA) es una característica de autenticación utilizada en los servicios de escritorio remoto (Servidor RDP) o en las conexiones a escritorio remoto (Cliente RDP), introducida en la versión RDP 6.0 para Windows Vista y superiores. NLA requiere que el usuario que se conecta se autentique antes de establecer la sesión con el dispositivo remoto, ya que el inicio de una sesión remota en un dispositivo consume recursos de CPU. Este consumo se puede evitar exigiendo al usuario una autenticación precia a la conexión: si la autenticación no es correcta la conexión no tendrá lugar y, por lo tanto, no utilizará recursos del dispositivo. Este esquema también ofrece una capa de protección contra los ataques de denegación de servicio (DoS).

Cuando un usuario intenta establecer una conexión con un dispositivo con NLA activado, NLA enviará las credenciales del usuario al servidor para ejecutar la autenticación antes de crear la sesión. Para establecer la conexión es indispensable que la autenticación del usuario sea correcta.

Para habilitar la autenticación NLA sigue una de las siguientes rutas:

- **Menú Inicio** > **Panel de control** > **Sistema y seguridad** > **Sistema** > **Configuración remota** > **Remoto** >

Escritorio remoto > selecciona **Permitir conexiones sólo desde equipos que ejecuten Escritorio remoto con autenticación a nivel de red**.

- **Menú de inicio** > **Panel de control** > haz clic con el botón derecho en **Equipo** > **Propiedades** > **Configuración remota** > **Remoto** > **Escritorio remoto** > selecciona **Permitir conexiones sólo desde equipos que ejecuten Escritorio remoto con autenticación de nivel de red.**

Abrir una sesión RDP con un dispositivo con NLA activado

- Inicia sesión en agente PCSM y conecta con un servidor.
- Haz clic en el icono de RDP, introduce el nombre de usuario y contraseña y selecciona **Usar autenticación a nivel de red**. La opción de utilizar NLA aparecerá en gris en los dispositivos incompatibles.
- Selecciona **Recordar contraseñas para este dispositivo** si quieres que la contraseña sea recordada para futuras sesiones RDP.
- Haz clic en **Iniciar sesión** para establecer la conexión. La conexión se establecerá si la autenticación del usuario ha sido exitosa.

Control remoto por Web Remote

Comparte el escritorio, el ratón y el teclado del dispositivo remoto mediante tecnología de control remoto HTML5, que ofrece tiempos de conexión más rápidos y está disponible para servidores, portátiles y equipos de sobremesa.

Web Remote admite varias conexiones simultáneas a un mismo dispositivo. Consulta "**Añadir técnicos a una sesión de Web Remote**".

Requisitos

- Cualquier dispositivo compatible con Panda Systems Management puede iniciar una conexión Web Remote.
- No requiere tener instalado un agente PCSM en el equipo del administrador.
- Los dispositivos Windows y macOS con un agente PCSM instalado pueden ser controlados por Web Remote.
- Disponer de la última versión de un navegador compatible. Consulta "**Exploradores compatibles**" en la página **319**.
- El cortafuegos corporativo debe permitir el tráfico por el puerto 3478 (UDP).
- Activar el permiso **Web Remote** en la cuenta del administrador que accede a la consola Panda Systems Management:
  - En el menú superior **Ajustes** haz clic en la pestaña **Roles**. Se mostrarán todos los roles definidos.
  - Haz clic en el rol de la cuenta que utilizará la herramienta Web Remote. Se mostrará la ventana **Detalle del rol** con los permisos disponibles.

- Haz clic en la sección **Herramientas de control remoto** y en el botón asociado a **Web Remote**. Se activará la función **Web Remote** para todas las cuentas que tengan asignado el rol modificado.

Para que Web Remote funcione correctamente en macOS, deben aparecer en la lista **Preferencias del sistema** > **Seguridad y privacidad** > **Privacidad** las siguientes aplicaciones en las secciones:

- **Accesibilidad**: agente PCSM, Vine Server.
- **Acceso a todo el disco**: agente PCSM, Vine Server.
- **Captura de pantalla**: agente PCSM, Vine Server

Requisitos para el acceso por WebRTC

WebRTC es un marco de desarrollo abierto que añade capacidades de comunicación en tiempo real al navegador web. Web Remote aprovecha esta tecnología para establecer por defecto una conexión punto a punto entre dispositivos. Si no es posible utilizar una ruta directa, WebRTC conectará ambos dispositivos en modo relay a través de los servidores de Panda Systems Management.

Para una mayor fiabilidad, se establece automáticamente una conexión WebSocket en paralelo con cada conexión WebRTC. Se distinguen los casos siguientes:

- Si WebRTC no logra conectarse pero WebSocket sí, se utiliza este canal para la comunicación.
- Si WebRTC logra conectarse pero se desconecta en medio de la sesión, se conmuta de forma automática al canal WebSocket sin que el usuario experimente desconexiones.
- Si WebSocket no consigue conectarse y WebRTC sí, se utiliza WebRTC.
- Siempre se prefiere WebRTC a WebSocket, tanto si se trata de una conexión directa entre dispositivos como relay.

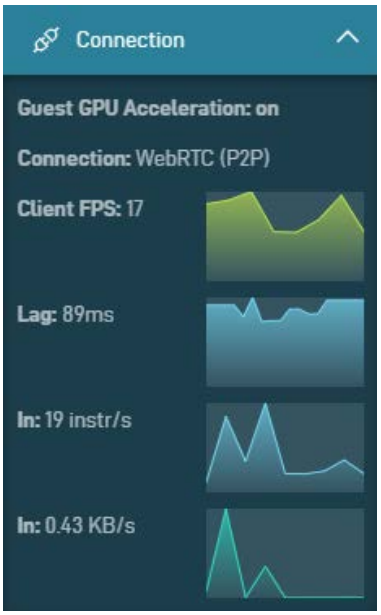


Figura 18.3: Panel Connection en una conexión de control remoto

Para comprobar el tipo de conexión y de aceleración gráfica negociada en el establecimiento de la conexión con el dispositivo del usuario, haz clic en el menú lateral derecho **Connection**. Se desplegará un panel con toda la información necesaria:

- **Guest GPU Acceleration**: aceleración gráfica por GPU activada o no.
- **Connection**: tipo de conexión negociada.
- **Client FPS**: fotogramas por segundo recibidos.
- **Lag**: retardo en milisegundos de la comunicación.
- **In**: número de primitivas de dibujo recibidas por segundo.
- **In**: ancho de banda medido en Kbytes por segundo.

Para que Web Remote pueda establecer conexiones, se añaden al firewall del equipo las siguientes reglas que permiten el tráfico de entrada y salida:

- **RMM RTC Proxy**: servicio RMM Web Remote RTC Proxy
- **RMM RTO Proxy**: servicio RMM Web Remote RTO Proxy
- **RMM Web Remote**: proceso RMM Web Remote

Aceleración mediante GPU en el equipo del administrador

A partir de Windows NT 6.2 (Windows 8/Windows Server 2012) se permite la aceleración por hardware al compartir el escritorio del dispositivo del usuario, lo que mejora la calidad y la capacidad de respuesta de la comunicación.

Los requisitos de la aceleración mediante GPU son:

- Windows NT 6.2 (Windows 8/Windows Server 2012) o superiores. Windows NT 6.1 (Windows 7/ Windows Server 2008 R2) o inferior deben utilizar VNC.
- El agente PCSM requiere .NET 6. Si no está instalado, utiliza Control remoto mediante VNC. Consulta "**Control remoto mediante VNC**".

Para comprobar si está activada la aceleración mediante GPU:

- En la barra de herramientas lateral haz clic en **Connection**. Se desplegará la información asociada al tipo de conexión establecida con el dispositivo.
- Comprueba que se muestra **Guest GPU Acceleration: on**.

Aceleración mediante GPU en sistemas híbridos

Los sistemas híbridos son dispositivos con una tarjeta gráfica integrada en la placa base y otra tarjeta gráfica adicional independiente, también conocida como tarjeta gráfica discreta. Para obtener más información consulta el artículo **https://docs.microsoft.com/en-us/troubleshoot/windows-client/shell-experience/error-when-dda-capable-app-is-against-gpu**.

A partir de Windows 10 Build 17093 el agente PCSM detecta si se está ejecutando en un sistema híbrido y utiliza la aceleración por GPU de la tarjeta gráfica discreta. Para obtener más información consulta la sección New Graphics settings for Multi-GPU Systems del artículo **https://blogs.windows.com/windows-insider/2018/02/07/announcing-windows-10-insider-preview-build-17093-pc/**.

Para sistemas híbridos con tarjetas gráficas de la marca NVIDIA y sistemas anteriores a Windows 10 Build 17093:

- Abre el panel de control de NVIDIA y haz clic en **Configuración 3D** > **Controlar la configuración 3D**.
- Selecciona la pestaña **Configuración de programa** y haz clic en el botón **Agregar**.
- Elige el proceso RMM.WebRemote y haz clic en **Agregar el programa seleccionado**.
- Selecciona **Integrated processor as the preferred graphic processor** y haz clic en **Aplicar** y en **Aplicar los cambios**.

Para híbridos con tarjetas de la marca AMD Radeon y sistemas anteriores a Windows 10 Build 17093:

- Abre el panel de control de Radeon.
- Selecciona **System** > **Switchable Graphics**.
- Selecciona en la lista el proceso RMM.WebRemote para mostrar el menú desplegable asociado y selecciona **Power Saving**. Los cambios tendrán efecto la próxima vez que el proceso Web Remote se inicie.

Iniciar una sesión de Web Remote

- Selecciona en la consola Panda Systems Management el dispositivo con el que quieres iniciar la sesión de Web Remote:
  - Selecciona el menú superior **Zonas** y haz clic en la zona a la que pertenece el dispositivo. Se mostrará la pestaña **Resumen** de la zona elegida.
  - Haz clic en la pestaña **Dispositivo** del menú de pestañas. Se mostrarán todos los dispositivos asociados a la zona elegida.
  - Haz clic en el nombre del dispositivo elegido. Se mostrará la pestaña **Resumen** del dispositivo.
- Haz clic en el desplegable **Acciones remotas** y selecciona la opción **Web Remote**. Se abrirá una nueva pestaña en el navegador con el entorno Web Remote y una cuenta atrás indicando el tiempo que falta para finalizar la conexión con el dispositivo elegido.
- Haz clic en el enlace **Control Screen**. Se mostrará el escritorio del dispositivo y una barra de herramientas lateral con información y opciones de configuración de la sesión de control remota.

Añadir técnicos a una sesión de Web Remote

Cada técnico del MSP puede repetir el procedimiento indicado en "**Iniciar una sesión de Web Remote Chat**" para unirse a una sesión de Web Remote previamente creada por otro técnico. El acceso al escritorio del usuario por parte de los técnicos conectados es simultáneo.

Modo de privacidad

*Para obtener más información sobre los modos de privacidad consulta "***Opciones del modo privacidad***" en la página* **102**

Si el dispositivo remoto tiene establecida una configuración de privacidad, se le pedirá al usuario del dispositivo que acepte o rechace la conexión. Para ello, el agente PCSM mostrará al usuario del dispositivo una ventana emergente con el nombre y la dirección de correo electrónico del técnico que se desea conectar a su dispositivo. Si la pantalla del usuario final está bloqueada, no se mostrará el aviso y se le notificará al administrador en la pantalla de conexión.

Una vez que la conexión esté en curso, se mostrará un mensaje al usuario final de que se está realizando una sesión de control remoto. Este mensaje sólo aparecerá cuando el usuario final haya

aceptado la solicitud de conexión. Si se corta momentáneamente la conexión, Web Remote volverá a conectarse con la misma sesión y no aparecerá un segundo mensaje de solicitud de modo de privacidad.

> *Si en macOS no aparece el mensaje de solicitud, comprueba que la casilla Eventos del sistema está seleccionada en **Preferencias del sistema** > **Seguridad y privacidad** > **Privacidad** > **Agente PCSM**.*

Sincronizar Portapapeles

> *El navegador Safari no es compatible con la funcionalidad Sincronizar portapapeles.*

Panda Systems Management permite sincronizar el portapapeles del administrador y el del usuario en ambos sentidos para transferir información de forma sencilla. Sin embargo, esta funcionalidad puede desactivarse para evitar fugas de información:

- Conecta con el dispositivo del usuario. Consulta "**Iniciar una sesión de Web Remote**".
- En la barra de herramientas lateral haz clic en la opción **Preferences**. Se mostrarán las opciones de configuración disponibles:
  - **Sync Clipboard**: sincroniza el portapapeles del administrador y del usuario gestionado.
  - **Clear Clipboard On Close**: limpia el portapapeles del dispositivo remoto al terminar la sesión Web Remote. La funcionalidad Historial del Portapapeles de Windows y la sincronización del portapapeles del dispositivo del usuario con la nube de Microsoft está siempre desactivada para evitar la propagación de la información a otros dispositivos que estén configurados con la misma cuenta de usuario.

Para que Sincronizar Portapapeles funcione correctamente en los navegadores soportados es necesario asignar los permisos mostrados a continuación:

- Google Chrome:
  - En la barra de direcciones escribe `chrome://settings/content/clipboard`
  - Activa el permiso **Preguntar cuando un sitio quiera ver texto e imágenes copiadas en el portapapeles (recomendado)** en la pantalla.
  - Añade en el apartado **Permitir** la URL de la consola Panda Systems Management **https://sm.pandasecurity.com**
- Microsoft Edge:
  - En la barra de direcciones escribe `edge://settings/content/clipboard`
  - Activa el permiso **Preguntar cuando un sitio quiera ver texto e imágenes copiadas en el portapapeles (recomendado)** en la pantalla.
  - Añade en el apartado **Permitir** la URL de la consola Panda Systems Management **https://**

sm.pandasecurity.com

- Firefox:
  - En la barra de direcciones escribe `about:config`
  - Asigna a `dom.events.testing.asyncClipboard` el valor `True`.
  - Asigna a `dom.events.asyncClipboard.clipboardItem` el valor `True`.
  - Asigna a `dom.events.asyncClipboard.readText` el valor `True`.

Bloquear el teclado y el ratón

Panda Systems Management permite impedir el uso del teclado y del ratón al usuario del dispositivo o al administrador cuando éste se encuentra en una sesión de Web Remote:

- Conecta con el dispositivo del usuario. Consulta "**Iniciar una sesión de Web Remote**".
- En la barra de herramientas lateral haz clic en la opción **Preferences**. Se mostrarán las opciones de configuración disponibles:
  - **View Only Mode:** las pulsaciones del teclado y movimientos del ratón del administrador no se enviarán al dispositivo remoto.
  - **Block Remote Input:** se bloquearán las pulsaciones del teclado y movimientos del ratón del usuario.

Ajustar automáticamente la calidad de la imagen

Permite establecer la calidad de la imagen del escritorio remoto en conexiones lentas o inestables:

- Conecta con el dispositivo del usuario. Consulta "**Iniciar una sesión de Web Remote**".
- En la barra de herramientas lateral haz clic en la opción **Preferences**. Se mostrarán las opciones de configuración disponibles:
  - **Image quality**: elige una calidad de imagen fija (Low, Medium, High) o Auto para adaptar la calidad al tipo de conexión disponible.

Web Remote Chat

Panda Systems Management incluye un sistema de chat que los administradores pueden utilizar para comunicarse en tiempo real con los usuarios sin necesidad de tomar el control del dispositivo e interrumpir su trabajo.

Requisitos

- Cualquier dispositivo compatible con Panda Systems Management puede iniciar una conexión Web Remote Chat.
- Los usuarios de dispositivos Windows y macOS con un agente PCSM instalado pueden comunicarse por Web Remote Chat.
- No requiere tener instalado un agente PCSM en el equipo del administrador.

- Disponer de la última versión de un navegador compatible. Consulta "**Exploradores compatibles**" en la página **319**.
- Activar el permiso **Chat** en la cuenta del administrador que accede a la consola Panda Systems Management:
  - En el menú superior **Ajustes** haz clic en la pestaña **Roles**. Se mostrarán todos los roles definidos.
  - Haz clic en el rol de la cuenta que utilizará la herramienta Web Remote Chat. Se mostrará la ventana **Detalle del rol** con los permisos del rol seleccionado.
  - Haz clic en la sección **Herramientas de control remoto** y en el botón asociado a **Chat**. Se activará la función **Web Remote Chat** para todas las cuentas que tengan asignado el rol modificado.

Iniciar una sesión de Web Remote Chat

Solo los administradores de Panda Systems Management pueden crear una sesión de chat con los usuarios.

- Selecciona en la consola Panda Systems Management el dispositivo con el que quieres iniciar la sesión de chat:
  - Selecciona el menú superior **Zonas** y haz clic en la zona a la que pertenece el dispositivo. Se mostrará la pestaña **Resumen** de la zona elegida.
  - Haz clic en la pestaña **Dispositivo** del menú de pestañas. Se mostrarán todos los dispositivos asociados a la zona elegida.
  - Haz clic en el nombre del dispositivo elegido. Se mostrará la pestaña **Resumen** del dispositivo.
- Haz clic en el desplegable **Acciones remotas** y selecciona la opción **Web Remote**. Se abrirá una nueva pestaña en el navegador con el entorno Web Remote y una cuenta atrás indicando el tiempo que falta para finalizar la conexión con el dispositivo elegido.
- Si el dispositivo del usuario está encendido y el usuario se ha logeado en el dispositivo, haz clic en el enlace **Chat**. Si nunca se ha chateado previamente con el dispositivo del usuario, se creará una sesión de chat; en caso contrario, se conectará a la sesión creada anteriormente. Panda Systems Management muestra la ventana de chat con la información siguiente:
  - **(1) Equipo de usuario:** muestra el equipo del usuario con el que se inició la sesión de chat.
  - **(2) Número de participantes activos en el chat**: en un primer momento solo estará conectado el administrador que creó la sesión de chat.
  - **(3) Información de las cuentas conectadas al chat:** para los administradores se muestra el nombre y apellidos o la cuenta que inició sesión en la consola Panda Systems Management. Para los usuarios se muestra el nombre del dispositivo conectado.
  - **(4) Historial del chat**: todos los administradores que se conecten a una sesión de chat pueden ver el historial de mensajes que se han enviado y recibido previamente con el usuario.
  - **(5) Export**: consulta "**Exportar historial del chat**".

- **(6) CHAT INVITE / CONTROL SCREEN:** botón para invitar al chat al usuario o para tomar el control de la pantalla de su dispositivo.
- **(7) Caja de texto.** Consulta "**Características de una sesión Web Remote Chat**".

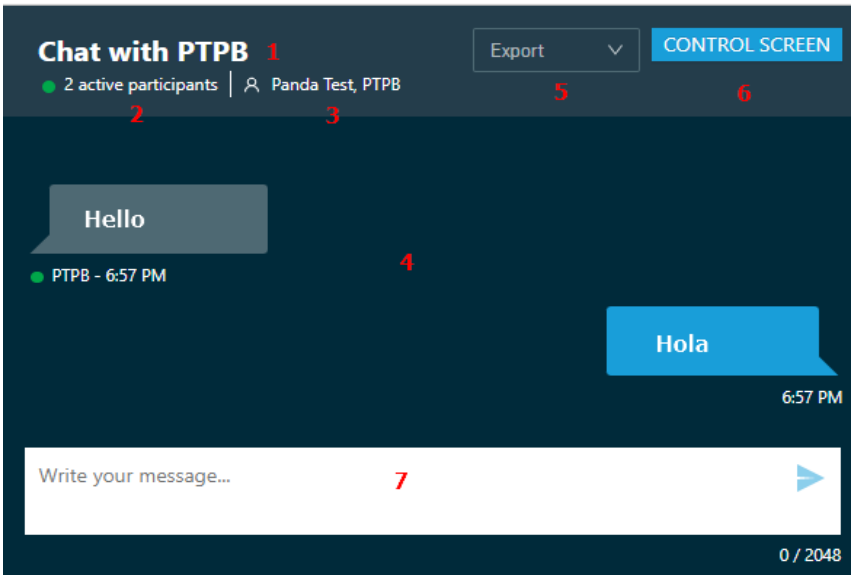


Figura 18.4: Sesión de chat iniciada con un usuario

- Haz clic en el botón **CHAT INVITE**. En la consola de Panda Systems Management se mostrará el mensaje **Connecting** y en el equipo del usuario el agente mostrará una ventana indicando el nombre del administrador que intenta establecer una sesión de chat.
- En el equipo del usuario, haz clic en el botón **Approve**. Se abrirá una pestaña en el navegador configurado por defecto donde el usuario podrá chatear con el administrador.
- Si el dispositivo del usuario no está encendido o el usuario no se ha logeado en el dispositivo, no será posible iniciar una sesión de chat. Se mostrará el enlace **View Chat History** para ver el historial de mensajes previos con el usuario y el botón **CHAT INVITE** estará desactivado.

Características de una sesión Web Remote Chat

- Una sesión de chat puede alojar a un único usuario de un dispositivo y a un número de administradores sin limitar.
- Cada mensaje del chat escrito en la caja de texto **(6)** tiene un límite de 2048 caracteres. Se aceptan caracteres Unicode, saltos de linea (`Shift + Enter`), copiar y pegar emojis y URLs.
- Los idiomas del navegador admitidos en la ventana de chat del usuario son: inglés, alemán, español, francés e italiano.
- Cada mensaje del chat lleva asociado el nombre del participante y un circulo de color verde si está conectado o transparente si está desconectado o reconectando.
- Si todos los participantes permanecen inactivos durante más de 30 minutos, la sesión de chat se cierra automáticamente.

Añadir técnicos a una sesión Web Remote Chat

Cada técnico del MSP puede repetir el procedimiento indicado en "**Iniciar una sesión de Web Remote Chat**" para unirse a un chat ya creado. Una sesión de chat ya creada tiene las siguientes características:

- Los técnicos que se conectan a una sesión de chat ya creada por otro técnico no pueden invitar al usuario a unirse al chat, solo el técnico que creó el chat tiene esta capacidad.
- El historial del chat completo está disponible para todos los técnicos que se unan al chat.
- Todos los técnicos y usuarios unidos al chat se muestran en **(1)**.
- Todos los mensajes escritos tanto por técnicos como por usuarios son visibles para todos los participantes del chat.

Exportar historial del chat

Una vez conectado a una sesión de chat, sigue los pasos mostrados a continuación:

- Haz clic en el botón **Export (5)**. Se mostrará un menú desplegable.
- Haz clic el intervalo de tiempo que deseas exportar. La zona historial de chat **(1)** mostrará únicamente los mensajes que pertenecen al intervalo de tiempo elegido.
- Haz clic en el botón **Export (5)**. Se descargará en el equipo del técnico un fichero .txt con el historial del chat.

Web Remote PowerShell

Una sesión Web Remote PowerShell permite al técnico acceder a los recursos del dispositivo del usuario sin tomar el control de su escritorio, y por tanto, sin interrumpir su trabajo. Consiste en una linea de comandos remota que utiliza la interfaz de consola avanzada PowerShell.

Requisitos

- Cualquier dispositivo compatible en Panda Systems Management puede iniciar una conexión Web Remote PowerShell.
- Disponer de la última versión de un navegador compatible. Consulta "**Exploradores compatibles**" en la página **319**.
- Los usuarios de dispositivos Windows 10 versión 1809 y superiores o Windows Server 2019 y superiores con un agente PCSM instalado pueden recibir conexiones por Web Remote PowerShell. La versión de PowerShell ejecutada en el dispositivo del usuario será la que esté instalada en la ruta `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.
- Activar el permiso **PowerShell** en la cuenta del técnico que accede a la consola Panda Systems Management:
  - En el menú superior **Ajustes** haz clic en la pestaña **Roles**. Se mostrarán todos los roles definidos.
  - Haz clic en el rol de la cuenta que utilizará la herramienta Web Remote PowerShell. Se mostrará la ventana **Detalle del rol** con los permisos del rol seleccionado.

- Haz clic en la sección **Herramientas de control remoto** y en el botón asociado a **PowerShell**. Se activará la función **Web Remote PowerShell** para todas las cuentas que tengan asignado el rol modificado.

Iniciar una sesión Web Remote PowerShell

- Selecciona en la consola Panda Systems Management el dispositivo con el que quieres iniciar la sesión de PowerShell:
  - Selecciona el menú superior **Zonas** y haz clic en la zona a la que pertenece el dispositivo. Se mostrará la pestaña **Resumen** de la zona elegida.
  - Haz clic en la pestaña **Dispositivo** del menú de pestañas. Se mostrarán todos los dispositivos asociados a la zona elegida.
  - Haz clic en el nombre del dispositivo elegido. Se mostrará la pestaña **Resumen** del dispositivo.
- Haz clic en el desplegable **Acciones remotas** y selecciona la opción **Web Remote**. Se abrirá una nueva pestaña en el navegador con el entorno Web Remote y una cuenta atrás indicando el tiempo que falta para finalizar la conexión con el dispositivo elegido.
- Si el dispositivo del usuario está encendido, haz clic en el enlace **PowerShell**. Se mostrará una ventana con el interprete de comandos PowerShell iniciado en el dispositivo del usuario.
- Si el modo privado está activado, se mostrará durante 30 segundos un mensaje de confirmación en el equipo del usuario indicando que un técnico está intentando abrir una sesión en su dispositivo. Si el usuario acepta la conexión el técnico podrá ejecutar comandos en el dispositivo del usuario. Si el usuario no contesta en 30 segundos o no acepta la invitación, la conexión del técnico se deniega.

Finalizar una sesión Web Remote PowerShell

- **Manualmente**: tecleando el comando `Exit`. Para reconectar la sesión, recarga la pestaña del navegador que contiene la sesión Web Remote PowerShell pulsando F5.
- **Manualmente**: cerrando la pestaña del navegador que contiene la sesión Web Remote PowerShell
- **Automáticamente**: tras 30 minutos sin activar la pestaña del navegador que contiene la sesión Web Remote PowerShell.

Registro de sesiones Web Remote PowerShell

- Selecciona en la consola Panda Systems Management el dispositivo:
  - Selecciona el menú superior **Zonas** y haz clic en la zona a la que pertenece el dispositivo. Se mostrará la pestaña **Resumen** de la zona elegida.
  - Haz clic en la pestaña **Dispositivo** del menú de pestañas. Se mostrarán todos los dispositivos asociados a la zona elegida.
  - Haz clic en el nombre del dispositivo elegido. Se mostrará la pestaña **Resumen** del dispositivo.
- Haz clic en la pestaña **Auditoria** y en el selector **Actividad**. Se mostrarán todas la acciones ejecutadas por Panda Systems Management en ese dispositivo.

- Localiza las acciones de tipo **Web Remote Shell by**.

Acceso a dispositivos no compatibles 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 el proceso siguiente:

- El agente PCSM 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 Panda 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.

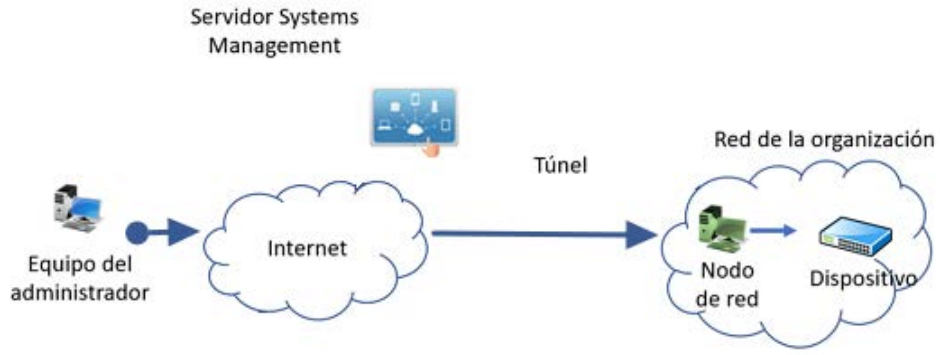


Figura 18.5: esquema general de conexión entre el equipo del administrador hasta el nodo de red a través del túnel

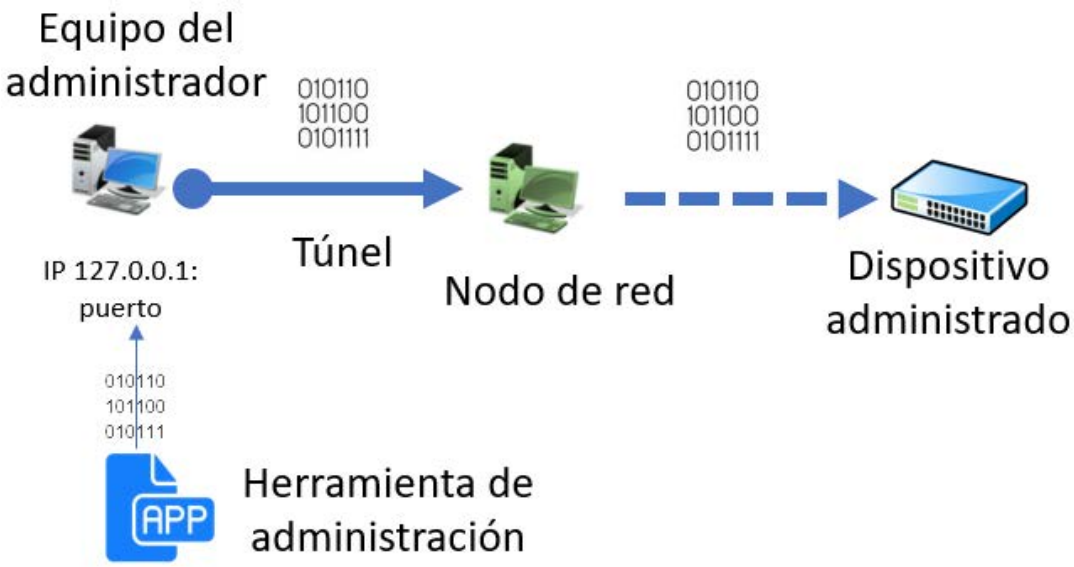


Figura 18.6: esquema de acceso de la herramienta de administración al dispositivo administrado

Para acceder a un dispositivo de red mediante HTTPS:

- 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 el desplegable **Connect (HTTPS)**.
- 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.

Gestión remota de dispositivos móviles

A continuación, se detallan las herramientas disponibles para gestionar dispositivos móviles desde la consola, su modo de funcionamiento y sus beneficios asociados.

Acceso a las herramientas de gestión remota de dispositivos móviles

Las funcionalidades específicas de la consola se muestran únicamente en el Nivel dispositivo que se corresponde al dispositivo a administrar:

- Haz clic en el menú general **Zonas**, elige la zona donde reside el dispositivo móvil y haz clic en el dispositivo a gestionar.
- Haz clic en el menú de pestañas **Resumen**. El menú de contexto de acciones se adapta de forma automática mostrando las herramientas de gestión compatibles con dispositivos móviles.

Borrado del dispositivo (Dispositivo Wipe)

Haz clic en el icono  para devolver el dispositivo a su estado original y 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.

Geolocalización

Haz clic en el icono  para representar la posición del dispositivo en un mapa. Las coordenadas 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.

Bloqueo del dispositivo

Haz clic en el icono  para apagar la pantalla del dispositivo. Si estaba establecido un PIN de seguridad se le solicitará de nuevo al usuario cuando active el móvil. Este bloqueo del dispositivo resulta útil en caso de robo del terminal.

Desbloqueo del dispositivo

Haz clic en el icono  para borrar el PIN en el caso de que el usuario haya olvidado su contraseña.

Política de códigos de acceso

Haz clic en el icono para obligar 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.

Parte 6

Seguridad del servicio Panda Systems Management

Capítulo 19: Cuentas de usuario y roles

Capítulo 20: Seguridad y control de acceso al servicio

Capítulo 21: Registro de actividad

Capítulo 19

Cuentas de usuario y roles

Una cuenta de usuario es un recurso formado por información que regula el acceso a la consola Panda Systems Management 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 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 de administración. 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.*

CONTENIDO DEL CAPÍTULO

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 Panda Systems Management 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.

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.

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.

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.

Crear, configurar y borrar cuentas de usuario

Añadir una cuenta de usuario

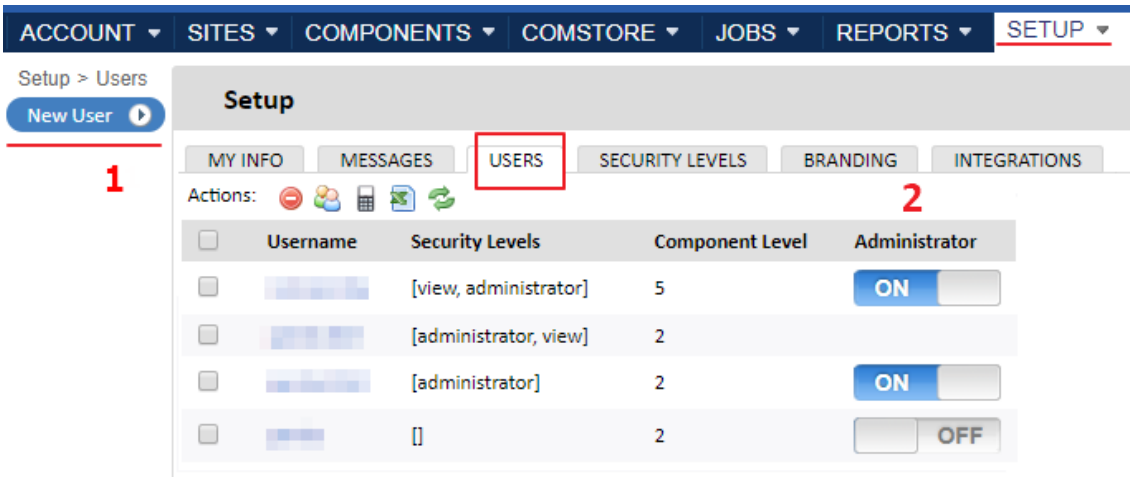


Figura 19.1: acceso a la ventana de gestión de usuarios

Para añadir una nueva cuenta de usuario sigue los pasos mostrados a continuación:

- Haz clic en el menú general **Ajustes**, menú de pestañas **Usuarios.**
- Haz clic en el botón **Añadir usuario (1)** del panel lateral.
  - Establece el nombre de usuario, contraseña, dirección de correo y el nombre y apellidos del técnico que usará la cuenta.
  - Programa la desactivación de la cuenta si el usuario dejará de poder acceder a la consola de Panda Systems Management a partir de cierta fecha.
  - Establece el **Nivel componente** de la cuenta (de 1 a 5) para restringir el acceso a los componentes importados de la ComStore cuyo **Nivel componente** sea superior al configurado en la cuenta. Consulta el punto "**Carga del componente de tipo monitor en la plataforma Panda Systems Management**" en la página **149**.
  - Selecciona los roles asignados a la cuenta y el rol establecido por defecto.

Editar una cuenta de usuario

- Haz clic en el nombre de la cuenta a modificar. Se abrirá una ventana con los campos editables del usuario.
- Haz clic en el botón **Guardar**.

Borrar una cuenta de usuario

- Al pasar el ratón sobre las cuentas de usuario que se quieren eliminar, al final de la línea aparecerá el icono . Pulsa el icono en la línea correspondiente. Se mostrará una ventana de confirmación.
- En la ventana de confirmación haz clic en la casilla **Asignar datos a usuario** para copiar la

configuración del usuario antes de su borrado. Los elementos que se copian son:

- Tareas programadas
- Informes programados
- Filtros
- Tickets

- Haz clic en la casilla **Comprendo que esta acción es irreversible** y en el botón **Eliminar usuario permanentemente** para finalizar el borrado de la cuenta de usuario.

> *Al eliminar usuarios, los administradores tienen la posibilidad de mover los datos de configuración a otro usuario.*

Desactivar cuentas de usuario

- Selecciona las cuentas de usuario a desactivar con las casillas de selección.
- Haz clic en el icono de la barra de acciones.

Exportar el listado de usuarios

- Selecciona las cuentas de usuario a exportar con las casillas de selección.
- Haz clic en el icono de la barra de iconos.

Asignar y retirar el rol de administrador a una cuenta de usuario

Haz clic en el botón **On/Off (2)** para activar o retirar rol de administrado a una cuenta de usuario.

Cambiar el rol efectivo de una cuenta de usuario

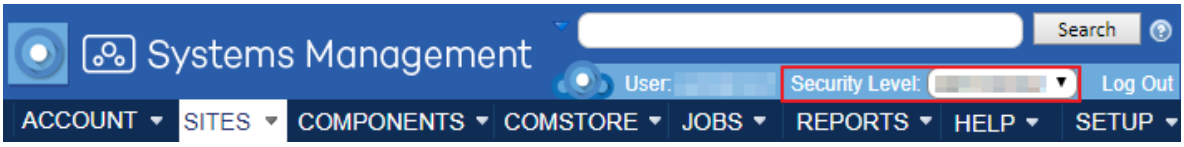


Figura 19.2: cambio de rol de la cuenta con una sesión ya iniciada

Una cuenta de usuario puede pertenecer a un único rol o a varios. 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. Por lo tanto no es necesario hacer un proceso de salida e inicio de sesión para cambiar de rol.Crear, configurar y borrar roles

Añadir un rol

Para añadir un nuevo rol a una cuenta de usuario sigue los pasos mostrados a continuación:

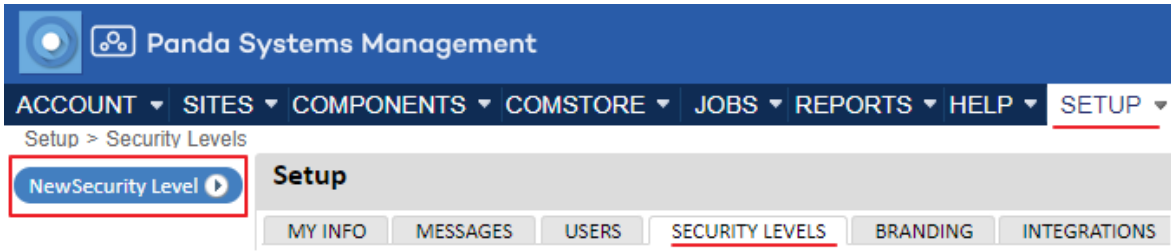


Figura 19.3: ventana para la gestión de roles

- Haz clic en el menú general **Ajustes** y en el botón **Nuevo rol** del panel lateral izquierdo.
- Indica el nombre, la descripción y un rol anterior si quieres copiar su configuración para modificarla posteriormente.
- Haz clic en el botón **Salvar**. Se mostrará la pantalla de configuración de roles. Consulta el punto "**Configuración de roles**" en la página **302** para obtener más información sobre los permisos asignados a un rol.

Borrar un rol

Haz clic en el icono situado a la derecha del rol a borrar.

> *Si al borrar un rol tiene cuentas de usuario asignadas, se nos preguntará qué nuevo rol será asignado a esas cuentas.*

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.

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

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.

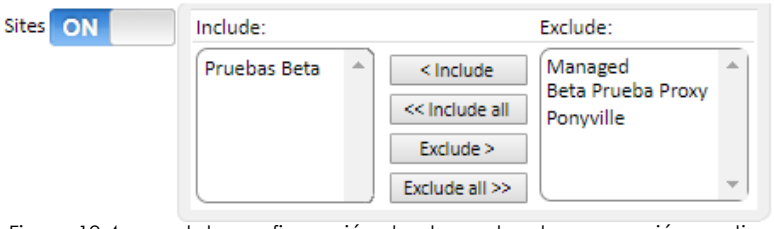


Figura 19.4: panel de configuración de elementos de agrupación por tipo

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.

Visibilidad de filtros

La visibilidad de dispositivos a través de filtros no cuenta con una configuración especifica en el menú de pestañas **Roles**, sino que se accede al crear o editar un filtro de forma independiente. Para modificar el acceso a un filtro sigue los pasos mostrados a continuación:

- Haz clic en el menú general **Zonas** para acceder a los filtros de cuenta o haz clic en una zona para acceder a los filtros de zona.
- Crea un filtro nuevo o edita uno existente. Consulta "**Filtros**" en la página **75**.
- En la ventana de configuración activa la casilla **Compartir este filtro con usuarios con los siguientes roles** y utiliza los botones **Añadir** y **Eliminar** para incluir o excluir roles del acceso al filtro.

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.

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 (menú de pestañas). 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.

Herramientas del Agente explorador

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).

Miembros

Configura las cuentas de usuario que pertenecen al rol modificado.

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.

Roles de tipo horizontal

Como norma general, una empresa con varias delegaciones y un equipo de IT independiente por cada delegación buscarán 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:

- Una zona o grupo de dispositivos que agrupe a los dispositivos de la delegación.
- Un 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.

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.

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.

Capítulo 20

Seguridad y control de acceso al servicio

Para mejorar la seguridad del acceso al servicio Panda Systems Management 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.

CONTENIDO DEL CAPÍTULO

Autenticación en dos fases (2FA)

Autenticación en dos fases (2FA - Two Factor Authentication) obliga al uso de un segundo dispositivo para validar las credenciales del administrador introducidas en la pantalla de inicio de sesión 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.*

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.

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**.

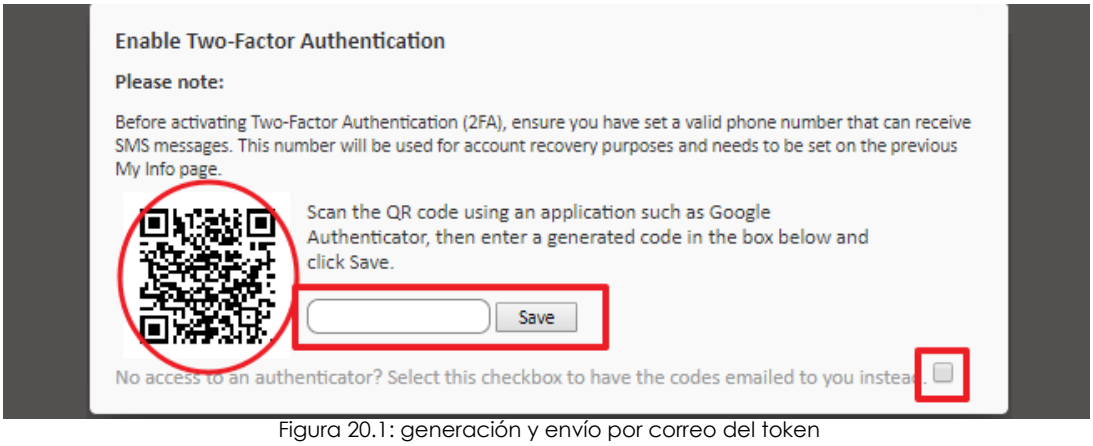


Figura 20.1: generación y envío por correo del token

- Se mostrará 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**" en la página **309**).
- 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`.
- 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.

Instalación de Google Authenticator

Para la instalación de `Google Authenticator` 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**.
- Pulsa en **Scan a barcode** para escanear el código QR mostrado en la consola.
- La aplicación comenzará a generar token de forma automática. Cada token tiene un periodo de validez de 30 segundos.

Habilitar 2FA 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.

Desactivar 2FA desde la pantalla de inicio de sesión

Desde la pantalla de inicio de sesión, 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.

Restablecer el estado

Los administradores pueden restablecer el estado 2FA de un usuario en caso de que haya perdido su dispositivo móvil. Para ello sigue los pasos mostrados a continuación:

- Accede a **Ajustes** desde el menú general y desde aquí a la pestaña **Usuarios**.

- En esta pantalla se encuentra el icono  con el que se realiza la recuperación.
- Selecciona el usuario, o usuarios, sobre los que se va a realizar la recuperación con la casilla de selección y haz clic en el icono indicado.

La autenticación en dos pasos habrá sido desactiva, y requiere su reactivación, tal y como se presenta en "**Configuración**".

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.

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.

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.

Capítulo 21

Registro de actividad

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.

CONTENIDO DEL CAPÍTULO

Registro de actividad del Nivel Cuenta

Haz clic en el menú general **Cuenta**, 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.

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.

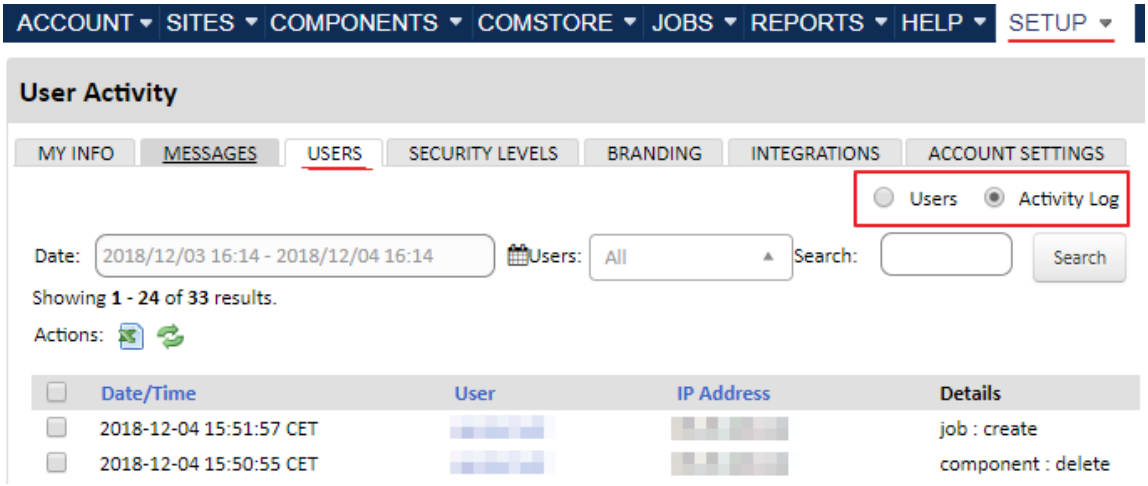


Figura 21.1: listado de acciones ejecutadas por el administrador

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.

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.

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** haz clic en la zona que contiene el dispositivo y en el dispositivo que quieres visualizar el registro de acciones.
- Haz clic en la pestaña **Auditoría** y en el control de selección **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.
- **Política**: si la actividad fue generada por una política, indica el nombre de la misma.
- **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.

Parte 7

Apéndices

Capítulo 22: Plataformas soportadas y requisitos

Capítulo 23: Código fuente

Capítulo 22

Plataformas soportadas y requisitos

En este capítulo se detallan las plataformas compatibles y los requisitos que tienen que cumplir los dispositivos de usuario para poder instalar y ejecutar correctamente el agente PCSM. No obstante, para aquellos dispositivos que no cumplan los requisitos indicados recuerda que Panda Systems Management es compatible con todo tipo de dispositivos a través del protocolo SNMP. Consulta el "**Integración de dispositivos de red**" en la página **57**.

CONTENIDO DEL CAPÍTULO

Plataformas soportadas por el agente PCSM

Para obtener información más detallada y actualizada consulta el enlace **https://www.pandasecurity.com/es/support/card?id=300102**

Windows

El agente PCSM requiere .NET6, conocido anteriormente como .NET Core.

Todos los dispositivos que utilizan TLS 1.0 y TLS 1.1 dejan de estar soportados por Panda Systems Management.

- Windows 7 32/64-bit (con KB4457144 [incluye KB2533623] y KB2999226 instalados)
- Windows 8/8.1 32/64-bit (con KB2999226 instalado)
- Windows 10 32/64-bit
- Windows 11
- Windows Server 2008 R2 SP1 64-bit (edición Standard) (con KB2533623 y KB2999226 instalados)
- Windows Server 2012 64-bit (con KB2999226 instalado)
- Windows Server 2012 R2 64-bit (con KB2999226 instalado)
- Windows Server 2016 64-bit
- Windows Server 2019 64-bit
- Windows Server 2022

Otros sistemas operativos Windows

- Las ediciones Home no están soportadas.
- Windows 10 Embedded (Windows IoT) no está soportado.
- Windows Server 2016 64-bit, Windows Server 2019 64-bit, y Windows Server 2022: el agente PCSM funcionará en Windows Server Core sin las funcionalidades de control remoto.

Apple Macintosh

El agente PCSM requiere las librerías Mono. Si el dispositivo no tiene instaladas las librerías Mono, el script de instalación las descargará e instalará de forma automática.

Dos últimas versiones de macOS.

Linux

El agente PCSM requiere las librerías Mono (paquete mono-devel) versión 4.8 y superiores. Si el dispositivo no tiene instaladas las librerías Mono, el script de instalación las descargará e instalará de forma automática, pero si ya está instalada una versión anterior de la librería, el agente PCSM no la actualizará y no funcionará de forma correcta. Puedes descargar las librerías de forma manual desde EPEL.

El agente PCSM puede funcionar en otras distribuciones de Linux diferentes de las indicadas. No obstante solo se soportan de forma oficial las distribuciones listadas.

- **Fedora**: versión 33 y superiores con el paquete yum-utils instalado
- **Debian**: versión10 y superiores con los paquetes libicu-dev, libssl-dev, libcurl4 y yum-utils instalados.
- **CentOS**: versión 7 y superiores con el paquete libicu instalado.
- **Ubuntu**: versión 18.04 y versiones 20.04 y superiores con los paquetes libicu-dev y libssl-dev instalados.
- **Red Hat Enterprise Linux:** versión 7 y superiores.

Exploradores compatibles

La consola web está probada con las dos últimas versiones de los navegadores listados a continuación:

- **Google Chrome**: aunque todos los navegadores basados en Chromium deberían de funcionar sin problemas, solo se ofrece soporte técnico para Google Chrome. Algunos navegadores que utilizan el motor Chromium son:
  - Microsoft Edge
  - Vivaldi
  - Brave
- **Mozilla FireFox**
- **Safari**

Requisitos de administración VMWare ESXi

Los servidores VMWare se gestionan a través de dispositivos con el rol Nodo de red activado. No es necesario que el nodo de red y el servidor ESXi residan en la misma subred.

Requisitos del dispositivo Nodo de red que gestiona servidores ESXi

- La cuenta utilizada para conectar con el servidor ESXi tiene que ser root.

- Se recomienda que el dispositivo con el rol Nodo de red asignado para monitorizar al servidor ESXi no resida en el propio servidor ESXi.

Requisitos VMWare ESXi

Panda Systems Management es compatible con las versiones ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 y 7.0.

Para la versión VMWare ESXi 6.5 y superiores 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
```

Capítulo 23

Código fuente

A continuación se incluye el código fuente en Visual Basic Script de los componentes mostrados en los capítulos "**Componentes y ComStore**" y "**Distribución e instalación centralizada de software**".

Quarantine monitor

```
Option Explicit
'**********************************************************************
'Quarantine_Monitor v1.0
'v.1.0: 4/12/2018
'v.099b: 06/03/2013
'By Oscar Lopez / Panda Security
'Target: this script monitors changes on EP quarantine folder
'Input:EP_PATH environment variable
'Output: stdout "Result=n new items detected in EP quarantine",
'**********************************************************************

dim WshShell,WshSysEnv
dim objFSO,objFolder,colFiles
dim iCountPast,iCountNow,iCount

Set WshShell=CreateObject("WScript.Shell")
Set objFSO=CreateObject("Scripting.FileSystemObject")

'Access to environment variable and quarantine path
On error resume Next
    Set WshSysEnv=WshShell.Environment("PROCESS")
    Set objFolder=objFSO.GetFolder(WshSysEnv("EP_PATH"))

    if Err.number<>0 then
        'PCSM didn't send the environment variable
```

```
        Err.clear
        WScript.Echo"<-StartResult->"
        WScript.Echo"Result=PCOP_PATH variable not defined on PCSM console or path
not found"
        WScript.Echo"<-EndResult->"
        Set WshShell=nothing
        Set WshSysEnv=nothing
        Set objFolder=nothing
        WScript.Quit(1)
    end if
On error goto 0

'get the collection that contains the folder files
set colFiles=objFolder.files

'access to the registry for saving the count
On error resume Next
    'get previous file count
    iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor"))
    if Err.Number<>0 then
        'if error set to 0
        iCountPast=0
    end if
    iCountNow=colFiles.count
    'save the count
    WshShell.RegWrite "HKLM\Software\Panda Security\Monitor", iCountNow, "REG_SZ"

    Err.Clear
    Set colFiles = nothing
    set objFolder = nothing
    set WshShell = nothing
    set WshSysEnv = nothing
    set objFSO = nothing

    if iCountPast < iCountNow then
        iCount=iCountNow-iCountPast
    else
        iCount=0
    end if
    WScript.Echo "<-Start Result->"
```

```
    WScript.Echo "Result=" & iCount & " new items in EP quarantine"
    WScript.Echo "<-End Result->"
    WScript.Quit (0)
On error goto 0
WScript.Quit (0)
```

Deploy Files

```
Option Explicit
'**********************************************************************
'Deploy_documents v1.0
'v.099b: 12/03/2013
'v.1.0: 4/12/2018
'By Oscar Lopez / Panda Security
'Target: It creates a folder in the user's desktop and copy on it the
'documents to deploy
'Input:
'-Files to copy
'-PCSM_PATH: script var with the folder on user's desktop where files will be
copied
'-USERDESKTOP: global var with the path to the user desktop.
'Output: code 0: OK
'Output: code 1: NO OK. "Deploy unsuccessful"
'**********************************************************************

Dim CONST_PATH
Dim objFSO,objFolder,colFiles
dim WshShell,WshSysEnv

Set WshShell=WScript.CreateObject("WScript.Shell")

On Error Resume Next
    Set objFSO=CreateObject("Scripting.FileSystemObject")
    Set WshSysEnv=WshShell.Environment("PROCESS")
    Set objFolder=objFSO.GetFolder(WshSysEnv("PCSM_PATH"))

    If Err.Number=0 Then
        WScript.Echo "Deploy unsuccessful: The folder already exists"
        WScript.Quit (1)
    End If
```

```
    Err.Clear

    'The folder will be created in the user's desktop
     Set     objFolder     =     objFSO.CreateFolder(WshSysEnv("USERDESKTOP")     &
WshSysEnv("PCSM_PATH"))
    'the documents will be moved to the folder
    objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
    If Err.Number<>0 Then
        WScript.Echo "Deploy unsuccessful: " & Err.Description
        WScript.Quit (1)
    Else
        WScript.Echo "Deploy OK: All files were copied"
        WScript.Quit (0)
    End If
On Error Goto 0
WScript.Quit (0)
```