AUTHORIZED DOCUMENTATION

Ayuda de la consola de gestión

August 1, 2008

Novell®
ZENworks Endpoint Security Management

3.5

www.novell.com

Información legal

Novell, Inc. no otorga ninguna garantía respecto al contenido y el uso de esta documentación y específicamente renuncia a cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado. Asimismo, Novell, Inc. se reserva el derecho a revisar esta publicación y a realizar cambios en su contenido en cualquier momento, sin obligación de notificar tales cambios a ninguna persona o entidad.

Además, Novell, Inc. no ofrece ninguna garantía con respecto a ningún software y rechaza específicamente cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado. Por otra parte, Novell, Inc. se reserva el derecho a realizar cambios en cualquiera de las partes o en la totalidad del software de Novell en cualquier momento, sin obligación de notificar tales cambios a ninguna persona ni entidad.

Los productos o la información técnica que se proporcionan bajo este Acuerdo pueden están sujetos a los controles de exportación de Estados Unidos o a la legislación sobre comercio de otros países. Usted acepta acatar las regulaciones de los controles de exportaciones y obtener todas las licencias necesarias para exportar, reexportar o importar bienes. De la misma forma, acepta no realizar exportaciones ni reexportaciones a las entidades que se incluyan en las listas actuales de exclusión de exportaciones de EE.UU., así como a ningún país terrorista o sometido a embargo, tal y como queda recogido en las leyes de exportación de los EE.UU. Asimismo, se compromete a no usar el producto para fines prohibidos, como la creación de mísiles o armas nucleares, químicas o biológicas. Consulte la página Web de International Trade Services de Novell (http://www.novell.com/info/exports/) para obtener más información sobre la exportación del software de Novell. Novell no se responsabiliza de la posibilidad de que usted no pueda obtener los permisos de exportación necesarios.

Novell, Inc. posee derechos de propiedad intelectual relacionados con la tecnología que representa el producto descrito en este documento. En concreto, y sin limitación, estos derechos de propiedad intelectual pueden incluir una o más de las patentes de EE. UU. que aparecen en la página Web de Novell sobre patentes legales (http://www.novell.com/company/legal/patents/), y una o más patentes adicionales o solicitudes de patentes pendientes en EE. UU. y en otros países.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
EE. UU.
www.novell.com

Documentación en línea: para acceder a la documentación en línea más reciente acerca de éste y otros productos de Novell, visite la página Web de documentación de Novell (http://www.novell.com/documentation).

Marcas comerciales de Novell

Para obtener información sobre las marcas comerciales de Novell, consulte la lista de marcas registradas y marcas de servicio de Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiales de otros fabricantes

Todas las marcas comerciales de otros fabricantes son propiedad de sus propietarios respectivos.

Tabla de contenido

1 Uso de la consola de gestión de ZENworks Endpoint Security Management

La consola de gestión es el acceso y control central de Management Service de Novell® ZENworks® Endpoint Security.

Para lanzar la ventana de inicio de sesión de la consola de gestión, haga clic en *Inicio* > *Todos los programas* > *Novell* > *Consola de gestión ESM* > *Consola de gestión*. Para entrar en la consola, especifique el nombre y la contraseña del administrador. El nombre de usuario introducido debe ser un usuario autorizado de Management Service (consulte Sección 1.3, “En uso Parámetros de configuración de los permisos”, en la página 10).

Nota: Recomendamos que cierre o minimice la consola si no se está utilizando.

1.1 Uso de la barra de tareas

La barra de tareas situada a la izquierda proporciona acceso a las tareas de la consola de gestión. Si no se puede ver la barra de tareas, haga clic en el botón *Tareas* situado en la parte izquierda de la consola.

Las siguientes secciones contienen más información sobre las tareas que se pueden realizar mediante la barra de tareas:

- Sección 1.1.1, “Tareas de directiva”, en la página 8
- Sección 1.1.2, “Recursos”, en la página 8

- Sección 1.1.3, “Configuración”, en la página 8
- Sección 1.1.4, “Auditoría de los puntos finales”, en la página 9

1.1.1 Tareas de directiva

La función principal de la consola de gestión consiste en crear y aplicar directivas de seguridad para los dispositivos de punto final gestionados. Las tareas de directiva guían al administrador a través de la creación y edición de las directivas de seguridad que utiliza ZENworks® Security Client para aplicar la seguridad gestionada centralmente a todos los dispositivos de punto final.

Entre las tareas de directivas se incluyen las siguientes:

- **Directivas activas:** muestra una lista de directivas actuales que se pueden revisar y editar. Haga clic en una directiva para abrirla.
- **Crear directiva:** lanza el asistente para directivas nuevas, lo cual le permite crear una directiva de seguridad nueva.
- **Importar directiva:** muestra el cuadro de diálogo Importar una directiva, lo cual le permite importar directivas creadas con otros servicios de gestión. Para obtener más información, consulte la Sección 2.3.1, “Importación de directivas”, en la página 107.

Si hace clic en cualquiera de las tareas de directivas, se minimizará la barra de tareas. Haga clic en el botón *Tareas* situado a la izquierda para volver a abrirla.

Consulte Capítulo 2, “Creación y distribución de las directivas de seguridad”, en la página 45 para obtener más información acerca de las tareas de directiva y cómo crear y gestionar directivas de seguridad.

1.1.2 Recursos

La lista de tareas de Recursos muestra los recursos de ayuda y asistencia técnica disponibles:

- **Póngase en contacto con el servicio de asistencia técnica:** lanza un navegador y muestra la página de oficinas y contacto de Novell®.
- **Asistencia técnica en línea:** lanza un navegador y muestra la página de asistencia y formación de Novell.
- **Ayuda de la consola de gestión:** lanza la ayuda en línea de ZENworks® Endpoint Security Management.

1.1.3 Configuración

La ventana Configuración de Management Service proporciona controles tanto para la infraestructura de servidores de ZENworks® Endpoint Security Management como para monitorizar los servicios adicionales de directorio de empresas. Para obtener más información, consulte la Sección 1.4, “Utilización de la ventana Configuración”, en la página 14. Este control no está disponible cuando se ejecuta la consola de gestión independiente. Para obtener más información, consulte la *Guía de instalación de ZENworks Endpoint Security Management*.

1.1.4 Auditoría de los puntos finales

La ventana de auditoría final proporciona acceso a las características de alertas e informes de ZENworks® Endpoint Security Management.

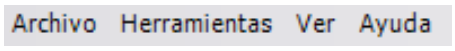
Generación de informes: La generación de informes es fundamental en la evaluación e implementación de directivas de seguridad robustas. A los informes se puede acceder a través de la consola de gestión, haciendo clic en *Informes*. La información de seguridad de los puntos finales recopilada y devuelta también es totalmente configurable, y se puede recopilar por dominio, grupo o usuario individual. Para obtener más información, consulte la Sección 1.6, “Utilización de informes”, en la página 29.

Alertas: La monitorización de alertas garantiza que cualquier intento de poner en peligro las directivas de seguridad corporativas se indica en la Consola de gestión. Las alertas informan al administrador de ZENworks Endpoint Security Management de los posibles problemas, y permiten al administrador tomar las medidas correctivas adecuadas. La consola de alertas es totalmente configurable, y proporciona un control sobre el momento y la frecuencia con la que se activan las alertas. Para obtener más información, consulte la Sección 1.5, “Utilización de la monitorización de alertas”, en la página 25.

1.2 Uso de la barra de menús

La barra de menús de ZENworks® Endpoint Security Management proporciona acceso a todas las funciones de la consola de gestión

Están disponibles las siguientes opciones:



- **Archivo:** utilice el menú Archivo para crear y gestionar directivas de seguridad.
  - **Crear directiva nueva:** lanza el asistente de directivas nuevas que le permite crear una directiva de seguridad nueva.
  - **Actualizar lista de directivas:** actualiza la lista de directivas para mostrar todas las directivas activas.
  - **Directiva de supresión:** suprime la directiva seleccionada.
  - **Importar directiva:** le permite importar una directiva a la consola de gestión.
  - **Exportar directiva:** exporta una directiva y el archivo `setup.sen` necesario a una ubicación especificada fuera de la base de datos de Management Service.
  - **Salir:** cierra el software de la consola de gestión y saca al usuario de la sesión.
- **Herramientas:** utilice el menú Herramientas para controlar la configuración de Management Service, las claves de cifrado y los permisos.
  - **Configuración:** abre la ventana Configuración.
  - **Exportar claves de cifrado:** abre el cuadro de diálogo de exportación de las claves de cifrado, en el que se especifican las claves que desea exportar y la contraseña.
  - **Importar claves de cifrado:** abre el cuadro de diálogo de importación de las claves de cifrado, en el que se especifican las claves que desea importar y la contraseña.

- **Generar clave nueva:** genera una clave de cifrado nueva que se utiliza para aplicar la protección de datos.
- **Permisos:** abre la ventana Permisos.

- **Ver:** utilice el menú Ver para realizar las tareas de directivas de claves sin utilizar la barra de tareas.
  - **Directiva:** si hay alguna directiva abierta, cambia la vista a dicha directiva.
  - **Activar directivas:** muestra la lista de directivas.
  - **Alertas:** muestra la consola de alertas.
  - **Generación de informes:** muestra la consola de informes.
- **Ayuda:** muestra la herramienta de ayuda de la consola de gestión y el cuadro de diálogo Acerca de:
  - **Ayuda:** lanza la ayuda en línea de la consola de gestión, que le guía a través de la creación de directivas y de las tareas de la consola de gestión. También podrá acceder a la ayuda presionando la tecla F1 de su teclado.
  - **Acerca de la consola de gestión:** lanza la ventana Acerca de, que muestra el tipo de instalación (ZENworks Endpoint Security Management o UWS) y el número de versión actual de la consola de gestión. Esta ventana es también el lugar en que se introduce la clave de licencia, en caso de que se adquiera después de la instalación.

1.3 En uso Parámetros de configuración de los permisos

este control se encuentra en el menú Herramientas y a él sólo puede acceder el Administrador primario de Management Service y cualquiera al que dicho administrador haya otorgado permisos de acceso. Este control no está disponible cuando se ejecuta la consola de gestión independiente.

Los parámetros de configuración de los permisos definen el usuario o grupo de usuarios a los que se les permite acceso a la consola de gestión, permisos administrativos o parámetros de configuración de la publicación.

Durante la instalación del servidor de gestión, se introduce un nombre de cuenta de recurso o administrador para el usuario de recurso en el formulario de configuración (consulte la *Guía de instalación de ZENworks Endpoint Security Management*). Una vez que se haya realizado una prueba satisfactoria y se haya guardado la información de usuario, se concederán automáticamente todos los permisos a ese usuario.

Una vez que se haya instalado la consola de gestión, el usuario del recurso es el único usuario con permisos completos, aunque a todos los grupos de usuarios dentro del dominio se les concede acceso a la consola de gestión. El usuario del recurso debe eliminar el acceso de todos los grupos o usuarios que no necesiten tener acceso. El usuario del recurso puede definir permisos adicionales para los usuarios designados.

Cuando se lanza la Consola de gestión, los permisos se recuperan de la tabla de permisos. Estos permisos indican a la consola si el usuario tiene los derechos necesarios para entrar en la consola, crear o suprimir directivas, cambiar los parámetros de configuración de los permisos y si puede o no publicar directivas, y a quién tiene permiso para publicárselas.

Los parámetros de configuración de acceso disponibles son los siguientes:

- **Acceso a la consola de gestión:** el usuario puede ver las directivas y los componentes y editar las directivas existentes. Los usuarios a los que sólo se les haya otorgado este privilegio no se les permitirá añadir o suprimir directivas; las opciones de publicación y permisos no estarán disponibles.
- **Publicar directiva:** el usuario puede publicar directivas únicamente en los usuarios o grupos asignados.
- **Cambiar permisos:** el usuario puede acceder y cambiar los parámetros de configuración de los permisos de otros usuarios ya definidos, y puede otorgar permisos a usuarios nuevos.
- **Crear directivas:** El usuario puede crear directivas nuevas en la consola de gestión.
- **Suprimir directivas:** el usuario puede suprimir cualquier directiva en la consola de gestión.

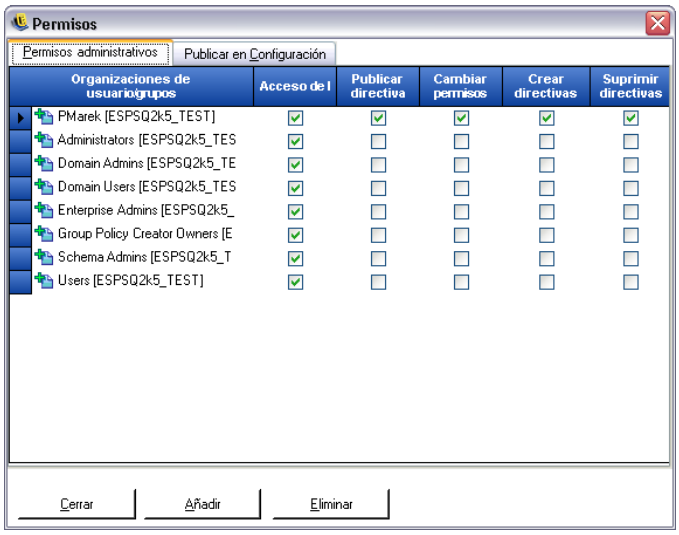
Nota: Por cuestiones de seguridad, se recomienda que los permisos de cambiar y suprimir directivas se otorguen sólo al usuario del recurso o a muy pocos administradores.

1.3.1 Permisos administrativos

Para ajustar los permisos administrativos:

1 Haga clic en *Herramientas* > *Permisos*.

Se mostrarán los grupos asociados a este dominio.

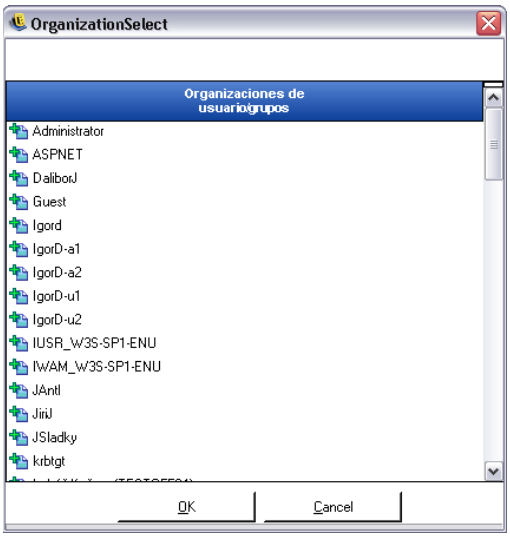


Nota: Por defecto, a todos los grupos se les otorgará acceso a la consola de gestión, aunque no puede realizar tareas de la directiva. El acceso a la consola se puede eliminar desmarcando el permiso.

---

2 Para cargar usuarios o grupos en esta lista:

2a Haga clic en el botón *Añadir* situado en la parte inferior de la pantalla.



2b Seleccione los usuarios o grupos pertinentes en la lista. Para seleccionar varios usuarios, selecciónelos uno a uno manteniendo pulsada la tecla Ctrl, o bien seleccione una serie seleccionando el primero, luego pulsando la tecla Mayús y, a continuación, seleccionando el último.

2c Cuando se hayan seleccionado todos los usuarios o grupos, haga clic en el botón *Aceptar*.

3 Asigne cualquiera de los permisos (o todos) a los usuarios o grupos disponibles.

Para eliminar un usuario o grupo seleccionado, seleccione el nombre y, a continuación, haga clic en *Eliminar*. El nombre seleccionado se devolverá a la Tabla Organización.

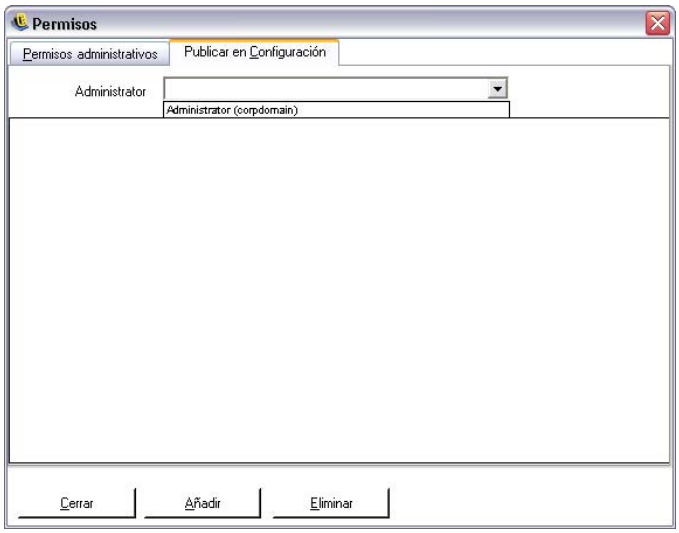
1.3.2 Parámetros de configuración de la publicación

A los usuarios o grupos que tienen *Publicar directiva* marcada se les debe asignar usuarios o grupos a los que publicar.

Para ajustar los parámetros de configuración de la publicación:

1 Haga clic en la pestaña *Parámetros de configuración de la publicación*.

2 Seleccione los usuarios o grupos de la lista desplegable a los que se les han concedido permisos de publicación.



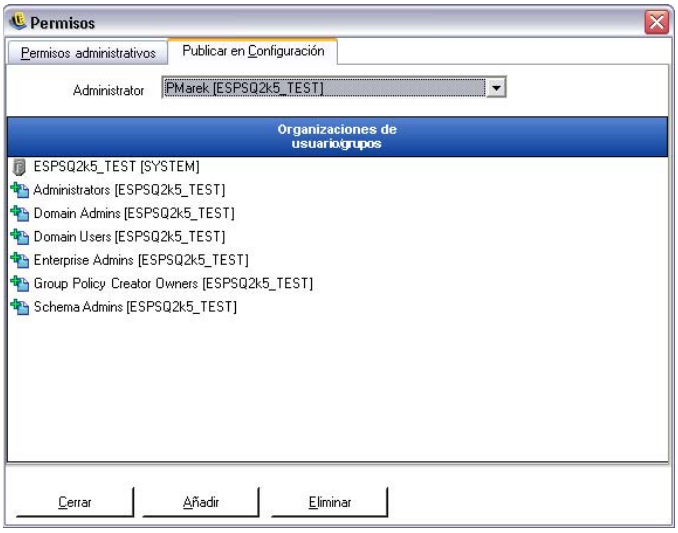
3 Asigne usuarios o grupos a este usuario/grupo:

3a Haga clic en el botón *Añadir* situado en la parte inferior de la pantalla para visualizar la Tabla Organización.

3b Seleccione los usuarios o grupos pertinentes de la lista. Puede utilizar las teclas Ctrl y Mayús para seleccionar varios usuarios.

3c Una vez que se hayan seleccionado todos los usuarios o grupos, haga clic en el botón *Aceptar* para añadir usuarios y grupos a la lista de la publicación

del nombre seleccionado.



Los conjuntos de permisos se implementan inmediatamente.

4 Para eliminar un usuario o grupo seleccionado, seleccione el nombre en la lista y, a continuación, haga clic en *Eliminar*.

5 Haga clic en *Cerrar* para aceptar los cambios y volver al editor.

El nombre seleccionado se devolverá a la Tabla Organización.

Si se añade un nuevo servicio de directorio (consulte “Autenticación de directorios” en la página 16), se le conceden permisos totales a la cuenta de recursos introducida, como se ha descrito anteriormente.

1.4 Utilización de la ventana Configuración

La ventana Configuración proporciona al administrador de ZENworks® Endpoint Security Management acceso a los controles *Infraestructura y programación*, *Autenticación de directorios* y *Sincronización de servidor*. Haga clic en el enlace *Configuración* de la página principal, o haga clic en el menú *Herramientas* y, a continuación, en *Configuración*. Se visualizará la ventana Configuración.

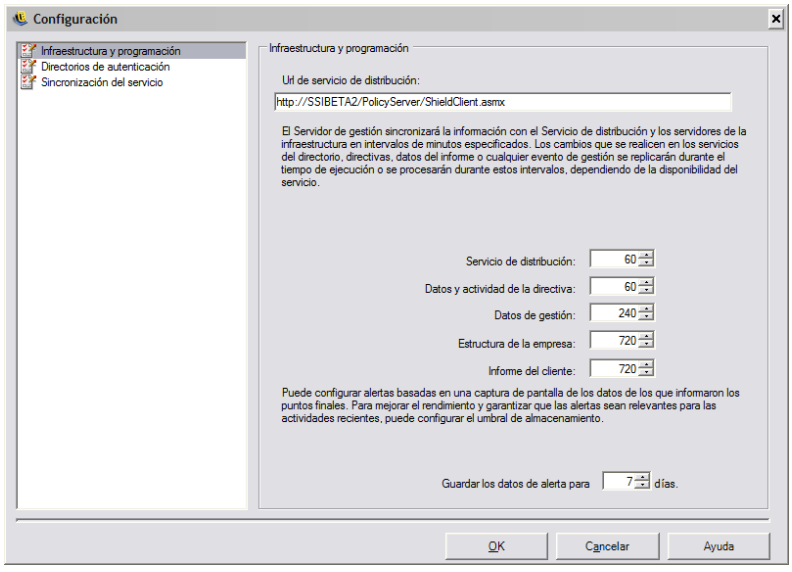
Nota: Esta función no está disponible con una consola de gestión independiente.

Las secciones siguientes contienen más información sobre:

- Sección 1.4.1, “Infraestructura y programación”, en la página 14
- Sección 1.4.2, “Autenticación de directorios”, en la página 16
- Sección 1.4.3, “Sincronización de servicios”, en la página 24

1.4.1 Infraestructura y programación

El módulo de infraestructura y programación permite al administrador de ZENworks Endpoint Security Management designar y cambiar la URL de Policy Distribution Service y controla los intervalos de sincronización de los componentes de ZENworks Endpoint Security Management.



Las secciones siguientes contienen más información sobre:

- “URL de Distribution Service” en la página 15
- “Programación” en la página 15

URL de Distribution Service

El parámetro de configuración*URL de Distribution Service* actualizará la ubicación de Policy Distribution Service tanto en Management Service como en todos los ZENworks Security Clients (sin que sea necesario volver a instalar) si Policy Distribution Service se mueve a un servidor nuevo. La URL del servidor actual aparece en el campo de texto.

Si necesita cambiar el servidor, cambie únicamente el nombre del servidor para que apunte al servidor nuevo. Una vez que haya cambiado el nombre del servidor, no cambie más información.

Por ejemplo, si la URL actual aparece como `http:\\ACME\PolicyServer\ShieldClient.asmx` y Policy Distribution Service se instala en un servidor nuevo con el nombre ACME 43, la URL se debe actualizar a lo siguiente: `http:\\ACME43\PolicyServer\ShieldClient.asmx`

Una vez que se haya actualizado la URL, haga clic en *Aceptar* para actualizar todas las directivas y enviar una actualización automática de Policy Distribution Service. Así también se actualiza Management Service.

Al cambiar la URL del servidor, no debe terminar el antiguo Policy Distribution Service hasta que las directivas actualizadas tengan un nivel de adherencia del 100% (consulte Sección 1.6, “Utilización de informes”, en la página 29).

Programación

Los componentes de Programación permiten al administrador de ZENworks Endpoint Security Management designar el momento en que Management Service se va a sincronizar con los restantes componentes de ZENworks Endpoint Security Management, con el fin de garantizar que todos los datos y tareas en cola coinciden con alguna actividad reciente, y para programar las tareas de mantenimiento de SQL. Todos los incrementos de tiempo son en minutos.

La programación se desglosa de la siguiente forma:

- **Distribution Service:** programa de sincronización con Policy Distribution Service.
- **Policy Data and Activity:** programa de sincronización con las actualizaciones de las directivas.
- **Datos de gestión:** sincronización de directivas con Management Service.
- **Estructura empresarial:** programa de sincronización con el servicio de directorio de la empresa (eDirectory™, Active Directory*, NT Domain*, y/o LDAP). Los cambios en el servicio de directorio de la empresa se supervisan para que los cambios correspondientes en las asignaciones de directivas de usuario se puedan detectar y enviar a Policy Distribution Service para la autenticación de los clientes.
- **Creación de informes de clientes:** La frecuencia con la que Management Service interroga y descarga datos de informes de Policy Distribution Service.
- **Keep alert data for:** puede configurar alertas basándose en una instantánea de los datos que han enviado los puntos finales. Para optimizar el rendimiento y asegurarse de que las alertas son relevantes para una actividad reciente, puede ajustar el umbral de almacenamiento en función de un número concreto de días.

1.4.2 Autenticación de directorios

Después de instalar ZENworks® Endpoint Security Management, debe crear y configurar un servicio de directorio antes de empezar a gestionar los dispositivos en el sistema.

El nuevo asistente de configuración del servicio de directorio le permite crear una configuración del servicio de directorio que define el ámbito de las instalaciones clientes de ZENworks Endpoint Security Management de las que disponga. Esta nueva configuración hace uso del servicio de directorio existente para definir el límite lógico para las instalaciones clientes basadas tanto en el equipo como en el usuario.

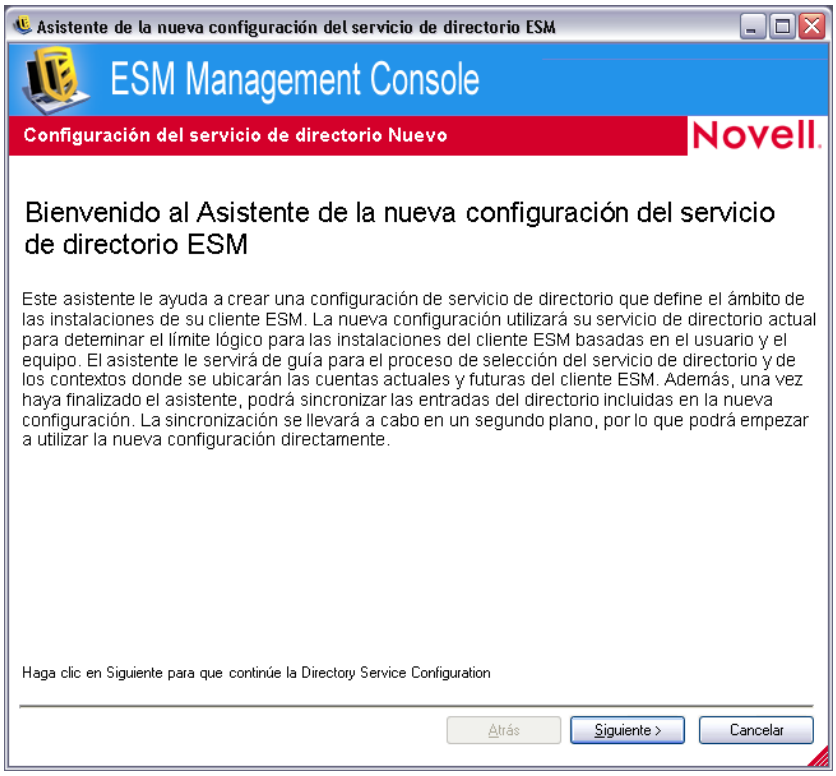
El asistente le guía en el proceso de selección del servicio de directorio y de los contextos en los que se encuentran las cuentas clientes actuales y futuras.

Además, este asistente le permite sincronizar las entradas de directorio incluidas en la nueva configuración. La sincronización se realiza en segundo plano, de forma que puede empezar a utilizar inmediatamente la nueva configuración.

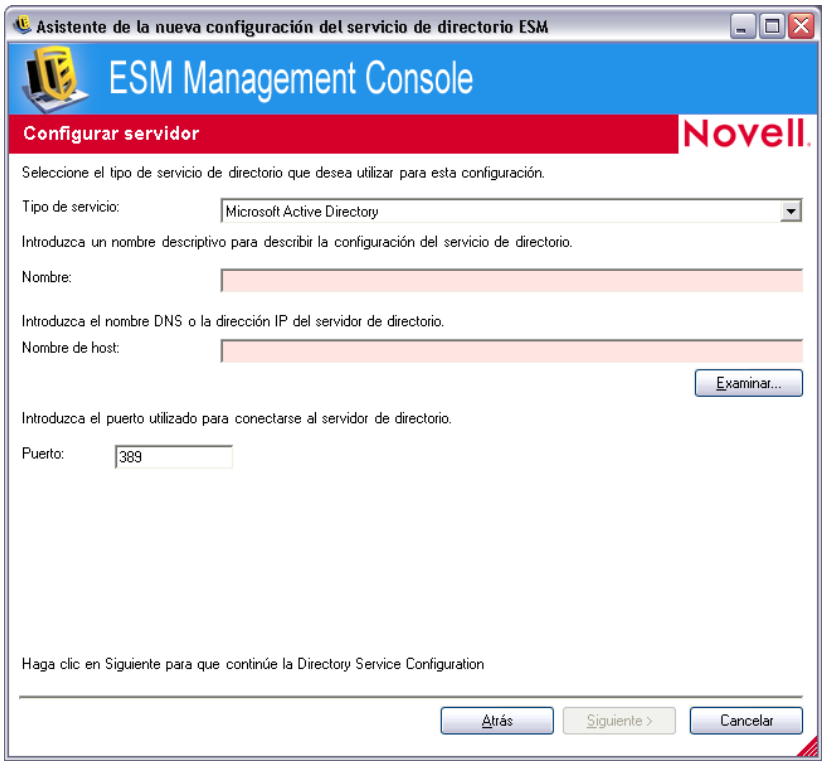
Después de instalar ZENworks Endpoint Security Management, aparece automáticamente el nuevo asistente de configuración del servicio de directorio. En caso de que ya haya instalado el producto y de que la página de bienvenida ya haya aparecido, vaya directamente a Paso 4 en el siguiente proceso.

Para configurar el servicio de directorio:

1. En la Consola de gestión, haga clic en *Herramientas* > *Configuración*.
2. Haga clic en *Directorios de autenticación*.
3. Haga clic en *Nuevo* para lanzar el nuevo asistente de configuración del servicio de directorio.



4 Haga clic en *Siguiente* para que aparezca la página Configurar servidor.

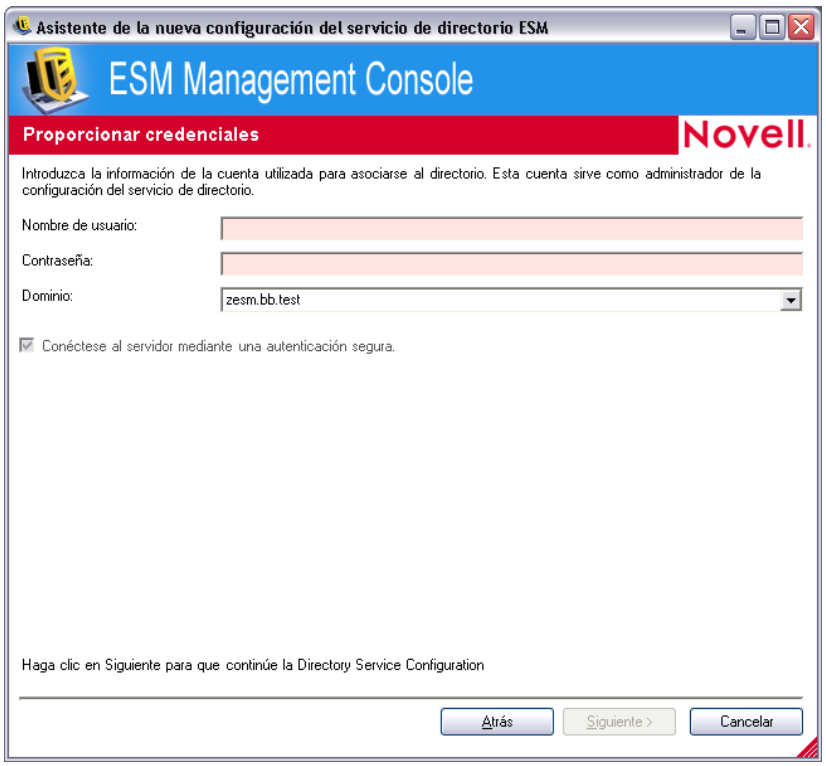


5 Rellene los campos:

- **Tipo de servicio:** Seleccione un tipo de servicio en la lista desplegable *Tipo de servicio*:
  - Microsoft Active Directory
  - Novell eDirectory
- **Nombre:** Especifique un nombre descriptivo para describir la configuración del servicio de directorio.
- **Nombre del host:** Especifique o examine el nombre DNS o la dirección IP del servidor de directorio.
- **Puerto:** Especifique el puerto utilizado para conectarse al servidor de directorio.

  El puerto por defecto es el 389. Si utiliza un puerto diferente para conectarse al servidor de directorio, puede especificar dicho puerto.

6 Haga clic en *Siguiente* para que aparezca la página Proporcionar credenciales.



7 Rellene los campos:

- **Usuario:** Especifique el administrador de la cuenta para asociarse al directorio.

  Esta cuenta sirve como administrador de la configuración del servicio de directorio. El nombre de entrada introducido debe ser un usuario que tenga permiso para ver todo el árbol del directorio. Es aconsejable que este usuario sea el administrador del dominio o un administrador de OU. Utilice un formato LDAP si va a configurar eDirectory, por ejemplo: `cn=admin,o=acmeserver` donde `cn` es el usuario y `o` es el objeto en el que se almacena la cuenta del usuario.

- **Contraseña:** Especifique la contraseña del administrador de la cuenta.

  Esta cuenta sirve como administrador de la configuración del servicio de directorio.

  La contraseña no debe ajustarse para que caduque, y esta cuenta no se debe inhabilitar nunca.

- **Domain (Dominio):** Especifique el dominio al que pertenece el administrador de la cuenta.

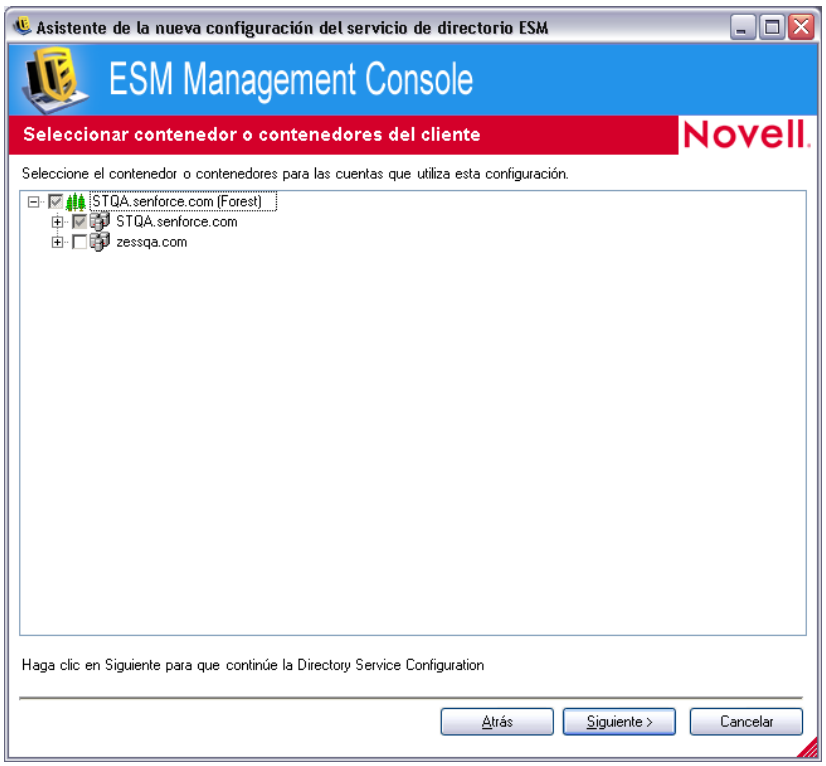
- **Conectarse al servidor mediante una autenticación segura:** Deseleccione esta opción si no desea usar la autenticación segura. Esta opción está habilitada por defecto.

8 Haga clic en *Next* (Siguiente) para continuar.

9 Si el usuario del administrador de la configuración que ha especificado en Paso 7 no puede encontrar el dominio, aparecerá la página Localizar entrada de la cuenta.

Especifique el contenedor en el que se encuentra el administrador y, a continuación, haga clic en *Siguiente*.

10 En la página Seleccionar Dominio o dominios de autenticación, examine el árbol para seleccionar los dominios que se usan para autenticar a los usuarios y equipos de esta configuración.



El dominio en el que se encuentra el usuario administrativo que ha especificado en Paso 7 se selecciona y no hay posibilidad de deseleccionarlo.

Cualquier instalación cliente que intente controlar la entrada con el servidor de gestión falla en caso de que no pertenezca a alguno de los dominios seleccionados en la configuración.

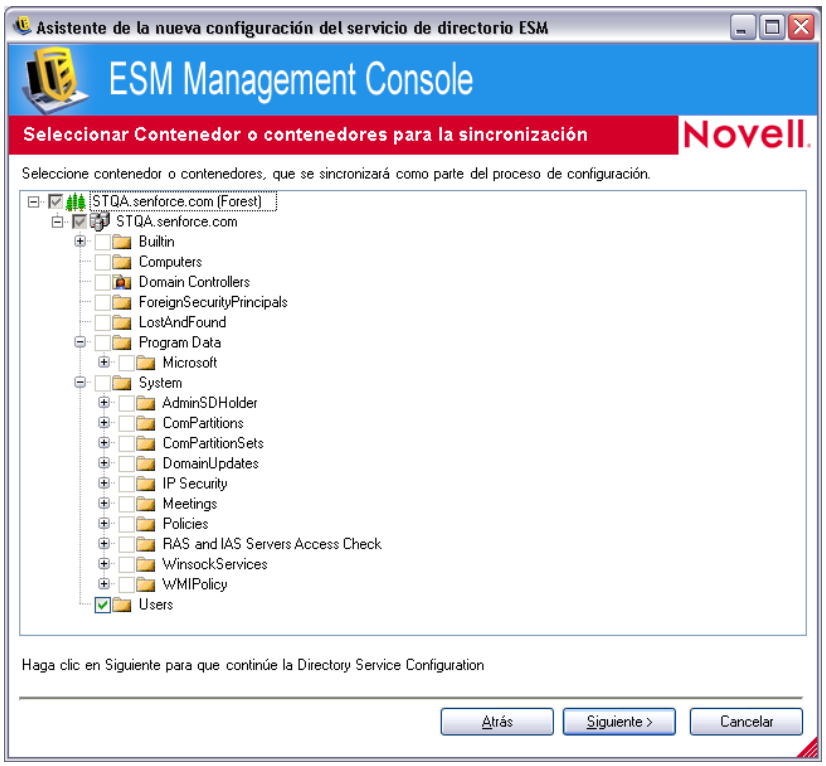
11 Haga clic en *Siguiente* para que aparezca la página Seleccionar contenedor o contenedores cliente y, a continuación, seleccione los contenedores para las cuentas que utiliza esta configuración.

El contenedor en el que se encuentra el usuario administrativo que ha especificado en Paso 7 se selecciona y no hay posibilidad de deseleccionarlo.

La página Seleccionar contenedor o contenedores clientes le permite limitar la búsqueda a aquellos contenedores que contengan usuarios y equipos gestionados, hecho que mejora el rendimiento.

Cualquier instalación cliente que intente controlar la entrada con el servidor de gestión falla en caso de que no se encuentre en alguno de los contenedores seleccionados en la configuración.

12 Haga clic en *Siguiente* para que aparezca la página Contenedor o contenedores para sincronización.



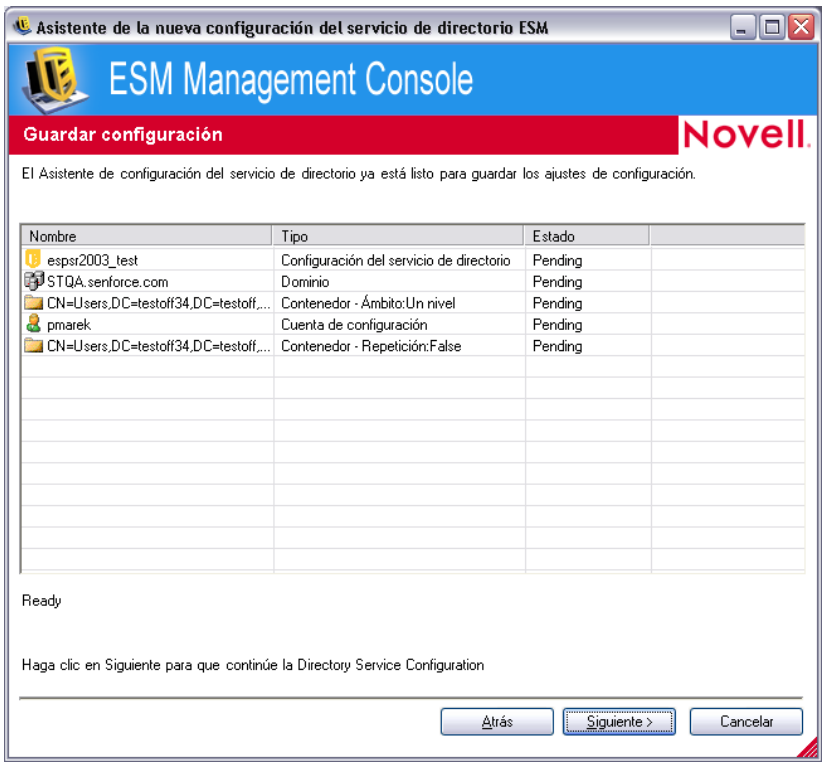
13 (Opcional) Seleccione los contenedores para sincronizarlos como parte del proceso de configuración.

La sincronización se realiza en segundo plano, de forma que puede empezar a utilizar inmediatamente la nueva configuración. En caso de que disponga de muchos equipos y usuarios para sincronizar, esta operación puede tardar algunas horas.

Si no especifica contenedores para sincronizar, los usuarios y los equipos que se encuentren en dichos contenedores se llenan en la Consola de gestión cuando controlan la entrada.

Al sincronizar los contenedores, la Consola de gestión se llena con antelación con dichos usuarios y equipos, de forma que le permite realizar acciones inmediatamente, tales como la creación de directivas de seguridad. Cuando los usuarios o equipos controlan la entrada en el sistema, dichas directivas se trasladan y se aplican. Al llenar la Consola de gestión con antelación, puede empezar inmediatamente a crear las directivas que son específicas para los usuarios y equipos independientes, más que a crear una directiva que se aplique a todos los usuarios y equipos del contenedor. Si no sincroniza el contenedor, debe esperar hasta que dichos usuarios y equipos controlen la entrada en el sistema antes de crear directivas exclusivas para los diferentes equipos y usuarios.

14 Haga clic en *Siguiente* para que aparezca la página Guardar configuración.

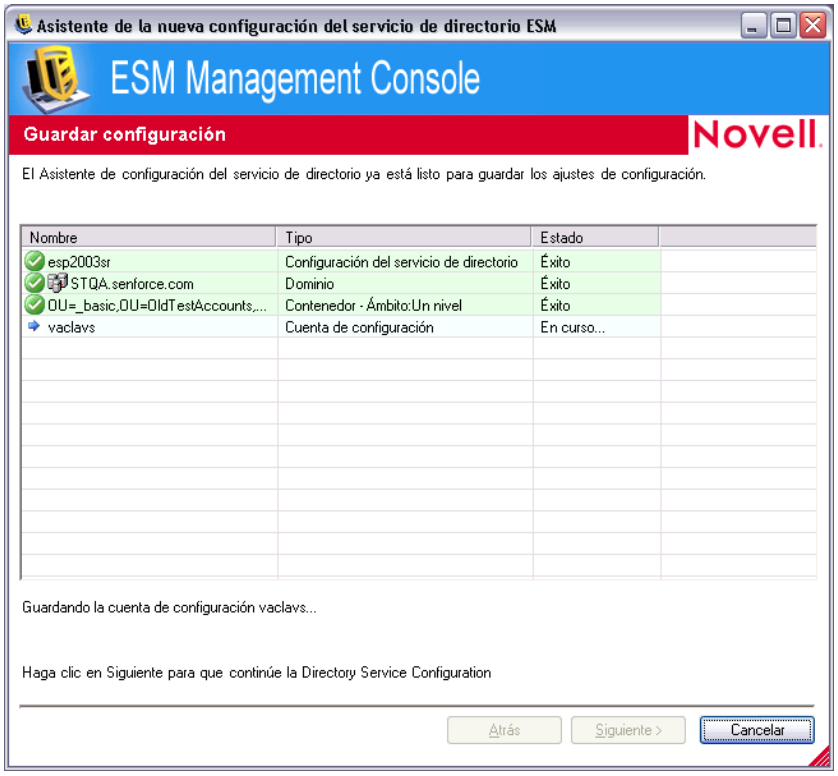


15 Revise la información y, a continuación, haga clic en *Siguiente* para guardar la configuración.

Puede hacer clic en *Atrás* para modificar cualquier valor de configuración en caso de que sea necesario.

16 Haga clic en *Finalizar.*

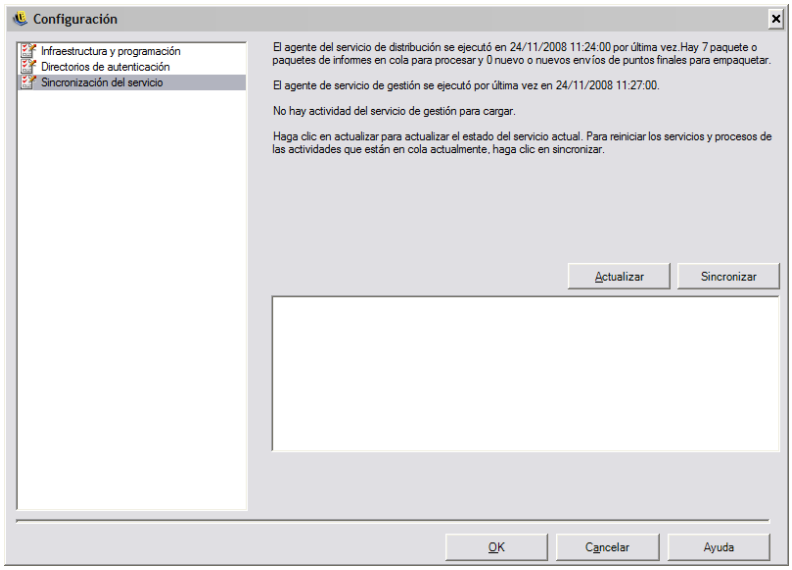
Al hacer clic en *Finalizar*, el icono aparece en la zona de notificación de Windows y empieza la sincronización. Puede hacer doble clic en el icono para que aparezca el cuadro de diálogo Sincronización de servicios de directorio.



La sincronización se produce en segundo plano. Si sale de la Consola de gestión, se detiene la sincronización. Si vuelve a abrir la consola de gestión, la sincronización se reanuda desde donde se detuvo.

1.4.3 Sincronización de servicios

Este control permite forzar una sincronización de Management Service y Policy Distribution Service. De esta forma se actualizarán todas las alertas, informes y la distribución de las directivas.

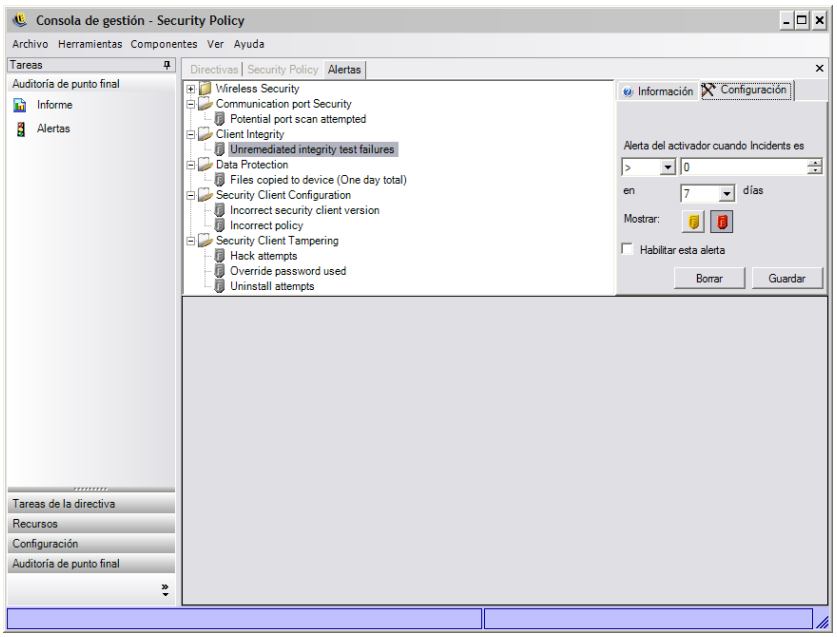


1. Para actualizar el estado actual de los servicios, haga clic en *Actualizar*.
2. Para reiniciar los servicios y procesar las actividades que están actualmente en la cola, haga clic en *Sincronizar*.

1.5 Utilización de la monitorización de alertas

La monitorización de alertas permite al administrador de ZENworks® Endpoint Security Management indicar el estado de seguridad de todos los puntos finales gestionados de ZENworks Endpoint Security Management de la empresa. Los activadores de alertas son totalmente configurables y pueden informar de una advertencia o una alerta de emergencia completa. A esta herramienta se accede a través de *Auditoría de los puntos finales* en la barra de tareas o del menú *Ver*.

1 Para acceder a alertas, haga clic en el icono Alertas (Alertas).



La monitorización de alertas está disponible para las siguientes áreas:

- **Integridad de los clientes:** Envía notificación de los resultados de las pruebas de integridad no solucionadas.
- **Seguridad de los puertos de comunicaciones:** Envía notificación de los potenciales intentos de exploraciones de puertos.
- **Protección de datos:** Envía notificación de los archivos que se copian a dispositivos de almacenamiento extraíbles dentro de un período de un día.
- **Configuración de los clientes de seguridad:** Envía notificación de que las versiones del cliente de seguridad no son correctas y de que las directivas no son correctas.
- **Manipulación de los clientes de seguridad:** Envía notificación de intentos de intrusión en el usuario, intentos de desinstalación y uso de la contraseña anulada.
- **Seguridad inalámbrica:** Envía notificación de los puntos de acceso no seguros, detectados y conectados por el usuario.

1.5.1 Configuración de las alertas de ZENworks Endpoint Security Management

La monitorización de alertas requiere que los datos de informes se recopilen y se carguen a intervalos regulares, con el fin de proporcionar la imagen más exacta posible del entorno actual de seguridad de los puntos finales. Los ZENworks® Security Clients no gestionados no proporcionan datos de informes y, por consiguiente, no se incluirán en la monitorización de alertas.

Las secciones siguientes contienen más información sobre:

- “Activación de le generación de informes” en la página 27
- “Optimización de la sincronización” en la página 27

Activación de le generación de informes

La generación de informes se debe activar en todas las directivas de seguridad. Para obtener información sobre cómo configurar la generación de informes en las directivas de seguridad, consulte Sección 2.2.4, “Información de cumplimiento”, en la página 102. Ajuste los tiempos de envíos de informes a un intervalo que le proporcione actualizaciones coherentes sobre el estado de los puntos finales. Además, ninguna alerta se activará si no hay un informe. Todas las actividades de las que desee recibir alertas, deben tener un informe pertinente asignado en la directiva de seguridad.

Optimización de la sincronización

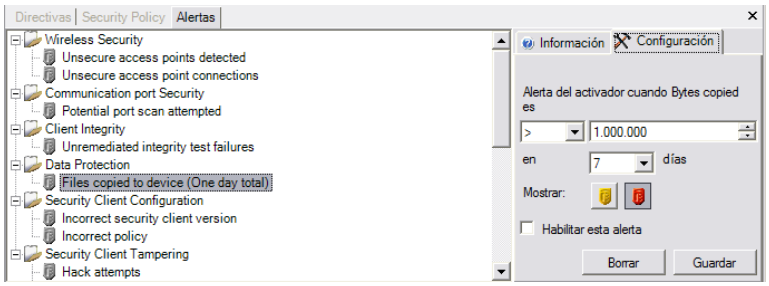
Por defecto, el servicio de información de ZENworks Endpoint Security Management se sincroniza cada 12 horas. Esto implica que el informe inicial y los datos de alerta no están listos hasta que hayan transcurrido 12 horas desde la instalación de ZENworks Endpoint Security Management. Para ajustar este marco temporal, abra la herramienta Configuración (consulte “Programación” en la página 15) y ajuste el tiempo de *informes de clientes* al número de minutos que más se ajuste a sus necesidades y a su entorno.

Si los datos se necesitan inmediatamente, la opción *Sincronización de servicios* de la herramienta Configuración puede lanzar inmediatamente Policy Distribution Service (que recopila los datos de los informes de los puntos finales) y Reporting Service (que actualizará todas las alertas en función de los datos recién recopilados). Consulte el Sección 1.4.3, “Sincronización de servicios”, en la página 24 para obtener más información.

1.5.2 Configuración de activadores de alertas

los activadores de alertas se pueden ajustar a los umbrales que más se ajusten a las necesidades de seguridad de la empresa.

1. Seleccione una alerta de la lista y haga clic en la pestaña *Configuración* situada a la derecha de la consola de gestión.



2. Para ajustar el umbral de los activadores, en primer lugar seleccione un estado de la lista desplegable. Así se indica si el número del activador es:
   - Igual a (=)
   - Mayor que (<)
   - Mayor o igual que (<=)
   - Menor que (>)
   - Menor o igual que (>=)
3. Ajuste el número del activador. Este número varía en función del tipo de alerta.

4 Seleccione el intervalo en el que se debe encontrar este número.

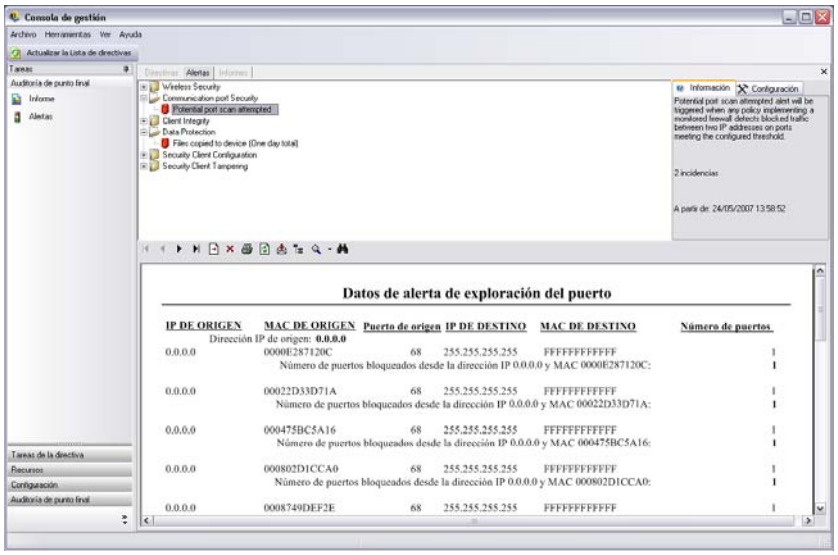
5 Seleccione el tipo de activador. Puede ser un icono de advertencia ( ) o un icono de emergencia ( ).

6 Compruebe que está habilitada la casilla *Habilitar esta alerta*.

7 Haga clic en *Guardar* para guardar la alerta.

1.5.3 Gestión de alertas

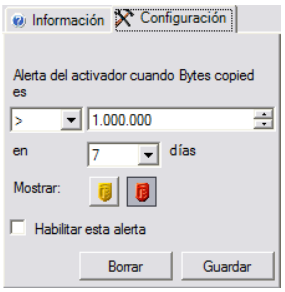
las alertas le notifican los problemas que se tienen que solucionar dentro del entorno de seguridad de los puntos finales. Las medidas correctoras se gestionan normalmente de forma individual o en grupo. Para ayudar a identificar el problema, se visualizan informes de las alertas al seleccionar la alerta.



Este informe muestra el resultado del activador actual, y la información se muestra por usuario o dispositivo afectado. Los datos que se aportan aquí proporcionan la información necesaria para tomar las medidas oportunas para corregir todos los potenciales problemas de seguridad de la empresa. Para encontrar información adicional, abra Informes.

Una vez que se hayan adoptado las medidas correctoras, la alerta permanecerá activa hasta la próxima actualización de los informes. Para borrar una alerta antes de una actualización programada:

1 Seleccione una alerta de la lista y haga clic en la pestaña *Configuración* situada a la derecha de la consola de gestión.



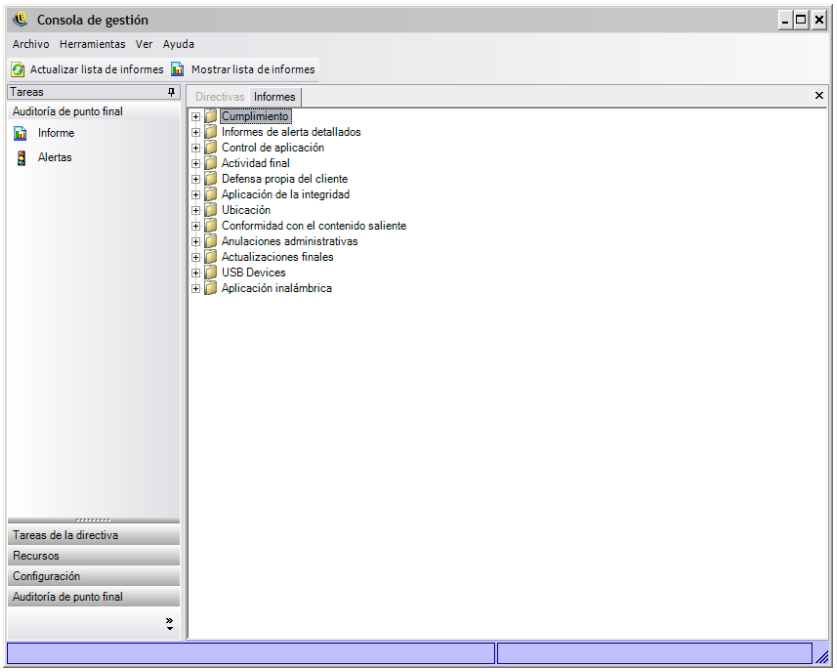
2 Haga clic en *Borrar*.

Así se borran los datos de informes de las alertas (estos datos aún están disponibles en la base de datos de informes). No se reactiva hasta que se reciben datos nuevos.

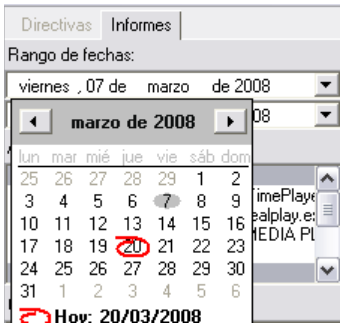
1.6 Utilización de informes

Reporting Service proporciona informes de cumplimiento y estado de la empresa. Los datos disponibles se proporcionan tanto para los directorios como para los grupos de usuarios de los mismos. Los informes de Novell® proporcionan información sobre los efectos que los componentes individuales de las directivas pueden tener en los puntos finales de la empresa. Las peticiones de estos informes se definen en la Directiva de seguridad (consulte Sección 2.2.4, “Información de cumplimiento”, en la página 102) y pueden proporcionar datos útiles para determinar las actualizaciones de las directivas.

Seleccione *Informes* de la barra de tareas *Auditoría de los puntos finales* o del menú *Ver*. Se visualizará la lista de informes disponibles (para expandir la lista, haga clic en los iconos con el signo más que hay junto a cada tipo de informe).



Los informes se configuran mediante la identificación del rango de fechas y otros parámetros, es decir, usuario o ubicación. Para ajustar las fechas, expanda la vista de calendario y, a continuación, seleccione el mes y el día. Asegúrese de hacer clic en el día para cambiar el parámetro de la fecha.



Haga clic en *Ver* para generar el informe.

Una vez que se genera un informe, puede utilizar la barra de herramientas de infomes para ver el informe a través de la consola de gestión, imprimir el informe y enviar por correo electrónico o exportar el informe como un archivo `.pdf`.

Durante la revisión de informes, los botones de flecha le ayudarán a desplazarse por cada una de las páginas del informe. Normalmente, los informes tendrán diagramas y gráficos en la primera página, y los datos recopilados en las páginas restantes, ordenados por fecha y tipo.

El botón de la *Impresora* imprimirá todo el informe utilizando la impresora por defecto de este equipo.

El botón *Exportar* guarda el informe como un archivo PDF, una hoja de cálculo de Excel*, un documento de Word o un archivo RTF.

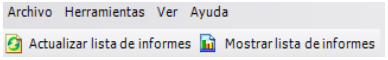
El botón *Árbol de grupos* conmutará una lista de parámetros en el lateral del informe. Seleccione cualquiera de estos parámetros para detallar más en el informe. Haga clic en el botón *Árbol de grupos* para cerrar la barra lateral.

El botón de la *lupa* proporciona un menú desplegable para ajustar el tamaño de la vista actual.

El botón de los *binoculares* abre una ventana de búsqueda.

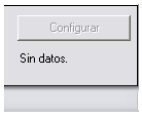
Al pasar el ratón sobre un parámetro concreto, como por ejemplo un nombre de usuario o un nombre de dispositivo, el puntero cambia y se convierte en una lupa. En ese momento puede hacer doble clic en ese elemento concreto y mostrar un informe nuevo de dicho objeto. Haga clic en el botón *Cerrar* para cerrar la vista actual y volver al informe original.

Para volver a la lista de informes, haga clic en el icono *Lista de informes*, que se encuentra encima de la ventana de informes.



Los informes no están disponibles hasta que los datos se hayan cargado desde los ZENworks® Security Clients. Por defecto, el servicio de informes de ZENworks Endpoint Security Management se sincroniza cada 12 horas. Esto significa que los informes iniciales y los datos de alertas no están preparados hasta que hayan transcurrido 12 horas desde la instalación de ZENworks Endpoint Security Management. Para ajustar este marco temporal, abra la herramienta Configuración (consulte "Programación" en la página 15) y ajuste el tiempo de *informes de clientes* al número de minutos que más se ajuste a sus necesidades y a su entorno.

Los informes que no tengan datos disponibles tendrán el botón *Configurar* o *Vista previa* atenuado y aparecerán las palabras "Sin datos" debajo.



Están disponibles los siguientes informes:

- Sección 1.6.1, "Informes de cumplimiento", en la página 31
- Sección 1.6.2, "Información adicional de las alertas", en la página 32
- Sección 1.6.3, "Informes de control de aplicaciones", en la página 33
- Sección 1.6.4, "Informes de soluciones de cifrado", en la página 34
- Sección 1.6.5, "Informes de la actividad de los puntos finales", en la página 34
- Sección 1.6.6, "Informes de actualizaciones de punto final", en la página 34
- Sección 1.6.7, "Informes de autodefensa de clientes", en la página 35
- Sección 1.6.8, "Informes de aplicación de la integridad", en la página 35
- Sección 1.6.9, "Informes de ubicación", en la página 35
- Sección 1.6.10, "Informes de cumplimiento del contenido saliente", en la página 36
- Sección 1.6.11, "Informe de anulaciones administrativas", en la página 37
- Sección 1.6.12, "Informes de actualizaciones de punto final", en la página 37
- Sección 1.6.13, "Informes de ejecución inalámbrica", en la página 38

1.6.1 Informes de cumplimiento

los informes de cumplimiento proporcionan información del cumplimiento relativa a la distribución de las directivas de seguridad a los usuarios gestionados. Un resultado de un 100% de cumplimiento indica que todos los usuarios gestionados han pasado por el control de entrada y han recibido la directiva actual.

Están disponibles los informes siguientes:

- **Cumplimiento del control de entrada de los puntos finales:** Proporciona un resumen de los días desde el control de entrada realizado por los puntos finales de la empresa y la antigüedad de su directiva actual. Se hace una media de estos números para resumir el informe. Este

informe requiere que no se introduzcan variables. El informe mostrará los usuarios por nombre, qué directivas se les han asignado, los días transcurridos desde su último control de entrada y la antigüedad de su directiva.

- **Versiones del cliente final:** Muestra la última versión que se conoce del cliente de cada punto final. Defina los parámetros de los datos para generar este informe.
- **Puntos finales que nunca realizan el control de entrada:** Enumera las cuentas de usuario que se han registrado en el Servicio de gestión, pero que nunca han buscado actualizaciones de directivas en el Servicio de distribución. Para generar el informe, seleccione uno o varios grupos.

  Es posible que haya usuarios de la consola de gestión que no tengan ningún cliente de seguridad instalado en sus nombres.
- **Incumplimiento de las directivas de grupos:** Muestra los grupos en los que algunos usuarios no tienen la directiva correcta. Para generar el informe se pueden realizar selecciones de uno o varios grupos.
- **Historial del estado de los puestos finales por equipo:** muestra el estado más reciente (en un rango de fechas dado) de los puntos finales protegidos por ZENworks Endpoint Security Management, agrupados por nombre de equipo. Muestra el nombre de usuario que ha iniciado sesión, la directiva actual, la versión del cliente de ZENworks Endpoint Security Management y la ubicación de la red. Este informe requiere que se introduzca un rango de fechas. El administrador puede profundizar haciendo doble clic en cualquiera de las entradas y verá una lista completa de informes sobre el estado de un equipo concreto.
- **Asignación de directivas:** muestra qué usuarios y grupos (cuentas) han recibido la directiva especificada. Seleccione en la lista la directiva deseada y haga clic en *Ver* para ejecutar el informe.
- **Historial del estado de los puntos finales por usuario:** Muestra el estado más reciente (en un rango de fechas dado) de los puntos finales protegidos por ZENworks Endpoint Security Management, agrupados por nombre de usuario. Muestra el nombre de la máquina, la directiva actual, la versión del cliente de ZENworks Endpoint Security Management y la ubicación de la red. Este informe requiere que se introduzca un rango de fechas. El administrador puede profundizar haciendo doble clic en cualquiera de las entradas y verá una lista completa de informes sobre el estado de un usuario concreto.

1.6.2 Información adicional de las alertas

La información adicional de las alertas proporciona información sobre las alertas . Estos informes sólo muestran datos cuando se activa una alerta. Al borrar cualquier alerta, también se borrará el informe de la alerta; sin embargo, en los informes estándar los datos seguirán estando disponibles.

Están disponibles los informes siguientes:

- **Datos de alerta de manipulación de cliente:** Muestra instancias en las que un usuario ha realizado un intento no autorizado de modificación o inhabilitación de ZENworks Security Client.
- **Datos de alerta de archivos copiados:** muestra cuentas que han copiado datos a dispositivos de almacenamiento extraíbles.

- **Datos de alerta de versión incorrecta del cliente:** muestra el historial del estado del proceso de actualización de ZENworks Security Client.
- **Datos de alerta de directiva incorrecta del cliente:** Muestra los usuarios que no tienen la directiva correcta.
- **Datos de alerta de errores en la integridad:** informa sobre el historial de las comprobaciones con éxito y fallidas de la integridad de los clientes.
- **Datos de alerta de intentos de redefinición:** muestra las instancias en las que los mecanismos de autodefensa del cliente se han redefinido administrativamente, otorgando control con privilegios sobre ZENworks Security Client.
- **Datos de alerta de exploración de puertos:** muestra el número de paquetes bloqueados en el número de puertos diferentes (un número de puertos elevado puede indicar que se ha producido una exploración de puertos).
- **Datos de alerta de intentos de desinstalación:** enumera los usuarios que han intentado desinstalar ZENworks Security Client.
- **Datos de alerta de puntos de acceso no seguros:** enumera los puntos de acceso no seguros detectados por ZENworks Security Client.
- **Datos de alerta de conexiones a puntos de acceso no seguros:** enumera los puntos de acceso no seguros conectados mediante ZENworks Security Client.

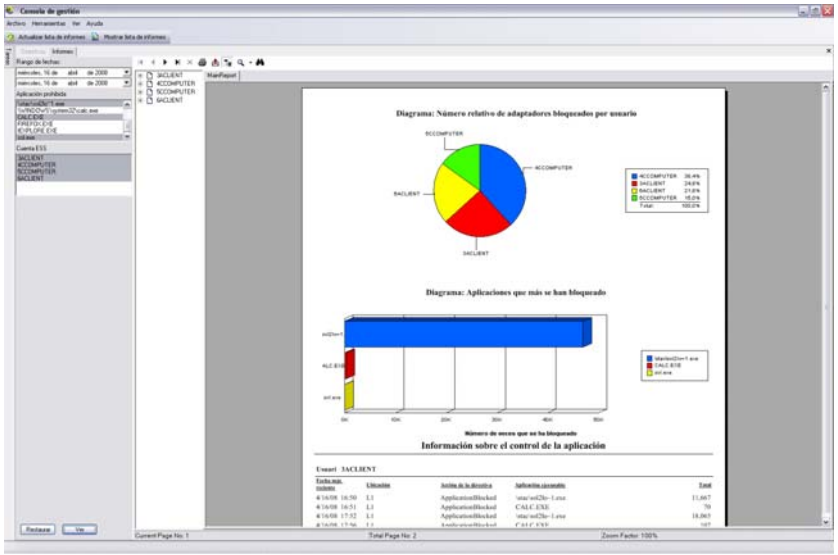
1.6.3 Informes de control de aplicaciones

los informes de control de aplicaciones muestran todos los intentos no autorizados que realizan las aplicaciones bloqueadas para acceder a la red o para ejecutarse cuando la directiva no lo permite.

Está disponible el siguiente informe:

- **Detalles del control de aplicaciones:** Muestra la fecha, ubicación, medida emprendida por ZENworks® Security Client, la aplicación que se intentó ejecutar y el número de veces que se lanzó la aplicación. Las fechas se muestran en formato UTC.

Especifique los parámetros de fecha, seleccione en la lista los nombres de la aplicación, seleccione las cuentas de usuario y haga clic en *Ver* para ejecutar el informe.



1.6.4 Informes de soluciones de cifrado

Si se activa el cifrado del punto final, los informes de soluciones de cifrado muestran la transferencia de archivos a y desde las carpetas cifradas.

Están disponibles los siguientes informes:

- **Actividad del cifrado de archivos:** Muestra los archivos a los que se ha aplicado el cifrado.
- **Excepciones del cifrado:** muestra los errores del subsistema de cifrado (por ejemplo, un archivo protegido no se pudo descifrar porque el usuario no tenía las claves correctas).
- **Volúmenes del cifrado de archivos:** muestra los volúmenes (por ejemplo, las unidades extraíbles o las particiones del disco duro) que ha gestionado la solución de cifrado de Novell.

1.6.5 Informes de la actividad de los puntos finales

los informes de actividad de los puntos finales proporcionan información de los componentes individuales de la directiva y el efecto que tienen en la operación del punto final.

Están disponibles los informes siguientes:

- **Paquetes bloqueados por direcciones IP:** Muestra los paquetes bloqueados filtrados por IP de destino. Las fechas se visualizan en formato UTC.

  Seleccione en la lista la IP de destino y defina los parámetros de fecha. El informe muestra las fechas, ubicaciones, puertos afectados y el nombre de los paquetes bloqueados.
- **Paquetes bloqueados por usuario:** Muestra los paquetes bloqueados filtrados por usuario. Las fechas se muestran en formato UTC. Los datos son esencialmente los mismos que los paquetes bloqueados por IP de destino, pero desglosados por usuario.
- **Network Usage Statistics by User:** Enumera los paquetes enviados, recibidos o bloqueados, y los errores de la red, filtrados por usuarios. Este informe requiere un rango de fechas. Las fechas se muestran en formato UTC.
- **Network Usage Statistics by Adapter Type (datos de uso de red por tipo de adaptador):**

  Enumera los paquetes enviados, recibidos o bloqueados, y errores de la red filtrados por tipo de adaptador. Este informe requiere que se introduzca un rango de fechas y la ubicación. Las fechas se muestran en formato UTC.

1.6.6 Informes de actualizaciones de punto final

Los informes de actualizaciones de punto final muestran el estado del proceso de actualización de ZENworks Security Client (consulte “Actualizar ZSC” en la página 63). Las fechas se muestran en formato UTC.

Están disponibles los informes siguientes:

- **Diagrama del porcentaje de errores en las actualizaciones del cliente de seguridad:** Crea un diagrama de las actualizaciones de ZENworks Security Client que han fallado y para las que no se ha encontrado solución. Para generar este informe no se requieren parámetros.

- **Historial del estado de actualización de Security Client:** Muestra el historial del estado del proceso de actualización de ZENworks Security Client. Seleccione el rango de fechas y haga clic en *Ver* para ejecutar el informe. El informe muestra qué usuarios han pasado el control de entrada y han recibido la actualización.
- **Diagrama de los tipos de actualizaciones del cliente de segurridad fallidos:** Muestra las actualizaciones de ZENworks Security Client que han dado error y no se han remediado. Seleccione el rango de fechas y haga clic en Vista para ejecutar el informe. El informe muestra qué usuarios han pasado el control de entrada, pero no pudieron instalar las actualizaciones.

1.6.7 Informes de autodefensa de clientes

Los informes de autodefensa de clientes le permiten saber cuándo intentan los usuarios modificar o inhabilitar ZENworks® Security Client.

Está disponible el siguiente informe:

- **Intentos de intrusión en ZENworks Security Client:** informa de las instancias en las que un usuario ha realizado un intento no autorizado de modificar o inhabilitar ZENworks Security Client. Las fechas se muestran en formato UTC.

  Introduzca los parámetros de fecha y haga clic en *Ver* para ejecutar el informe.

1.6.8 Informes de aplicación de la integridad

los informes de aplicación de la integridad proporcionan resultados de integridad antivirus/programa de protección anti-espía.

Están disponibles los siguientes informes:

- **Historial de la integridad de los clientes:** Informa sobre el éxito o error de las comprobaciones de integridad de los clientes. Las fechas se muestran en formato UTC.

  Seleccione el rango de fechas para el informe, las reglas de integridad y los nombres de usuarios.
- **Errores de integridad sin solucionar por regla:** Los informes sobre las reglas de integridad y las pruebas que han fallado y aún no se han solucionado.

  Seleccione las reglas de integridad y haga clic en *Ver* para ejecutar el informe.
- **Errores de integridad sin solucionar por usuario:** Informa de los usuarios que no han superado las pruebas de integridad y aún no han obtenido ninguna solución.

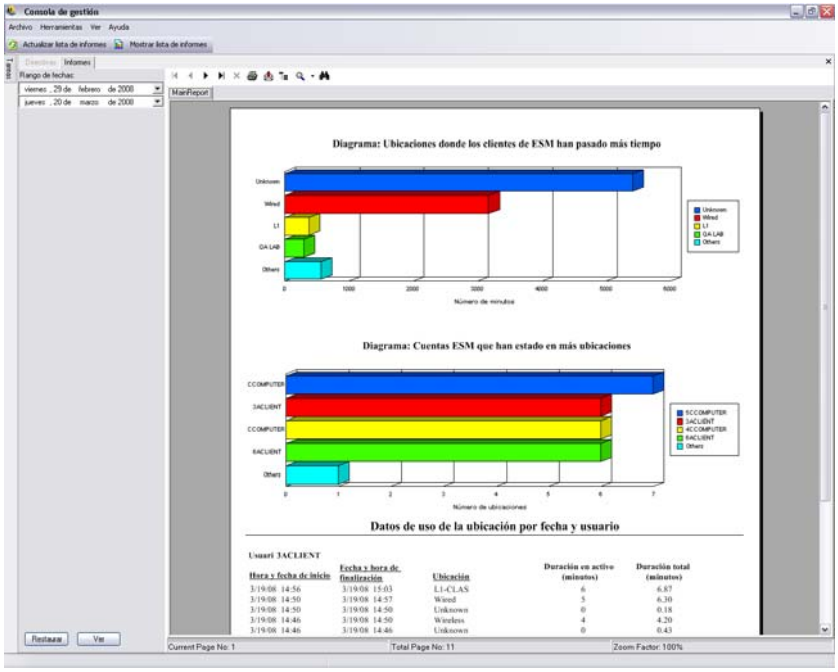
  Seleccione los nombres de usuarios y haga clic en *Ver* para ejecutar el informe.

1.6.9 Informes de ubicación

El informe de ubicación proporciona datos para el uso de ubicación habitual, como las ubicaciones que los usuarios utilizan más habitualmente.

Está disponible el siguiente informe:

Datos de uso de la ubicación por fecha y usuario: Proporciona información recogida de los clientes individuales acerca de qué ubicaciones se utilizan y cuándo se utilizan. Las fechas se muestran en formato UTC. Las ubicaciones visualizadas son las ubicaciones que utiliza el usuario; las ubicaciones no utilizadas no se visualizan. Seleccione el rango de fechas para generar el informe.

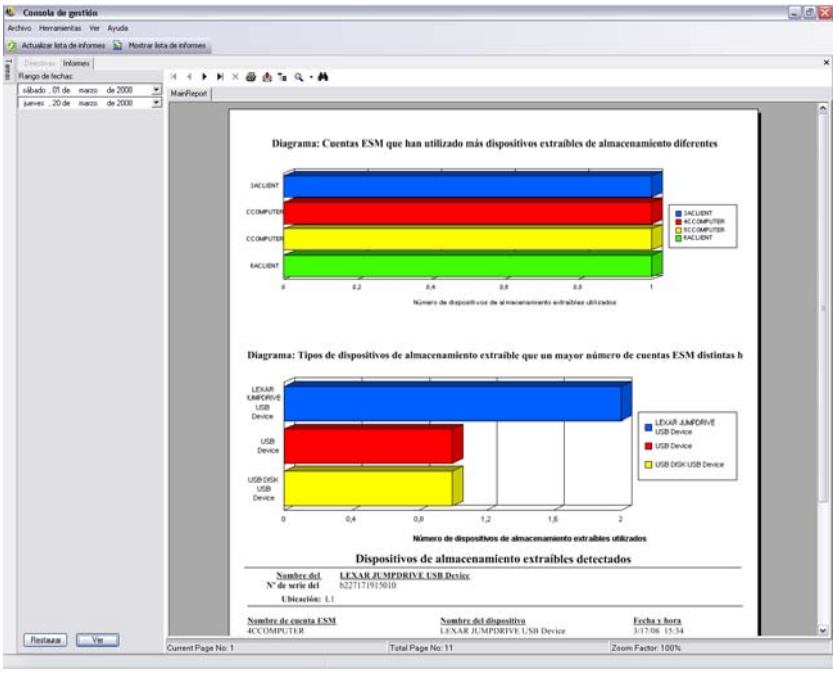


1.6.10 Informes de cumplimiento del contenido saliente

Los informes de cumplimiento del contenido saliente proporcionan información relativa al uso de unidades extraíbles e identifica qué archivos se han cargado en dichas unidades.

Están disponibles los siguientes informes:

- **Actividad del almacenamiento extraíble por cuenta:** Muestra cuentas que han copiado datos a un dispositivo de almacenamiento extraíble. Para generar este informe no se requieren parámetros.
- **Actividad del almacenamiento extraíble por dispositivo:** Muestra los dispositivos de almacenamiento extraíbles a los que se han copiado los archivos. Seleccione el rango de fechas, nombres de usuarios y ubicaciones para generar este informe.
- **Copias del almacenamiento extraíble por cuenta:** Muestra los archivos que se han copiado desde los dispositivos de almacenamiento extraíbles en los dispositivos gestionados.
- **Dispositivos de almacenamiento extraíble detectados:** Muestra los dispositivos de almacenamiento extraíbles que se han detectado en el punto final. Seleccione el rango de fechas, nombres de usuarios y ubicaciones para generar este informe.



- **Diagrama de actividad del almacenamiento extraíble en 7 días:** Muestra un diagrama de las cuentas que se han copiado recientemente a un dispositivo de almacenamiento extraíble. Para generar este informe introduzca el rango de datos.

1.6.11 Informe de anulaciones administrativas

El informe de redefiniciones administrativas muestra las instancias en las que los mecanismos de autodefensa del cliente se han anulado administrativamente, otorgando control con privilegios sobre ZENworks® Security Client.

Está disponible el siguiente informe:

- **Anulaciones de ZENworks Security Client:** Muestra los intentos de anulación con éxito por usuario y fecha. Las fechas se muestran en formato UTC.

  Para ejecutar el informe, seleccione el usuario y el rango de fechas y, a continuación, haga clic en *Ver*.

1.6.12 Informes de actualizaciones de punto final

Los informes de actualizaciones de punto final muestran el estado del proceso de actualización de ZENworks® Security Client (consulte “Actualizar ZSC” en la página 63). Las fechas se muestran en formato UTC.

Están disponibles los siguientes informes:

- **Diagrama del porcentaje de errores en las actualizaciones de seguridad:** Crea un diagrama del porcentaje de actualizaciones de ZENworks Security Client que han dado error y para los que no se ha encontrado una solución. Para generar este informe no se requieren parámetros.

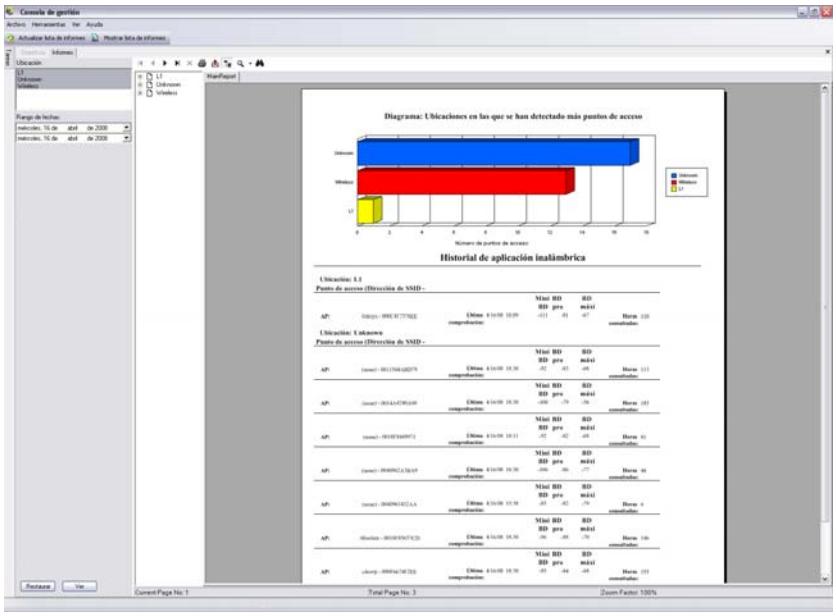
- **Historial del estado de actualización de Security Client:** Muestra el historial del estado del proceso de actualización de ZENworks Security Client. Seleccione el rango de fechas y haga clic en *Ver* para ejecutar el informe. El informe muestra qué usuarios han pasado el control y han recibido la actualización.
- **Diagrama de los tipos de actualizaciones del cliente de segurridad fallidos:** Muestra las actualizaciones de ZENworks Security Client que han dado error y que no se han solucionado. Seleccione el rango de fechas y haga clic en *Ver* para ejecutar el informe. El informe muestra qué usuarios han pasado el control de entrada, pero no pudieron instalar las actualizaciones.

1.6.13 Informes de ejecución inalámbrica

Los informes de ejecución inalámbrica proporcionan informes relativos a los entornos Wi-Fi a los que está expuesto el punto final.

Están disponibles los siguientes informes:

- **Disponibilidad de la conexión inalámbrica:** Muestra los puntos de acceso disponibles para la conexión por directiva y ubicación. Incluye el canal, SSID, la dirección MAC y si el punto de acceso está o no cifrado.
- **Intentos de conexión inalámbrica:** Proporciona una lista de puntos de acceso a los que se intentan conectar los dispositivos, por ubicación y cuenta.
- **Historial del entorno inalámbrico:** Proporciona un análisis de todos los puntos de acceso detectados, independientemente de la propiedad. Incluye la frecuencia, la fuerza de la señal y si el punto de acceso está o no cifrado. Las fechas se muestran en formato UTC. Para generar este informe, seleccione las ubicaciones deseadas y el rango de fechas.



1.7 Utilización de ZENworks Storage Encryption Solution

ZENworks® Storage Encryption Solution proporciona una gestión completa y centralizada de todos los datos móviles aplicando activamente una directiva de cifrado corporativa al propio punto final.

ZENworks Storage Encryption Solution permite hacer lo siguiente:

- Crear, distribuir, aplicar y auditar centralmente las directivas de cifrado de todos los puntos finales y dispositivos de almacenamiento extraíbles.
- Cifrar todos los archivos guardados o copiados en un directorio concreto en todas las particiones fijas del disco duro.
- Cifrar todos los archivos copiados a los dispositivos de almacenamiento extraíbles.
- Compartir archivos libremente dentro de una organización, al mismo tiempo que bloquea el acceso no autorizado a los archivos.
- Compartir archivos cifrados y protegidos mediante contraseña con personas fuera de la organización a través de una utilidad de descifrado disponible.
- Actualizar, realizar copias de seguridad y recuperar claves fácilmente a través de la directiva sin perder ningún dato.

1.7.1 Conocimiento de ZENworks Storage Encryption Solution

El cifrado de datos se aplica a través de la creación y distribución de las directivas de seguridad del cifrado de datos. Los datos confidenciales del punto final se pueden almacenar en una carpeta cifrada. El usuario puede acceder a estos datos y copiarlos fuera de la carpeta cifrada y compartir los archivos; sin embargo, mientras estén en dicha carpeta, los datos permanecen cifrados. Los intentos de lectura de los datos por parte de cualquiera que no sea un usuario autorizado de dicho equipo son infructuosos. Cuando la directiva se activa, una carpeta `Safe Harbor`(puerto seguro) cifrada se añade al directorio raíz de todos los volúmenes no pertenecientes al sistema en el puesto final.

Los datos confidenciales colocados en una memoria USB o en otro dispositivo de medios de almacenamiento extraíbles se cifrarán de inmediato y sólo pueden leerse en el equipo del mismo grupo de directivas. Como opción, se puede activar una carpeta compartida, lo que permitirá a los usuarios compartir los archivos con personas de fuera de su grupo de directivas a través de una contraseña (consulte “Cifrado de datos” en la página 61).

1.7.2 Uso compartido de archivos cifrados

los usuarios del mismo grupo de directivas (aquellos usuarios que han recibido la misma directiva de seguridad), disponen de las claves necesarias para acceder a los datos almacenados en el punto final, así como los datos movidos a las memorias USB y otros dispositivos extraíbles.

Los usuarios de otro grupo de directivas (con cifrado activado) pueden acceder a los datos cifrados colocados en la carpeta `Shared Files` a través de una contraseña de acceso. Estos usuarios no pueden leer los archivos cifrados que estén fuera de la carpeta `Shared Files`.

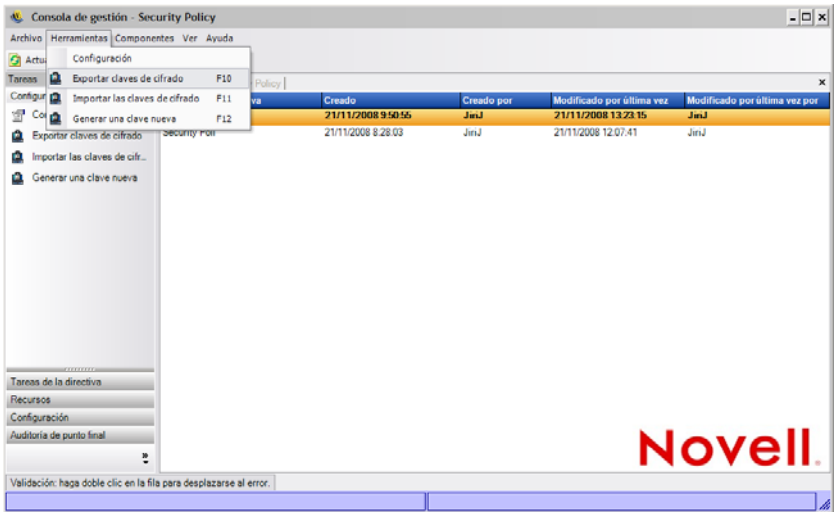
Los usuarios que no tienen habilitado el cifrado en su directiva y los usuarios que no tienen ZENworks Security Client instalado en sus equipos (por ejemplo, fuera de los contratistas) no pueden leer archivos fuera de la carpeta `Shared Files`. Requieren la utilidad ZENworks® File Decryption para leer archivos con acceso protegido con contraseña. Para obtener más información, consulte la Sección 1.9, “Uso de la utilidad de descifrado de archivos de ZENworks”, en la página 41.

1.8 Utilización de la gestión de claves

la gestión de claves permite hacer copias de seguridad, importar y actualizar una clave de cifrado. Se recomienda exportar y guardar las claves de cifrado, ya que así se tiene la certeza de que los datos se pueden descifrar en caso de fallo del sistema o cambio imprevisto de directiva.

La clave común es la clave de cifrado que se utiliza por defecto en todos los agentes de cifrado de datos. La clave de cifrado se puede actualizar si se ve comprometida, o como una precaución de seguridad. La generación de una clave común nueva provoca una reducción temporal del rendimiento, mientras el contenido gestionado se vuelve a cifrar.

A los controles de las claves de cifrado se accede a través del menú *Herramientas* de la consola de gestión.



1.8.1 Exportación de las claves de cifrado

con el fin de realizar copias de seguridad o enviar la clave a otra instancia de Management Service, el conjunto actual de claves de cifrado se puede exportar a una ubicación de archivo designada.

1. Haga clic en *Herramientas* > *Exportar claves de cifrado*.
2. Especifique la ruta con un nombre de archivo, o haga clic en el botón *Examinar* para navegar y seleccionar una ubicación del archivo.
3. Especifique una contraseña. Sin dicha contraseña la clave no se puede importar.
4. Haga clic en *Aceptar*.

En el archivo exportado se incluyen todos los archivos de claves de la base de datos.

1.8.2 Importación de las claves de cifrado

es posible importar claves de una copia de seguridad o de cualquier otra instancia de Management Service. Esto permite a los puntos finales gestionados por este Management Service leer archivos protegidos por otras instalaciones de ZENworks Endpoint Security Management. Al importar claves

se ignoran los duplicados. Las claves importadas pasan a formar parte de su conjunto de claves, pero no sustituyen a la clave común actual. Cuando se publica una directiva nueva, todas las claves bajan de nivel.

1. Haga clic en *Herramientas* > *Importar claves de cifrado*.
2. Especifique el nombre de archivo, incluida la ubicación del archivo, o haga clic en el botón *Examinar* para navegar y seleccionar el archivo de claves.
3. Especifique la contraseña de la clave de cifrado.
4. Haga clic en *Aceptar* para importar la clave a la base de datos.

1.8.3 Generación de una clave nueva

1. Haga clic en *Herramientas* > *Generar clave nueva*.

Todas las claves anteriores se almacenan en la directiva.

1.9 Uso de la utilidad de descifrado de archivos de ZENworks

La utilidad de descifrado de archivos de ZENworks® extrae los datos protegidos de la carpeta `Shared Files` de los dispositivos de almacenamiento cifrado extraíbles. Esta sencilla herramienta se puede proporcionar a terceros para que puedan acceder a los archivos de la carpeta `Shared Files`, aunque no se puede ubicar en el dispositivo de almacenamiento extraíble.

- Sección 1.9.1, “Uso de la utilidad de descifrado de archivos de”, en la página 41
- Sección 1.9.2, “Configuración de la utilidad de descifrado de archivos”, en la página 42

Las secciones siguientes contienen más información sobre:

1.9.1 Uso de la utilidad de descifrado de archivos de

Para emplear la utilidad de descifrado de archivos:

1. Conecte el dispositivo de almacenamiento en el puerto adecuado del equipo.
2. Abra la utilidad de descifrado de archivos.
3. Examine el directorio `Shared Files` del dispositivo de almacenamiento y seleccione el archivo que desee.
4. Para extraer directorios (carpetas) en lugar de archivos, haga clic en el botón *Avanzadas*, seleccione *Directorios* y, a continuación, examine el directorio adecuado (haga clic en *Basic* para volver a la vista por defecto).
5. Examine y seleccione el destino en el equipo local en el que están almacenados los archivos.
6. Haga clic en *Extraer*.

La transacción se puede monitorizar haciendo clic en el botón *Mostrar progreso*.

1.9.2 Configuración de la utilidad de descifrado de archivos

La utilidad de descifrado de archivos se puede configurar en modo administrador con el conjunto de claves actual y puede extraer todos los datos de un dispositivo de almacenamiento cifrado. No se recomienda esta configuración, ya que puede comprometer a todas las claves actuales utilizadas por ZENworks Storage Encryption Solution; no obstante, en los casos en los que los datos no se pueden recuperar, esta configuración podría ser necesaria.

Para configurar la herramienta:

1. Cree un acceso directo de la utilidad de descifrado de archivos en su directorio actual.
2. Haga clic con el botón derecho en el acceso directo y, a continuación, haga clic en *Propiedades*.
3. Al final del nombre de destino y después de las comillas, introduzca -k (por ejemplo: `"C:\Admin Tools\stdecrypt.exe" -k`).
4. Haga clic en *Aplicar* > *Aceptar*.
5. Abra le herramienta mediante el acceso directo y haga clic en *Avanzadas*.
6. Haga clic en el botón *Cargar claves* para abrir el cuadro de diálogo Importar clave.
7. Busque el archivo de claves y especifique la contraseña de las mismas.

Ya se pueden extraer todos los archivos cifrados con estas claves.

1.10 Utilización del generador de claves de contraseñas de anulación

Es probable que la merma de productividad que un usuario puede sufrir debido a restricciones de conectividad, la ejecución de software inhabilitado o el acceso a dispositivos de almacenamiento extraíbles se deba a la directiva de seguridad que ZENworks® Security Client aplica. El cambio de ajustes del cortafuegos o ubicaciones normalmente eleva estas restricciones y restaura la funcionalidad interrumpida. Sin embargo, en algunos casos, la restricción se puede implementar de tal forma que los usuarios estén restringidos en todas las ubicaciones y ajustes del cortafuegos, o que no puedan realizar ningún cambio de ubicación ni en los ajustes del cortafuegos.

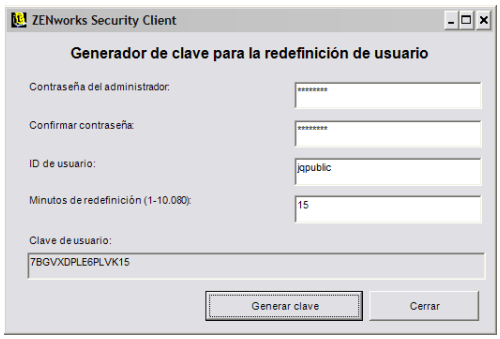
Cuando esto suceda, las restricciones de la directiva actual se pueden relajar a través de una anulación de contraseña, con el fin de permitir la productividad hasta que la directiva se pueda modificar. Esta función permite a los administradores configurar la anulación protegida mediante contraseña de usuarios y funciones específicas, lo que permite temporalmente las actividades necesarias.

Las anulaciones de contraseña inhabilitan la directiva de seguridad actual y restauran la directiva Todos abiertos por defecto durante un período de tiempo predefinido. Una vez que el límite de tiempo ha caducado, se restaura la directiva actual o actualizada. La contraseña de una directiva se define en los ajustes de reglas globales de la directiva de seguridad.

La anulación de la contraseña hace lo siguiente:

- Anula el bloqueo de las aplicaciones
- Permite a los usuarios cambiar las ubicaciones
- Permite a los usuarios cambiar los ajustes del cortafuegos
- Anula el control de hardware (memorias USB, CD-ROM, etc.).

La contraseña introducida en la directiva nunca se debería generar para un usuario. Debe utilizar el generador de claves de contraseña de anulación para generar una clave para su uso a corto plazo.



Para generar una clave de anulación:

1. Abra el generador de claves de contraseña de anulación *Inicio > Todos los programas > Novell > Consola de gestión de ESM > Generador de contraseñas de anulación*.
2. Especifique la contraseña de la directiva en el campo *Contraseña del administrador*, y confírmela en el siguiente campo.
3. Especifique el nombre de usuario con el que ha iniciado sesión el usuario final.
4. Especifique la cantidad de tiempo que debe estar inhabilitada la directiva.
5. Haga clic en el botón *Generar clave* para generar una clave de anulación.

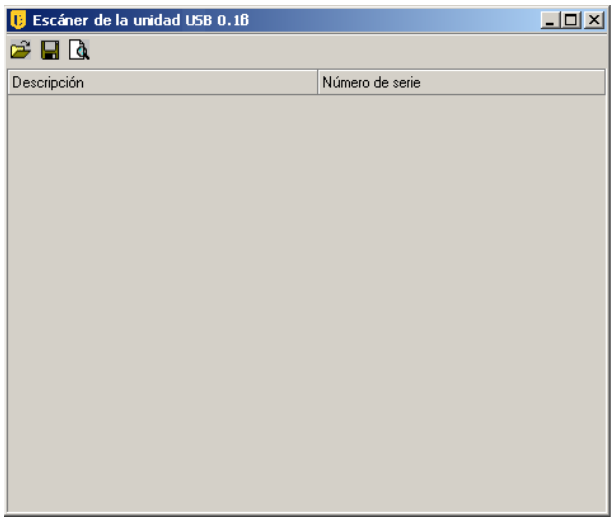
Esta clave la puede leer el usuario final durante una llamada al servicio de ayuda técnica, o se puede copiar y pegar a un correo electrónico. A continuación el usuario introduce la clave en la ventana de gestión de ZENworks Security Client (consulte la *Guía del usuario de ZENworks Endpoint Security Management Security Client*). Esta clave sólo será válida para la directiva de ese usuario y únicamente durante el intervalo de tiempo especificado. Una vez que se haya utilizado la clave, no podrá volver a utilizarse.

Nota: Si el usuario finaliza sesión o reinicia el equipo durante la anulación de la contraseña, la contraseña caduca y se debe emitir una nueva.

Si se ha escrito una directiva nueva antes de que caduque el límite de tiempo, el usuario deberá comprobar la actualización de una directiva, en lugar de hacer clic en el botón *Cargar directiva* del cuadro de diálogo Acerca de ZENworks Security Client.

1.11 Escáner de la unidad USB

Se puede generar una lista de dispositivos USB autorizados e importarla a una directiva utilizando la herramienta del escáner de la unidad USB opcional (incluida con el paquete de instalación).



Para generar una lista de dispositivos autorizados:

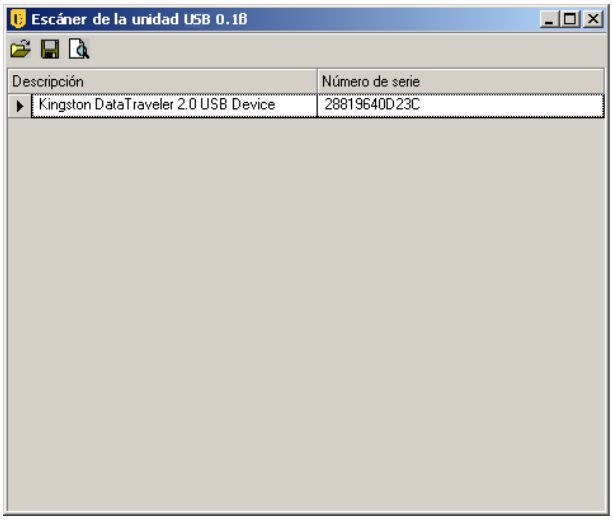
1 Abra la aplicación del escáner de la unidad USB.

Nota: Ésta es una instalación independiente de Management Service y Consola de gestión. Se visualiza un acceso directo a la herramienta que aparece en el escritorio.

---

2 Inserte un dispositivo USB en el puerto USB del equipo. El dispositivo debe tener un número de serie.

3 Haga clic en el icono *Explorar* (). El nombre del dispositivo y su número de serie aparecen en los campos correspondientes.



4 Repita Paso 2 y Paso 3 hasta que todos los dispositivos se hayan incluido en la lista.

5 Haga clic en el icono `Guardar` ().

Consulte Sección , “Dispositivos preferidos”, en la página 54 para obtener instrucciones acerca de la importación de la lista en una directiva.

Para editar un archivo guardado, haga clic en el icono *Examinar* () para abrir el archivo.

Creación y distribución de las directivas de seguridad

2

ZENworks® Security Client utiliza las directivas de seguridad para aplicar la seguridad de la ubicación a los usuarios móviles. Las decisiones sobre la disponibilidad de los puertos de redes, disponibilidad de aplicaciones de red, acceso al dispositivo de almacenamiento de archivos y conectividad alámbrica o Wi-Fi las determina el administrador de cada ubicación.

Las directivas de seguridad se pueden crear de forma personalizada para la empresa, grupos de usuarios individuales o equipos/usuarios individuales. Las directivas de seguridad pueden permitir la productividad completa de los empleados a la vez que protegen el puesto final, o bien restringir al empleado para la ejecución de sólo determinadas aplicaciones y el acceso de hardware sólo autorizado disponible para los mismos.

Las secciones siguientes contienen más información sobre:

2.1 Navegación en la consola de gestión

Para empezar a crear una directiva de seguridad:

1. En la consola de gestión, haga clic en *Archivo* > *Crear directiva nueva*.
2. Especifique el nombre de la directiva nueva y haga clic en *Crear* para visualizar la consola de gestión con la barra de herramientas Directiva y sus pestañas visualizadas.

Las siguientes secciones describen la interfaz de usuario de la consola de gestión, ya que guarda relación con la creación y distribución de las directivas de seguridad a través de ZENworks® Endpoint Security Management:

2.1.1 Utilización del árbol y pestañas de la directiva

Una directiva de seguridad se escribe o edita navegando por las pestañas disponibles situadas en la parte superior de la consola de gestión y utilizando las opciones del árbol *Configuración global* del panel izquierdo.

Entre las pestañas disponibles se incluye lo siguiente:

- **Configuración de la directiva global:** La configuración de la directiva global se aplica por defecto a la directiva y no es específica de la ubicación.

  La configuración de la directiva global le permite configurar los siguientes parámetros:

  - Valores de directiva

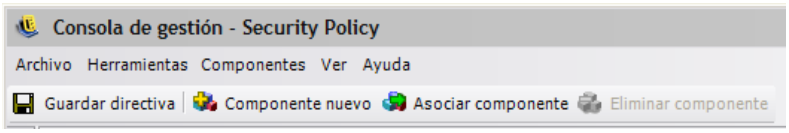
- Control inalámbrico
- Hardware de comunicación
- Control del dispositivo de almacenamiento
- Conectividad USB
- Cifrado de datos
- Cliente de seguridad ZENworks
- Aplicación de VPN

- **Ubicaciones:** Estas reglas de la directiva se aplican en un tipo de ubicación específico, sea éste una red única o un tipo de red como una cafetería o aeropuerto.
- **Reglas de solución·e integridad:** Estas reglas garantizan la ejecución del software esencial (como antivirus y programa espía) y la actualización en el dispositivo.
- **Información de cumplimiento:** Da instrucciones sobre si la creación de informes de datos (incluido el tipo de datos) se recopila para esta directiva concreta.
- **Publican:** Publica la directiva completa para los usuarios individuales, grupos de usuarios del servicio de directorio y/o equipos individuales.

El Árbol de directivas muestra los componentes disponibles del subconjunto para las categorías con pestañas. Por ejemplo, la *Configuración de la directiva global* incluye subconjuntos de *Valores de directiva*, *Control inalámbrico*, *Hardware de comunicación* y *Control del dispositivo de almacenamiento*. Únicamente los elementos contenidos en la página del subconjunto principal deben definir una categoría. Los subconjuntos restantes son componentes opcionales.

2.1.2 Utilización de la barra de herramientas Directiva

La barra de herramientas Directiva proporciona seis controles. El control *Guardar directiva* está disponible mediante la creación de directivas, mientras que los controles del componente sólo están disponibles en las pestañas *Ubicaciones* e *Integridad y solución*.



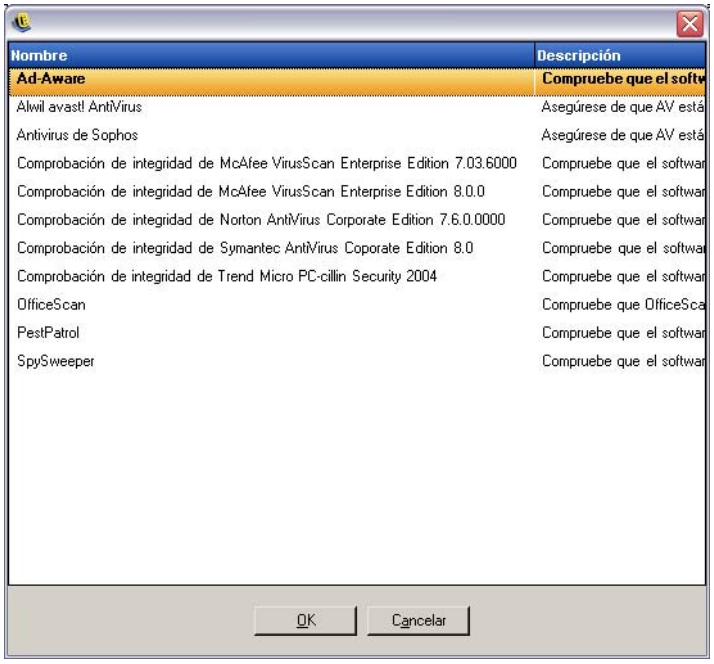
A continuación se explican las herramientas:

- **Guardar Directiva:** guarda la directiva en su estado actual.

  Importante: A medida que complete cada subconjunto de componentes, es altamente recomendable que haga clic en el icono *Guardar* de la barra de herramientas *Directiva*. Si se introducen datos incompletos o incorrectos en un componente, aparece la pantalla de notificación de errores (ver Sección 2.2.6, “Notificación de error”, en la página 106 para obtener más información).

- **Componente nuevo:** crea un componente nuevo en un subconjunto de Integridad o Ubicación. Una vez que se guarda la directiva, está disponible un componente nuevo para su asociación con otras directivas.

- **Asociar componente:** abre la pantalla Seleccionar componente para el subconjunto actual. Entre los componentes disponibles se incluyen los componentes predefinidos incluidos en la instalación, y todos los componentes creados en otras directivas.



Importante: Los cambios realizados en los componentes asociados afectarán al resto de instancias de ese componente.

Por ejemplo, puede crear un único componente de ubicación con el nombre "trabajo", lo cual define los ajustes de seguridad y entorno de red empresarial que se aplican siempre que un puesto final accede a ese entorno. Este componente se puede aplicar ahora a todas las directivas de seguridad. Las actualizaciones de los ajustes de seguridad o del entorno se pueden cambiar en el componente de una directiva, y actualizarán el mismo componente en el resto de las directivas a las que se asocien.

Utilice el comando *Mostrar uso* para ver el resto de directivas asociadas a este componente.

- **Eliminar componente:** elimina un componente de la directiva. El componente aún está disponible para su asociación a ésta y otras directivas.
- **Actualizar lista de directivas:** actualiza la lista de directivas.
- **Lista de informes:** muestra la lista de informes.

2.2 Creación de directivas de seguridad

1. En la consola de gestión, haga clic en *Archivo* > *Crear directiva nueva*.
2. Especifique el nombre de la directiva nueva y haga clic en *Crear* para mostrar la consola de gestión con la barra de herramientas Directiva y sus pestañas visualizadas.
3. Configure los parámetros de la directiva utilizando la información de las siguientes secciones:

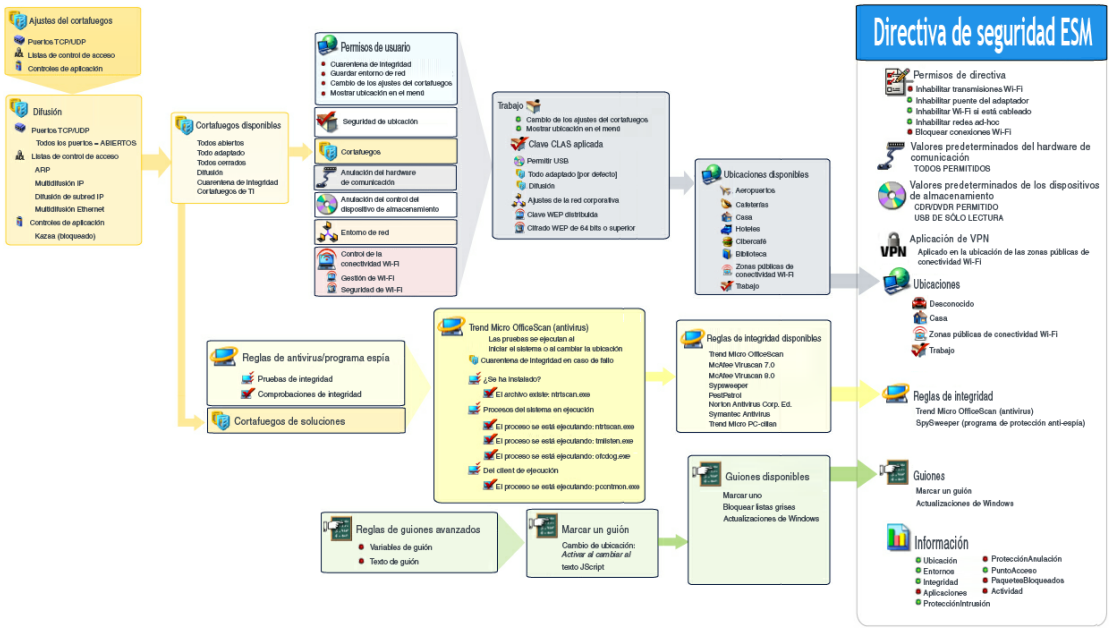
- Sección 2.2.1, “Configuración de la directiva global”, en la página 48
- Sección 2.2.2, “Locations”, en la página 70

- Sección 2.2.3, “Reglas de solución·e integridad”, en la página 94
- Sección 2.2.4, “Información de cumplimiento”, en la página 102
- Sección 2.2.5, “Publican”, en la página 104
- Sección 2.2.6, “Notificación de error”, en la página 106
- Sección 2.2.7, “Mostrar uso”, en la página 106

Las directivas de seguridad se crean definiendo todas las configuraciones globales (comportamientos por defecto), creando y asociando los componentes existentes de esa directiva, como las ubicaciones, cortafuegos y reglas de integridad, y finalmente estableciendo el informe de cumplimiento de la directiva.

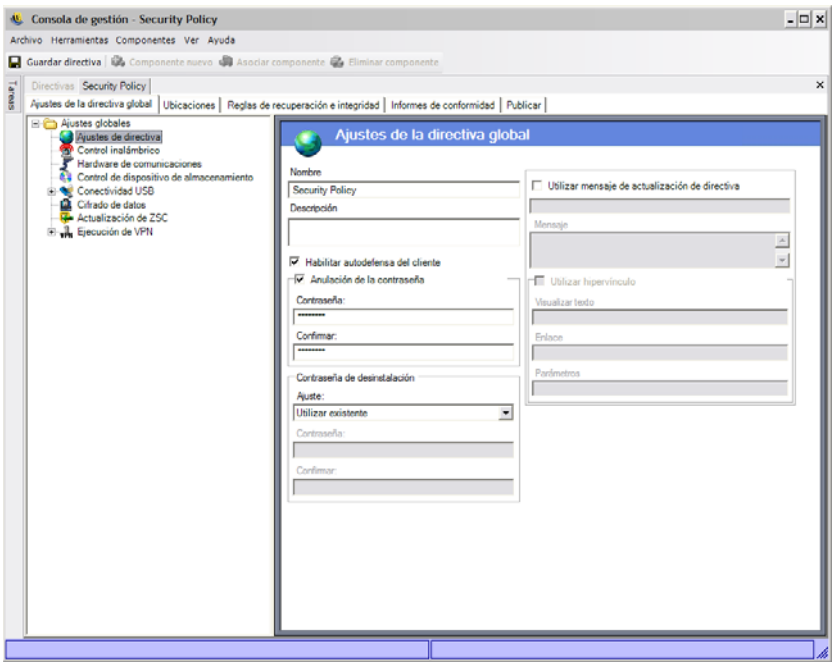
Los componentes se crean en una directiva simulada, o bien se asocian a partir de otras directivas. Se da por sentado que para sus primeras directivas, usted crea todas las ubicaciones exclusivas, ajustes del cortafuegos y reglas de integridad para la empresa. Estos componentes se almacenan en la base de datos de Management Service para un posible uso futuro en otras directivas.

El siguiente diagrama muestra los componentes de cada nivel, y una directiva resultante de las selecciones.



2.2.1 Configuración de la directiva global

La configuración de la directiva global se aplica como valor por defecto de la misma. Para acceder a este control, vaya a la consola de gestión y haga clic en la pestaña *Configuración de la directiva global*.



Las siguientes secciones contienen más información sobre los parámetros de configuración que puede configurar de forma global:

- “Valores de directiva” en la página 49
- “Control inalámbrico” en la página 50
- “Hardware de comunicación” en la página 51
- “Control del dispositivo de almacenamiento” en la página 52
- “Conectividad USB” en la página 55
- “Cifrado de datos” en la página 61
- “Actualizar ZSC” en la página 63
- “Aplicación de VPN” en la página 64
- “Mensaje del usuario personalizado” en la página 68
- “Hiperenlaces” en la página 69

Valores de directiva

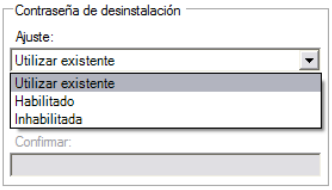
La configuración global principal incluye:

- **Nombre y descripción:** el nombre de la directiva se especifica al principio del proceso de creación de directivas. Puede editar el nombre o proporcionar una descripción de la directiva.
- **Habilite la autodefensa del cliente:** la autodefensa del cliente se puede habilitar o inhabilitar mediante la directiva. Si se deja seleccionada esta casilla se garantiza que la autodefensa del cliente está activa. Si se anula su selección, se desactiva la autodefensa del cliente para todos los puntos finales utilizando esta directiva.
- **Anulación de contraseña:** Esta función permite al administrador configurar una anulación de contraseña que puede inhabilitar temporalmente la directiva durante un período especificado de tiempo. Seleccione la casilla *Anulación de contraseña* y escriba la contraseña en el campo

proporcionado. Escriba la contraseña de nuevo en el campo de confirmación de contraseña. Utilice esta contraseña en el generador de contraseña de anulación para generar la clave de contraseña de esta directiva. Para obtener más información, consulte la Sección 1.10, "Utilización del generador de claves de contraseñas de anulación", en la página 42.

Advertencia: Es muy recomendable que no se facilite esta contraseña a los usuarios. El generador de contraseñas de anulación se debe utilizar para generar una clave temporal para ellas.

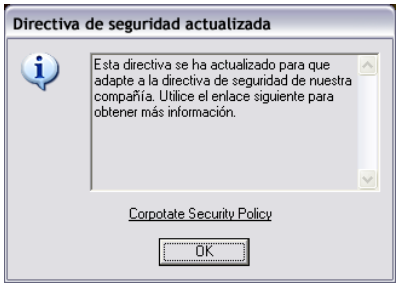
- **Contraseña de desinstalación:** Recomendamos que se instale cada ZENworks* Security Client con una contraseña de desinstalación para evitar que los usuarios desinstalen el software. Esta contraseña normalmente se configura durante la instalación; no obstante, la contraseña se puede actualizar, habilitar o inhabilitar mediante la directiva.



Puede seleccionar uno de los siguientes ajustes de la lista desplegable:

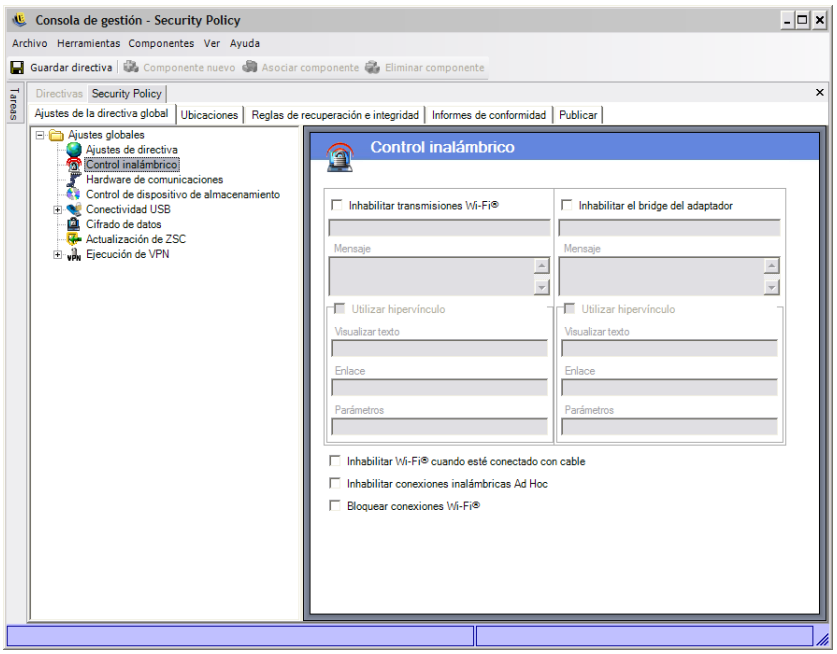
- **Utilizar existente:** Se trata del ajuste por defecto. Deja la contraseña actual sin modificar.
- **Habilitada:** activa una contraseña de desinstalación o la cambia. Especifique la contraseña nueva y confírmela.
- **Inhabilitado:** Desactiva el requisito de contraseña de desinstalación.

- **Utilizar mensaje de actualización de la directiva:** puede ver un mensaje de usuario personalizado siempre que se actualice la directiva. Haga clic en la casilla de verificación y especifique la información del mensaje en los campos proporcionados.
- **Utilizar hiperenlace:** Puede incluir un hiperenlace a la información adicional, directiva corporativa, etc. (consulte "Hiperenlaces" en la página 69 para obtener más información).



Control inalámbrico

El control inalámbrico ajusta globalmente los parámetros de conectividad del adaptador para proteger el punto final y la red. Para acceder a este control, haga clic en la pestaña *Configuración de la directiva global* y haga clic en el icono *Control inalámbrico* en el árbol de directivas situado a la izquierda.



La configuración del control inalámbrico incluye lo siguiente:

- **Inhabilitar transmisiones Wi-Fi:** inhabilita globalmente todos los adaptadores Wi-Fi, hasta e incluyendo la opción de silencio total de una radio Wi-Fi integrada.

  Puede elegir visualizar un mensaje de usuario personalizado e hiperenlace cuando el usuario intenta activar una conexión Wi-Fi. Consulte la “Mensaje del usuario personalizado” en la página 68 para obtener más información.
- **Inhabilitar puente del adaptador:** inhabilita globalmente la funcionalidad del puente de red incluida con Windows* XP, lo cual permite al usuario aunar varios adaptadores y actuar como nodo central de la red.

  Puede elegir visualizar un mensaje de usuario personalizado e hiperenlace cuando el usuario intente una conexión Wi-Fi. Consulte la “Mensaje del usuario personalizado” en la página 68 para obtener más información.
- **Inhabilitar Wi-Fi si está cableado:** inhabilita globalmente todos los adaptadores Wi-Fi cuando el usuario tiene una conexión con cable (LAN a través de NIC).
- **Inhabilitar redes Ad Hoc:** inhabilita globalmente toda la conectividad ad hoc, la cual aplica la conectividad Wi-Fi sobre una red (por ejemplo, mediante un punto de acceso) y restringe la conexión a red de igual a igual de este tipo.
- **Bloquear conexiones Wi-Fi:** bloquea globalmente las conexiones Wi-Fi sin silenciar la radio Wi-Fi. Utilice este valor si desea inhabilitar las conexiones Wi-Fi, pero desea utilizar puntos de acceso para la detección de la ubicación. Consulte la Sección 2.2.2, “Locations”, en la página 70 para obtener más información.

Hardware de comunicación

La configuración del hardware de comunicación controla por ubicación qué tipos de hardware permiten una conexión en este entorno de red.

Nota: Puede ajustar los controles del hardware de comunicación globalmente en la pestaña *Configuración de la directiva global* o para las ubicaciones individuales en la pestaña *Ubicaciones*.

Para ajustar los controles del hardware de comunicación globalmente, haga clic en la pestaña *Configuración de la directiva global*, expanda *Configuración global* en el árbol y haga clic en *Hardware de comunicación*.

Para ajustar los controles del hardware de comunicación para una ubicación, haga clic en la pestaña *Ubicaciones*, expanda la ubicación deseada en el árbol y haga clic en *Hardware de comunicación*. Para obtener más información acerca de la configuración del hardware de comunicación de una ubicación, consulte "Hardware de comunicación" en la página 72.

Seleccione la habilitación o inhabilitación de la configuración global de cada dispositivo del hardware de comunicación que aparece en:

- **1394 (FireWire):** Controla el puerto de acceso FireWire* en el punto final.
- **IrDA:** Controla el puerto de acceso por infrarrojos en el puesto final.
- **Bluetooth:** Controla el puerto de acceso Bluetooth* en el punto final.
- **Serie/Paralelo:** Controla el acceso del puerto de serie y paralelo en el puesto final.

Control del dispositivo de almacenamiento

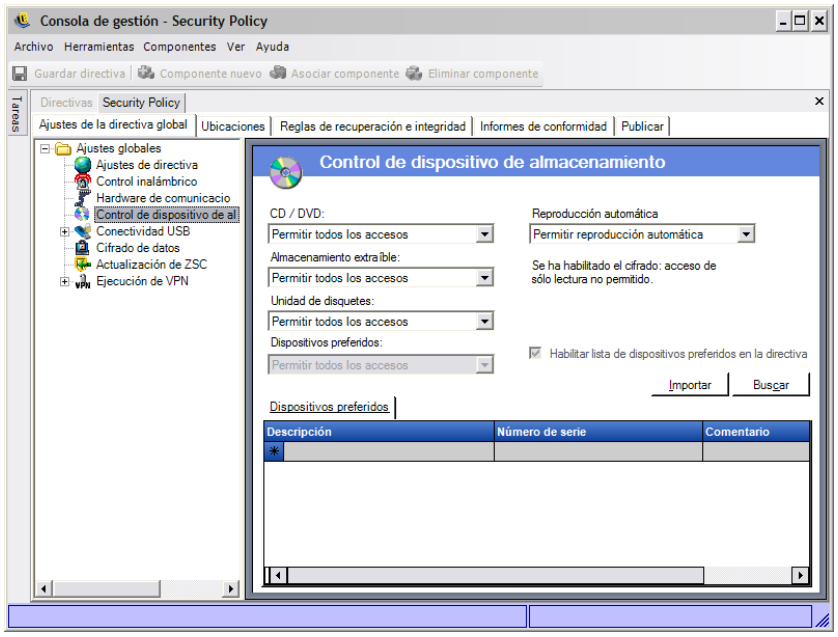
Los controles del dispositivo de almacenamiento ajustan los parámetros de configuración del dispositivo de almacenamiento por defecto para la directiva. Esto incluye especificar si a los dispositivos de almacenamiento de archivos externos se les permite leer o escribir archivos, funcionar en un estado de sólo lectura, o inhabilitarse por completo. Si están inhabilitados, estos dispositivos no pueden recuperar datos del punto final; no obstante, la unidad de disco duro y todas las unidades de red seguirán estando operativas y accesibles.

El control del dispositivo de almacenamiento de ZENworks Endpoint Security Management no está permitido si está activada la solución de cifrado de almacenamiento.

Nota: Puede ajustar los controles del dispositivo de almacenamiento globalmente en la pestaña *Configuración de la directiva global* o para las ubicaciones individuales en la pestaña *Ubicaciones*.

Para ajustar los controles del dispositivo de almacenamiento globalmente, haga clic en la pestaña *Configuración de la directiva global*, expanda *Configuración global* en el árbol y haga clic en *Control del dispositivo de almacenamiento*.

Para ajustar los controles del dispositivo de almacenamiento para una ubicación, haga clic en la pestaña *Ubicaciones*, expanda la ubicación deseada en el árbol y haga clic en *Control del dispositivo de almacenamiento*. Para obtener más información, consulte la "Hardware de comunicación" en la página 72.



El control del dispositivo de almacenamiento está dividido en las siguientes categorías:

- **CD/DVD:** controla todos los dispositivos que aparecen en las *unidades de DVD/CD-ROM* en Windows Device Manager.
- **Almacenamiento extraíble:** controla todos los dispositivos notificados como almacenamiento extraíble de las *Unidades de disco* en Windows Device Manager.
- **Floppy Drive:** controla todos los dispositivos que aparecen en las *Unidades de disquete* en Windows Device Manager.
- **Dispositivos preferidos:** permite únicamente los dispositivos de almacenamiento extraíbles que aparecen en la ventana Control del dispositivo de almacenamiento. No se permite el resto de dispositivos notificados como almacenamiento extraíble.

Siempre se permite el almacenamiento fijo (unidades de disco duro) y unidades de red (si están disponibles).

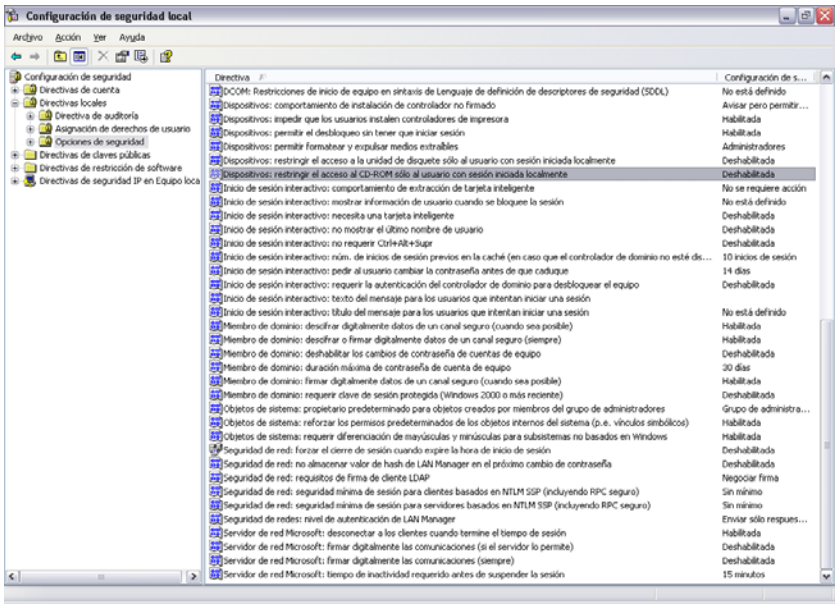
Para ajustar el valor por defecto de la directiva de los dispositivos de almacenamiento, seleccione la configuración global para ambos tipos de las listas desplegables:

- **Activar:** El tipo de dispositivo se permite por defecto.
- **Inhabilitar:** el tipo de dispositivo no está permitido. Cuando los usuarios intentan acceder a los archivos en un dispositivo de almacenamiento definido, éstos reciben un mensaje de error del sistema operativo, o de la aplicación que intenta acceder al dispositivo de almacenamiento local, indicando que se ha producido un error en la acción
- **Sólo lectura:** el tipo de dispositivo está establecido como Sólo lectura. Cuando los usuarios intentan escribir en el dispositivo, éstos reciben un mensaje de error del sistema operativo, o de la aplicación que intenta acceder al dispositivo de almacenamiento local, indicando que se ha producido un error en la acción

---

Nota: Si desea inhabilitar las unidades de CD-ROM o unidades de disquete en un grupo de puntos finales, o ajustarlas como Sólo lectura, la configuración de seguridad local (bajada de nivel a través de un objeto de directiva del grupo de servicios de directorio) debe tener *Dispositivos: restringir*

acceso de CD-ROM únicamente para el usuario que ha iniciado sesión localmente y *Dispositivos: restringir acceso de disquete únicamente para el usuario que ha iniciado sesión localmente ajustado como Inhabilitado*. Para verificar esto, abra el objeto de directiva del grupo, o bien abra las herramientas administrativas en un equipo. Mirar configuración de la seguridad local: opciones de seguridad y comprobar que ambos dispositivos están inhabilitados. El valor por defecto es Inhabilitado.



Las secciones siguientes contienen más información sobre:

- “Dispositivos preferidos” en la página 54
- “Importación de listas de dispositivos” en la página 55

Dispositivos preferidos

Los dispositivos de almacenamiento extraíbles preferidos se pueden añadir opcionalmente a una lista, lo que permite que sólo los dispositivos autorizados accedan cuando se utilice la configuración global en una ubicación. Los dispositivos añadidos a esta lista deben tener un número de serie.

Para enumerar un dispositivo preferido:

1. Inserte el dispositivo en el puerto USB del equipo en el que está instalada la Consola de gestión.
2. Una vez que el dispositivo esté listo, haga clic en el botón *Explorar*. Si el dispositivo tiene un número de serie, su descripción y número de serie aparecen en la lista.
3. Seleccione un valor de la lista desplegable (el valor del *Dispositivo extraíble global* no se aplicará a esta directiva):
   - **Habilitada:** Los dispositivos de la lista de preferidos pueden utilizar la función de lectura/escritura y el resto de USB y dispositivos de almacenamiento externo están inhabilitados.
   - **Sólo lectura:** Los dispositivos que aparezca en la lista de preferidos tienen la capacidad de sólo lectura; el resto de dispositivos USB y de almacenamiento externo están inhabilitados.

Repita estos pasos para cada dispositivo permitido en esta directiva. Se aplica la misma configuración a todos los dispositivos.

Nota: Los ajustes del control del dispositivo de almacenamiento basado en la ubicación anularán la configuración global. Por ejemplo, podría ajustar todos los dispositivos de almacenamiento externo para que se permitan en la ubicación de trabajo, mientras se permite únicamente el valor por defecto global en el resto de ubicaciones, limitando los usuarios a los dispositivos de la lista de preferidos.

Importación de listas de dispositivos

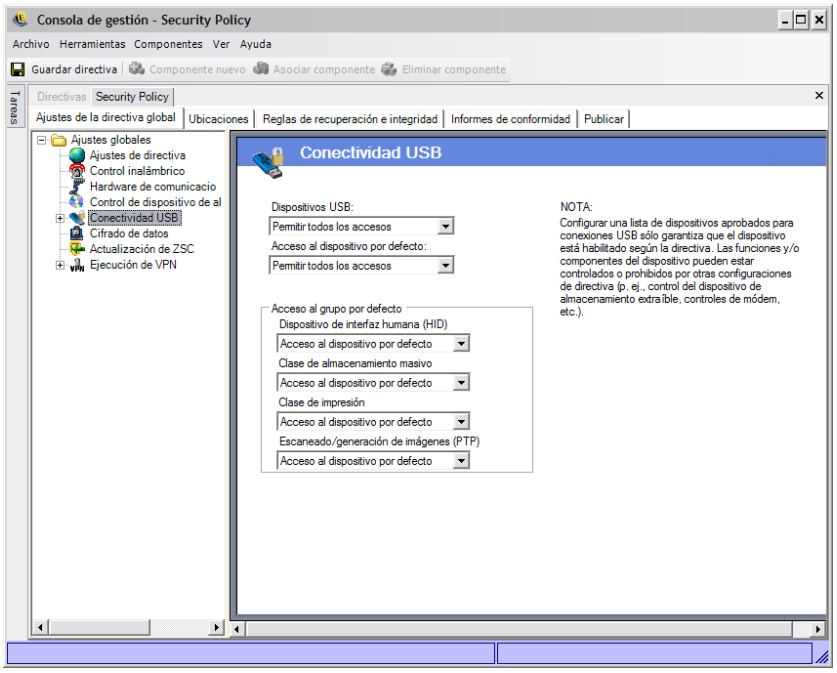
La aplicación del escáner de la unidad USB de Novell genera una lista de dispositivos y sus números de serie (Sección 1.11, “Escáner de la unidad USB”, en la página 43). Para importar esta lista, haga clic en *Importar* y navegue hasta la lista. La lista rellena los campos *Descripción* y *Número de serie*.

Conectividad USB

Todos los dispositivos que se conectan mediante el BUS USB se pueden permitir o denegar por directiva. Estos dispositivos se pueden escanear en la directiva desde el informe del inventario de dispositivos USB o escaneando todos los dispositivos actualmente conectados a un equipo. Estos dispositivos se pueden filtrar en función del fabricante, nombre del producto, números de serie, tipo, etc. A efectos de compatibilidad, el administrador puede configurar la directiva para que acepte un conjunto de dispositivos, por tipo de fabricante, (por ejemplo, todos los dispositivos HP están permitidos) o por tipo de producto (todos los dispositivos de interfaz humana USB, como el ratón y el teclado, están permitidos). Asimismo, se puede permitir a los dispositivos individuales que eviten la introducción en la red de·los dispositivos no compatibles (por ejemplo, no se permite ninguna impresora a excepción de la de la directiva).

Para acceder a este control, haga clic en *Configuración de la directiva global* y haga clic en *Conectividad USB* del árbol de directivas de la izquierda.

Figura 2-1 *Página de conectividad USB.*



En primer lugar, se evalúa el acceso en función de que el bus se encuentre activado o no. Esto se determina por el valor de configuración de los *Dispositivos USB*. En caso de que el valor de configuración se encuentre establecido en *Inhabilitar todos los accesos*, también se inhabilitará el dispositivo y se detendrá la evaluación. En caso de que el valor de configuración se encuentre establecido en *Permitir todos los accesos*, el cliente continuará con la evaluación y con la búsqueda de coincidencias de filtro. Como sucede con otros campos de la Consola de gestión de ZENworks, cuando se establecen en una ubicación, los valores de los *Dispositivos USB* también se pueden configurar con la opción *Aplicar ajustes globales* y, en su lugar, se utilizará el valor global de este campo.

El cliente agrupa los filtros que se aplican desde la directiva en función de la ubicación y de los valores de configuración globales. Por tanto, el cliente llevará a cabo dicha agrupación según el acceso a los siguientes grupos:

- **Bloquear siempre:** Bloquear siempre el dispositivo. Este valor no se puede modificar.
- **Permitir siempre:** Permitir siempre el acceso, a menos que el dispositivo coincida con el filtro *Bloquear siempre*.
- **Bloquear:** Bloquear el acceso, a menos que el dispositivo coincida con el filtro *Permitir siempre*.
- **Permitir:** Permitir el acceso, a menos que el dispositivo coincida con el filtro *Bloquear siempre* o *Bloquear*.
- **Acceso al dispositivo por defecto:** En caso de que no se encuentre otra coincidencia, al dispositivo se le da el mismo nivel de acceso que con la opción *Acceso al dispositivo por defecto*.

Se evalúa un dispositivo en cada grupo siguiendo el orden anterior (en primer lugar, el grupo *Bloquear siempre*, seguido del grupo *Permitir siempre*, etc.). Cuando un dispositivo coincide con, al menos, un filtro de·un grupo, el acceso al dispositivo se establece en dicho nivel y se detiene la evaluación. En caso de que el dispositivo se evalúe con todos los filtros y no se encuentre ninguna coincidencia, se aplica el nivel *Acceso al dispositivo por defecto*.

El acceso al dispositivo que se encuentre establecido en el área del *Acceso al grupo del dispositivo* se considera con todos los·filtros que se utilicen en dicha ubicación. Esto se realiza mediante la generación de coincidencias de los filtros para cada agrupación cuando la directiva se publica al cliente. Estos filtros son los siguientes:

Acceso al grupo del dispositivo:	Filtros:
Dispositivo de interfaz humana (HID)	"Clase de dispositivo" igual a 3.
Clase de almacenamiento masivo	"Clase de dispositivo" igual a 8.
Clase de impresión	"Clase de dispositivo" igual a 7.
Escaneo/generación de imágenes	"Clase de dispositivo" igual a 6.

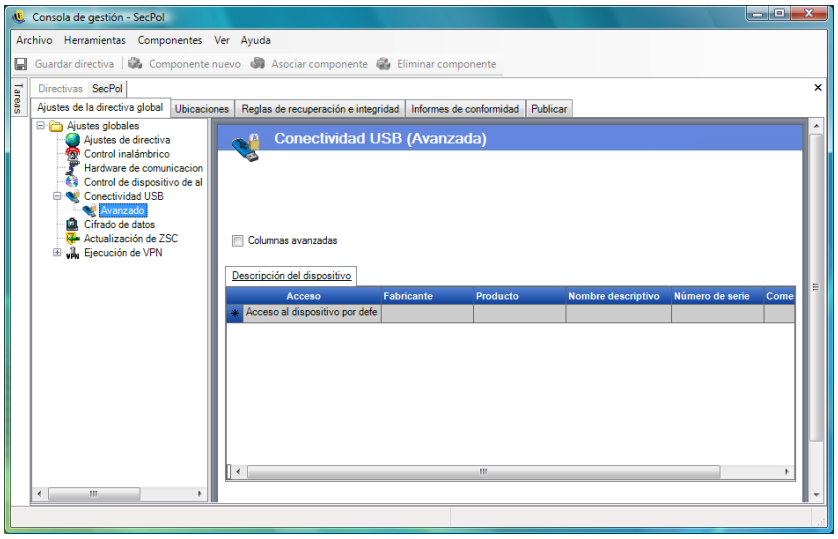
Avanzadas

En la mayoría de las situaciones, los cuatro grupos de dispositivos enumerados en la página de conectividad USB (dispositivo de interfaz humana, clase de almacenamiento masivo, clase de impresión y escaneo/generación de imágenes) son suficientes para permitir o denegar el acceso a la mayoría de los dispositivos USB. En caso de que tenga dispositivos que no estén registrados en uno de estos grupos, puede configurar los ajustes en la página avanzada de conectividad USB. También

puede usar los ajustes de la página avanzada para ofrecer acceso a la lista blanca a determinados dispositivos, incluso si se les ha denegado el acceso debido a los valores de configuración que se encuentran en la página de conectividad USB.

Para poder acceder a las opciones de Conectividad de USB avanzadas, haga clic en el signo más junto a *Conectividad USB*en el árbol *Configuración global* y a continuación haga clic en*Avanzadas* Puede utilizar el informe de auditoría del dispositivo USB a fin de obtener toda la información que pudiera ser de gran ayuda en la página avanzada de control de la conectividad USB.

Figura 2-2 *Página avanzada de conectividad USB.*



En las columnas por defecto, se incluye lo siguiente:

- **Acceso:** Active *Acceso al dispositivo por defecto* con el ratón y, a continuación, especifique el nivel de acceso:
  - **Bloquear siempre:** Bloquear siempre el dispositivo. Este valor no se puede modificar.
  - **Permitir siempre:** Permitir siempre el acceso, a menos que el dispositivo coincida con el filtro *Bloquear siempre*.
  - **Bloquear:** Bloquear el acceso, a menos que el dispositivo coincida con el filtro *Permitir siempre*.
  - **Permitir:** Permitir el acceso, a menos que el dispositivo coincida con el filtro *Bloquear siempre* o *Bloquear*.
  - **Acceso al dispositivo por defecto:** En caso de que no se encuentre otra coincidencia, al dispositivo se le da el mismo nivel de acceso que con la opción *Acceso al dispositivo por defecto*.
- **Fabricante:** Haga clic en la columna *Fabricante* y, a continuación, introduzca el nombre del fabricante que desee incluir en el filtro (p. ej.: Canon).
- **Producto:** Haga clic en la columna *Producto* y, a continuación, introduzca el nombre del producto que desee incluir en el filtro.
- **Nombre descriptivo:** Haga clic en la columna *Nombre descriptivo* y, a continuación, introduzca el nombre descriptivo del dispositivo que desee incluir en el filtro.

- **Número de serie:** Haga clic en la columna *Número de serie* y, a continuación, introduzca el número de serie del dispositivo que desee incluir en el filtro.
- **Comentario:** Haga clic en la columna *Comentario* y, a continuación, introduzca el comentario que desee incluir en el filtro (p. ej., Canon).

Puede hacer clic en el recuadro *Columnas avanzadas* para añadir las siguientes columnas: *Versión USB*, *Clase de dispositivo, Subclase de dispositivo, Protocolo del dispositivo, ID del proveedor, ID del producto, Dispositivo BCD, ID del dispositivo del SO* y *Clase de dispositivo del SO*.

Un dispositivo pone a disposición del SO un conjunto de atributos. El cliente hace coincidir dichos atributos con los campos que requiere el filtro. Para tener una coincidencia, todos los campos de un filtro deben coincidir con un atributo propio del dispositivo. El filtro no coincidirá en caso de que el dispositivo no ofrezca un atributo o campo que sea necesario para dicho filtro.

Por ejemplo, considere que un dispositivo ofrece los siguientes atributos: Fabricante: Clase Acme: 8 y Número de serie: "1234".

El filtro: Clase == 8 coincidiría con este dispositivo. El filtro: Producto == "Acme" no coincidiría, porque el dispositivo no proporcionó un atributo de producto para el dispositivo del SO.

Los siguientes campos coinciden en subcadenas: Fabricante, Producto y Nombre descriptivo. El resto de los campos coinciden perfectamente.

Es importante destacar que el campo número de serie (NS) USB mediante especificación es único si se tiene en cuenta al especificar los siguientes campos junto con el NS: Versión USB, ID del proveedor, ID de producción y Dispositivo BCD.

Los valores decimales actuales que son válidos para la versión USB son: 512 - USB 2.0, 272 - USB 1.1 y 256 - USB 1.0.

Las secciones siguientes contienen más información sobre:

- “Adición manual de dispositivos” en la página 58
- “Añadir un dispositivo a la lista blanca o a la lista negra por tipo de producto” en la página 59

Adición manual de dispositivos

Los siguientes métodos permiten rellenar la lista para que pueda permitir o denegar la conectividad USB a los dispositivos:

Para añadir un dispositivo manualmente:

1. Inserte el dispositivo en el puerto USB del equipo en el que está instalada la Consola de gestión.
2. Una vez que el dispositivo esté listo, haga clic en el botón *Explorar*. Si el dispositivo tiene un número de serie, su descripción y número de serie aparecen en la lista.
3. Seleccione un valor de la lista desplegable (el valor del *Dispositivo extraíble global* no se aplica a esta directiva):
   - **Activar:** Los dispositivos de la lista de preferidos pueden utilizar la función de lectura/escritura, y el resto de USB y dispositivos de almacenamiento externo están inhabilitados
   - **Sólo lectura:** Los dispositivos de la lista de preferidos pueden utilizar la función de sólo lectura; el resto de dispositivos USB y de almacenamiento externo están inhabilitados

Repita los pasos para cada dispositivo que se vaya a permitir en esta directiva. Se aplica la misma configuración a todos los dispositivos.

Añadir un dispositivo a la lista blanca o a la lista negra por tipo de producto

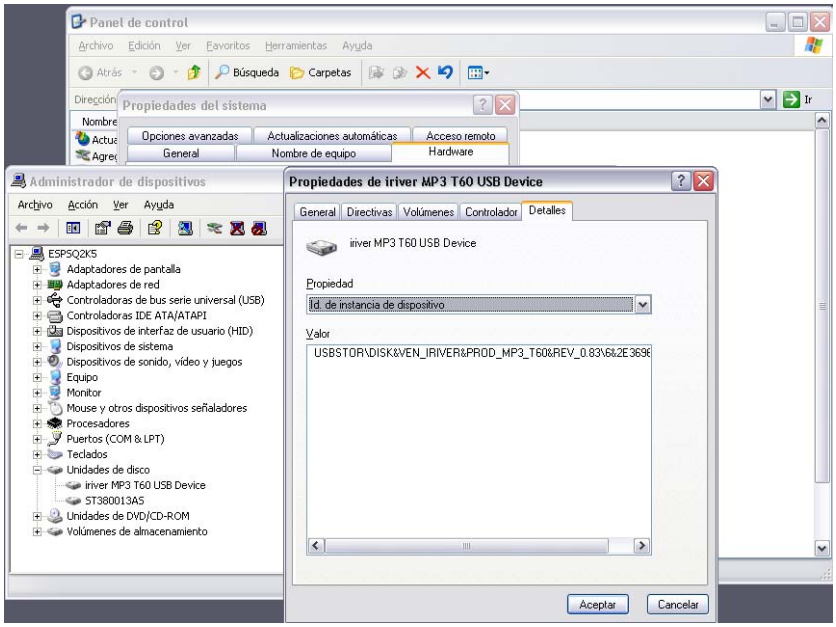
En la siguiente sección se describe cómo añadir a la lista blanca o a la lista negra un dispositivo USB según el tipo de producto.

Nota: El siguiente procedimiento se proporciona como ejemplo de cómo puede encontrar el tipo de producto de su dispositivo de almacenamiento USB extraíble. Dependiendo de la información que el fabricante del dispositivo facilite, el procedimiento funcionará o no. Puede utilizar el informe de auditoría del dispositivo USB a fin de obtener toda la información que pudiera ser de gran ayuda en la página avanzada de control de la conectividad USB.

Para determinar el tipo de producto de un dispositivo de almacenamiento USB extraíble:

1. En la ventana de la Consola de gestión del equipo con Microsoft Windows, haga clic en *Gestor·de dispositivos*.
2. Haga clic en el signo más junto a *Unidades de disco* para expandir el árbol.
3. Haga clic con el botón derecho del ratón en el dispositivo USB y, a continuación, haga clic en *Propiedades* para que se muestre el recuadro de diálogo Propiedades del dispositivo.
4. Haga clic en la pestaña *Detalles* y seleccione *ID de instancia de dispositivo* en la lista desplegable.

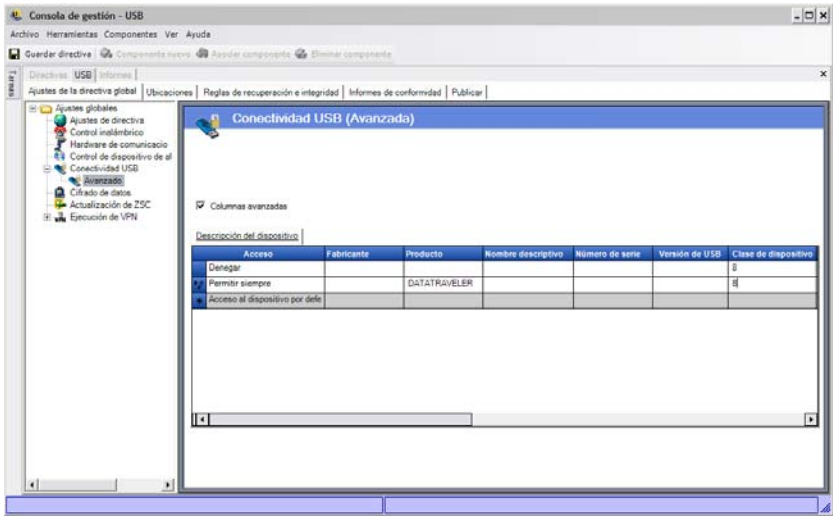
   El tipo de producto aparece después de &PROD en el ID de instancia del dispositivo. En el siguiente ejemplo, DATATRAVELER es el tipo de producto.



Añadir a la lista blanca un dispositivo USB: deje los parámetros de configuración predeterminados de la página Conectividad USB. En la página Configuración Avanzada, cree dos filas. En la primera fila, especifique *Denegar* en la columna *Acceso* y 8 en la columna *Clase de dispositivo* (si *Clase de dispositivo* no está disponible, seleccione la casilla de verificación *Columnas*

avanzadas. En la segunda fila, especifique *Permitir siempre* en la columna *Acceso*, el tipo de producto (DATATRAVELER, en este ejemplo) en la columna *Producto* y 8 en la columna *Clase de dispositivo*.

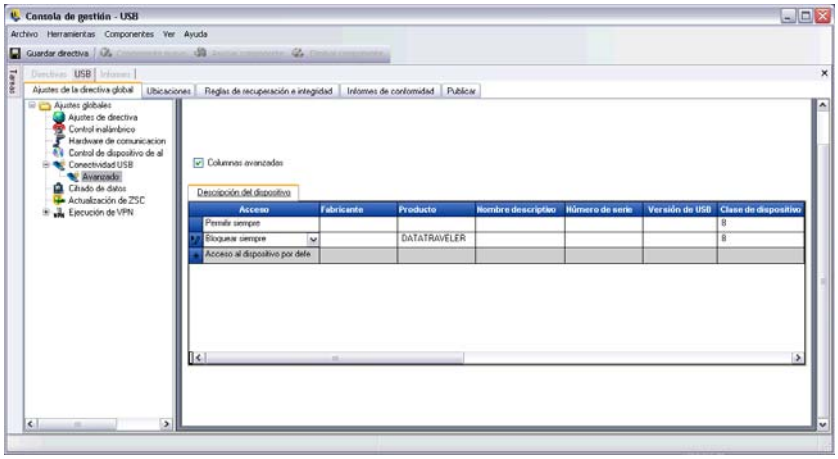
La página Conectividad USB (Avanzada) debería tener el siguiente aspecto:



el dispositivo USB DATATRAVELER está ahora en la lista blanca, lo que significa que ZENworks Endpoint Security Management le ha concedido acceso y el resto de los dispositivos de almacenamiento USB extraíbles tienen el acceso denegado.

Añadir a la lista negra·un dispositivo USB: deje los parámetros de configuración predeterminados de la página Conectividad USB. En la página Configuración Avanzada, cree dos filas. En la primera fila, especifique *Permitir siempre* en la columna *Acceso* y 8 en la columna *Clase de dispositivo* (si *Clase de dispositivo* no está disponible, seleccione la casilla de verificación *Columnas avanzadas*). En la segunda fila, especifique *Bloquear siempre* en la columna *Acceso*, el tipo de producto (DATATRAVELER, en este ejemplo) en la columna *Producto* y 8 en la columna *Clase de dispositivo*.

La página Conectividad USB (Avanzada) debería tener el siguiente aspecto:



el dispositivo USB DATATRAVELER está ahora en la lista negra, lo que significa que ZENworks Endpoint Security Management no le concede el acceso y el resto de los dispositivos de almacenamiento USB extraíbles tienen el acceso concedido.

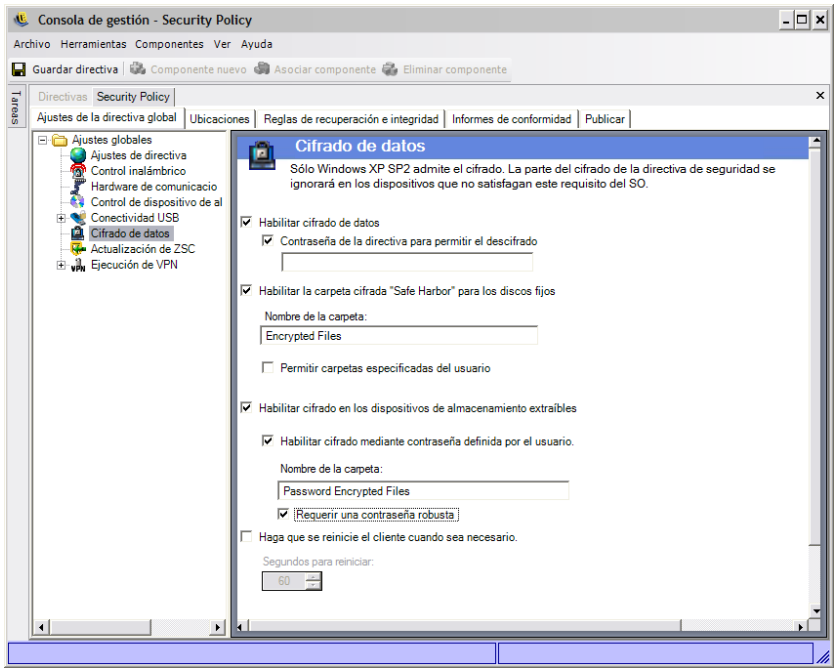
Cifrado de datos

El cifrado de datos determina si el cifrado de archivos se aplica en el punto final y qué tipo de cifrado está disponible. Se pueden cifrar los datos para permitir compartir archivos (con protección por contraseña), o los datos se pueden cifrar para que sean de sólo lectura en los equipos que ejecuten ZENworks Storage Encryption Solution.

Nota: El cifrado sólo lo admite Windows XP SP2. La parte de cifrado de la directiva de seguridad se ignora en los dispositivos que no cumplan este requisito del sistema operativo.

El control del dispositivo de almacenamiento de ZENworks Endpoint Security Management no está permitido si está activada ZENworks Storage Encryption Solution.

Para acceder a este control, abra la pestaña *Configuración de la directiva global* y haga clic en el icono *Cifrado de datos* en el árbol de directivas situado a la izquierda.



Para activar los controles individuales, haga clic en la casilla de verificación *Habilitar cifrado de datos*.

Nota: Las claves de cifrado se distribuyen a todas las máquinas que reciben las directivas de Policy Distribution Service, independientemente de si el cifrado de datos está o no activado. No obstante, este control proporciona instrucciones a ZENworks Security Client para activar sus controladores de cifrado, de tal forma que los usuarios puedan leer los archivos que se les haya enviado sin necesidad de la utilidad de descifrado de archivos. Consulte Sección 1.9, “Uso de la utilidad de descifrado de archivos de ZENworks”, en la página 41 para obtener más información.

Determine los niveles de cifrado que permite esta directiva:

- **Contraseña de la directiva para permitir el descifrado:** Especifique una contraseña para que todos los usuarios que utilicen esta directiva tengan que introducir esta contraseña antes de descifrar los archivos cifrados almacenados en sus carpetas `Puerto seguro`.

  Éste valor de configuración es opcional. Déjelo en blanco para que no sea necesario introducir la contraseña.

- **Habilite la carpeta cifrada "Safe Harbor" (puerto seguro) para los discos fijos (volumen no perteneciente al sistema):** Genera una carpeta en la raíz de todos los volúmenes no pertenecientes al sistema en el puesto final, con el nombre `Archivos protegidos con cifrado`. Todos los archivos ubicados en esta carpeta los cifra y gestiona ZENworks Security Client. Los datos que se encuentran en esta carpeta se cifran automáticamente y sólo podrán acceder a ellos los usuarios autorizados de este equipo.

  El nombre de la carpeta se puede cambiar haciendo clic en el campo *Nombre de la carpeta*, seleccionando el texto actual y especificando el nombre deseado.

  - **Cifrar la carpeta "Mis documentos" del usuario:** Active esta casilla para ajustar la carpeta `Mis documentos` del usuario como una carpeta cifrada (esto se aplica además a la carpeta `Puerto seguro`). Esto sólo se aplica a la carpeta local `Mis documentos`.
  - **Permitir carpetas específicas del usuario (volumen no perteneciente al sistema):**

    Active esta casilla para permitir a los usuarios seleccionar qué carpetas de su equipo se van a cifrar. Esto sólo se aplica a las carpetas locales; no se pueden cifrar dispositivos de almacenamiento extraíbles ni unidades de red.

Advertencia: Antes de inhabilitar el cifrado de datos, compruebe que todos los datos almacenados en estas carpetas los haya extraído el usuario y almacenado en otra ubicación.

- **Habilite el cifrado para los dispositivos de almacenamiento extraíbles:** Se pueden cifrar todos los datos escritos en dispositivos de almacenamiento extraíbles desde un punto final protegido por esta directiva. Los usuarios con esta directiva en sus equipos pueden leer los datos, por lo que es posible la compartición de archivos mediante los dispositivos de almacenamiento extraíbles de un grupo de directivas. Los usuarios que no pertenezcan a este grupo de directivas no pueden leer los archivos cifrados en la unidad y sólo se podrá acceder a los archivos de la carpeta `Shared Files` (si están activados) si se facilita la contraseña.
  - **Habilitar cifrado mediante la contraseña definida por el usuario:** Este valor da al usuario la capacidad de almacenar archivos en una carpeta de `Shared Files` del dispositivo de almacenamiento extraíble (esta carpeta se genera automáticamente cuando se aplique este valor). El usuario puede especificar una contraseña cuando los archivos se añaden a esta carpeta, la cual pueden utilizar los usuarios que no se encuentren en el grupo de directivas actual para extraer los archivos.

    El nombre de la carpeta se puede cambiar haciendo clic en el campo *Nombre de la carpeta*, seleccionando el texto actual y especificando el nombre deseado.
  - **Requerir contraseña segura:** Este valor obliga al usuario a definir una contraseña segura para la carpeta Shared Files. Una contraseña segura debe tener:
    - siete caracteres o más
    - al menos uno de los siguientes tipos de caracteres:
      - letras mayúsculas de la "A" a la" Z"

- letras minúsculas de la "a" a la "z"
- números del 0 al 9
- al menos un carácter especial ~!@#$%^&*()+{}[]:;<>?,./

Por ejemplo: y9G@wb?

Advertencia: Antes de inhabilitar el cifrado de datos, compruebe que todos los datos almacenados en los dispositivos de almacenamiento extraíbles los ha extraído el usuario y los ha almacenado en otra ubicación.

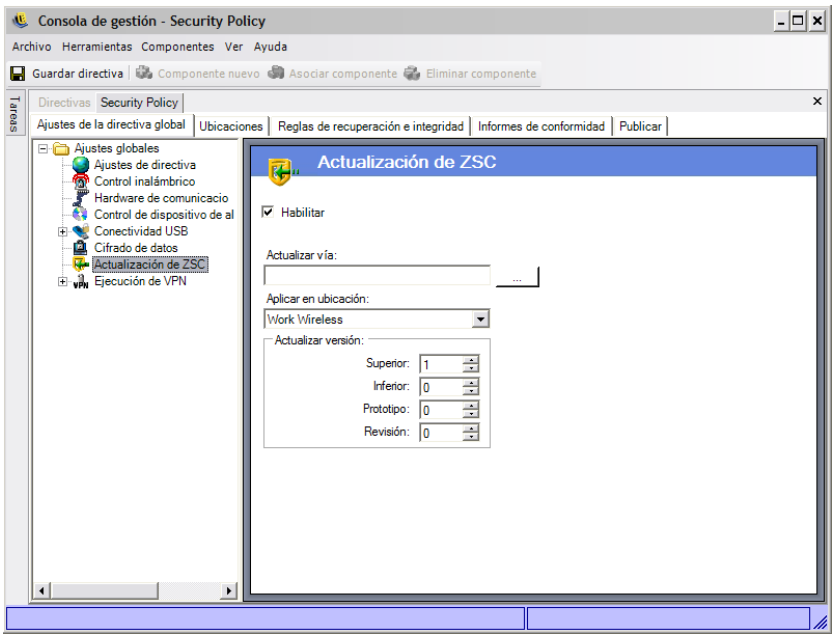
- **Pida al cliente que reinicie si es necesario:** Cuando se añade cifrado a una directiva, ésta no se activa hasta que se reinicie el puesto final. Este valor fuerza el reinicio necesario mostrando un temporizador de cuenta atrás, advirtiendo al usuario de que el equipo se reiniciará en el número de segundos especificado. El usuario dispone de ese intervalo de tiempo para guardar trabajo antes de que se reinicie el equipo.

  Se debe reiniciar cuando el cifrado se active primero en una directiva y una segunda vez cuando se active el cifrado de almacenamiento extraíble o "Safe Harbor" (puerto seguro) (si se activa de forma independiente de la activación del cifrado). Por ejemplo, cuando se aplica por primera vez una directiva de cifrado, se debe reiniciar el equipo dos veces: una para inicializar las unidades y una segunda vez para cifrar todos los puertos seguros. Si posteriormente se seleccionan más puertos seguros una vez se haya aplicado la directiva, sólo deberá reiniciar el equipo una vez para que los puertos seguros se incluyan en la directiva.

Actualizar ZSC

Las revisiones para reparar los pequeños defectos en ZENworks Security Client están disponibles con las actualizaciones regulares de ZENworks Endpoint Security Management. En lugar de proporcionar un nuevo instalador que necesita distribuirse a través de MSI a todos los puntos finales, la actualización de ZENworks Security Client permite al administrador dedicar una zona de la red que distribuya revisiones de actualización a los usuarios finales cuando estos se asocien al entorno de red.

Para acceder a este control, haga clic en la pestaña *Configuración de la directiva global* y haga clic en *Actualizar ZSC* en el árbol de directivas situado a la izquierda.



Para facilitar la distribución segura y sencilla de estas revisiones a todos los usuarios de ZENworks Security Client:

1. Active *Habilitar* para activar la pantalla y la regla.
2. Especifique la ubicación en la que ZENworks Security Client busca las actualizaciones.

   Debido a las recomendaciones del siguiente paso, la ubicación asociada al entorno empresarial (por ejemplo, la ubicación de trabajo) es el candidato recomendado.
3. Especifique la URI en la que se ha almacenado la revisión.

   Esto tiene que apuntar al archivo de revisiones, que puede ser el archivo setup.exe para ZENworks Security Client o un archivo MSI creado a partir del archivo .exe. A efectos de seguridad, se recomienda que estos archivos se almacenen en un servidor seguro tras el cortafuegos de la empresa.
4. Especifique la información de la versión para este archivo en los campos proporcionados.

   La información de la versión se encuentra al instalar ZENworks Security Client y al abrir a continuación el cuadro de diálogo Acerca de (consulte la *Guía de instalación de ZENworks Endpoint Security Management* para obtener más información). El número de versión de `STEngine.exe` es el número de versión que deseará utilizar en los campos.

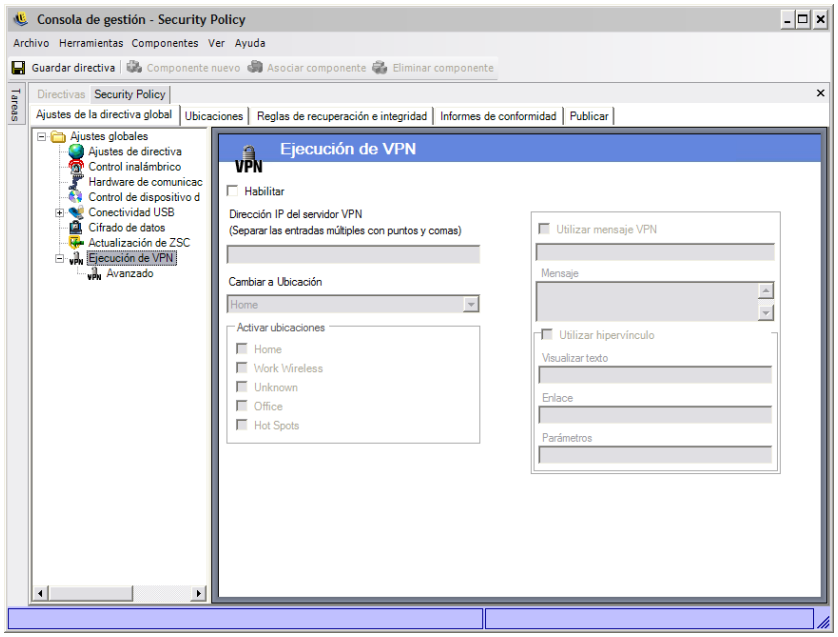
Cada vez que el usuario introduzca la ubicación asignada, ZENworks Security Client comprueba la URI de una actualización que coincida con el número de versión. Si hay disponible una actualización, ZENworks Security Client la descarga y la instala.

Aplicación de VPN

Esta regla aplica el uso de un SSL o VPN (Red Privada Virtual) basada en el cliente. Esta regla se aplica normalmente a los enlaces directos inalámbricos, permitiendo al usuario asociar y conectarse a la red pública, a la hora a la que la regla intenta establecer la conexión de VPN y, a continuación, cambiar el usuario a una ubicación definida y ajustes del cortafuegos. Todos los parámetros son a criterio del administrador. Todos los parámetros anulan la configuración de la directiva existente. El componente de aplicación de VPN requiere que el usuario se conecte a una red antes de su inicio.

Nota: Esta función sólo está disponible en la instalación de ZENworks Endpoint Security Management y no puede utilizarse para directivas de seguridad UWS.

Para acceder a este control, haga clic en la pestaña *Configuración de la directiva global* y haga clic en *Aplicación de VPN* en el árbol de directivas situado a la izquierda.



Para utilizar la regla de aplicación de VPN, deben existir dos ubicaciones como mínimo.

Para añadir la aplicación de VPN a una directiva de seguridad nueva o existente:

1. Active *Habilitar* para activar la pantalla y la regla.
2. Especifique las direcciones IP para el servidor de VPN en el campo proporcionado. Si se especifican varias direcciones, sepárelas con un punto y coma (por ejemplo: 10.64.123.5;66.744.82.36).
3. Seleccione *Cambiar a ubicación* de la lista desplegable.

   Ésta es la ubicación a la que ZENworks Security Client cambia cuando se activa la VPN. Esta ubicación debe contener algunas restricciones y sólo debe utilizar ajustes del cortafuegos restrictivos únicos como su valor por defecto.

   Es recomendable que los ajustes del cortafuegos sean *Todo cerrado*, que cierra todos los puertos TCP/UDP, para una aplicación estricta de VPN. Este valor evita la conectividad no autorizada, mientras que la dirección IP de la red privada virtual actúa como un ACL al servidor de VPN, y permite la conectividad de la red.
4. Seleccione las ubicaciones del activador en las que se aplicará la regla de aplicación de VPN. Para la aplicación de VPN estricta, se debe utilizar la ubicación desconocida por defecto para esta directiva. Una vez que se haya autenticado la red, la regla de VPN se activa y cambia al cambio de ubicación asignado.

Nota: El cambio de ubicación tiene lugar antes de la conexión de VPN, una vez que se haya autenticado la red.

5 Proporcione un mensaje del usuario personalizado para que aparezca cuando la VPN se haya autenticado para la red. Para las redes privadas virtuales que no sean de cliente, esto debería ser suficiente.

Para las redes privadas virtuales con un cliente, incluya un hiperenlace que apunte al cliente de VPN.

Ejemplo: `C:\Archivos de programa\Cisco Systems\Cliente de VPN\ipsecdialer.exe`

Este enlace lanza la aplicación, pero el usuario aún debe iniciar sesión. Se puede introducir un parámetro en el campo *Parámetros*, o bien se puede crear e indicar un archivo por lotes, en lugar del cliente ejecutable).

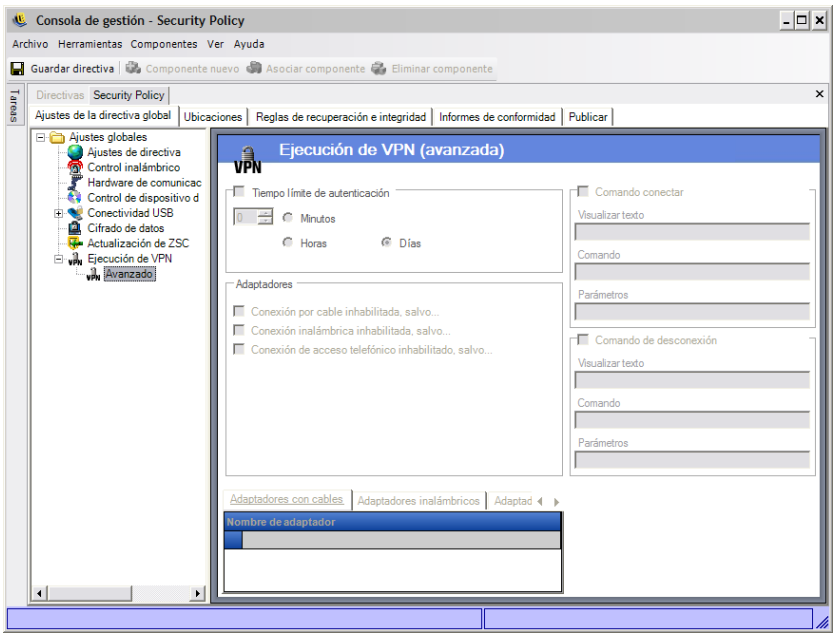
Nota: Los clientes de VPN que generen adaptadores virtuales (por ejemplo, Cisco Systems* VPN Client 4.0) visualizan el mensaje `La directiva se ha actualizado`. La directiva no se ha actualizado; ZENworks Security Client está simplemente comparando el adaptador virtual con cualquier restricción del adaptador en la directiva actual.

El valor de aplicación de VPN estándar descrito anteriormente convierte a la conectividad de VPN en una opción. Se concederá a los usuarios conectividad a la red actual se inicie o no su VPN. Para una aplicación más estricta, consulte la Configuración de VPN avanzada.

Configuración de VPN avanzada

Los controles de VPN avanzada ajustan los tiempos de espera de la autenticación para protegerse frente a los fallos de la VPN, conectar comandos para las redes privadas virtuales basadas en el cliente y usar los controles de adaptador para controlar a los que se permite acceso a la red privada virtual.

Para acceder a este control, haga clic en la pestaña *Configuración de la directiva global*, haga clic en el símbolo "+" situado junto a la *Aplicación de VPN* y haga clic en *Avanzadas* en el árbol de directivas situado a la izquierda.



Se pueden configurar los siguientes valores avanzados de la aplicación de VPN:

Tiempo límite de autenticación: Los administradores pueden colocar el puesto final en unos ajustes del cortafuegos seguros (la configuración del cortafuegos *Cambiar a ubicación*) para protegerse frente a los fallos de conectividad de la VPN. El *Tiempo límite de autenticación* es la cantidad de tiempo que ZENworks Security Client espera hasta obtener la autenticación en el servidor de la VPN. Este parámetro se debe ajustar por encima de 1 minuto para permitir la autenticación en conexiones más lentas.

Conectar/desconectar comandos: Al utilizar el temporizador de la autenticación, los comandos *Conectar* y *Desconectar* controlan la activación de la VPN basada en el cliente. Especifique la ubicación del cliente de VPN y los parámetros necesarios en los campos de *Parámetros*. El comando Desconectar es opcional y se proporciona a los clientes de la VPN que requieren que el usuario se desconecte antes de finalizar sesión de la red.

Nota: Los clientes de VPN que generan adaptadores virtuales (por ejemplo, Cisco Systems VPN Client 4.0) visualizan el mensaje `La directiva se ha actualizado` y pueden alternar desde la ubicación actual temporalmente. La directiva no se ha actualizado; ZENworks Security Client está simplemente comparando el adaptador virtual con cualquier restricción del adaptador en la directiva actual. Al ejecutar los clientes de la VPN de este tipo, no se debe utilizar el hiperenlace del comando Desconectar.

Adaptadores: Esto es esencialmente una directiva del mini adaptador específica de la aplicación de VPN.

Si se selecciona un adaptador (cambiándolo a Habilitado, Excepto), a estos adaptadores (inalámbrico siendo específico para el tipo de tarjeta) se les permite conectividad a la red privada virtual.

A los adaptadores que aparecen en la lista de excepciones se les deniega la conectividad a la VPN, mientras que al resto de ese tipo se les proporciona conectividad.

Si no se ha seleccionado un adaptador (Inhabilitado, Excepto), sólo los adaptadores especificados en la lista de excepciones podrán conectarse a la VPN. Al resto se le deniega la conectividad.

Este control se puede utilizar para los adaptadores incompatibles con la red privada virtual, por ejemplo, o adaptadores no compatibles con el departamento de TI.

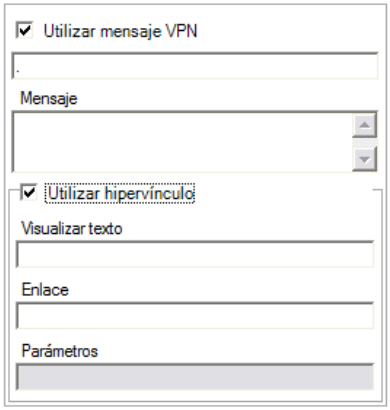
Esta regla anula el conjunto de directivas del adaptador para el cambio a ubicación.

Mensaje del usuario personalizado

Los mensajes del usuario personalizados permiten al administrador de ZENworks Endpoint Security Management crear mensajes que respondan directamente a las preguntas de la directiva de seguridad a medida que el usuario encuentre restricciones de seguridad aplicadas por la directiva. Los mensajes del usuario personalizados también pueden proporcionar instrucciones específicas al usuario. Los controles de los mensajes del usuario están disponibles en varios componentes de la directiva.

Para crear un mensaje de usuario personalizado:

1. Especifique un título para el mensaje. Esto aparece en la barra de títulos del cuadro de mensaje.
2. Especifique el mensaje. El mensaje está limitado a 1.000 caracteres.
3. Si se necesita un hiperenlace, active la casilla *Mostrar hiperenlaces* y especifique la información necesaria.



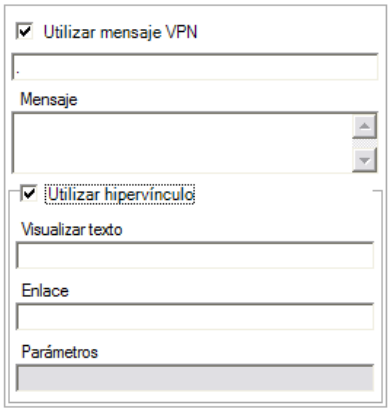
Nota: La modificación del mensaje o hiperenlace en un componente compartido cambia en el resto de instancias de ese componente. Utilice el comando *Mostrar uso* para ver el resto de directivas asociadas a este componente.

Hiperenlaces

Un administrador puede incorporar hiperenlaces en mensajes personalizados para ayudar a explicar las directivas de seguridad o proporcionar enlaces a las actualizaciones de software para mantener el cumplimiento de la integridad. Los hiperenlaces están disponibles en varios componentes de directiva. Se puede crear un hiperenlace de VPN que puede apuntar al ejecutable del cliente de VPN, o a un archivo por lotes que se ejecute y registre completamente el usuario en la VPN (consulte "Aplicación de VPN" en la página 64 para obtener más información).

Para crear un hiperenlace:

1. Especifique un nombre para el enlace. Éste es el nombre que aparece debajo del mensaje. Esto también es necesario para los hiperenlaces de la VPN avanzada.
2. Especifique el hiperenlace.
3. Especifique los cambios u otros parámetros para el enlace.

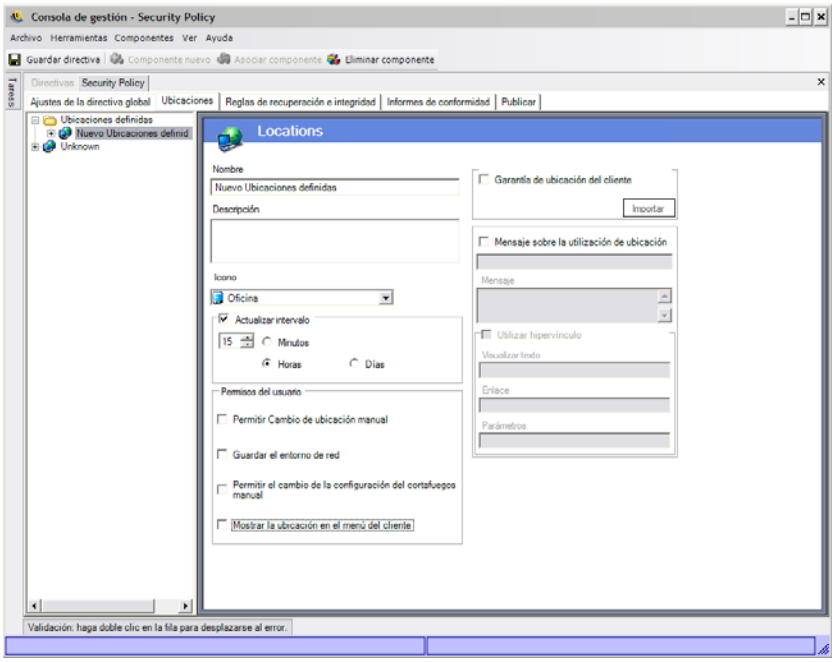


Nota: La modificación del mensaje o del hiperenlace en un componente compartido cambia en el resto de instancias de ese componente. Utilice el comando *Mostrar uso* para ver el resto de directivas asociadas a este componente.

2.2.2 Locations

Las ubicaciones son grupos de reglas asignadas a los entornos de red. Estos entornos se pueden ajustar en la directiva (ver “Entornos de red” en la página 87), o bien definirlos el usuario, si está permitido. A cada ubicación se le puede dar un único valor de seguridad, denegando el acceso a determinados tipos de redes y hardware en entornos de red más hostiles, y concediendo más acceso en entornos de confianza.

Para acceder a los controles de la ubicación, haga clic en la pestaña *Ubicaciones*.



Las secciones siguientes contienen más información sobre:

- “Acerca de las ubicaciones” en la página 70
- “Hardware de comunicación” en la página 72
- “Control del dispositivo de almacenamiento” en la página 74
- “Configuración del cortafuegos” en la página 76
- “Entornos de red” en la página 87
- “Conectividad USB” en la página 88
- “Gestión de Wi-Fi” en la página 90
- “Seguridad de Wi-Fi” en la página 93

Acerca de las ubicaciones

Se pueden configurar los siguientes tipos de ubicaciones:

Ubicación desconocida: Todas las directivas tienen una ubicación desconocida por defecto. Ésta es la ubicación a la que ZENworks Security Client cambia los usuarios cuando abandonan un entorno de red conocido. Esta ubicación desconocida es única para cada directiva y no está disponible como un componente compartido. Los entornos de red no se pueden ajustar ni guardar para esta ubicación.

Para acceder a los controles de la ubicación desconocida, haga clic en la pestaña *Ubicaciones* y haga clic en la ubicación *Desconocida* en el árbol de directivas situado a la izquierda.

Ubicaciones definidas: Las ubicaciones definidas se pueden crear para la directiva, o bien se pueden asociar las ubicaciones existentes (aquellas creadas para otras directivas).

Para crear una ubicación nueva:

1. Haga clic en *Ubicaciones definidas* y haga clic en el botón *Componente nuevo* de la barra de herramientas.
2. Asigne un nombre a la ubicación y proporcione una descripción.
3. Definir los valores de la ubicación:

   Icono: Seleccione un icono de la ubicación para proporcionar una imagen visual al usuario para identificar la ubicación actual. El icono de la ubicación se visualiza en la barra de tareas en el área de notificación. Utilice la lista desplegable para ver y seleccionar desde los iconos de la ubicación disponible.

   Intervalo de actualización: Especifique el valor que determinará la frecuencia con la que ZENworks Security Client comprueba la actualización de una directiva al acceder a esta ubicación. El tiempo de frecuencia se ajusta en minutos, horas o días. Si se anula la selección de este parámetro, ZENworks Security Client no comprueba la actualización en esta ubicación.

   Permisos del usuario: Especifique los permisos de usuario:

   - **Permitir cambio manual de la ubicación:** Permite al usuario cambiar a y desde esta ubicación. Para las ubicaciones no gestionadas (lugares de acceso público, aeropuertos, hoteles, etc.), se debe conceder este permiso. En los entornos controlados en los que se conocen los parámetros de la red, este permiso se puede inhabilitar. El usuario no puede cambiar a o desde las ubicaciones si está habilitado este permiso; en su lugar, ZENworks Security Client confía en los parámetros del entorno de red especificados para esta ubicación.
   - **Guardar entorno de red:** Permite al usuario guardar el entorno de red en esta ubicación para permitir el cambio automático a la ubicación cuando el usuario vuelva. Este valor se recomienda para las ubicaciones al que el usuario necesite cambiar. Se pueden guardar varios entornos de red para una única ubicación. Por ejemplo, si una ubicación definida como Aeropuerto es parte de la directiva actual, cada aeropuerto que visite el usuario puede guardarse como un entorno de red de esta ubicación. De esta forma, un usuario móvil puede volver a un entorno de aeropuerto guardado y ZENworks Security client cambia automáticamente a la ubicación del aeropuerto y aplica la configuración de seguridad definida. Por supuesto, un usuario puede cambiar a una ubicación y no guardar el entorno.
   - **Permitir cambio de los ajustes del cortafuegos manual:** Permite al usuario cambiar los ajustes del cortafuegos.
   - **Mostrar ubicación en el menú Cliente:** Permite la visualización de la ubicación en el menú del cliente. Si no está seleccionada, la ubicación no se visualiza.

   Seguridad de la ubicación del cliente: Dado que la información del entorno de red utilizada para determinar una ubicación se puede falsificar fácilmente, exponiendo potencialmente al punto final a intrusión, la opción de la comprobación cifrada de una ubicación está disponible a través de Client Location Assurance Service (CLAS). Este servicio sólo es fiable en los entornos de red que se encuentran única y exclusivamente bajo el control de la empresa. La

adición de seguridad de la ubicación del cliente implica que los permisos y los ajustes del cortafuegos se pueden configurar como menos restrictivios, dando por sentado que el punto final está ahora protegido detrás del cortafuegos de la red.

ZENworks Security Client utiliza un puerto configurable de la empresa, fijo, para enviar un desafío al Servicio de seguridad de ubicación del cliente. El Servicio de seguridad de ubicación del cliente descifra el paquete y responde al desafío, siempre que la clave privada coincida con la clave pública. El icono de la barra de tareas incluye una marca de verificación, indicando que el usuario se encuentra en la ubicación correcta.

ZENworks Security Client no puede cambiar a la ubicación, salvo que pueda detectar el servidor de CLAS. Si no se ha detectado el servidor de CLAS, aun cuando el resto de parámetros de la red coincidan, ZENworks Security Client permanece en la ubicación desconocida para proteger el punto final.

Para activar CLAS para una ubicación, active la casilla de verificación *Seguridad de la ubicación del cliente*, haga clic en *Importar* y busque y seleccione el archivo. La palabra Configurado aparece cuando se importe correctamente la clave.

Esta opción no está disponible para la Ubicación desconocida.

Utilizar mensaje de ubicación: Permite que se visualice un mensaje del usuario personalizado opcional cuando ZENworks Security Client cambia a esta ubicación. Este mensaje puede facilitar instrucciones al usuario final, detalles sobre las restricciones de la directiva bajo esta ubicación, o bien incluir un hiperenlace para obtener más información.

4 Haga clic en *Guardar directiva*. Si su directiva contiene errores, consulte Sección 2.2.6, “Notificación de error”, en la página 106.

Para asociar una ubicación existente:

1 Haga clic en *Ubicaciones definidas* y, a continuación, en el botón *Asociar componente* de la barra de herramientas.

2 Seleccione las ubicaciones deseadas de la lista.

3 Si lo desea, edite la configuración.

Nota: Si cambia los ajustes en un componente compartido, esto afecta al resto de instancias del mismo componente. Utilice el comando *Mostrar uso* para ver el resto de directivas asociadas a este componente.

---

4 Haga clic en *Guardar directiva*. Si su directiva contiene errores, consulte Sección 2.2.6, “Notificación de error”, en la página 106.

Se deben definir varias ubicaciones definidas (más allá de las ubicaciones desconocida y de trabajo sencillas) en la directiva para proporcionar al usuario varios permisos de seguridad cuando éstos se conectan fuera del cortafuegos de la empresa. Mantener la sencillez de los nombres de ubicaciones (por ejemplo, cafeterías, aeropuertos, casa) y proporcionar una imagen visual a través del icono de la barra de herramientas de la ubicación ayuda a los usuarios a cambiar fácilmente a la configuración de seguridad adecuada necesaria para cada entorno de red.

Hardware de comunicación

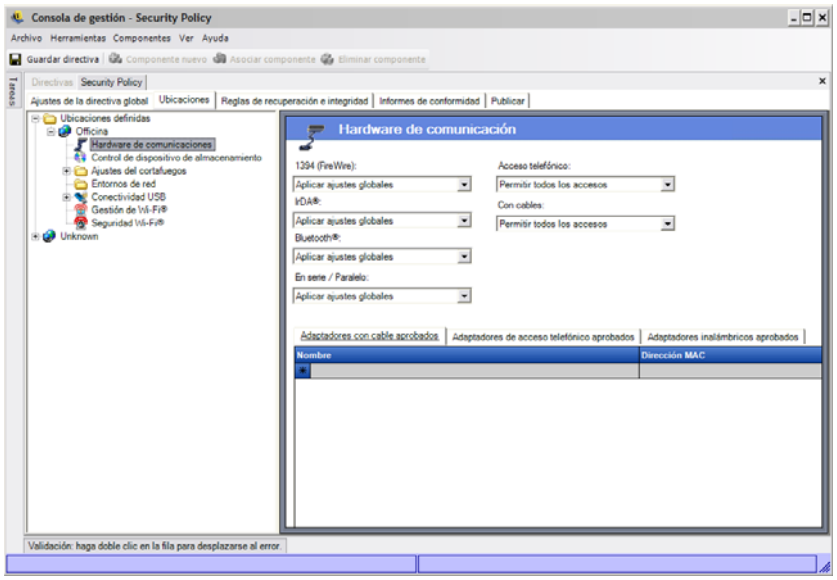
La configuración del hardware de comunicación controla por ubicación qué tipos de hardware permiten una conexión en este entorno de red.

Nota: Puede ajustar los controles del hardware de comunicación globalmente en la pestaña *Configuración de la directiva global* o para las ubicaciones individuales en la pestaña *Ubicaciones*.

Para ajustar los controles del hardware de comunicación para una ubicación, haga clic en la pestaña *Ubicaciones*, expanda la ubicación deseada en el árbol y haga clic en *Hardware de comunicación*.

O bien

Para ajustar los controles del hardware de comunicación globalmente, haga clic en la pestaña *Configuración de la directiva global*, expanda *Configuración global* en el árbol y haga clic en *Hardware de comunicación*. Para obtener más información, consulte la "Hardware de comunicación" en la página 51.



Seleccione la habilitación, inhabilitación o aplicación de la configuración global de cada dispositivo del hardware de comunicación que aparece en:

- **1394 (FireWire):** Controla el puerto de acceso FireWire* en el punto final.
- **IrDA:** Controla el puerto de acceso por infrarrojos en el puesto final.
- **Bluetooth:** Controla el puerto de acceso Bluetooth* en el punto final.
- **Serie/Paralelo:** Controla el acceso de los puertos de serie y paralelo del puesto final.
- **Marcación:** Controla la conectividad del módem por ubicación. Esta opción no está disponible al configurar los valores del hardware de comunicación de forma global a través de la pestaña *Configuración de la directiva global*.
- **Wired:** Controla la conectividad de la tarjeta LAN por ubicación. Esta opción no está disponible al configurar los valores del hardware de comunicación de forma global a través de la pestaña *Configuración de la directiva global*.

La habilitación permite el acceso completo al puerto de comunicación.

La inhabilitación deniega todo el acceso al puerto de comunicación.

Nota: Los adaptadores de Wi-Fi se controlan globalmente o se inhabilitan localmente mediante los controles de seguridad de Wi-Fi. Los adaptadores se pueden especificar según la marca mediante la lista de adaptadores inalámbricos aprobados.

Lista de adaptadores de marcación aprobados: ZENworks Security Client puede bloquear todos los adaptadores excepto los de marcación aprobados y especificados (módems) para su conexión. Por ejemplo, un administrador puede implementar una directiva que únicamente permita una marca o tipo específicos de tarjeta de módem. Esto reduce los costes de asistencia asociados al uso de los empleados de hardware no compatible.

Lista de adaptadores inalámbricos aprobados: ZENworks Security Client puede bloquear todos los adaptadores excepto los inalámbricos aprobados y especificados para su conexión. Por ejemplo, un administrador puede implementar una directiva que únicamente permita una marca o tipo específico de tarjeta inalámbrica. Esto reduce los costes de asistencia asociados al uso de los empleados de hardware incompatible y habilita asistencia mejorada, y la aplicación de las iniciativas de seguridad basadas en los estándares de IEEE, así como LEAP, PEAP, WPA, TKIP y otros.

Uso de la función AdapterAware:

ZENworks Security Client recibe notificación siempre que un dispositivo de red se instala en el sistema, y determina si el dispositivo está o no autorizado. Si no está autorizado, la solución inhabilita el controlador del dispositivo, lo cual inhabilita este nuevo dispositivo y notifica al usuario acerca de la situación.

Nota: Cuando un nuevo adaptador no autorizado (de marcación e inalámbrico) instala en primer lugar sus controladores en el puesto final (mediante PCMCIA o USB), el adaptador se mostrará como habilitado en el administrador de dispositivos de Windows hasta que se reinicie el sistema, aunque se bloqueará toda la conectividad de la red.

Especifique el nombre de cada adaptador permitido. Se permiten los nombres de adaptadores parciales. Los nombres de adaptadores están limitados a 50 caracteres y distinguen entre mayúsculas y minúsculas. El sistema operativo Windows 2000 necesita el nombre del dispositivo para proporcionar esta funcionalidad. Si no se introduce ningún adaptador, se permiten todos los adaptadores del tipo. Si sólo se introduce un adaptador, sólo se permite un único adaptador en esta ubicación.

Nota: Si el puesto final se encuentra en una ubicación que define únicamente un SSID del punto de acceso como la identificación de la red, ZENworks Security Client cambiará a esa ubicación antes de inhabilitar el adaptador no autorizado. Se debe utilizar una anulación de contraseña para proporcionar un parámetro de ubicación manual si esto sucede.

Control del dispositivo de almacenamiento

Los controles del dispositivo de almacenamiento ajustan la configuración del dispositivo de almacenamiento por defecto para la directiva, donde todos los dispositivos de almacenamiento de archivos externos son de lectura o escritura, funcionan en un estado de sólo lectura, o bien están completamente inhabilitados. Si están inhabilitados, estos dispositivos no pueden recuperar datos del punto final, pero la unidad de disco duro y todas las unidades de red seguirán estando operativas y accesibles.

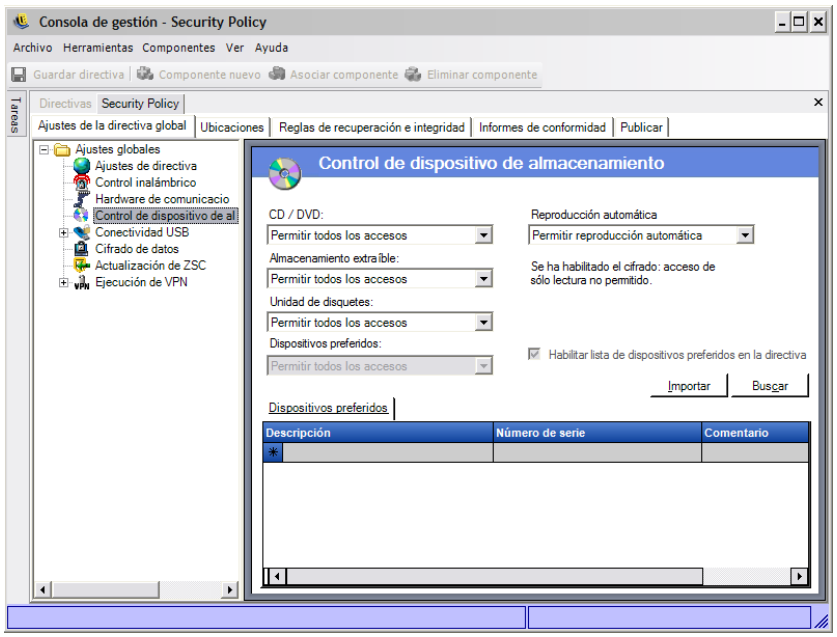
El control del dispositivo de almacenamiento de ZENworks Endpoint Security Management no está permitido si está activada ZENworks Storage Encryption Solution.

Nota: Puede ajustar los controles del dispositivo de almacenamiento globalmente en la pestaña *Configuración de la directiva global* o para las ubicaciones individuales en la pestaña *Ubicaciones*.

Para ajustar los controles del dispositivo de almacenamiento para una ubicación, haga clic en la pestaña *Ubicaciones*, expanda la ubicación deseada en el árbol y haga clic en *Control del dispositivo de almacenamiento*.

O bien

Para ajustar los controles del dispositivo de almacenamiento globalmente, haga clic en la pestaña *Configuración de la directiva global*, expanda *Configuración global* en el árbol y haga clic en *Control del dispositivo de almacenamiento*. Para obtener más información, consulte la "Control del dispositivo de almacenamiento" en la página 52.



El control del dispositivo de almacenamiento está dividido en las siguientes categorías:

- **CD/DVD:** controla todos los dispositivos que aparecen en las *unidades de DVD/CD-ROM* en Windows Device Manager.
- **Almacenamiento extraíble:** controla todos los dispositivos notificados como almacenamiento extraíble de las *Unidades de disco* en Windows Device Manager.
- **Floppy Drive:** controla todos los dispositivos que aparecen en las *Unidades de disquete* en Windows Device Manager.

El almacenamiento fijo (unidades de disco duro) y unidades de red (si están disponibles) siempre están permitidos.

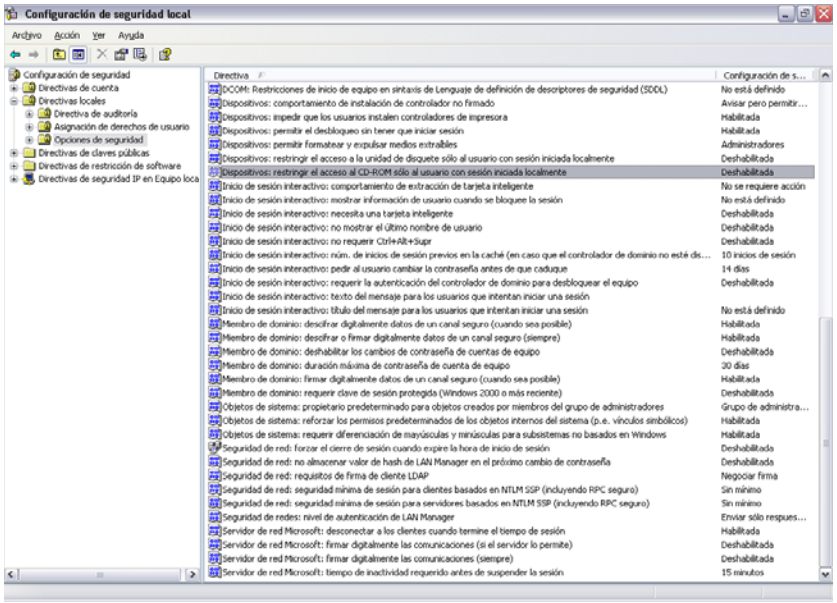
Para ajustar el valor por defecto de la directiva de los dispositivos de almacenamiento, seleccione la configuración global para ambos tipos de las listas desplegables:

- **Activar:** El tipo de dispositivo se permite por defecto.

- **Inhabilitar:** el tipo de dispositivo no está permitido. Cuando los usuarios intentan acceder a los archivos en un dispositivo de almacenamiento definido, éstos reciben un mensaje de error del sistema operativo, o de la aplicación que intenta acceder al dispositivo de almacenamiento local, indicando que se ha producido un error en la acción
- **Sólo lectura:** el tipo de dispositivo está establecido como Sólo lectura. Cuando los usuarios intentan escribir en el dispositivo, éstos reciben un mensaje de error del sistema operativo, o de la aplicación que intenta acceder al dispositivo de almacenamiento local, indicando que se ha producido un error en la acción

---

Nota: Si desea inhabilitar las unidades de CD-ROM o unidades de disquete en un grupo de puntos finales, o ajustarlas como Sólo lectura, la configuración de seguridad local (bajada de nivel a través de un objeto de directiva del grupo de servicios de directorio) debe tener *Dispositivos: restringir acceso de CD-ROM únicamente para el usuario que ha iniciado sesión localmente* y *Dispositivos: restringir acceso de disquete únicamente para el usuario que ha iniciado sesión localmente ajustado como Inhabilitado*. Para verificar esto, abra el objeto de directiva del grupo, o bien abra las herramientas administrativas en un equipo. Mirar configuración de la seguridad local: opciones de seguridad y comprobar que ambos dispositivos están inhabilitados. El valor por defecto es Inhabilitado.



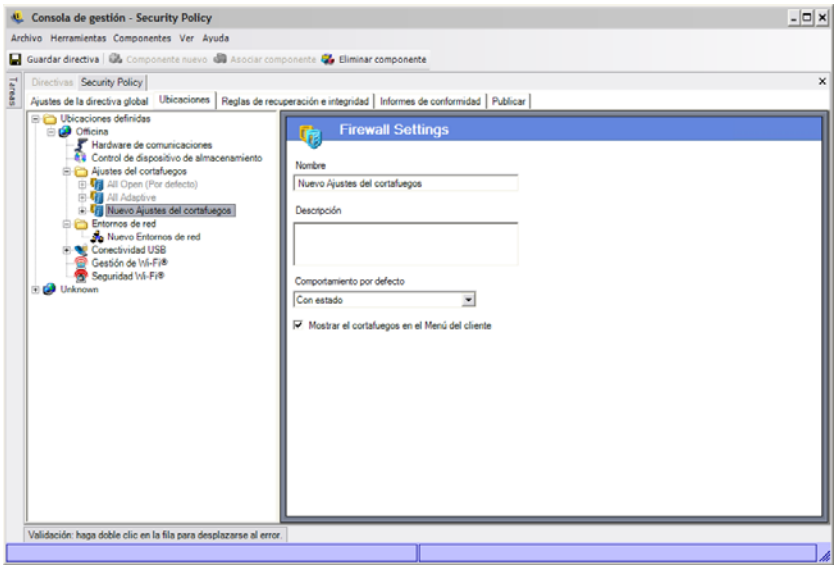
Configuración del cortafuegos

Los ajustes del cortafuegos controlan la conectividad de todos los puertos de red, listas de control de acceso, paquetes de red (ICMP, ARP, etc.) y qué aplicaciones pueden obtener un zócalo o una función una vez que se apliquen los ajustes del cortafuegos.

Nota: Esta función sólo está disponible en la instalación de ZENworks Endpoint Security Management y no puede utilizarse para directivas de seguridad UWS.

Para acceder a este control, haga clic en la pestaña *Ubicaciones* y haga clic en el icono *Ajustes del cortafuegos* en el árbol de directivas situado a la izquierda.

Cada componente de una configuración del cortafuegos se configura de forma independiente, con el único requisito de ajustar el comportamiento predeterminado de los puertos TCP/UDP. Esta configuración afecta a todos los puertos TCP/UDP cuando está habilitada. Los puertos individuales o agrupados se pueden crear con un valor diferente.



Para crear una nueva configuración del cortafuegos:

1. Seleccione *Ajustes del cortafuegos* en el árbol de componentes y haga clic en el botón *Componente nuevo*.
2. Asigne un nombre a la configuración del cortafuegos y realice una descripción.
3. Haga clic con el botón derecho en *Puertos TCP/UDP* del árbol de componentes y haga clic en *Añadir nuevos puertos TCP/UDP* para seleccionar el comportamiento por defecto para todos los puertos TCP/UDP.

   Los puertos y listas adicionales se pueden añadir a los ajustes del cortafuegos, y se les pueden asignar comportamientos únicos que anulen la configuración por defecto.

   Por ejemplo, el comportamiento por defecto de todos los puertos se establece como Todo con estado. Esto significa que las listas de puertos para los medios de emisión y exploración Web se añaden a los ajustes del cortafuegos. El puerto de los medios de emisión continua se establece como Cerrado y el comportamiento del puerto de exploración Web se establece como Abierto. El tráfico de redes a través de los puertos TCP 7070, 554, 1755 y 8000 se bloquea. El tráfico de redes a través de los puertos 80 y 443 se abre y está visible en la red. El resto de los puertos funciona en el modo Con estado, siendo necesario que en primer lugar se solicite el tráfico a través de los mismos.

   Para obtener más información, consulte la "Puertos TCP/UDP" en la página 78.
4. Haga clic con el botón derecho en *Listas de control de acceso* y haga clic en *Añadir nuevas listas de control de acceso* para añadir direcciones que podrían requerir el paso de tráfico no solicitado, independientemente del comportamiento del puerto actual.

   Para obtener más información, consulte la "Listas de control de acceso" en la página 82.
5. Haga clic con el botón derecho en *Controles de aplicación* y haga clic en *Añadir nuevos controles de aplicación* para bloquear el acceso a la red de las aplicaciones o simplemente su ejecución.

Para obtener más información, consulte la "Controles de aplicación" en la página 85.

6 Seleccione si desea visualizar este cortafuegos en el menú de ZENworks Security Client (si esta opción no está seleccionada, el usuario no ve estos ajustes del cortafuegos).

7 Haga clic en *Guardar directiva*. Si su directiva contiene errores, consulte Sección 2.2.6, "Notificación de error", en la página 106.

Para asociar un ajuste de cortafuegos existente:

1 Seleccione *Ajustes del cortafuegos* en el árbol de componentes y haga clic en el botón *Asociar componente*.

2 Seleccione los ajustes del cortafuegos deseados de la lista,

3 Si es necesario cambie la configuración del comportamiento por defecto.

Nota: El cambio de los ajustes en un componente compartido afecta al resto de instancias del mismo componente. Utilice el comando *Mostrar uso* para ver el resto de directivas asociadas a este componente.

---

4 Haga clic en *Guardar directiva*. Si su directiva contiene errores, consulte Sección 2.2.6, "Notificación de error", en la página 106.

Se pueden incluir varias configuraciones del cortafuegos en una única ubicación. Uno se define como el ajuste por defecto y el resto de ajustes se encuentran disponibles como opciones para que el usuario pueda intercambiarlas. Resulta útil disponer de varios ajustes cuando un usuario necesita determinadas restricciones de seguridad en un entorno de red y cuando, en algunas ocasiones, necesita que estas restricciones aumenten durante un período corto de tiempo, para determinados tipos de conectividad, por ejemplo, difusiones ICMP.

En la instalación se incluyen los siguientes ajustes del cortafuegos:

- **Todo adaptado:** Define todos los puertos de conectividad como con estado (se bloquea todo el tráfico de red entrante no solicitado y todo el tráfico de red saliente está permitido), los paquetes ARP y 802.1x y todas las aplicaciones de red están permitidos como conexiones de red.
- **Todos abiertos:** Define todos los puertos de conectividad como abiertos (se permite todo el tráfico de red) y se permiten todos los tipos de paquetes. Todas las aplicaciones de red están permitidas como conexiones de red.
- **Todos cerrados:** Cierra todos los puertos de conectividad y restringe todos los tipos de paquetes.

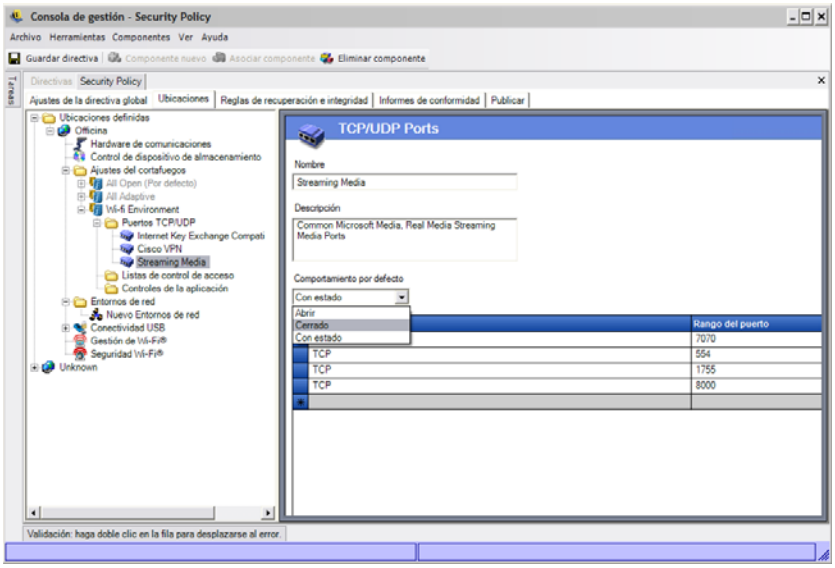
Una nueva ubicación tiene los ajustes del cortafuegos únicos, Todos abiertos, configurado como el valor por defecto. Para definir unos ajustes del cortafuegos distintos como el valor por defecto, haga clic con el botón derecho en los ajustes del cortafuegos deseados y seleccione *Ajustar por defecto*.

Puertos TCP/UDP

Los datos del extremo principalmente se protegen mediante el control de la actividad de los puertos TCP/UDP. Esta función le permite crear una lista de puertos TCP/UDP que se gestionará excepcionalmente en estos ajustes del cortafuegos. Las listas incluyen un conjunto de puertos y rangos de puertos, junto con su tipo de transporte, que define la función del rango.

Nota: Esta función sólo está disponible en la instalación de ZENworks Endpoint Security Management y no puede utilizarse para directivas de seguridad UWS.

Para acceder a este control, haga clic en la pestaña *Ubicaciones*, haga clic en el símbolo + junto a *Ajustes del cortafuegos*, haga clic en el símbolo "+" junto al cortafuegos que desee y haga clic en el icono *Puertos TCP/UDP* del árbol de directivas de la izquierda.



Las nuevas listas de puertos TCP/UDP pueden definirse con puertos individuales o como un rango (1-100) por cada línea de la lista.

Para crear un nuevo ajuste de puerto TCP/UDP:

1. Haga clic con el botón derecho en *Puertos TCP/UDP* del árbol de componentes y haga clic en *Añadir nuevos puertos TCP/UDP*.
2. Asigne un nombre a la lista de puertos e incluya una descripción.
3. Seleccione el comportamiento de puerto de la lista desplegable:
   - **Abierto:** Se permite todo el tráfico entrante y saliente de red. Dado que se permite todo el tráfico de red, la identidad de su equipo se encuentra visible para este puerto o rango de puerto.
   - **Cerrado:** Se bloquea todo el tráfico de red entrante y saliente. Dado que todas las solicitudes de identificación de red se bloquean, la identidad de su equipo se oculta para este puerto o rango de puerto.
   - **Con estado:** Se bloquea todo el tráfico de red entrante no solicitado. Se permite todo el tráfico de red saliente de este puerto o rango de puerto.
4. Especifique el tipo de transporte haciendo clic en la flecha abajo de la columna *Tipo de puerto*:
   - TCP/UDP
   - Ether
   - IP
   - TCP
   - UDP

5 Introduzca puertos y rangos de puertos como uno de los siguientes:

- Puertos únicos
- Un rango de puertos con el número del primer puerto, seguido de un guión y el número del último puerto

  Por ejemplo, 1-100 agregaría todos los puertos entre el 1 y el 100

  Visite las páginas de autoridad de números asignadas (http://www.iana.org) de Internet para obtener una lista completa de tipos de transporte y puertos.

6 Haga clic en *Guardar directiva*.

Para asociar un puerto TCP/UDP existente a este ajuste de cortafuegos:

1 Seleccione *Puertos TCP/UDP* del árbol de componentes y haga clic en el botón *Asociar componente*.

2 Seleccione los puertos que desee de la lista.

3 Configure los ajustes de comportamiento por defecto.

  Si cambia los ajustes en un componente compartido, esto afecta al resto de instancias del mismo componente. Utilice el comando *Mostrar uso* para ver el resto de directivas asociadas a este componente.

4 Haga clic en *Guardar directiva*.

Se incluyen algunos grupos de puertos TCP/UDP que están disponibles en la instalación:

Nombre	Descripción	Transporte	Valor
Todos los puertos	Todos los puertos	Todos	1-65535
BlueRidge VPN	Puertos utilizados por el cliente de VPN Blue Ridge	UDP	820
Cisco VPN	Puertos utilizados por el cliente Cisco* VPN	IP	50,51
		UDP	500,4500
		UDP	1000-1200
		UDP	62514,62515,62517
		UDP	62519-62521
		UDP	62532,62524
Conectividad común	Puertos de conectividad necesarios habitualmente para crear cortafuegos	TCP	53
		UDP	53
		UDP	67,68
		TCP	546, 547
		UDP	546, 547
		TCP	647, 847
		UDP	647, 847

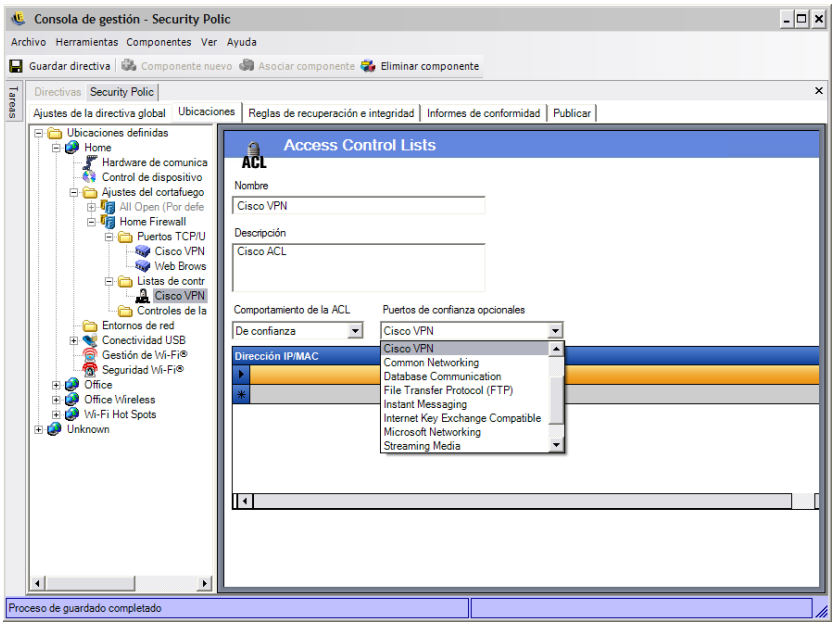
Nombre	Descripción	Transporte	Valor
Comunicación de bases de datos	Puertos de bases de datos Microsoft*, Oracle*, Siebel*, Sybase*, SAP*	TCP	4100
		TCP	1521
		TCP	1433
		UDP	1444
		TCP	2320
		TCP	49998
		TCP	3200
		TCP	3600
Protocolo de transferencia de archivos (FTP)	Puerto de protocolo de transferencia de archivos	TCP/UDP	21
Mensajería instantánea	Puertos de mensajería instantánea Microsoft, AOL* y Yahoo*	TCP	6891-6900
		TCP	1863,443
		UDP	1863,443
		UDP	5190
		TCP	6901
		UDP	6901
		TCP	5000-5001
		UDP	5055
		TCP	20000-20059
		UDP	4000
		TCP	4099
		TCP	5190
VPN compatible con Internet Key Exchange	Puertos utilizados por clientes VPN compatibles con Internet Key Exchange	UDP	500
Conectividad con Microsoft	Compartición de archivos comunes / puertos de directorios activos *	TCP/UDP	135-139, 445
Puertos abiertos	Puertos que abre este cortafuegos	TCP/UDP	80
Medios de emisión continua	Puertos de medios de emisión continua reales y comunes de Microsoft	TCP	7070, 554, 1755, 8000
Navegación por Internet	Puertos comunes de navegadores Web, incluyendo SSL	Todos	80, 443

Listas de control de acceso

Podría haber algunas direcciones que requieren tráfico no solicitado para pasar, independientemente del comportamiento del puerto actual (por ejemplo, el servidor de copia de seguridad de la empresa, el servidor de intercambio, etc.). En instancias en las que resulte necesario el paso de tráfico no solicitado entre servidores de confianza, una lista de control de acceso (ACL) resuelve este problema.

Nota: Esta función sólo está disponible en la instalación de ZENworks Endpoint Security Management, y no se puede utilizar para las directivas de seguridad UWS.

Para acceder a este control, haga clic en la pestaña *Ubicaciones*, haga clic en el símbolo + junto a *Ajustes del cortafuegos*, haga clic en el símbolo + junto al cortafuegos que desee, haga clic con el botón derecho en *Listas de control de acceso* del árbol de directivas de la izquierda y haga clic en *Añadir nuevas listas de control de acceso*.



Para crear un nuevo ajuste ACL:

1. Haga clic con el botón derecho en *Listas de control de acceso* del árbol de componentes y haga clic en *Añadir nuevas listas de control de acceso*.
2. Asigne un nombre a la ACL e incluya una descripción.
3. Especifique una macro o dirección ACL.
4. Especifique el tipo de ACL:
   - **IP:** Este tipo limita la dirección a 15 caracteres y sólo incluye los números 0-9 y los puntos, por ejemplo, 123.45.6.189. Las direcciones IP también se pueden introducir como un rango, como 123.0.0.0 - 123.0.0.255.
   - **MAC:** Este tipo limita la dirección a 12 caracteres y sólo incluye los números 0-9 y las letras A-F (mayúsculas y minúsculas); separados por dos puntos, por ejemplo 00:01:02:34:05:B6).

5 Seleccione la lista desplegable Comportamiento ACL y determine si las ACL que se indican deben ser *De confianza* (permitirlas siempre aun cuando los puertos TCP/UDP se encuentren cerrados) o *De no confianza* (acceso bloqueado).

6 Si ha seleccionado *De confianza*, seleccione los *puertos de confianza opcionales (TCP/UDP) que esta ACL utilizará*. Estos puertos permiten todo el tráfico ACL, mientras que otros puertos TCP/UDP mantienen sus ajustes actuales. Si selecciona *Ninguno* equivale a que ACL no puede utilizar ningún puerto.

7 Haga clic en *Guardar directiva*.

Para asociar una ACL o Macro existente a estos ajustes del cortafuegos:

1 Seleccione *Lista de control de acceso* del árbol de componentes y haga clic en el botón *Asociar componente*.

2 Seleccione las ACL o macros de la lista.

3 Configure los ajustes del comportamiento de ACL, según convenga.

Nota: Si se cambian los ajustes en un componente compartido, esto afecta al resto de instancias del mismo componente. Utilice el comando *Mostrar uso* para ver el resto de directivas asociadas a este componente.

---

4 Haga clic en *Guardar directiva*.

Lista de macros de direcciones de red

La siguiente es una lista de macros de control de acceso. Estas macros pueden asociarse de forma individual como parte de una ACL en un ajuste de cortafuegos.

Tabla 2-1 *Macros de direcciones de red*

Macro	Descripción
[Arp]	Permite paquetes ARP (protocolo de resolución de direcciones). El término *resolución de direcciones* hace referencia al proceso de búsqueda de una dirección de un equipo en una red. La dirección se resuelve mediante un protocolo en el que la información se envía a través de un proceso de cliente que se ejecuta en el ordenador local a un proceso de servidor que se ejecuta en un ordenador remoto. La información que recibe el servidor permite al servidor identificar al sistema de red para el que se exigió la dirección para proporcionar la dirección requerida. El procedimiento de resolución de dirección finaliza cuando el cliente recibe una respuesta del servidor en la que se incluye la dirección requerida.
[Icmp]	Permite paquetes ICMP (protocolo de mensajes de control de Internet). Los routers, dispositivos intermediarios u hosts utilizan los protocolos ICMP para comunicar actualizaciones o información acerca de errores a otros routers, dispositivos intermediarios u hosts. Los mensajes ICMP se envían en distintas situaciones: por ejemplo, cuando un datagrama no puede alcanzar su destino, cuando el gateway no cuenta con capacidad de buffer para remitir un datagrama y cuando el gateway puede indicar al host que envíe tráfico en una ruta más corta.

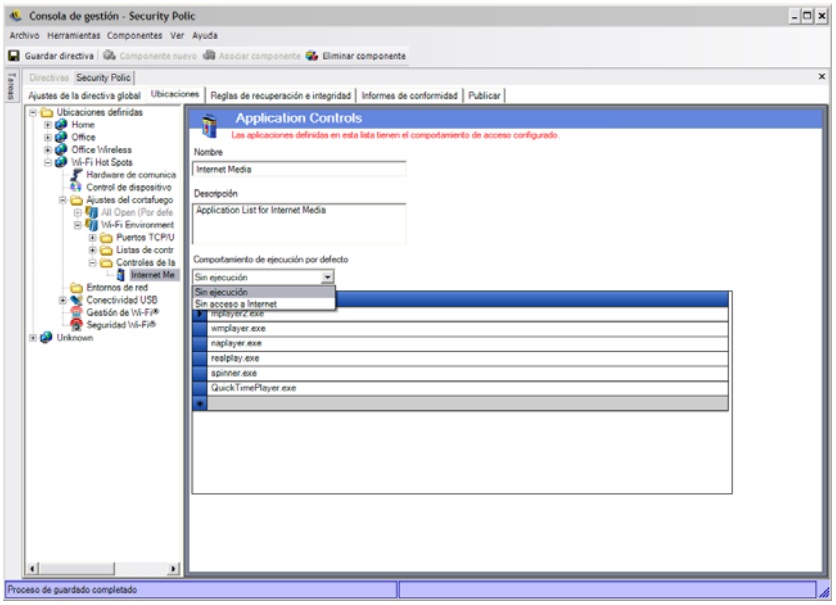
Macro	Descripción
[IpMulticast]	Permite paquetes multidifusión IP. La multidifusión es una tecnología que conserva ancho de banda que reduce el tráfico mediante la entrega simultánea de un único flujo de información a miles de destinatarios corporativos y hogares. Entre las aplicaciones que sacan partido de la multidifusión se incluyen videoconferencias, comunicaciones corporativas, formación a distancia y distribución de software, cotizaciones de acciones y noticias. Los paquetes multidifusión se pueden distribuir mediante direcciones IP o Ethernet.
[EthernetMulticast]	Permite paquetes multidifusión Ethernet.
[IpSubnetBrdcast]	Permite paquetes difusión de subred. Las multidifusiones de subred se utilizan para enviar paquetes a todos los hosts de una subred, superred o, de lo contrario, red de ningún tipo. Todos los hosts de una red de ningún tipo escuchan y procesan los paquetes dirigidos a la dirección de difusión de subred.
[Snap]	Permite paquetes codificados para instantáneas.
[LLC]	Permite paquetes codificados para LLC.
[Allow8021X]	Permite paquetes de 802.1x. Para superar deficiencias en claves de Confidencialidad equivalente al cableado (WEP), Microsoft y otras compañías están utilizando 802.1x como método alternativo de autenticación. 802.1x es un control de acceso desde la red basado en puertos que utiliza certificados o un protocolo de autenticación extensible (EAP). En la actualidad, la mayoría de los principales proveedores de tarjetas inalámbricas y un gran número de proveedores de punto de acceso admiten 802.1x. Este ajuste también permite el Protocolo de autenticación extensible ligero (LEAP) y paquetes de autenticación de acceso protegido WiFi (WPA).
[Gateway]	Representa la dirección de gateway por defecto de la dirección IP actual. Cuando se introduce este valor, ZENworks Security Client permite todo el tráfico de red desde el gateway por defecto de la configuración IP actual como una ACL de confianza.
[GatewayAll]	Igual que [Gateway], pero para todos los gateways definidos.
[Wins]	Representa la dirección de servidor WINS por defecto de la configuración IP del cliente actual. Cuando se introduce este valor, ZENworks Security Client permite todo el tráfico de red desde el servidor WINS por defecto de la configuración IP actual como una ACL de confianza.
[WinsAll]	Igual que en [Wins] pero para todos los servidores WINS definidos.
[Dns]	Representa la dirección de servidor DNS por defecto de la configuración IP del cliente actual. Cuando se introduce este valor, ZENworks Security Client permite todo el tráfico de red desde el servidor DNS por defecto de la configuración IP actual como una ACL de confianza.
[DnsAll]	Igual que [Dns] pero para todos los servidores DNS definidos.
[Dhcp]	Representa la dirección de servidor DHCP por defecto de la configuración IP del cliente actual. Cuando se introduce este valor, ZENworks Security Client permite todo el tráfico de red desde el servidor DHCP por defecto de la configuración IP actual como una ACL de confianza.
[DhcpAll]	Igual que [Dhcp] pero para todos los servidores DHCP definidos.

Controles de aplicación

Esta función permite al administrador impedir a aplicaciones que accedan a la red o que simplemente se ejecuten.

Nota: Esta función sólo está disponible en la instalación de ZENworks Endpoint Security Management y no puede utilizarse para directivas de seguridad UWS.

Para acceder a este control, haga clic en la pestaña *Ubicaciones*, haga clic en el símbolo + junto a *Ajustes del cortafuegos*, haga clic en el símbolo + junto al cortafuegos que desee y haga clic en el icono *Controles de aplicaciones* del árbol de directivas de la izquierda.



Para crear un nuevo ajuste de control de aplicaciones:

1. Haga clic con el botón derecho en *Controles de aplicación* del árbol de componentes y haga clic en *Añadir nuevos controles de aplicación*.
2. Asigne un nombre a la lista de control de aplicaciones e incluya una descripción.
3. Seleccione un comportamiento de ejecución. Este comportamiento se aplica a todas las aplicaciones que aparezcan. Si se requieren varios comportamientos (por ejemplo, algunas aplicaciones de conectividad no tienen acceso a la red, pero todas las aplicaciones de compartición de archivos no pueden ejecutarse), deben definirse varios controles de aplicaciones. Seleccione una de las siguientes opciones:
   - **Todas permitidas:** Todas las aplicaciones que aparecen pueden ejecutar y disponer de acceso a la red.
   - **Sin ejecución:** No se puede ejecutar todas las aplicaciones que aparecen.
   - **Sin acceso a la red:** Se deniega el acceso a la red a todas las aplicaciones que aparecen. A las aplicaciones (como el explorador Web) iniciadas desde una aplicación también se les deniega el acceso a la red.

Nota: El bloqueo de acceso a la red de una aplicación no afecta al proceso de guardar archivos en unidades de red asignadas. Los usuarios pueden guardar en todas las unidades de red que se encuentren disponibles.

4 Especifique las aplicaciones que desee bloquear. Se debe introducir una aplicación por fila.

Importante: La ejecución de bloqueo de aplicaciones importantes podría afectar de forma adversa al funcionamiento del sistema. Las aplicaciones Blocked Microsoft Office intentan ejecutar el programa de instalación.

5 Haga clic en *Guardar directiva*.

Para asociar una lista de control de aplicaciones existente a este ajuste de cortafuegos:

1 Seleccione Controles de aplicaciones en el árbol de componentes y haga clic en el botón *Asociar componente*.

2 Seleccione un conjunto de aplicaciones de la lista.

3 Configure las aplicaciones y el nivel de restricción, según convenga.

Nota: Si cambia los ajustes en un componente compartido, esto afecta al resto de instancias del mismo componente. Utilice el comando *Mostrar uso* para ver el resto de directivas asociadas a este componente.

4 Haga clic en *Guardar directiva*.

Los controles de aplicaciones disponibles se identifican a continuación. El comportamiento de ejecución por defecto es Sin acceso a la red.

Tabla 2-2 *Controles de aplicaciones*

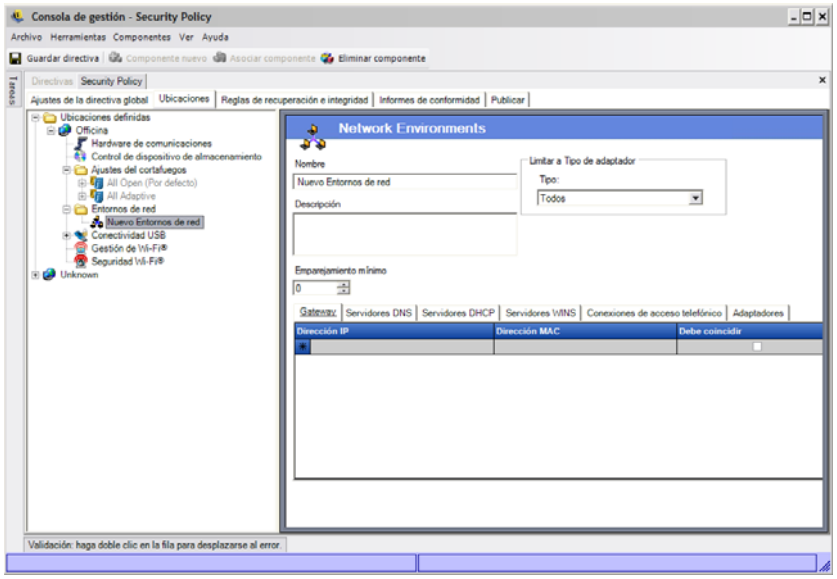
Nombre	Aplicaciones
Navegadores Web	explore.exe; netscape.exe; netscp.exe
Mensajería instantánea	aim.exe; icq.exe; msmsgs.exe; msnmsgr.exe; trillian.exe; ypager.exe
Compartición de archivos	blubster.exe; grokster.exe; imesh.exe; kazaa.exe; morpheus.exe; napster.exe; winmx.exe
Medios de Internet	mplayer2.exe; wmplayer.exe; naplayer.exe; realplay.exe; spinner.exe; QuickTimePlayer.exe

Si la misma aplicación se agrega a dos controles de aplicación distintos de los mismos ajustes del cortafuegos (es decir, se impide la ejecución de `kazaa.exe` en un control de aplicación y se bloquea su acceso a la red en otro control de aplicación definido en los mismos ajustes del cortafuegos), se aplica el control más restrictivo (se impediría la ejecución de kazaa).

Entornos de red

Si se conocen los parámetros de la red (servidores de Gateway, servidores DNS, servidores DHCP, servidores WINS, puntos de accesos disponibles y conexiones de adaptador específicas) para una ubicación, la información del servicio (IP y MAC), que identifica la red, se puede especificar en la directiva para proporcionar un cambio de ubicación inmediata sin que el usuario tenga que guardar el entorno como una ubicación.

Para acceder a este control, haga clic en la pestaña *Ubicaciones* y haga clic en la carpeta *Entornos de red* en el árbol de directivas situado a la izquierda.



La lista proporcionada permite al administrador definir qué servicios de red están presentes en el entorno. Cada servicio de red puede contener varias direcciones. El administrador determina cuántas direcciones son necesarias para que coincidan en el entorno a fin de activar el parámetro de la ubicación.

Debe utilizar dos o más parámetros de la ubicación en cada definición del entorno de red.

Para definir un entorno de red:

1. Seleccione *Entornos de red* en el árbol de componentes y haga clic en el botón *Componente nuevo*.
2. Asigne un nombre al entorno de red y proporcione una descripción.
3. En la lista desplegable *Limitar a tipo de adaptador*, seleccione qué tipo de adaptadores se permite para acceder a este entorno de red:
   - Inalámbrico
   - Todos
   - Módem
   - Wired
   - Inalámbrico
4. Especifique el número mínimo de servicios de red necesarios para identificar este entorno de red.

Cada entorno de red tiene un número mínimo de direcciones que ZENworks Security Client utiliza para identificarlo. El número establecido en *Coincidencia mínima* no debe exceder del número total de direcciones de red identificadas como necesarias en las listas con pestañas. Especifique el número mínimo de servicios de red necesarios para identificar este entorno de red.

5 Especifique la siguiente información para cada servicio:

- **IP Address (Dirección IP):** Especifique hasta 15 caracteres que contengan únicamente los números del 0 al 9 y puntos. Por ejemplo, 123.45.6.789
- **Dirección MAC:** También puede especificar hasta 12 caracteres que contengan únicamente los números del 0 al 9 y las letras A-F (mayúsculas y minúsculas), separados por dos puntos. Por ejemplo, 00:01:02:34:05:B6
- Seleccione la casilla de verificación *Debe coincidir* si la identificación de este servicio es necesaria para definir el entorno de red.

6 Para las pestañas *Conexiones de marcación* y *Adaptadores*, especifique los siguientes requisitos:

- Para las *Conexiones de marcación*, especifique el nombre de entrada de RAS del listín telefónico o el número marcado.

  Nota: Las entradas del listín telefónico deben contener caracteres alfanuméricos y no pueden contener caracteres especiales (@, #, $,%, -, etc.) o caracteres numéricos (1-9). Se da por sentado que las entradas que sólo contengan caracteres especiales y numéricos son números de marcación.

- Para los adaptadores, especifique el SSID de cada adaptador permitido. Se pueden especificar los adaptadores para que restrinjan exactamente qué adaptadores pueden acceder a este entorno de red. Si no se introduce ningún SSID, se concederá acceso a todos los adaptadores del tipo permitido.

Para asociar un entorno de red existente a esta ubicación:

Nota: La asociación de un único entorno de red con dos o más ubicaciones de la misma directiva de seguridad provoca resultados impredecibles y no es recomendable.

1 Seleccione *Entornos de red* en el árbol de componentes y haga clic en el botón *Asociar componente*.

2 Seleccione los entornos de red de la lista.

3 Configure los parámetros del entorno, según convenga.

Nota: Si cambia los ajustes en un componente compartido, esto afecta al resto de instancias del mismo componente. Utilice el comando *Mostrar uso* para ver el resto de directivas asociadas a este componente.

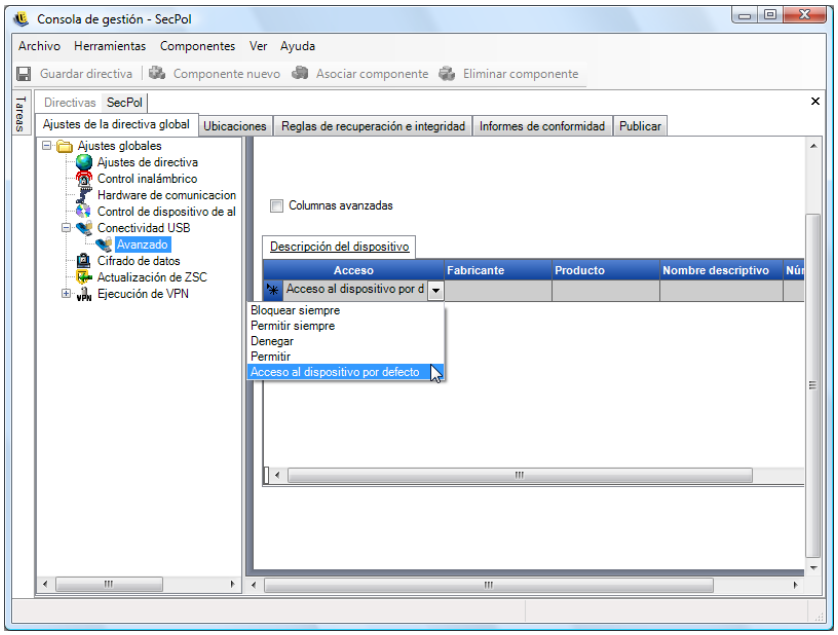
4 Haga clic en *Guardar directiva*.

Conectividad USB

La directiva puede permitir o denegar todos los dispositivos que se conectan mediante el BUS USB. Estos dispositivos se pueden escanear en la directiva desde el informe del inventario de dispositivos USB o escaneando todos los dispositivos actualmente conectados a un equipo. Estos dispositivos se pueden filtrar en función del fabricante, nombre del producto, números de serie, tipo, etc. A efectos

de compatibilidad, el administrador puede configurar la directiva para que acepte un conjunto de dispositivos, por tipo de fabricante, (por ejemplo, todos los dispositivos HP están permitidos), o por tipo de producto (todos los dispositivos de interfaz humana USB, como el ratón y el teclado están permitidos). Asimismo, se puede permitir a los dispositivos individuales que eviten la introducción a la red a los dispositivos no compatibles (por ejemplo, no se permite ninguna impresora a excepción de la de la directiva).

Para acceder a este control, haga clic en *Configuración de la directiva global* y haga clic en *Conectividad USB* del árbol de directivas de la izquierda.



Especifique si desea permitir o denegar el acceso a los dispositivos que no se encuentren en la lista.

Los siguientes métodos permiten rellenar la lista para que pueda permitir o denegar la conectividad USB a los dispositivos:

- “Adición manual de dispositivos” en la página 89
- “Importación de listas de dispositivos” en la página 90

Adición manual de dispositivos

1. Inserte el dispositivo en el puerto USB del equipo en el que está instalada la Consola de gestión.
2. Una vez que el dispositivo esté listo, haga clic en el botón *Explorar*. Si el dispositivo tiene un número de serie, su descripción y número de serie aparecen en la lista.
3. Seleccione un valor de la lista desplegable (el valor del *Dispositivo extraíble global* no se aplica a esta directiva):
   - **Activar:** Los dispositivos de la lista de preferidos pueden utilizar la función de lectura/escritura y el resto de dispositivos USB y de almacenamiento externo están inhabilitados.
   - **Sólo lectura:** Los dispositivos que aparecen en la lista preferida tienen la capacidad de sólo lectura; el resto de dispositivos USB y de almacenamiento externo están inhabilitados.

Repita estos pasos para cada dispositivo permitido en esta directiva. Se aplica la misma configuración a todos los dispositivos.

Importación de listas de dispositivos

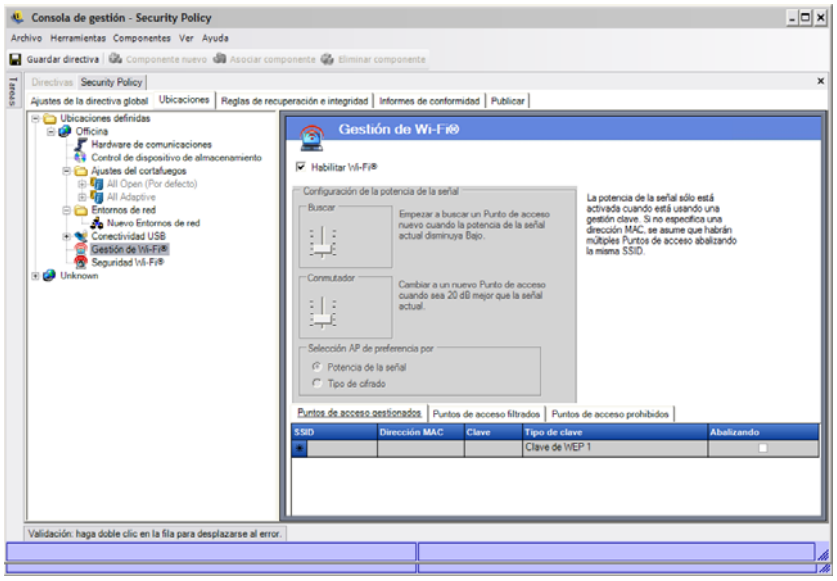
La aplicación del escáner de la unidad USB de Novell genera una lista de dispositivos y sus números de serie (Sección 1.11, “Escáner de la unidad USB”, en la página 43). Para importar esta lista, haga clic en *Importar* y navegue hasta la lista. La lista rellena los campos *Descripción* y *Número de serie*.

Gestión de Wi-Fi

La gestión de Wi-Fi permite al administrador crear listas de puntos de acceso. Los puntos de acceso inalámbrico especificados en estas listas determinan a qué puntos de acceso se permite la conexión al punto final en la ubicación, y qué puntos de acceso se permiten ver al punto final en el administrador de Microsoft Zero Configuration (Configuración cero). Los administradores de la configuración cableada de terceros no admiten esta funcionalidad. Si no se especifica ningún punto de acceso, todos estarán disponibles en el puesto final.

Para acceder a este control, haga clic en la pestaña *Ubicaciones* y haga clic en el icono *Gestión de Wi-Fi* en el árbol de directivas situado a la izquierda.

Nota: En la seguridad o gestión de Wi-Fi, la anulación de la selección de *Habilitar* inhabilita toda la conectividad Wi-Fi en esta ubicación.



Al introducir puntos de accesos a la lista de *Puntos de acceso gestionados* se desactiva la Configuración cero y obliga al punto final a conectarse únicamente a los puntos de acceso que aparecen cuando estén disponibles. Si los puntos de acceso gestionados no están disponibles, ZENworks Security Client hace referencia a la lista de puntos de acceso filtrados. Los puntos de acceso introducidos en los puntos de acceso prohibidos nunca se visualizan en Configuración cero.

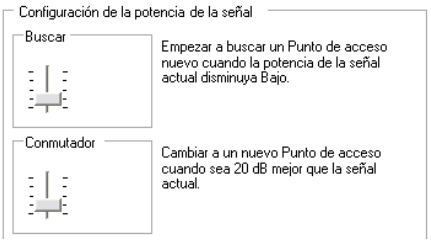
Nota: La lista de puntos de acceso sólo es compatible con el sistema operativo Windows * XP. Antes de implementar una lista de puntos de acceso, se recomienda que todos los extremos borren la lista de redes preferidas de Configuración de cero.

Las secciones siguientes contienen más información sobre:

- “Configuración de la intensidad de la señal de Wi-Fi” en la página 91
- “Puntos de acceso gestionados” en la página 92
- “Puntos de acceso filtrados” en la página 93
- “Puntos de acceso prohibidos” en la página 93

Configuración de la intensidad de la señal de Wi-Fi

Si se define más de un punto de acceso gestionado por WEP en la lista, se puede ajustar la alternancia de intensidad de la señal para el adaptador de Wi-Fi. Los umbrales de intensidad de la señal se pueden ajustar por ubicación para determinar cuándo ZENworks Security Client buscará, descartará y cambiará a otro punto de acceso definido en la lista.



Se puede ajustar la siguiente información:

- **Buscar:** Si se alcanza este nivel de intensidad de señal, ZENworks Security Client empieza a buscar un nuevo punto de acceso al que conectarse. El ajuste por defecto es Bajo [-70 dB].
- **Conmutador:** Para que ZENworks Security Client se conecte a un punto de acceso nuevo, ese punto de acceso debe difundirse con el nivel de intensidad de señal designado por encima de la conexión actual. El valor por defecto es +20 dB.

Los umbrales de intensidad de la señal vienen determinados por la cantidad de potencia (en dB) que notifica el controlador del minipuerto del PC. Dado que cada tarjeta Wi-Fi y radio puede tratar las señales de dB de forma diferente para su indicación de intensidad de la señal recibida (RSSI), los números varían de adaptador a adaptador.

Puede ajustar su preferencia para la selección del punto de acceso en función de lo siguiente:

- Intensidad de la señal
- Tipo de cifrado

Los números por defecto asociados a los umbrales definidos en la consola de gestión son genéricos para la mayoría de los adaptadores Wi-Fi. Debe investigar sus valores RSSI del adaptador Wi-Fi para introducir un nivel preciso. Los valores de Novell son:

Nombre	Valor por defecto
Excelente	-40 dB
Muy bueno	-50 dB
Bueno	-60 dB
Baja	-70 dB

Nombre	Valor por defecto
Muy bajo	-80 dB

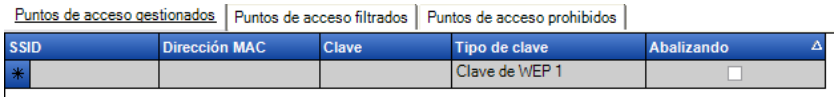
Nota: Aunque los nombres de intensidad de señal anteriores coinciden con los utilizados por el servicio de configuración de cero de Microsoft, es posible que los umbrales no coincidan. La Configuración de cero determina sus valores en función de la Relación señal-ruido (SNR), y no exclusivamente en el valor de dB notificado por RSSI. Por ejemplo, si un adaptador de Wi-Fi recibe una señal a -54 dB y tuviera un nivel de ruido de -22 dB, el SNR se notificaría como 32 dB (-54 - - - 22=32), lo cual, en la escala de configuración de cero se traduciría como intensidad de señal excelente, aun cuando en la escala de Novell, la señal de -54 dB (si se notifica de esa forma a través del controlador del minipuerto, posiblemente notificara un nivel más bajo) indicaría una intensidad de señal muy buena.

Es importante tener en cuenta que el usuario final nunca ve los umbrales de intensidad de la señal de Novell; esta información sólo se proporciona para mostrar la diferencia entre lo que el usuario puede ver a través de la configuración de cero y lo que realmente sucede "entre bastidores".

Puntos de acceso gestionados

ZENworks Endpoint Security Management proporciona un proceso sencillo para distribuir y aplicar automáticamente claves WEP (Wired Equivalent Privacy) sin la intervención del usuario (omitiendo y cerrando el administrador de Microsoft Zero Configuration). Esto protege la integridad de las claves al no dejarlas ver en un correo electrónico o memoria escrita. De hecho, el usuario final sólo necesita conocer la clave para conectarse automáticamente al punto de acceso. Esto ayuda a evitar la posible redistribución de las claves a usuarios no autorizados.

Debido a las vulnerabilidades de seguridad inherentes de la autenticación de la clave de WEP compartida, Novell sólo admite la autenticación de la clave de WEB abierta. Con autenticación compartida, el proceso de validación de la clave de AP/cliente envía un texto no cifrado y versión cifrada de una frase de desafío fácilmente captada de forma inalámbrica. Esto puede facilitar a un pirata informático las versiones cifradas y no cifradas de una frase. Una vez que dispongan de esta información, el descifrado de la clave se convierte en una tarea sencilla.



Facilite la siguiente información para cada punto de acceso:

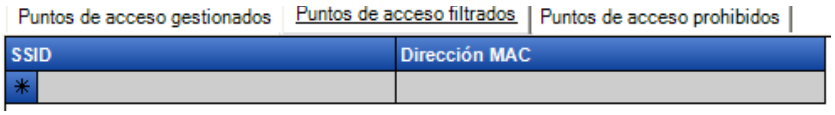
- **SSID:** Identifique el número SSID. El número SSID distingue entre mayúsculas y minúsculas.
- **Dirección MAC:** Identifique la dirección MAC (recomendada, debido a la afinidad entre los SSID). Si no se especifica, se dará por sentado que existen varios puntos de acceso que señalizan el mismo número SSID.
- **Clave:** Especifique la clave WEP para el punto de acceso (10 ó 26 caracteres hexadecimales).
- **Tipo de clave:** Identifique el índice de clave de cifrado seleccionando el nivel adecuado de la lista desplegable.
- **Señalización:** Compruebe si el punto de acceso está difundiendo actualmente su SSID. Deje desactivada esta opción si se trata de un punto de acceso de no señalización.

Nota: ZENworks Security Client primero intenta conectarse a cada punto de acceso de señalización que aparece en la directiva. Si no se ubica ningún acceso de señalización, ZENworks Security Client intenta conectarse a cualquier punto de acceso de no señalización (identificado por SSID) que aparezca en la directiva.

Si se define uno o más puntos de acceso en la lista de *Puntos de acceso gestionados*, se puede ajustar el cambio de intensidad de la señal para el adaptador de Wi-Fi.

Puntos de acceso filtrados

Los puntos de acceso introducidos en la lista de *Puntos de acceso filtrados* son los únicos puntos de acceso que aparecen en la Configuración cero. Esto evita que un punto final se conecte a los puntos de acceso no autorizados.

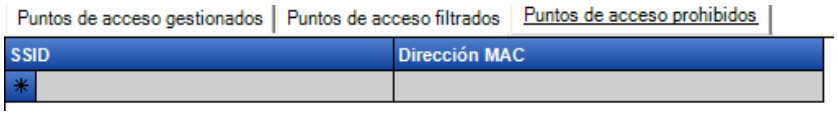


Introduzca la siguiente información para cada punto de acceso:

- **SSID:** Identifique el número SSID. El número SSID distingue entre mayúsculas y minúsculas.
- **Dirección MAC:** Identifique la dirección MAC (recomendada, debido a la afinidad entre los SSID). Si no se especifica, se dará por sentado que existen varios puntos de acceso que indican el mismo número SSID.

Puntos de acceso prohibidos

Los puntos de acceso introducidos en la lista de *Puntos de acceso prohibidos* no se visualizarán en Configuración cero, ni tampoco se permitirá que el punto final se conecte a ellos.



Introduzca la siguiente información para cada punto de acceso:

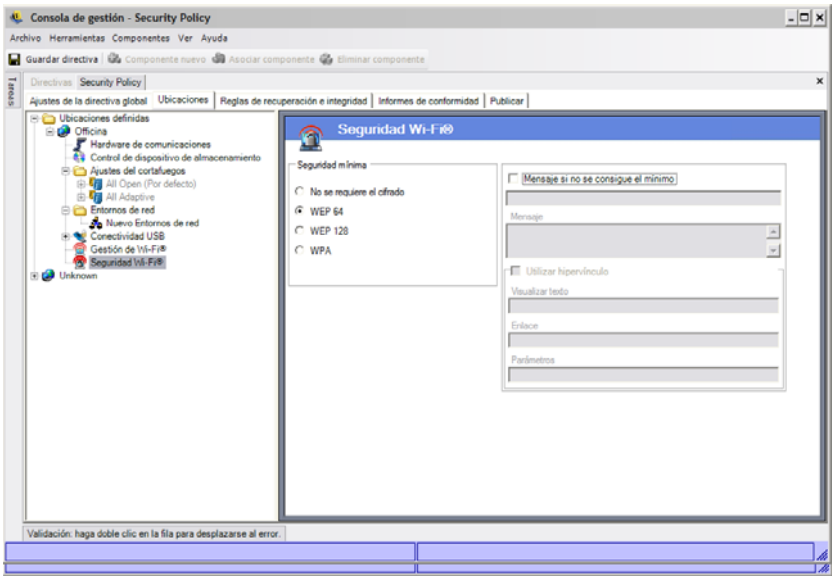
- **SSID:** Identifique el número SSID. El número SSID distingue entre mayúsculas y minúsculas.
- **Dirección MAC:** Identifique la dirección MAC (recomendada, debido a la afinidad entre los SSID). Si no se especifica, se dará por sentado que existen varios puntos de acceso que señalizan el mismo número SSID.

Seguridad de Wi-Fi

Si se permite globalmente hardware de comunicación (PCMCIA de adaptador de Wi-Fi u otras tarjetas, y radios Wi-Fi integradas (consulte "Control inalámbrico" en la página 50), se pueden aplicar valores adicionales al adaptador en esta ubicación.

Para acceder a este control, haga clic en la pestaña *Ubicaciones* y haga clic en *Seguridad de Wi-Fi* en el árbol de directivas situado a la izquierda.

Nota: En la seguridad o gestión de Wi-Fi, la anulación de la selección de *Habilitar* inhabilita toda la conectividad Wi-Fi en esta ubicación.



El adaptador de Wi-Fi se puede ajustar para únicamente comunicarse con los puntos de acceso con un nivel específico de cifrado en una determinada ubicación.

Por ejemplo, si se implementara una configuración de WPA de los puntos de acceso en una sucursal, el adaptador se puede restringir a sólo comunicación con los puntos de acceso con un nivel de cifrado de WEP 128 o superior, evitando que se asociara accidentalmente con puntos de acceso no seguros o malévolos.

Se debe escribir un mensaje del usuario personalizado cuando el valor se coloque encima de *No es necesario el cifrado*.

Se puede definir una preferencia para conectarse con los puntos de acceso mediante pedido del nivel de cifrado o mediante intensidad de señal al especificar dos o más puntos de acceso en las listas de *puntos de acceso filtrados* y *gestionados*. El nivel seleccionado aplica la conectividad con los puntos de acceso que cumplan los requisitos de cifrado mínimos o superiores.

Por ejemplo, si WEP 64 es el requisito de cifrado y el cifrado es la preferencia, los puntos de acceso con la mayor intensidad de cifrado tendrán preferencia frente al resto. Si la preferencia reside en la intensidad de la señal, la señal más intensa tiene preferencia durante la conexión.

2.2.3 Reglas de solución·e integridad

ZENworks Endpoint Security Management ofrece la posibilidad de verificar que el software requerido se está ejecutando en el puesto final y ofrece procedimientos de recuperación instantánea si se produce un error en la verificación.

Las secciones siguientes contienen más información sobre:

- “Reglas de antivirus y programa espía” en la página 95
- “Pruebas de integridad” en la página 96

- “Comprobaciones de integridad” en la página 98
- “Reglas de guiones avanzados” en la página 99

Reglas de antivirus y programa espía

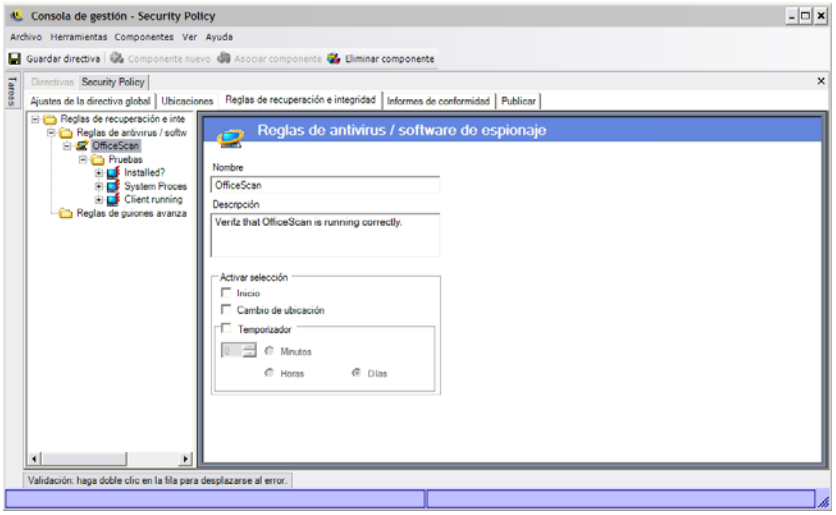
Las reglas de antivirus y programa espía verifican que el software de antivirus o programa espía designado del punto final se está ejecutando y se encuentra actualizado. Las pruebas se ejecutan para determinar si el software se está ejecutando y si la versión se encuentra actualizada. El éxito en ambas comprobaciones permite un intercambio entre las ubicaciones definidas. El fallo de cualquier prueba podría resultar en las siguientes acciones (definidas por el administrador):

- Se envía un informe al Servicio de informes.
- Aparece un mensaje del usuario personalizado, con un enlace de ejecución opcional que ofrece información acerca de cómo solucionar la violación de reglas.
- El usuario se cambia a un estado En cuarentena, que limita el acceso a la red por parte del usuario y no permite que algunos programas accedan a la red, lo que evita que el usuario infecte la red.

Una vez que se determina que los puestos finales·son compatibles mediante una prueba de seguimiento, los ajustes de seguridad volverán de forma automática a su estado original.

Nota: Esta función sólo está disponible en la instalación de ZENworks Endpoint Security Management y no puede utilizarse para directivas de seguridad UWS.

Para acceder a este control, haga clic en la pestaña *Reglas de solución e integridad*y haga clic en el icono *Reglas de antivirus/programa espía* del árbol de directivas de la izquierda.



Se pueden crear pruebas personalizadas para software que no se encuentra en la lista por defecto. Se puede crear una única prueba para ejecutar comprobaciones para una o más piezas de software de la misma regla. Cada conjunto de comprobaciones del archivo y proceso en ejecución cuenta con sus propios resultados de éxito o fallo.

Para crear una nueva regla de antivirus/programa espía:

1. Seleccione *Reglas de antivirus y programa espía* del árbol de componentes y haga clic en *Programa espía/antivirus nuevo*.
2. Haga clic en *Componente nuevo*.
3. Asigne un nombre a la regla e incluya una descripción.
4. Seleccione el activador para la regla:
   - **Inicio:** Ejecute pruebas en el inicio del sistema.
   - **Cambio de ubicación:** Ejecute las pruebas cada vez que ZENworks Security Client cambie a una nueva ubicación.
   - **Temporizador:** Ejecute pruebas de intensidad con un programa definido por minuto, hora o día.
5. Haga clic en *Guardar directiva*. Si su directiva contiene errores, consulte Sección 2.2.6, "Notificación de error", en la página 106.
6. Defina las pruebas de integridad.

Para asociar las reglas de antivirus o programa espía existentes:

1. Seleccione *Reglas de antivirus/programa espía* y haga clic en *Asociar componente*.
2. Seleccione las reglas que desee de la lista.
3. (Opcional) Redefina las pruebas, comprobaciones y los resultados.

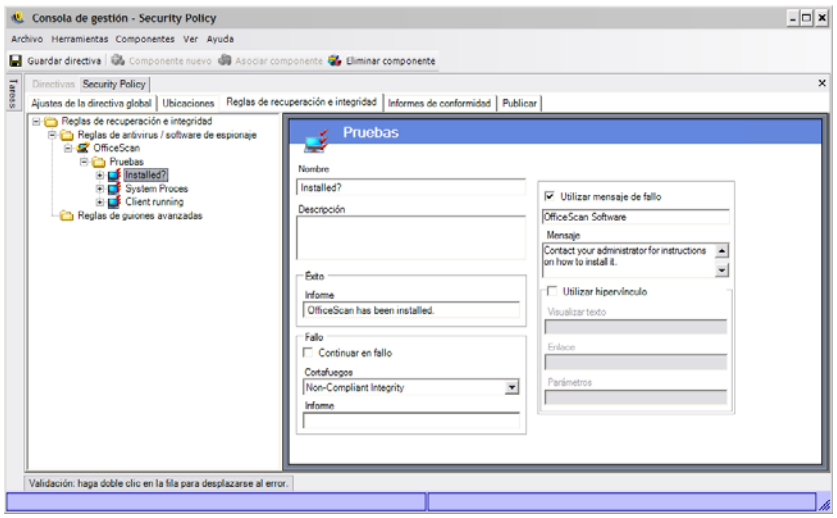
   Nota: Si cambia los ajustes en un componente compartido, esto afecta al resto de instancias del mismo componente. Utilice el comando *Mostrar uso* para ver el resto de directivas asociadas a este componente.

4. Haga clic en *Guardar directiva*. Si su directiva contiene errores, consulte Sección 2.2.6, "Notificación de error", en la página 106.

Se incluyen de forma automática comprobaciones y pruebas de integridad que pueden editarse, si es necesario.

Pruebas de integridad

Cada prueba de integridad puede ejecutar dos comprobaciones, *El archivo existe* y *Ejecución del proceso*. Cada prueba tiene sus propios resultados de éxito y fallo.



Todas las reglas de antivirus y programa espía definidas cuentan con comprobaciones y pruebas estándar escritas previamente. Se pueden agregar pruebas adicionales a la regla de integridad.

Se ejecutan varias pruebas según el orden que aparece aquí. La primera prueba debe completarse de forma correcta antes de que la próxima prueba se ejecute.

Para crear una prueba de integridad:

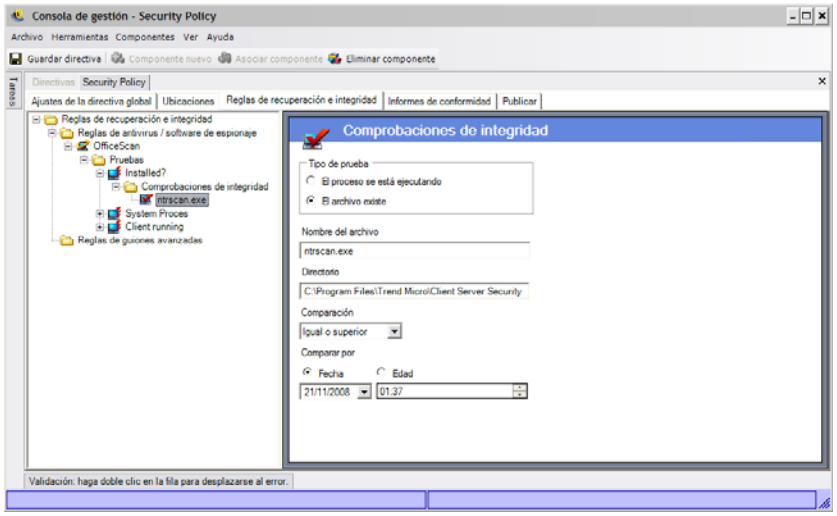
1. Seleccione *Pruebas de integridad* del árbol de componentes, haga clic en el signo + junto al informe deseado para expandir la lista, haga clic con el botón derecho en *Pruebas* y haga clic en *Añadir pruebas nuevas*.
2. Asigne un nombre a la prueba e incluya una descripción.
3. Especifique el texto de informe de éxito para la prueba.
4. Defina los siguientes pasos si se produce un fallo en la prueba:
   - **Continuar con el fallo:** Selecciónelo si el usuario puede continuar con la conectividad de red en el caso de que la prueba falle o si la prueba debe repetirse.
   - **Cortafuegos:** Este ajuste se aplica si la prueba falla. Todos cerrados, Integridad no compatible o ajustes del cortafuegos en cuarentena personalizados evitan que el usuario se conecte a la red.
   - **Mensaje:** Seleccione un mensaje del usuario personalizado para que se muestre en el fallo de la prueba. Puede incluir pasos de recuperación para el usuario final.
   - **Informe:** Proporcione el informe de errores que se envía al servicio de información.
5. Proporcione un mensaje de error. Este mensaje se visualiza sólo cuando una o más comprobaciones fallan. Haga clic en la casilla de verificación y especifique la información del mensaje que aparece en los recuadros proporcionados.
6. Se puede agregar un hiperenlace para proporcionar opciones de recuperación. Puede tratarse de un enlace para obtener más información o un enlace para descargar una revisión o actualizar el fallo de la prueba (consulte Sección , “Hiperenlaces”, en la página 69).
7. Haga clic en *Guardar directiva*. Si su directiva contiene errores, consulte Sección 2.2.6, “Notificación de error”, en la página 106.

8 Defina las comprobaciones de integridad.

9 Repita los pasos anteriores para crear una nueva prueba antivirus o programa espía, si lo desea.

Comprobaciones de integridad

Las comprobaciones de cada prueba determinan si uno o más de los procesos del antivirus/programa espía se ejecutan o si existen archivos esenciales. Al menos debe definirse una comprobación para la ejecución de una prueba de integridad.



Para crear una nueva comprobación, haga clic con el botón derecho en *Comprobaciones de integridad* del árbol de directivas de la izquierda y haga clic en *Agregar nuevas comprobaciones de integridad*. Seleccione uno de los dos tipos de comprobación e introduzca la información que se indica a continuación:

Se está ejecutando el proceso: Determine si el software se ejecuta en el momento del evento de activación (por ejemplo, el cliente AV). La única información necesaria para esta comprobación es el nombre ejecutable.

El archivo existe: Esta comprobación se utiliza para determinar si el software se encuentra actualizado en el momento en que se produjo el evento de activación.

Introduzca la siguiente información en los campos que aparecen:

- **Nombre de archivo:** Especifique el nombre de archivo que desee comprobar.
- **Directorio de archivos:** Especifique el directorio en el que reside el archivo.
- **Comparación de archivos:** Seleccione una comparación de fechas de la lista desplegable:
  - Ninguna
  - Igual

- Igual o superior
- Igual o inferior

- **Comparar por:** Especifique *Antigüedad* o *Fecha*.
  - La *Fecha* garantiza que el archivo no es más antiguo que la hora y fecha especificadas (por ejemplo, la fecha de la última actualización).
  - La *Edad* garantiza que un archivo no es más antiguo que un período de tiempo determinado, calculado en días.

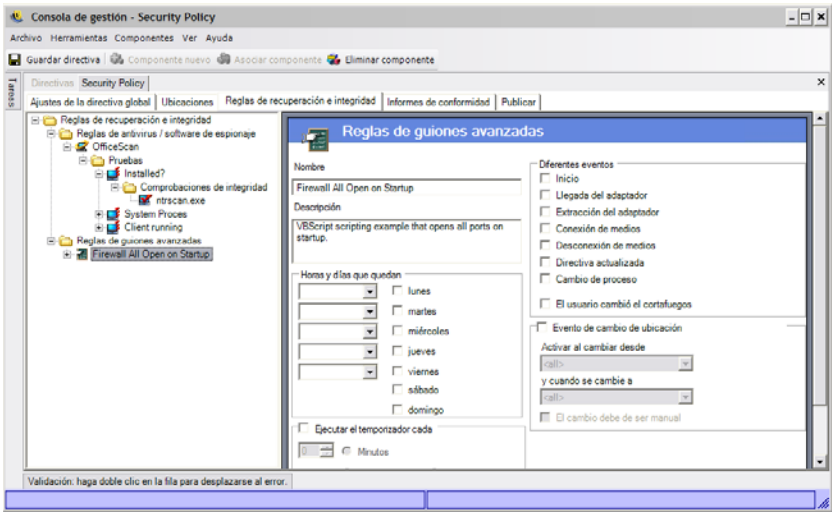
Nota: La comparación de archivos Igual se trata como Igual o Inferior al utilizar la comprobación *Antigüedad*.

Las comprobaciones se ejecutan en el orden en el que se han escrito.

Reglas de guiones avanzados

ZENworks Endpoint Security Management incluye una herramienta de elaboración de guiones de reglas avanzados que permite a los administradores crear reglas flexibles y complejas y acciones de recuperación.

Para acceder a este control, haga clic en la pestaña *Reglas de solución e integridad* y haga clic en el icono *Reglas de guiones avanzados* del árbol de directivas situado a la izquierda.



La herramienta para guiones utiliza los lenguajes para guiones comunes, VBScript o JScript, para crear reglas que incluyen un activador (para ejecutar la regla) y el guión real (la lógica de la regla). El administrador puede acceder al tipo de guión que desea ejecutar.

La creación de guiones avanzada se implementa de forma secuencial, junto con otras reglas de integridad. Por tanto, un guión de larga ejecución evita que se ejecuten otras reglas (incluidas las reglas de tiempo) hasta que el guión esté completo.

Para crear una nueva regla de guiones avanzados:

1. Haga clic con el botón derecho en *Reglas de guiones avanzados* del árbol de componentes y haga clic en *Añadir nuevas reglas de guiones*.
2. Asigne un nombre a la regla e incluya una descripción.

3 Especifique los eventos de activación

- **Horas y días de ejecución:** Especifique cinco veces distintas para que se ejecute el guión. El guión se ejecuta semanalmente, los días seleccionados.
- **Ejecución del temporizador cada:** Especifique la frecuencia con la que desea que se ejecute el temporizador.
- **Eventos varios:** Especifique los eventos del puesto final que activan el guión.
- **Evento de cambio de ubicación:** Especifique el evento de cambio de ubicación que activa el guión. Estos eventos no son independientes; son adicionales al evento anterior.
  - **Comprobar evento de ubicación:** El guión se ejecuta con todos los cambios de ubicación.
  - **Activar al cambiar de:** El guión sólo se ejecuta si el usuario deja esta ubicación (especificada) para cualquier otra ubicación.
  - **Activar al cambiar a:** El guión se ejecuta cuando el usuario introduce su ubicación especificada desde cualquier otra ubicación. Si a *Activar al cambiar de* se le ha asignado un parámetro de ubicación, por ejemplo, Oficina, el guión sólo se ejecuta cuando la ubicación cambia de la oficina a la ubicación especificada).
  - **Debe ser un cambio manual:** El guión sólo se ejecuta si el usuario cambia a o desde una ubicación manualmente.

4 Cree variables de guión. Para obtener más información, consulte "Variables de guión" en la página 100.

5 Escriba el texto de guión. Para obtener más información, consulte la "Texto de guión" en la página 101.

6 Haga clic en *Guardar directiva*. Si su directiva contiene errores, consulte Sección 2.2.6, "Notificación de error", en la página 106.

Para asociar una regla de guiones avanzados existente:

1 Seleccione *Reglas de guiones avanzados* del árbol de componentes y haga clic en *Asociar nueva*,

2 Seleccione las reglas deseadas de la lista.

3 Vuelva a definir el evento del activador, variables o guión, según convenga.

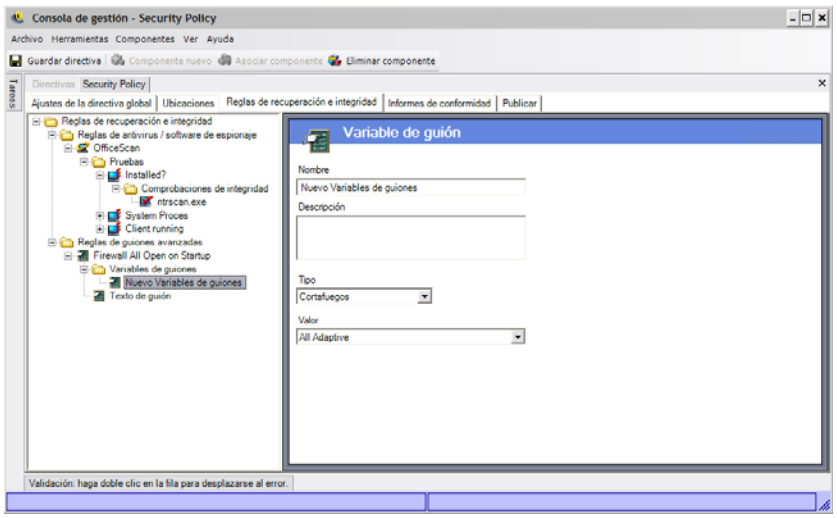
Nota: Si cambia los ajustes en un componente compartido, esto afecta al resto de instancias del mismo componente. Utilice el comando *Mostrar uso* para ver el resto de directivas asociadas a este componente.

---

4 Haga clic en *Guardar directiva*. Si su directiva contiene errores, consulte Sección 2.2.6, "Notificación de error", en la página 106.

Variables de guión

Se trata de un ajuste opcional que permite al administrador definir una variable (var) para el guión y utilizar la funcionalidad ZENworks Endpoint Security Management (por ejemplo, lanzar mensajes del usuario personalizados o hiperenlaces personalizados definidos; cambiar a una ubicación definida o ajustes del cortafuegos) o tener la libertad de cambiar el valor de una variable sin cambiar el propio guión.



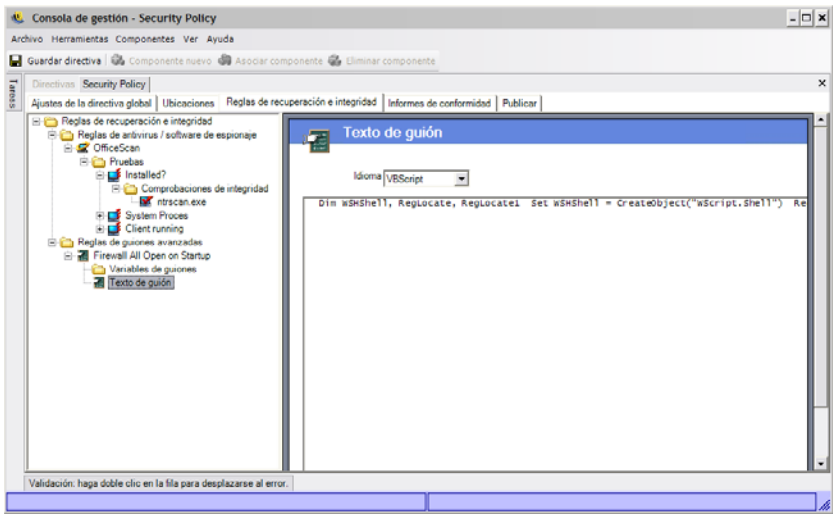
Para crear una nueva variable de guiones:

1. Haga clic con el botón derecho en *Variables de guión* del árbol de componentes y haga clic en *Añadir variables nuevas*.
2. Asigne un nombre a la variable e incluya una descripción.
3. Seleccione el tipo de variable:
   - **Mensajes del usuario personalizados:** Define un mensaje de usuario personalizado que puede lanzarse como una acción.
   - **Cortafuegos:** Define los ajustes del cortafuegos que pueden aplicarse como una acción.
   - **Hiperenlaces:** Define un hiperenlace que puede lanzarse como una acción.
   - **Ubicación:** Define una ubicación que puede aplicarse como una acción.
   - **Número:** Define un valor de número.
   - **Cadena:** Define un valor de cadena.
4. Especifique el valor de la variable:
   - Todos adaptables
   - Todos cerrados
   - Todos abiertos
   - Ajustes del cortafuegos nuevos
   - Integridad no compatible
5. Haga clic en *Guardar directiva*. Si su directiva contiene errores, consulte Sección 2.2.6, “Notificación de error”, en la página 106.

Texto de guión

El administrador de ZENworks Endpoint Security Management no está limitado al tipo de guión que ZENworks Security Client puede ejecutar. Los guiones se deben probar antes de distribuir la directiva.

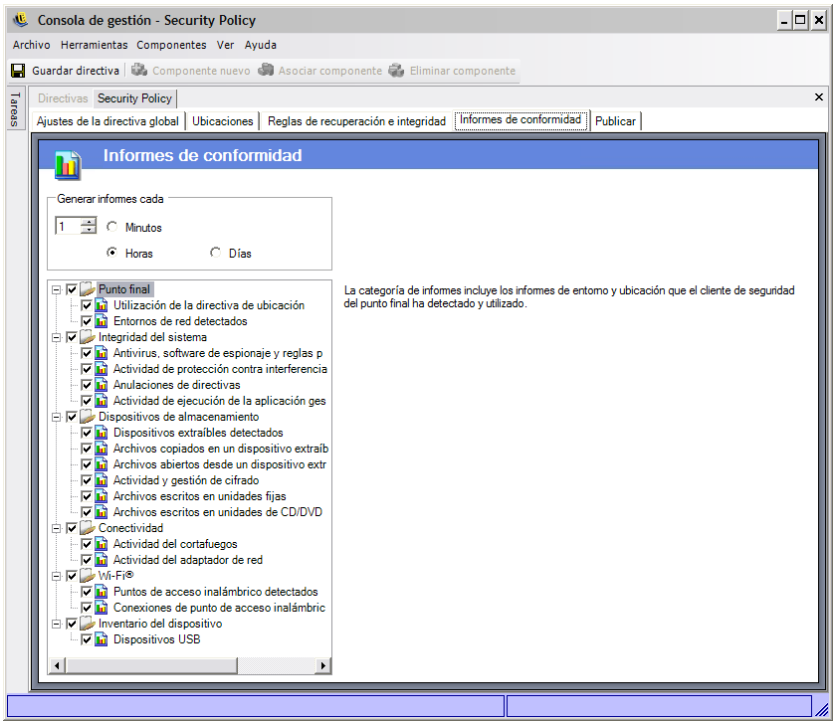
Seleccione el tipo de guión (Jscript o VBscript) e introduzca el texto de guión en el campo. El guión puede copiarse de otra fuente y pegarse en el campo.



2.2.4 Información de cumplimiento

Debido al nivel y acceso de los controladores de ZENworks Security Client, prácticamente se puede informar de cada transacción que el punto final realiza. El punto final puede ejecutar cada inventario de sistema opcional para solucionar problemas y crear directivas. Para acceder a estos informes, haga clic en la pestaña *Información de cumplimiento*.

Nota: La información no está disponible al ejecutar la Consola de gestión independiente.



Para ejecutar la información de cumplimiento de esta directiva:

1. Especifique la frecuencia con la que desea generar informes. Esto es la frecuencia con la que los datos se cargarán desde ZENworks Security Client a Policy Distribution Service.
2. Compruebe cada categoría de informes o escriba la que desee capturar.

Están disponibles los siguientes informes:

Puesto final

- **Uso de directivas de ubicación:** ZENworks Security Client informa de todas las directivas de ubicación aplicadas y la duración de esa ejecución.
- **Entornos de red detectados:** ZENworks Security Client informa de todos los ajustes de entorno de red detectados.

Integridad de sistema

- **Reglas personalizadas, antivirus, programa espía:** ZENworks Security Client informa de todos los mensajes de integridad configurados basados en resultados de pruebas.
- **Actividad de protección de manipulación del extremo:** ZENworks Security Client informa de todos los intentos de alterar el cliente de seguridad.
- **Redefinición de directivas:** ZENworks Security Client informa de todos los intentos de iniciar la redefinición administrativa en el cliente de seguridad.
- **Actividad de ejecución de aplicaciones gestionadas:** ZENworks Security Client informa de todas las actividades de ejecución para aplicaciones gestionadas.

Dispositivos de almacenamiento

- **Dispositivos extraíbles detectados:** ZENworks Security Client informa a todos los dispositivos de almacenamiento extraíbles detectados por el cliente de seguridad.
- **Archivos copiados a un dispositivo extraíble:** ZENworks Security Client informa de archivos que se copian a un dispositivo de almacenamiento extraíble.
- **Archivos abiertos desde un dispositivo extraíble:** ZENworks Security Client informa de archivos que se abren desde un dispositivo de almacenamiento extraíble.
- **Actividad y gestión de cifrado:** ZENworks Security Client informa de la actividad de cifrado/descifrado mediante ZENworks Storage Encryption Solution.
- **Archivos escritos en las unidades fijas:** ZENworks Security Client informa del número de archivos que se han escrito en las unidades fijas del sistema.
- **Archivos escritos en las unidades de CD/DVD:** ZENworks Security Client informa del número de archivos escritos en las unidades de CD/DVD del sistema.

Redes

- **Actividad de cortafuegos:** ZENworks Security Client informa de todo el tráfico bloqueado a través del cortafuegos configurado para la directiva de ubicación aplicada.

  Importante: Si habilita este informe, puede provocar la recopilación de grandes volúmenes de datos. Los datos pueden saturar una base de datos muy rápidamente. Una prueba de ZENworks Security Client informó de 1.115 cargas de datos de paquetes bloqueados durante un período de 20 horas. Debe ejecutar un período de sintonización y supervisión con un cliente de prueba en el entorno afectado antes de la implementación a gran escala.

- **Actividad de adaptador de red:** ZENworks Security Client informa de toda la actividad de tráfico para un dispositivo de red gestionado.

Wi-Fi

- **Puntos de acceso inalámbricos detectados:** ZENworks Security Client informa de todos los puntos de acceso detectados.
- **Conexiones de punto de acceso inalámbrico:** ZENworks Security Client informa de todas las conexiones de punto de acceso realizadas por el punto final.

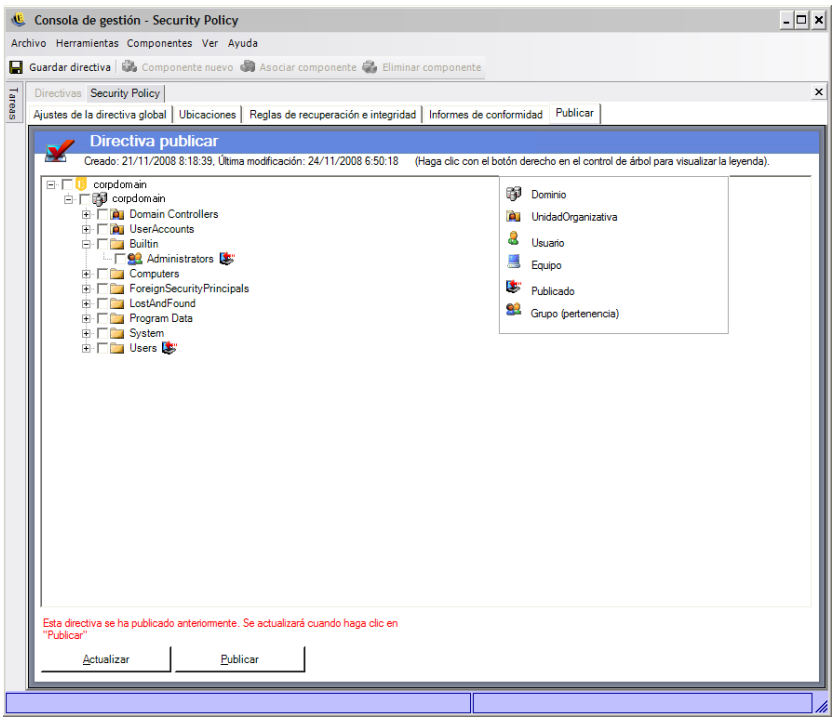
Inventario de dispositivo

- **Dispositivos USB:** ZENworks Security Client informa de todos los dispositivos USB detectados en el sistema.

2.2.5 Publican

Las directivas de seguridad terminadas se envían a los usuarios a través del mecanismo de publicación. Una vez que se ha publicado una directiva, puede actualizarse con los usuarios recibiendo actualizaciones en sus controles de entrada programados. Para publicar una directiva, haga clic en la pestaña *Publicar*. Se muestra la siguiente información:

- El árbol de directorios actuales
- Las fechas de creación y modificación de la directiva
- Los botones *Actualizar* y *Publicar*



Basándose en los permisos de publicación del usuario actual, el árbol de directorios puede mostrar una o más selecciones en color rojo. Los usuarios no pueden publicar en los usuarios/grupos que aparecen en rojo.

Los usuarios y sus grupos asociados no se visualizan hasta que se hayan autenticado en el Management Service. Es posible que los cambios en el servicio de directorios corporativos no se muestren inmediatamente en la consola de gestión. Haga clic en *Actualizar* para renovar el árbol de directorios para el Management Service.

Las secciones siguientes contienen más información sobre:

- “Publicación de una directiva” en la página 105
- “Actualización de una directiva publicada” en la página 106

Publicación de una directiva

1. Seleccione un grupo de usuarios (o usuarios individuales) en el árbol de directorios de la izquierda. Haga doble clic en los usuarios para seleccionarlos (si se ha seleccionado un grupo de usuarios, se incluirán a todos los usuarios).

   Los usuarios que no han recibido la directiva contarán con el icono junto a sus nombres. Si un usuario o grupo ya ha recibido la directiva, las entradas contarán con el icono junto a sus nombres en el árbol de directorios.

   Para eliminar la selección de un usuario o grupo, haga doble clic para eliminar el icono
2. Haga clic en *Publicar* para enviar la directiva a Policy Distribution Service.

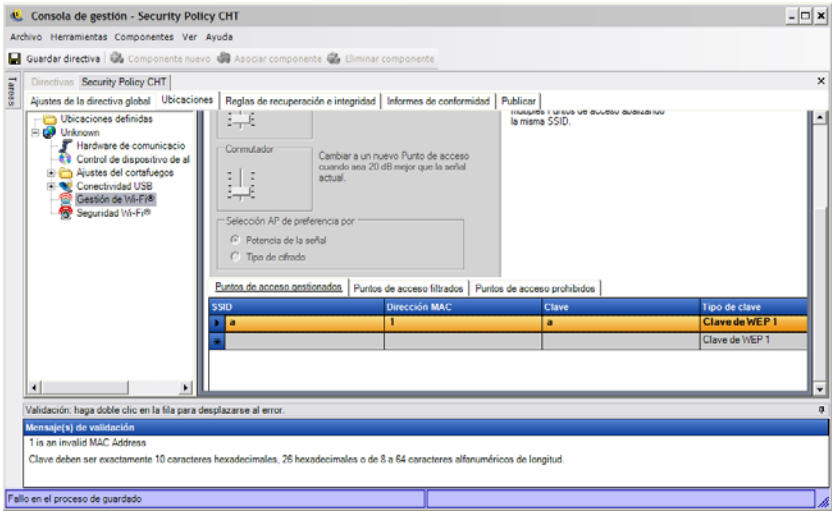
Actualización de una directiva publicada

Una vez que se haya publicado una directiva para los usuarios, se pueden mantener actualizaciones sencillas editando los componentes en una directiva y volviendo a publicarlas. Por ejemplo, si el administrador de ZENworks Endpoint Security Management necesita cambiar la clave WEP para un punto de acceso, el administrador sólo debe editar la clave, guardar la directiva y hacer clic en *Publicar*. Los usuarios afectados reciben la directiva actualizada (y la nueva clave) en su próximo control de entrada.

2.2.6 Notificación de error

Cuando el administrador intenta guardar una directiva con datos incompletos o incorrectos en un componente, aparece el panel de validación en la parte inferior de la consola de gestión, resaltando cada error. Cada error se debe corregir antes de guardar la directiva.

Haga doble clic en cada fila de validaciones para navegar hasta la pantalla con el error. Los errores se resaltan tal y como se muestra en la siguiente imagen.

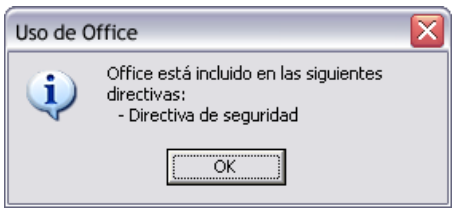


2.2.7 Mostrar uso

Los cambios realizados en los componentes de la directiva compartida afectan a todas las directivas con las que estén asociados. Antes de actualizar o de cambiar un componente de la directiva, se recomienda que ejecute el comando *Mostrar uso* para determinar las directivas afectadas por el cambio.

1 Haga clic con el botón derecho en el componente y, a continuación, haga clic en *Mostrar uso*.

Aparece una ventana emergente, mostrando cada ejemplo de este componente en otras directivas.



2.3 Importación y exportación de directivas

Las secciones siguientes contienen más información sobre:

- Sección 2.3.1, “Importación de directivas”, en la página 107
- Sección 2.3.2, “Exportación de una directiva”, en la página 107
- Sección 2.3.3, “Exportación de directivas a usuarios no gestionados”, en la página 107

2.3.1 Importación de directivas

Se puede importar una directiva desde cualquier ubicación de archivo de la red disponible.

1. En la Consola de gestión, haga clic en *Archivo* > *Importar directiva*.

   Si está editando o realizando un borrador de una directiva, el editor cierra la directiva (pidiéndoles que la guarde) antes de abrir la ventana Importar.
2. Examine para especificar la ubicación del archivo y especifique el nombre de archivo en el campo.

Una vez que se importe la directiva, puede editarse o publicarse de forma inmediata.

2.3.2 Exportación de una directiva

Las directivas se pueden exportar desde la Consola de gestión y distribuirse mediante correo electrónico o a través de un recurso de red compartido. Se puede utilizar para distribuir directivas a nivel empresarial en entornos en los que se implantan varios Editores de directivas y el Servicio de gestión.

Para exportar una directiva de seguridad:

1. En la consola de gestión, haga clic en *Archivo* > *Exportar*.
2. Especifique un destino y asigne un nombre de la directiva con una extensión de `.sen` (por ejemplo, `C:\Desktop\salespolicy.sen`) Puede hacer clic en el botón Examinar para navegar hasta una ubicación.
3. Haga clic en *Exportar*.

Se exportan dos archivos. El primero, es la directiva (`*.sen`). El segundo es el archivo `setup.sen`, necesario para descifrar la directiva en la importación.

Las directivas exportadas deben importarse en una Consola de gestión antes de que puedan publicarse para usuarios gestionados.

2.3.3 Exportación de directivas a usuarios no gestionados

Si los ZENworks Security Clients se han implementado en la empresa, deberá instalarse una Consola de gestión independiente para crear directivas. Consulte la “Guía de instalación de ZENworks Endpoint Security Management” para obtener más información.

Para distribuir las directivas sin gestionar:

1. Busque el archivo `setup.sen` de la consola de gestión y cópielo en una carpeta distinta.

El archivo `setup.sen` se genera durante la instalación de la Consola de gestión y se encuentra ubicado en el directorio `\Archivos de programa\Novell\ESM Management Console`.

2. Cree una directiva en la Consola de gestión. Para obtener más información, consulte la Sección 2.2, “Creación de directivas de seguridad”, en la página 47.
3. Utilice el comando *Exportar* para exportar la directiva a la misma carpeta que incluye el archivo `setup.sen`.

   Todas las directivas distribuidas deben tener un nombre `policy.sen` para que ZENworks Security Client las acepte.
4. Distribuya los archivos `policy.sen` y `setup.sen`. Estos archivos se deben copiar en el directorio `\Archivos de programa\Novell\ZENworks Security Client\` para todos los clientes no gestionados.

El archivo `setup.sen` se debe copiar a los ZENworks Security Clients sólo una vez con la primera directiva. Posteriormente, sólo deben distribuirse las nuevas directivas.