AUTHORIZED DOCUMENTATION

Guía de usuario de Endpoint Security Client 3.5

December 22, 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

Acerca de esta guía 7

1 Introducción 9

1.1 Refuerzo de la seguridad para equipos móviles 9
1.2 Nivel de protección del cortafuegos de NDIS 10

2 Descripción general de Endpoint Security Client 3.5 11

2.1 Terminología de ESM 11
2.2 Registro en Endpoint Security Client 3.5 13

3 Uso de Endpoint Security Client 3.5 15

3.1 Desplazamiento por los entornos de red 15
3.2 Cambiar ubicaciones 16
3.2.1 Guardar un entorno de red 16
3.2.2 Guardar un entorno Wi-Fi 17
3.2.3 Eliminación de un entorno guardado 18
3.3 Cambiar los ajustes del cortafuegos 18
3.4 Cifrado de los datos 19
3.4.1 Gestionar archivos en discos fijos 19
3.4.2 Gestionar archivos en el almacenamiento externo 19
3.5 Actualización de directivas 22
3.6 Visualización de la ayuda 23
3.7 Anulación de una contraseña 23
3.8 Diagnóstico 24

Acerca de esta guía

Esta *Guía de usuario de Novell® ZENworks® Endpoint Security Client 3.5* está orientada a proporcionar al usuario final directrices sobre el funcionamiento de Endpoint Security Client 3.5 para Windows* XP* y Windows 2000*.

La información incluida en la guía está organizada del modo siguiente:

- Capítulo 1, “Introducción”, en la página 9
- Capítulo 2, “Descripción general de Endpoint Security Client 3.5”, en la página 11
- Capítulo 3, “Uso de Endpoint Security Client 3.5”, en la página 15

Usuarios a los que va dirigida

Esta guía se puede distribuir a todos los empleados de la empresa para enseñarles a utilizar Endpoint Security Client 3.5.

Comentarios

Nos gustaría recibir sus comentarios y sugerencias acerca de este manual y del resto de la documentación incluida con este producto. Utilice la función de comentarios del usuario que se incluye en la parte inferior de cada página de la documentación en línea, o bien acceda al sitio Web de comentarios sobre la documentación de Novell (http://www.novell.com/documentation/feedback.html) e introduzca allí sus comentarios.

Documentación adicional

Existen otros documentos (en los formatos PDF y HTML) sobre ZENworks Endpoint Security Management que pueden utilizarze para obtener información e implementar el producto. Para obtener más información, consulte el sitio Web de documentación de ZENworks Endpoint Security Management 3.5 (http://www.novell.com/documentation/zesm35).

Convenciones de la documentación

En la documentación de Novell, los símbolos mayor que (>) se utilizan para separar acciones dentro de un paso y elementos en una ruta de referencia cruzada.

Un símbolo de marca comercial (®, ™, etc.) indica una marca comercial de Novell. Un asterisco (*) sirve para identificar una marca comercial de otro fabricante.

Cuando un nombre de vía de acceso se pueda escribir con una barra invertida para algunas plataformas y una barra normal para otras plataformas, el nombre de la vía de acceso aparecerá con una barra invertida. Los usuarios de plataformas que requieran una barra inclinada, como Linux*, deben usar estas barras, propias de dicho software.

Introducción

1

El sistema ZENworks® Endpoint Security Management (ESM) de Novell® está diseñado para proteger los activos de los datos corporativos a través de una herramienta de gestión centralizada llamada Endpoint Security Client. Endpoint Security Client 3.5 se instala en los equipos Windows XP y Windows 2000 de la empresa y refuerza las directivas de seguridad escritas y enviadas a través del sistema de distribución y gestión ESM. Esto permite que las empresas grandes y pequeñas creen, implanten, apliquen y controlen las directivas de seguridad de aquellos equipos que estén dentro y fuera del perímetro de seguridad corporativa.

Para equipos con Windows Vista y Windows 2008, consulte la *Guía de usuario de ZENworks Endpoint Security Client 4.0*.

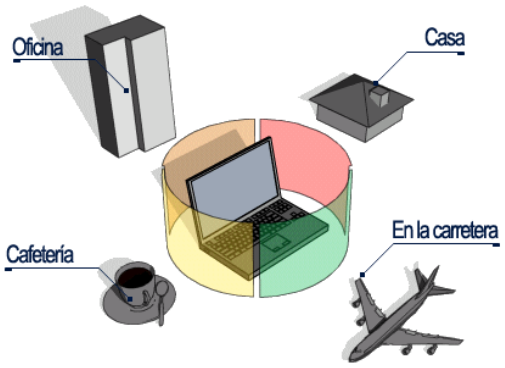
Las secciones siguientes contienen más información:

- Sección 1.1, “Refuerzo de la seguridad para equipos móviles”, en la página 9
- Sección 1.2, “Nivel de protección del cortafuegos de NDIS”, en la página 10

1.1 Refuerzo de la seguridad para equipos móviles

La seguridad se refuerza tanto a nivel general como por la ubicación de la red. Cada ubicación de la lista de directivas de seguridad determina los permisos del usuario para ese entorno de red y los ajustes activados del cortafuegos. Los ajustes del cortafuegos determinan los puertos, direcciones y aplicaciones de red que autorizan el acceso a la red, así como el modo de acceso permitido.

Figura 1-1 *ESM ajusta los valores de seguridad basados en el entorno de red detectado*

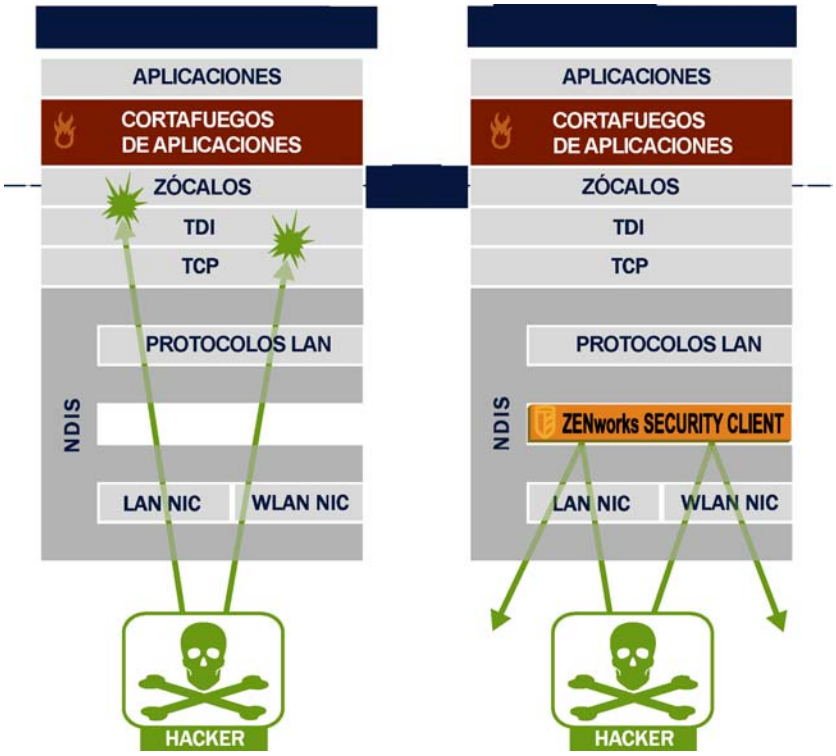


Las operaciones normales que Endpoint Security Client 3.5 lleva a cabo son transparentes para el usuario una vez que se haya definido el entorno de red. A veces, las medidas de protección de Endpoint Security Client 3.5 pueden interrumpir el funcionamiento normal. Cuando esto ocurre, aparecen mensajes e hiperenlaces para informar al usuario acerca de la directiva de seguridad y de los pasos de protección que se han seguido y, además, le proporcionan información adicional a fin de ayudarle a solucionar el problema.

1.2 Nivel de protección del cortafuegos de NDIS

En los dispositivos móviles de seguridad, ESM es superior a las típicas tecnologías personales de cortafuegos, que funcionan sólo a nivel de aplicación o como dispositivos de gancho de cortafuegos. La seguridad de los clientes ESM se integra en el controlador NDIS (Network Driver Interface Specification, Especificación de la Interfaz del controlador de Red) de las tarjetas de interfaz de red (NIC), lo que protege al tráfico desde el momento en que entra en el equipo. Las diferencias entre ESM y los cortafuegos del nivel de aplicación y los controladores de filtro se ilustran en Figura 1-2, “Eficacia del cortafuegos de un nivel de NDIS”, en la página 10.

Figura 1-2 *Eficacia del cortafuegos de un nivel de NDIS*



Tanto las decisiones de seguridad como el rendimiento del sistema se optimizan cuando las implementaciones de seguridad operan al nivel más bajo y adecuado de la pila de protocolos. Con la herramienta Endpoint Security Client 3.5, el tráfico no solicitado desciende a los niveles más bajos de la pila del dispositivo de NDIS mediante la tecnología de bloqueo de puertos adaptados (inspección del estado del paquete). Este método protege contra los ataques basados en el protocolo, entre los que se incluyen las exploraciones no autorizadas del puerto y los ataques de desbordamiento de SYN, entre otros.

Es recomendable que siga todas las instrucciones sobre operación y mantenimiento de este documento para garantizar la protección del entorno de seguridad de puesto final.

Descripción general de Endpoint Security Client 3.5

2

ZENworks® Security Client protege los equipos de ataques de invasiones a datos en casa, en la oficina y mientras viaja gracias a la aplicación de directivas de seguridad creadas por el administrador de Endpoint Security Management (ESM) de la empresa. Los ajustes del cortafuegos asignados a ubicaciones individuales se ajustan automáticamente cuando los usuarios del portátil cambian de la red corporativa a las personales, o cuando viajan y se conectan a una red pública o abierta.

Los niveles de seguridad se aplican a las diversas ubicaciones de usuario sin necesidad de tener conocimientos sobre la seguridad de la red, las configuraciones del puerto, los archivos compartidos ocultos y otra información técnica. Se puede acceder de forma inmediata a la información sobre la ubicación de Endpoint Security Client 3.5, sobre cuál es la configuración del cortafuegos y sobre qué adaptadores están actualmente activos o disponibles pasando el ratón sobre el icono de la barra de tareas para ver la información relacionada con las herramientas de Endpoint Security Client (consulte Figura 2-1).

Figura 2-1 *Información sobre herramientas de Endpoint Security Client*

Las secciones siguientes contienen más información:

- Sección 2.1, “Terminología de ESM”, en la página 11
- Sección 2.2, “Registro en Endpoint Security Client 3.5”, en la página 13

2.1 Terminología de ESM

Los siguientes términos se usan frecuentemente en esta documentación:

Ubicaciones: Las ubicaciones son simples definiciones que pueden ayudar a los usuarios a identificar el entorno de red en el que se encuentran, proporcionan ajustes de seguridad inmediatos (definidos por el administrador) y pueden permitir que el usuario guarde el entorno de red y cambie los ajustes aplicados del cortafuegos.

Cada ubicación tiene ajustes de seguridad exclusivos, que deniegan el acceso a algunas funciones de red y hardware en entornos de red más adversos y que permiten un acceso más amplio dentro de los entornos de confianza. Las ubicaciones definen la siguiente información:

- Frecuencia con la que Endpoint Security Client 3.5 comprueba si hay una actualización de directivas en esta ubicación
- Los permisos de administración de la ubicación otorgados al usuario
- Los ajustes del cortafuegos que se utilizarán en esta ubicación

- El hardware de comunicación que puede conectarse
- Cómo se maneja la conectividad Wi-Fi y la seguridad en esta ubicación
- A qué nivel se le permite al usuario utilizar dispositivos de almacenamiento extraíbles (como dispositivos en miniatura y tarjetas de memoria) y unidades de CD/DVD-RW
- Cualquier entorno de red que pueda ayudar a definir la ubicación

Ajustes del cortafuegos: Los ajustes del cortafuegos controlan la conectividad de todos los puertos de red (1-65535), paquetes de redes (ICMP, ARP, etc.), direcciones de red (IP o MAC) y las aplicaciones de red (archivos compartidos, software de mensajería instantánea, etc.) que están permitidos para conseguir una conexión de red al aplicar la configuración. Se incluyen tres ajustes del cortafuegos por defecto para ESM y puede que estén implementados en una ubicación. El administrador de ESM también puede crear ajustes específicos de cortafuegos, que no se pueden enumerar aquí.

- **Todo adaptado:** Esta configuración del cortafuegos establece todos los puertos de red como "con estado" (se bloquea todo el tráfico de red entrante no solicitado y se permite todo el tráfico de red saliente). Se permiten los paquetes ARP y 802.1x y todas las aplicaciones de red pueden establecer una conexión de red.
- **Todos abiertos:** Esta configuración del cortafuegos establece todos los puertos de red como abiertos (está permitido todo el tráfico de red) y todos los tipos de paquetes están permitidos. Todas las aplicaciones de red están permitidas como conexiones de red.
- **Todos cerrados:** Esta configuración del cortafuegos cierra todos los puertos de red y restringe todos los tipos de paquetes.

Adaptadores: Remite a tres adaptadores de comunicación que normalmente se encuentran en un puesto final:

- adaptadores con cable (conexiones LAN) y
- adaptadores Wi-Fi (tarjetas Wi-Fi y radios Wi-Fi incluidas de acuerdo con la PCMCIA).
- Adaptadores de conexión de acceso telefónico (módems internos y externos)

También remite a otro hardware de comunicación que se puede incluir en un equipo, como infrarrojos, Bluetooth*, Firewire *, y puertos paralelos y de serie.

Dispositivos de almacenamiento: remiten a dispositivos externos de almacenamiento que pueden resultar una amenaza para la seguridad cuando se copian datos desde, o se añaden a, estos dispositivos en un puesto final. Las "memorias" USB, las tarjetas de memoria Flash y PCMCIA SCSI, junto con las unidades Zip*, de disquete, externas de CDR y las de CD/DVD instaladas (incluyendo CD-ROM, CD-R/RW, DVD y DVD R/RW) se pueden bloquear, permitir o procesar como sólo lectura en una sola ubicación.

Entornos de red: Un entorno de red es la colección de servicios de red y direcciones de servicios que se necesitan para identificar una ubicación de red (consulte Sección 3.2.1, “Guardar un entorno de red”, en la página 16).

2.2 Registro en Endpoint Security Client 3.5

Si usted es miembro del dominio corporativo, Endpoint Security Client 3.5 utilizará su nombre de usuario y contraseña de Windows* para iniciarle en el servicio de distribución de la directiva (no se visualizará ninguna ventana emergente). Si usted es miembro del dominio en cuyo host se encuentra el servicio de distribución de directivas, Endpoint Security Client 3.5 le solicitará su nombre de usuario y contraseña para dicho dominio (consulte Figura 2-2).

Figura 2-2 *Entrada a Endpoint Security Client 3.5*

Introduzca su nombre de usuario y contraseña del dominio, y haga clic en *Aceptar*.

Nota: No es necesario que entre a Endpoint Security Client 3.5 cuando éste se esté ejecutando como "No gestionado". El administrador de ESM tiene un método distinto para proporcionar directivas a los usuarios no gestionados.

Uso de Endpoint Security Client 3.5

3

Las siguientes secciones contienen información adicional sobre las acciones que puede realizar con la aplicación de usuario final Novell® ZENworks® Endpoint Security, Endpoint Security Client 3.5:

- Sección 3.1, “Desplazamiento por los entornos de red”, en la página 15
- Sección 3.2, “Cambiar ubicaciones”, en la página 16
- Sección 3.3, “Cambiar los ajustes del cortafuegos”, en la página 18
- Sección 3.4, “Cifrado de los datos”, en la página 19
- Sección 3.5, “Actualización de directivas”, en la página 22
- Sección 3.6, “Visualización de la ayuda”, en la página 23
- Sección 3.7, “Anulación de una contraseña”, en la página 23
- Sección 3.8, “Diagnóstico”, en la página 24

Nota: El administrador puede restringir las acciones que se especifican a continuación en cualquier ubicación.

3.1 Desplazamiento por los entornos de red

Cada red a la que se desplaza el usuario final puede necesitar diferentes medidas de seguridad. Endpoint Security Client 3.5 proporciona seguridad y protección en ubicaciones que identifican las conexiones de redes disponibles. Endpoint Security Client 3.5 detecta los parámetros del entorno de red y conmuta a la ubicación oportuna mediante la aplicación de los niveles de protección necesarios en función de la directiva actual de seguridad.

La información del entorno de red está bien almacenada o preseleccionada dentro de una ubicación. Esto permite que Endpoint Security Client 3.5 conmute a una ubicación automáticamente cuando se detectan los parámetros del entorno.

- **Entornos de almacenamiento:** definido por el usuario (consulte Sección 3.2.1, “Guardar un entorno de red”, en la página 16).
- **Preseleccionar un entorno:** definido por el administrador de ESM de la empresa a través de una directiva de seguridad publicada.

Cuando el usuario introduce un nuevo entorno de red, el cliente compara el entorno de red detectado con cualquier valor almacenado y preseleccionado en la directiva de seguridad. Si se encuentra un emparejamiento, Endpoint Security Client 3.5 activa la ubicación asignada. Cuando el entorno detectado no se puede identificar como almacenado o preseleccionado, el cliente activa la ubicación desconocida por defecto.

La ubicación desconocida contiene las siguientes preselecciones:

- Cambiar ubicaciones: permitido
- Cambiar ajustes del cortafuegos: no permitido

- Guardar ubicación: no permitido
- Actualizar directiva: permitido
- Ajustes de cortafuegos por defecto: todos adaptados

Los tres tipos de adaptadores (wi-fi, alámbrico y de marcación) están permitidos en la ubicación desconocida. Esto permite que el equipo interfiera de forma periférica en su entorno de red e intente asociar una directiva de ubicación como se ha descrito anteriormente.

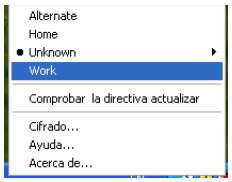
3.2 Cambiar ubicaciones

Al iniciar, Endpoint Security Client 3.5 conmuta a la ubicación desconocida. A continuación, intenta detectar el entorno de red actual y cambiar automáticamente la ubicación. Si no se reconoce el entorno de red o no se ha preseleccionado ni guardado (consulte Sección 3.2.1, “Guardar un entorno de red”, en la página 16), la ubicación debe cambiarse manualmente.

Si no puede realizar los siguientes pasos, es posible que el administrador de ZENworks Endpoint Security no le permita cambiar las ubicaciones manualmente.

Para cambiar una ubicación:

1. Haga clic con el botón derecho en el icono *Endpoint Security Client* de la barra de tareas para mostrar el menú de opciones.



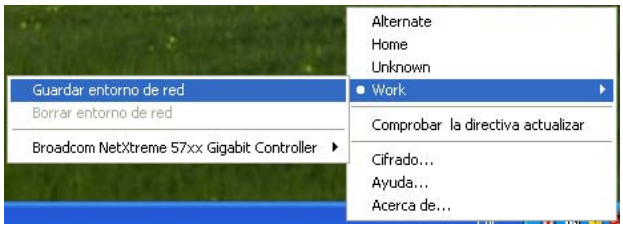
2. Haga clic en la ubicación adecuada.

3.2.1 Guardar un entorno de red

Es necesario que un entorno de red se encuentre preseleccionado en la directiva de seguridad o que el usuario final lo haya almacenado antes de que Endpoint Security Client 3.5 pueda cambiar las ubicaciones automáticamente. Al guardar un entorno de red, se graban los parámetros de dicha red para la ubicación actual y se permite que Endpoint Security Client 3.5 conmute automáticamente a esa ubicación la próxima vez que el usuario acceda al entorno de red. Al aplicarse en un entorno de red Wi-Fi, Endpoint Security Client 3.5 se conectará (LockOn™) al único punto de acceso seleccionado.

Para guardar un entorno:

1. Haga clic con el botón derecho en el icono *Endpoint Security Client* de la barra de tareas para visualizar el menú.
2. Haga clic en la ubicación a la que desea cambiarse.
3. Haga clic con el botón derecho en el icono *Endpoint Security Client*, pase el ratón por la ubicación actual para visualizar el submenú y, a continuación, haga clic en "Guardar entorno de red" para guardar el entorno.



Si este entorno de red ya se había guardado en una ubicación anterior, Endpoint Security Client 3.5 preguntará al usuario si desea guardar la nueva ubicación. Seleccione *Sí* para guardar el entorno en la ubicación actual y borrarlo de su anterior ubicación, o *No* para dejar el entorno en la ubicación anterior.

Nota: La función *Guardar entorno de red* puede verse restringida por el administrador de ESM en cualquier ubicación.

Los entornos de red adicionales pueden guardarse en una ubicación posteriormente. Por ejemplo, si una ubicación definida como Aeropuerto forma parte de la directiva actual, cada aeropuerto que el usuario visite se puede guardar como un entorno de red para esta ubicación. De este modo, cada vez que un usuario vuelve a un entorno de aeropuerto guardado, Endpoint Security Client 3.5 conmuta automáticamente a la ubicación Aeropuerto.

3.2.2 Guardar un entorno Wi-Fi

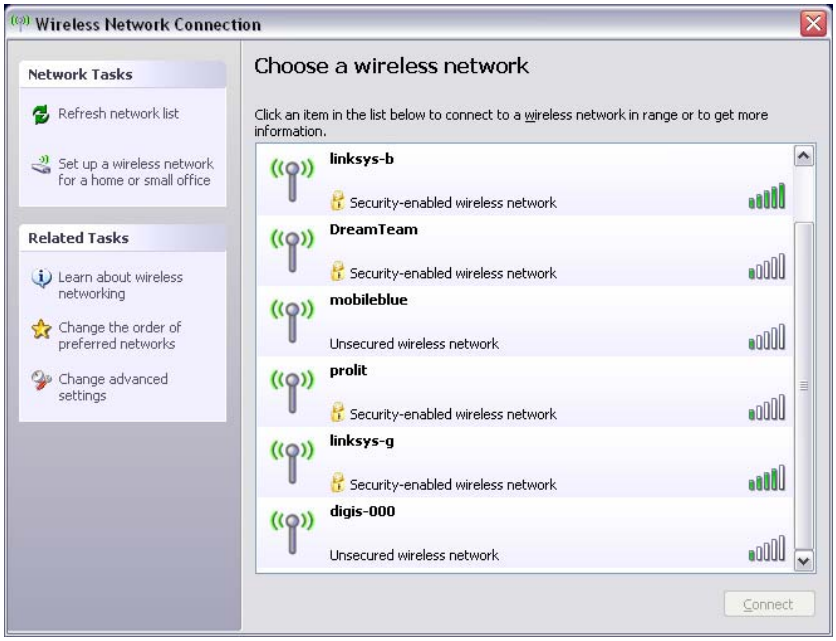
Cuando los usuarios activen los adaptadores Wi-Fi, es posible que observen docenas de puntos de acceso disponibles. Un adaptador Wi-Fi puede sincronizarse con un solo punto de acceso al principio, pero si hay demasiados puntos de acceso próximos al adaptador, se puede señalar el punto de acceso asociado y el administrador de conexión inalámbrica podría indicar al adaptador que conmute al punto de acceso que tenga la señal más fuerte. Si esto ocurre, la actividad actual de la red se verá alterada. A menudo, esto obliga a un usuario a reenviar ciertos paquetes y a reconectar su VPN (red privada virtual) a la red corporativa.

Si se guarda un punto de acceso como un parámetro de entorno de red en una ubicación, el adaptador se conectará a ese punto de acceso y no perderá la conectividad hasta que el usuario se aleje físicamente de él. Al regresar al punto de acceso, el adaptador se asocia automáticamente a éste, cambia la ubicación y todos los demás puntos de acceso no estarán visibles mediante el software de gestión de la conexión inalámbrica.

Para guardar un entorno Wi-Fi:

1 Abra el software de gestión de conexión y seleccione el punto de acceso deseado.

Nota: La ubicación puede anular el software de gestión de conexión cuando se instale la directiva de seguridad ESM para gestionar su conectividad inalámbrica.



2 Especifique cualquier información de seguridad necesaria (WEP u otra clave de seguridad) y haga clic en *Conectar*.

3 Realice los pasos descritos en Sección 3.2.1, “Guardar un entorno de red”, en la página 16 para guardar este entorno.

3.2.3 Eliminación de un entorno guardado

Para eliminar un entorno de red guardado de una ubicación:

1 Haga clic con el botón derecho en el icono *Endpoint Security Client* de la barra de tareas para visualizar el menú.

2 Cambie a la ubicación oportuna.

3 Haga clic con el botón derecho en el icono *Endpoint Security Client* y seleccione la ubicación actual para visualizar el submenú.

4 Haga clic en *Borrar entorno de red* para eliminar el entorno.

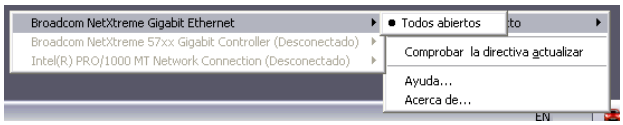
Nota: Esto borrará todos los entornos de red que se guardaron en esta ubicación.

3.3 Cambiar los ajustes del cortafuegos

A cada ubicación se le puede asignar más de una configuración de cortafuegos. Cambiar la configuración del cortafuegos puede abrir o cerrar puertos de red y permitir o no ciertos tipos de conectividad en una ubicación en particular.

Para cambiar los ajustes del cortafuegos:

1. Haga clic con el botón derecho en el icono *Endpoint Security Client* de la barra de tareas para visualizar el menú.
2. Pase el ratón por la ubicación actual para mostrar el submenú y haga clic en la selección para cambiar la configuración del cortafuegos.



Nota: El número de ajustes de cortafuegos disponible en una ubicación lo determina la directiva.

3.4 Cifrado de los datos

Cuando se activa mediante una directiva, Endpoint Security Client 3.5 gestiona el cifrado de los archivos ubicados en un directorio específico del puerto final y en dispositivos de almacenamiento extraíbles.

Las siguientes instrucciones le ayudarán a utilizar ZENworks Endpoint Security en el puesto final.

- Sección 3.4.1, “Gestionar archivos en discos fijos”, en la página 19
- Sección 3.4.2, “Gestionar archivos en el almacenamiento externo”, en la página 19

3.4.1 Gestionar archivos en discos fijos

Los discos fijos están definidos como unidades de disco duro instaladas en el equipo y como cualquier partición de una unidad de disco duro. Cada disco fijo en el puesto final tiene una carpeta de `Archivos cifrados` ubicada en el directorio raíz. Todos los archivos de esta carpeta se cifran utilizando la clave de cifrado actual. Sólo los usuarios autorizados en el equipo pueden descifrar estos archivos.

Al guardar un archivo, seleccione la carpeta de `Archivos cifrados` entre las carpetas disponibles de la unidad que desee.

3.4.2 Gestionar archivos en el almacenamiento externo

El almacenamiento externo se define como un dispositivo que está "conectado" al equipo. Incluye (entre otros): unidades USB de tamaño reducido, las tarjetas de memoria Flash y las de la PCMCIA, junto con las unidades Zip, de disquete, externas de CDR, cámaras digitales con capacidad de almacenamiento y reproductores de MP3.

Al ejecutar ZENworks Endpoint Security, los archivos almacenados en estos dispositivos se cifran a medida que el sistema operativo o el usuario accede a ellos. Los archivos copiados en el dispositivo se cifran inmediatamente. Al conectar el dispositivo de almacenamiento extraíble a un equipo no gestionado por el sistema ZENworks Endpoint Security, los archivos se mantendrán cifrados y no se podrán descifrar.

El cifrado del almacenamiento extraíble tiene lugar al insertar el dispositivo (consulte "¿Qué ocurriría si no quiero que el dispositivo esté cifrado?" en la página 21). Sin embargo, los archivos añadidos a un dispositivo de almacenamiento extraíble en otro equipo no se cifrarán y habrá que hacerlo manualmente.

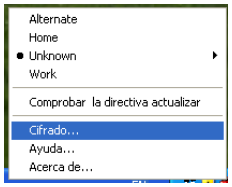
Las secciones siguientes contienen más información sobre:

- "Cifrado de archivos" en la página 20
- "¿Qué ocurriría si no quiero que el dispositivo esté cifrado?" en la página 21
- "Utilizar la Carpeta de archivos compartidos" en la página 21
- "Cambio de la contraseña en los archivos de la carpeta de archivos compartidos" en la página 21

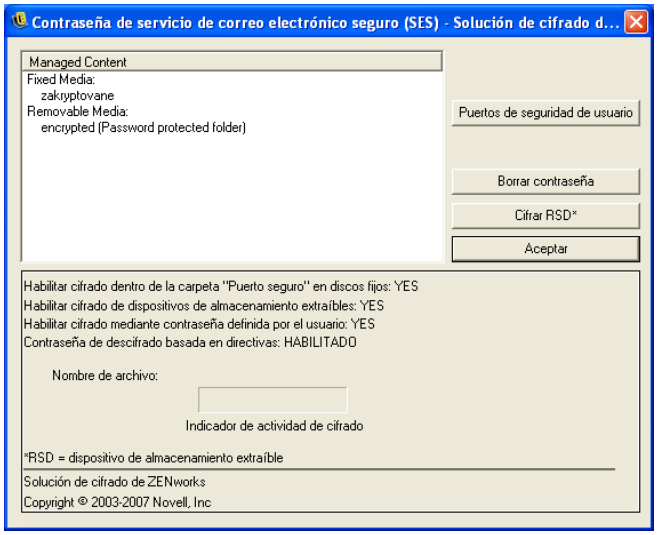
Cifrado de archivos

Para cifrar los archivos añadidos a un dispositivo de almacenamiento externo:

1. Conecte el dispositivo de almacenamiento al puerto apropiado de su equipo.
2. Haga clic con el botón derecho en el icono *Endpoint Security Client* de la barra de tareas.
3. Seleccione *Cifrado* en el menú.



4. Haga clic en *Cifrar RSD (dispositivo de almacenamiento remoto)*. De esta forma, se cifran todos los archivos del dispositivo de almacenamiento extraíble con la clave de cifrado actual.

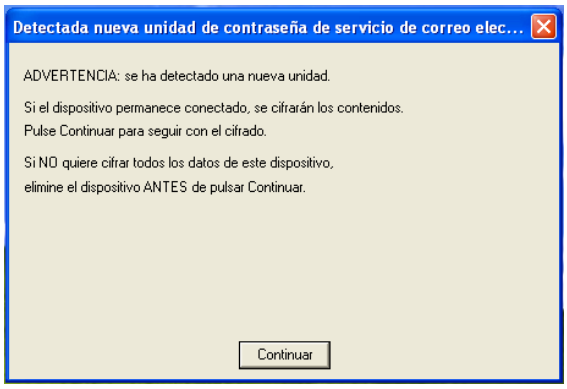


El tiempo necesario para cifrar los archivos depende de la cantidad de datos almacenados en el dispositivo.

¿Qué ocurriría si no quiero que el dispositivo esté cifrado?

Al insertar un dispositivo de almacenamiento extraíble, Endpoint Security Client le preguntará si desea cifrar la unidad o si prefiere eliminarla y no cifrar ningún archivo.

Figura 3-1 *Advertencia de cifrado cuando se ha insertado una unidad nueva*



Para impedir el cifrado, extraiga la unidad antes de hacer clic en *Continuar*. Haga clic en *Continuar* para cifrar la unidad o para cerrar la ventana después de quitar el dispositivo.

Utilizar la Carpeta de archivos compartidos

Cuando una directiva la proporciona, la carpeta de `Archivos compartidos` se crea en un dispositivo de almacenamiento extraíble conectado al equipo que ejecuta ZENworks Endpoint Security. Los usuarios pueden acceder a los archivos de esta carpeta dentro de otros grupos de directiva utilizando una contraseña creada por el usuario. Los usuarios que no ejecutan ZENworks Endpoint Security acceden a estos archivos mediante la utilidad ZENworks File Decryption y proporcionando una contraseña.

Nota: Las contraseñas se borran en cada reinicio. Los archivos añadidos a la carpeta de `Archivos compartidos` pedirán una contraseña después de reiniciar.

Para usar la carpeta de `Archivos compartidos`:

1. Mueva o guarde un archivo en la carpeta de `Archivos compartidos`.
2. Cuando se le solicite la contraseña, introduzca una contraseña y una contraseña de confirmación.
3. Introduzca una sugerencia de contraseña.

Los usuarios de ZENworks Endpoint Security no gestionados por la directiva pueden acceder a estos archivos proporcionando una contraseña. Los usuarios no gestionados por ZENworks Endpoint Security necesitarán la utilidad ZENworks File Decryption junto con la contraseña para acceder a los archivos.

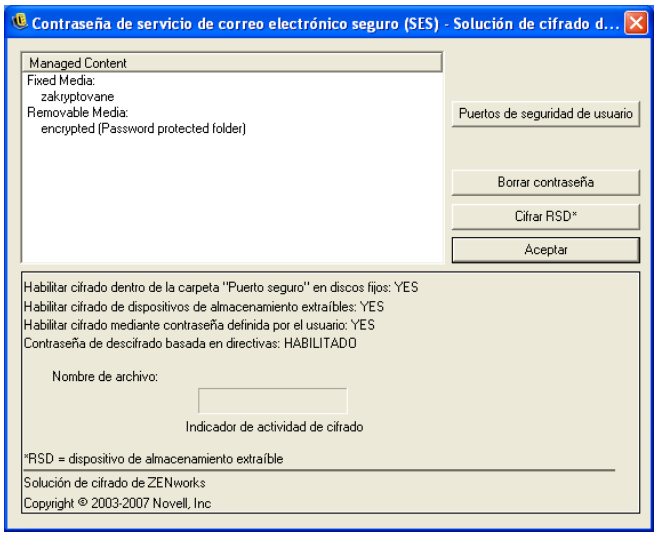
Cambio de la contraseña en los archivos de la carpeta de archivos compartidos

Puede usar el control de cifrado para cambiar las contraseñas de los archivos añadidos a la carpeta de `Archivos compartidos`.

Nota: Esto no cambiará ninguna contraseña existente, sólo la perteneciente a futuros archivos.

Para cambiar la contraseña:

1. Conecte el dispositivo de almacenamiento al puerto apropiado de su equipo.
2. Haga clic con el botón derecho en el icono *Endpoint Security Client* de la barra de tareas.
3. Seleccione *Cifrado* en el menú.
4. Haga clic en *Borrar contraseña.*



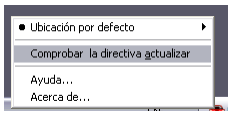
5. Arrastre un archivo a la carpeta de `Archivos compartidos` e introduzca la nueva contraseña y la sugerencia.

Todos los archivos nuevos añadidos a la carpeta necesitan la nueva contraseña para acceder.

3.5 Actualización de directivas

Las nuevas directivas de seguridad se publican con nuevas versiones para usuarios gestionados. Endpoint Security Client recibe automáticamente las actualizaciones en los intervalos que ha especificado el administrador de ESM. Sin embargo, el usuario gestionado puede comprobar las actualizaciones de directivas al acceder a una nueva ubicación.

1. Haga clic con el botón derecho en el icono *Endpoint Security Client* de la barra de tareas para visualizar el menú.
2. Haga clic en *Comprobar la actualización de la directiva*.



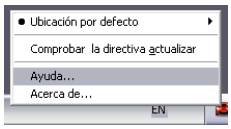
Nota: Las funciones de actualizaciones automáticas y comprobaciones de las actualizaciones de directivas no estarán disponibles cuando Endpoint Security Client 3.5 se esté ejecutando como "No gestionado". El administrador de ESM tiene un método diferente para proporcionar las actualizaciones de directivas a estos usuarios.

Endpoint Security Client 3.5 le notifica si se ha actualizado la directiva.

Nota: En ocasiones, el cambio de una tarjeta de acceso inalámbrico por otra mostrará el mensaje `Se ha actualizado la directiva`. La directiva no se ha actualizado, Endpoint Security Client 3.5 sólo está comparando el dispositivo con las restricciones de la directiva actual.

3.6 Visualización de la ayuda

1. Haga clic con el botón derecho en el icono *Endpoint Security Client* de la barra de tareas para visualizar el menú.
2. haga clic en *Ayuda*.



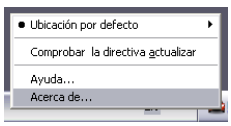
3.7 Anulación de una contraseña

Es posible que las interrupciones de productividad que podría experimentar un usuario debido a las restricciones de conectividad, software o unidades en miniatura se produzcan a causa de la directiva de seguridad que aplica Endpoint Security Client 3.5. La modificación de las ubicaciones o de los ajustes del cortafuegos normalmente anula estas restricciones y restablece las funciones interrumpidas. Sin embargo, en algunos casos, la restricción podrá implementarse de modo que afecta a todas las ubicaciones y ajustes del cortafuegos. Si se diera este caso, las restricciones deben anularse temporalmente para permitir la productividad.

Endpoint Security Client 3.5 está equipado con una función de redefinición de la contraseña, que inhabilita temporalmente la directiva de seguridad actual para permitir la actividad necesaria. El administrador de seguridad distribuye una clave de un solo uso únicamente cuando sea necesario, y debe estar informado de cualquier problema con una directiva de seguridad. Cuando haya caducado el tiempo de la clave de la contraseña, se habrá restaurado la directiva de seguridad que protege el puesto final. Reiniciar el puesto final también restaurará los ajustes de seguridad.

Para activar la anulación de la contraseña:

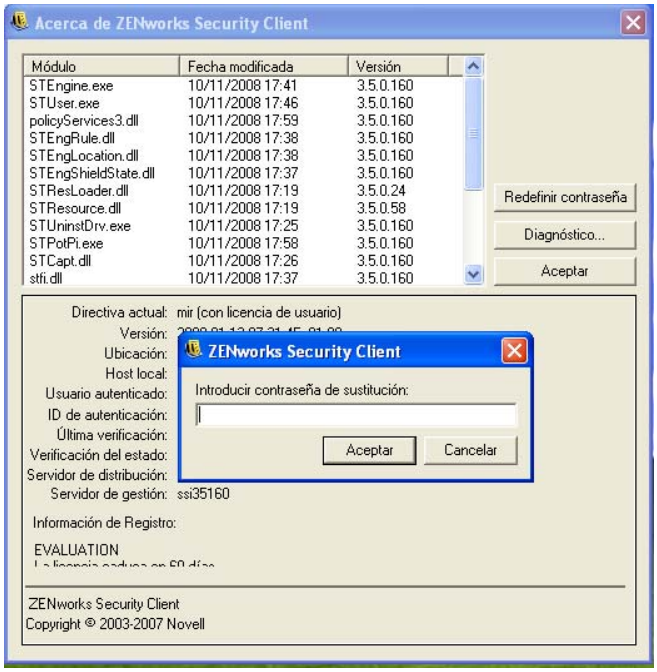
1. Póngase en contacto con el administrador de ESM de su compañía para obtener una clave de contraseña
2. Haga clic con el botón derecho en el icono *Endpoint Security Client* de la barra de tareas para visualizar el menú y, a continuación, haga clic en *Acerca de*.



3 Haga clic en *Anular contraseña* para ver la ventana de contraseña.

Nota: Si el botón *Anular contraseña* no se ve en esta ventana, significa que la directiva actual no cuenta con una anulación de contraseña.

Figura 3-2 *Ventana de contraseña*



4 Escriba la clave de contraseña proporcionada por el administrador de ZENworks Endpoint Security.

5 Haga clic en *Aceptar*. La directiva actual se remplazará por defecto por una directiva de Todo abierto durante el tiempo designado.

Al hacer clic en *Cargar directiva* (que sustituye el botón *Anular contraseña*) en la ventana *Acerca de*, se restaurará la directiva anterior. Si el administrador ha actualizado la directiva para solucionar problemas existentes, debería utilizar en su lugar *Comprobar la actualización de la directiva* para descargar la nueva inmediatamente.

3.8 Diagnóstico

Novell proporciona herramientas de diagnóstico para permitir que el administrador solucione los problemas de Endpoint Security Client 3.5. El administrador de ZENworks Endpoint Security le guiará en el proceso de diagnóstico.