

# Guía de instalación

January 5, 2009

# Novell® ZENworks® Endpoint Security Management

3.5

[www.novell.com](http://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 estar 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 misiles o armas nucleares, químicas o biológicas. Consulte la [página Web de International Trade Services de Novell \(http://www.novell.com/info/exports/\)](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.

Copyright © 2007-2008 Novell, Inc. Reservados todos los derechos. Ninguna parte de esta publicación puede ser reproducida, fotocopiada, almacenada en un sistema de recuperación o transmitida sin la expresa autorización por escrito del editor.

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 \(http://www.novell.com/company/legal/patents/\)](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](http://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 \(http://www.novell.com/documentation\)](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 \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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

<b>Acerca de esta guía</b>	<b>7</b>
<b>1 ZENworks Endpoint Security Management Descripción general</b>	<b>9</b>
1.1 Requisitos del sistema	10
1.2 Acerca de los manuales de ZENworks Endpoint Security Management	11
<b>2 Instalación de Novell ZENworks Endpoint Security Management</b>	<b>13</b>
2.1 Información previa a la instalación	13
2.2 Paquetes de instalación	13
2.2.1 Acerca del programa de instalación principal	13
2.3 Opciones de instalación	14
2.4 Orden de instalación	14
2.5 Antes de instalar ZENworks Endpoint Security Management	14
<b>3 Instalación en un único servidor</b>	<b>17</b>
3.1 Pasos de instalación	18
3.2 Iniciar el servicio	19
<b>4 Instalación en varios servidores</b>	<b>21</b>
<b>5 Instalación del Servicio de distribución de directivas</b>	<b>23</b>
5.1 Pasos de instalación	24
5.1.1 Instalación típica	26
5.1.2 Instalación personalizada	28
5.2 Iniciar el servicio	31
<b>6 Instalación del Servicio de gestión</b>	<b>33</b>
6.1 Pasos de instalación	34
6.1.1 Instalación típica	36
6.1.2 Instalación personalizada	39
6.2 Iniciar el servicio	43
<b>7 Instalación de la consola de gestión</b>	<b>45</b>
7.1 Pasos de instalación	45
7.1.1 Instalación típica	46
7.1.2 Instalación personalizada	46
7.2 Inicio de la consola	48
7.2.1 Adición de servicios de eDirectory	49
7.2.2 Configuración de los ajustes de los permisos de la consola de gestión	51
7.2.3 Publicación de una directiva	54
7.3 Instalación del lector USB	55

<b>8</b>	<b>Instalación del Servicio de seguridad de ubicación de clientes</b>	<b>57</b>
8.1	Pasos de instalación	58
8.2	Instalaciones de conmutación por error de CLAS	59
8.3	Transferencia de la clave pública al Servicio de gestión	59
<b>9</b>	<b>Instalación de Endpoint Security Client 3.5</b>	<b>61</b>
9.1	Instalación básica de Endpoint Security Client 3.5	61
9.2	Instalación de MSI	63
9.2.1	Variables de línea de comando	66
9.2.2	Distribución de una directiva con el paquete de MSI	68
9.2.3	Instalación de usuario de Endpoint Security Client 3.5 desde MSI	68
9.3	Ejecución de Endpoint Security Client 3.5	69
<b>10</b>	<b>Instalación de ZENworks Endpoint Security Client 4.0</b>	<b>71</b>
10.1	Instalación básica de Endpoint Security Client 4.0	71
10.2	Instalación de MSI	74
10.2.1	Uso del programa de instalación principal	75
10.2.2	Uso del archivo Setup.exe	75
10.2.3	Finalización de la instalación	75
10.2.4	Variables de línea de comando	77
10.2.5	Distribución de una directiva con el paquete de MSI	78
10.3	Ejecución de Endpoint Security Client 4.0	78
10.4	Funciones incompatibles con Endpoint Security Client 4.0	79
<b>11</b>	<b>Instalación no gestionada de ZENworks Endpoint Security Management</b>	<b>81</b>
11.1	Instalación de un cliente Endpoint Security Client no gestionado	81
11.2	Consola de gestión independiente	81
11.3	Distribución de directivas no gestionadas	82
<b>A</b>	<b>Actualizaciones de la documentación</b>	<b>83</b>
A.1	5 de enero de 2009	83

# Acerca de esta guía

La *Guía de instalación de Novell® ZENworks® Endpoint Security Management* proporciona todas las instrucciones necesarias para la instalación de los componentes de ZENworks Endpoint Security Management y ayuda a los administradores a poner en funcionamiento y ejecución dichos componentes.

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

- ♦ Capítulo 1, “ZENworks Endpoint Security Management Descripción general”, en la página 9
- ♦ Capítulo 2, “Instalación de Novell ZENworks Endpoint Security Management”, en la página 13
- ♦ Capítulo 3, “Instalación en un único servidor”, en la página 17
- ♦ Capítulo 4, “Instalación en varios servidores”, en la página 21
- ♦ Capítulo 5, “Instalación del Servicio de distribución de directivas”, en la página 23
- ♦ Capítulo 6, “Instalación del Servicio de gestión”, en la página 33
- ♦ Capítulo 7, “Instalación de la consola de gestión”, en la página 45
- ♦ Capítulo 8, “Instalación del Servicio de seguridad de ubicación de clientes”, en la página 57
- ♦ Capítulo 9, “Instalación de Endpoint Security Client 3.5”, en la página 61
- ♦ Capítulo 10, “Instalación de ZENworks Endpoint Security Client 4.0”, en la página 71
- ♦ Capítulo 11, “Instalación no gestionada de ZENworks Endpoint Security Management”, en la página 81

## Usuarios a los que va dirigida

Esta guía está destinada a los administradores de ZENworks Endpoint Security Management.

## 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 \(http://www.novell.com/documentation/feedback.html\)](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 utilizarse para obtener información e implementar el producto. Para obtener más información, consulte el [sitio Web de documentación de ZENworks Endpoint Security Management 3.5 \(http://www.novell.com/documentation/zesm35\)](http://www.novell.com/documentation/zesm35).



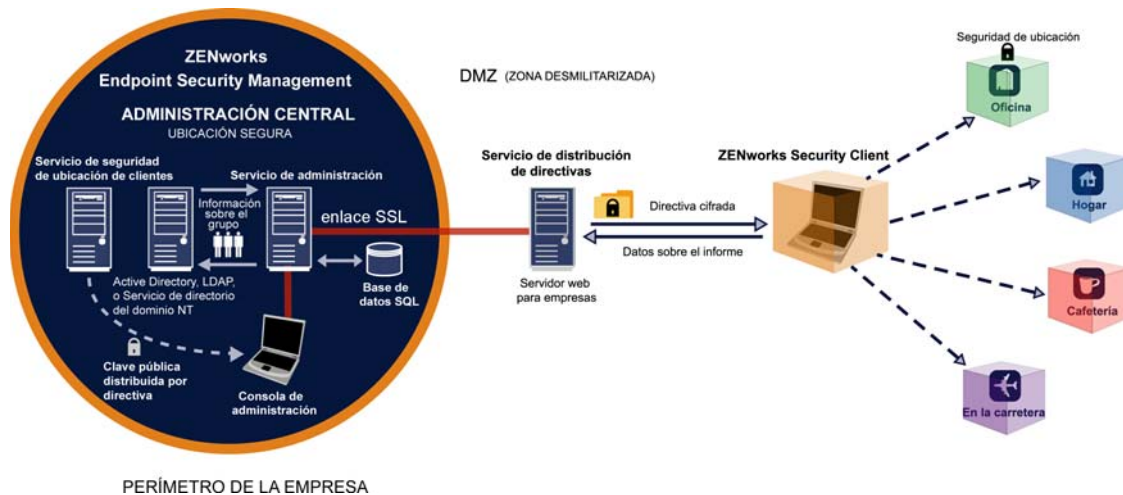


# ZENworks Endpoint Security Management Descripción general

# 1

Novell® ZENworks® Endpoint Security Management consta de cinco componentes funcionales de alto nivel: Servicio de distribución de directivas, Servicio de gestión, Consola de gestión, Servicio de seguridad de ubicación de clientes y Endpoint Security Client. La figura siguiente muestra la función de estos componentes en la arquitectura:

Figura 1-1 Arquitectura de ZENworks Endpoint Security Management



Endpoint Security Client se encarga de la aplicación de las directivas de seguridad distribuidas en el sistema del puesto final. Si el cliente Endpoint Security Client se instala en todos los equipos de una empresa, estos puestos finales podrán salir del perímetro corporativo sin perder su nivel de seguridad; los puestos finales que están dentro del perímetro recibirán comprobaciones adicionales de seguridad dentro del cortafuegos del perímetro.

Cada uno de los componentes de gestión central se instala por separado (a excepción de la instalación de un solo servidor). Consulte el [Capítulo 3, “Instalación en un único servidor”](#), en la [página 17](#) para obtener más información.

Los siguientes componentes se instalan en servidores que están protegidos dentro del perímetro corporativo:

- ♦ **Policy Distribution Service:** Se encarga de la distribución de directivas de seguridad a Endpoint Security Client y de la recuperación de los datos de los informes de Endpoint Security Client. Policy Distribution Service se puede distribuir en DMZ, fuera del cortafuegos de la empresa, con el fin de garantizar actualizaciones regulares de las directivas en los puntos finales móviles.
- ♦ **Management Service:** Se encarga de la asignación de las directivas de usuario, la autenticación de componentes, la recuperación de los datos de los informes, la distribución de los informes de ZENworks Endpoint Security Management y la creación y el almacenamiento de las directivas de seguridad.

- ♦ **Consola de gestión:** La interfaz de usuario visible, que se ejecuta en el servidor que aloja el Servicio de gestión o en una estación de trabajo que resida dentro del cortafuegos corporativo con conexión al servidor del Servicio de gestión. La consola de gestión se utiliza tanto para configurar el Servicio de gestión como para crear y gestionar las directivas de seguridad de usuarios y grupos. Las directivas se crean, copian, editan, distribuyen y suprimen con la consola de gestión.
- ♦ **Client Location Assurance Service:** Proporciona la garantía criptográfica de que los dispositivos que tienen instalados Endpoint Security Client se encuentran realmente en la ubicación definida, tal y como indican los demás parámetros del entorno de red.

## 1.1 Requisitos del sistema

Requisitos de sistema del servidor	Requisitos del sistema (cliente) para Endpoint
<b>Sistemas operativos:</b>	<b>Sistemas operativos:</b>
Microsoft Windows Server 2000 SP4	Windows XP SP1
Microsoft Windows 2000 Advanced Server SP4	Windows XP SP2
Windows 2003 Server	Windows 2000 SP4
	Windows Vista SP1 (32 bits)
	Windows Server 2008 (32 bits)
<b>Procesador:</b>	<b>Procesador:</b>
Pentium 4 HT de 3 GHz (o superior) con 768 MB de RAM como mínimo (se recomienda 1 GB o más)	600 MHz Pentium 3 (o superior)
	Un mínimo de 128 MB de RAM (se recomienda 256 MB o superior)
<b>Espacio de disco:</b>	<b>Espacio de disco:</b>
500 MB, sin la base de datos Microsoft SQL local	Se requieren 5 MB, se recomiendan 5 MB para los datos de los informes
5 GB, con la base de datos MS SQL local (se recomienda SCSI)	
<b>Software necesario:</b>	<b>Software necesario:</b>
RDBMS compatibles (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4 y SQL 2005)	Programa de instalación de Windows 3.1
Servicios de Internet Information Server de Microsoft (configurados para SSL)	Todas las actualizaciones de Windows deben ser las últimas
Servicios de directorio compatibles (eDirectory™ o Active Directory)	
.NET framework 3.5 (sólo para los servidores y la consola de gestión)	
<b>Consola de gestión independiente:</b>	
RDBMS compatibles (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4, SQL 2005 y SQL Express)	

Se necesita una cuenta local de ASP.NET 2.0 para habilitar los servicios de distribución de directivas, de gestión y de seguridad de ubicación de clientes. Si está inhabilitada, los servicios no funcionarán correctamente.

## 1.2 Acerca de los manuales de ZENworks Endpoint Security Management

Los manuales de ZENworks Endpoint Security Management proporcionan tres niveles de ayuda a los usuarios del producto.

- ♦ *Guía de instalación de ESM*: Esta guía ofrece completas instrucciones de instalación de los componentes de ZENworks Endpoint Security Management y ayuda a los administradores a poner en funcionamiento y ejecución dichos componentes. Es la guía que está leyendo.
- ♦ *Guía de administración de ZENworks Endpoint Security Management*: esta guía se dirige a los administradores de ZENworks Endpoint Security Management que tienen que gestionar los servicios, crear directivas de seguridad para la empresa, generar y analizar datos de informes, y solucionar los problemas de los usuarios finales. En este manual se proporcionan instrucciones para realizar estas tareas.
- ♦ *Guía de usuario de ZENworks Endpoint Security Client 3.5*: esta guía está diseñada para enseñar al usuario el funcionamiento de Endpoint Security Client. Esta guía se puede enviar a todos los empleados de la empresa para que aprendan a utilizar Endpoint Security Client.



# Instalación de Novell ZENworks Endpoint Security Management

# 2

Las siguientes secciones contienen información adicional sobre la instalación de Novell® ZENworks® Endpoint Security Management:

- ♦ [Sección 2.1, “Información previa a la instalación”, en la página 13](#)
- ♦ [Sección 2.2, “Paquetes de instalación”, en la página 13](#)
- ♦ [Sección 2.3, “Opciones de instalación”, en la página 14](#)
- ♦ [Sección 2.4, “Orden de instalación”, en la página 14](#)
- ♦ [Sección 2.5, “Antes de instalar ZENworks Endpoint Security Management”, en la página 14](#)

## 2.1 Información previa a la instalación

El software de instalación de ZENworks Endpoint Security Management se debe proteger físicamente para impedir cualquier manipulación indebida o uso no autorizado. Del mismo modo, los administradores deben consultar las directrices previas a la instalación y de la propia instalación para asegurarse de que el sistema ZENworks Endpoint Security Management pueda funcionar de forma ininterrumpida o ser vulnerable debido a una protección inadecuada del hardware.

El administrador que instale este software debe tener la función de administrador principal de los servidores y del dominio. Si utiliza certificados SSL de empresa, debe utilizar el mismo nombre de usuario para crear el certificado raíz de seguridad de SSL.

## 2.2 Paquetes de instalación

Si la instalación se realiza desde el DVD, se lanza un programa de instalación principal que utiliza una sencilla interfaz de usuario que guía al administrador de ZENworks Endpoint Security Management durante el proceso de instalación. Cargue el DVD de instalación en cada uno de los equipos para acceder al programa de instalación principal que instala los componentes deseados.

### 2.2.1 Acerca del programa de instalación principal

Durante el inicio, el programa de instalación principal muestra dos opciones de menú: *Productos* y *Documentación*.

El enlace *Productos* abre el menú de instalación. Los elementos de menú que aparecen en esta pantalla lanzan el programa de instalación designado para cada componente. En el caso de Endpoint Security Client 3.5 o Endpoint Security Client 4.0, hay una opción adicional disponible que permite lanzar la instalación en el modo de administrador, lo que ayuda al administrador de ZENworks Endpoint Security Management a crear un paquete de MSI de distribución sencilla (consulte [Capítulo 9.2, “Instalación de MSI”, en la página 63](#)).

Para obtener información sobre el completo funcionamiento de los componentes de ZENworks Endpoint Security Management, consulte [Guía de administración de ZENworks Endpoint Security Management](#), que está disponible a través del enlace *Documentación*.

## 2.3 Opciones de instalación

Los componentes de la interfaz final de ZENworks Endpoint Security Management se pueden instalar en un único servidor o en varios. Las instalaciones en un único servidor son ideales para las implantaciones de tamaño reducido en las que no es necesario realizar actualizaciones frecuente de directivas. Las instalaciones en varios servidores son ideales para las implantaciones grandes en las que es necesario realizar actualizaciones frecuentes de directivas. Consulte los servicios profesionales de Novell para determinar la instalación que mejor se adapte a sus necesidades.

Endpoint Security Client puede funcionar, si es necesario, sin conectividad con el servicio de distribución de directivas. Del mismo modo, se puede instalar de forma opcional una consola de gestión independiente con fines de evaluación. La instalación de este modo de operación no gestionado se describe en [Capítulo 11, “Instalación no gestionada de ZENworks Endpoint Security Management”](#), en la página 81.

## 2.4 Orden de instalación

ZENworks Endpoint Security Management se debe instalar en el siguiente orden:

1. Instalación en un único servidor o en varios servidores
  - ♦ Servicio de distribución de directivas
  - ♦ Servicio de gestión
2. Consola de gestión
3. Servicio de seguridad de ubicación del cliente
4. Endpoint Security Client 3.5 o Endpoint Security Client 4.0

## 2.5 Antes de instalar ZENworks Endpoint Security Management

Hay algunas preguntas que el administrador de ZENworks Endpoint Security Management debe plantearse antes de comenzar la instalación:

### **¿De qué forma van a recibir los usuarios sus directivas de seguridad de ZENworks Endpoint Security Management?**

Las opciones de distribución de directivas se centran en si los usuarios deben recibir una actualización de directivas en cualquier ubicación, incluido fuera de la red central, o si sólo deben recibirlas cuando se encuentran dentro de una red protegida (o conectados a ella mediante una VPN). Para las organizaciones que tengan previsto actualizar frecuentemente sus directivas de seguridad de ZENworks Endpoint Security Management, se recomienda una instalación en varios servidores que coloque el Servicio de distribución de directivas en un servidor Web fuera de la DMZ.

### **¿Qué tipo de implantaciones de servidor están disponibles?**

Si su organización sólo dispone de unos pocos servidores, es posible que sea necesario realizar una implantación de la instalación en un único servidor. Si la disponibilidad del servidor no supone ningún problema, deben tenerse en cuenta el tamaño de la implantación del cliente y el número de usuarios que se encuentran fuera del cortafuegos.

## ¿Cuál es su tipo disponible de implantación de servidor SQL?

ZENworks Endpoint Security Management crea tres bases de datos SQL durante la instalación. Si la implantación es pequeña, se puede instalar una sola base de datos SQL o una base de datos basada en servidor en los servidores de distribución de directivas y del Servicio de gestión. Para implantaciones de mayor tamaño, debe utilizarse un servidor de base de datos SQL independiente con el fin de recibir los datos del Servicio de distribución de directivas y del Servicio de gestión. Se permiten sólo los siguientes tipos de RDBMS:

- ◆ SQL Server Standard
- ◆ , SQL Server Enterprise
- ◆ y Microsoft SQL Server 2000 SP4

Si se utiliza una instancia con nombre, la configuración de los servidores debería ser parecida a la siguiente:

Provider=sqloledb

Origen de datos=NombreServidor\NombreInstancia (para instalar ZENworks Endpoint Security Management, se necesita este tipo de definición)

Initial Catalog=DatabaseName

User Id=Username

Password=Password

Defina SQL en el modo mixto.

Durante la instalación, el nombre de usuario y la contraseña no pueden hacer referencia a un usuario de dominio; debe ser un usuario SQL con derechos de administración del sistema.

## ¿Va a utilizar certificados existentes para establecer la comunicación SSL o los certificados autofirmados de Novell?

Para los diseños de de conmutación por error y recuperación tras fallos, debe utilizar certificados SSL de una autoridad certificadora (VeriSign, GeoTrust, Thawte, etc.) para empresa o generados de cualquier otra forma para las implantaciones completas de ZENworks Endpoint Security Management. Si utiliza sus propios certificados, el certificado del servicio Web y la CA raíz se deben crear en el equipo designado como Servicio de distribución de directivas y se distribuirán a continuación a los equipos adecuados. Para crear una autoridad certificadora empresarial, consulte las instrucciones paso a paso para configurar de forma segura una autoridad certificadora, que se encuentran disponibles en el sitio Web de Microsoft.

Para las evaluaciones o implantaciones pequeñas (con menos de cien usuarios), se pueden utilizar certificados autofirmados de ZENworks Endpoint Security Management. Los certificados SSL de Novell se instalan en los servidores al ejecutar la instalación típica.

## ¿Cómo implantará Endpoint Security Client?

El software Endpoint Security Client se puede implantar individualmente en cada puesto final o mediante un empuje de información de MSI. Las instrucciones sobre cómo crear un paquete MSI se encuentran en [Capítulo 9.2, “Instalación de MSI”, en la página 63.](#)

## ¿Desea que sus directivas estén basadas en equipos o en usuarios?

Las directivas pueden distribuirse a un único equipo en el que cada usuario que entre recibe la misma directiva, o se pueden definir para usuarios o grupos individuales.

Cada instalación presenta varios requisitos previos. Se recomienda que compruebe que se cumplan los requisitos previos de la lista de verificación antes de ejecutar la instalación de cualquier componente. Consulte las listas en las siguientes páginas:

- ♦ Capítulo 3, “Instalación en un único servidor”, en la página 17
- ♦ Capítulo 5, “Instalación del Servicio de distribución de directivas”, en la página 23
- ♦ Capítulo 6, “Instalación del Servicio de gestión”, en la página 33
- ♦ Capítulo 7, “Instalación de la consola de gestión”, en la página 45
- ♦ Capítulo 8, “Instalación del Servicio de seguridad de ubicación de clientes”, en la página 57
- ♦ Capítulo 9, “Instalación de Endpoint Security Client 3.5”, en la página 61



# Instalación en un único servidor

# 3

La instalación en un único servidor (SSI) de ZENworks® Endpoint Security Management permite la coexistencia del Servicio de distribución de directivas y el Servicio de gestión en el mismo servidor, lo que no es posible si no se utiliza esta opción de instalación. Por motivos de seguridad, el servidor debe implantarse dentro del cortafuegos para que los usuarios reciban las actualizaciones de directivas cuando se encuentren dentro de la infraestructura corporativa o estén conectados a ella mediante una VPN.

La implantación de la instalación en un único servidor en un controlador de dominio primario (PDC) no se admite por motivos de seguridad y funcionalidad.

---

**Nota:** Se recomienda configurar (reforzar) el servidor de SSI para que desactive todas las aplicaciones, los servicios, las cuentas y las demás opciones que no sean necesarias para la funcionalidad del servidor que se desea usar. Los pasos relacionados con esta tarea dependen de las características específicas del entorno local, por lo que no se pueden describir de antemano. Se recomienda a los administradores que consulten la sección adecuada de la [página Web de seguridad de Microsoft Technet \(http://www.microsoft.com/technet/security/default.mspix\)](http://www.microsoft.com/technet/security/default.mspix). En *Guía de administración de ZENworks Endpoint Security Management*, se proporcionan recomendaciones adicionales para el control de acceso.

Para restringir el acceso sólo a los equipos de confianza, el directorio virtual e IIS se pueden configurar para que dispongan de ACL. Consulte los artículos siguientes:

- ♦ [Concesión y denegación de acceso a equipos \(http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspix\)](http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspix)
- ♦ [Restricción de acceso al sitio por dirección IP o nombre de dominio \(http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066\)](http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- ♦ [Preguntas más frecuentes de IIS: restricciones de nombres de dominio y direcciones IP 2000 \(http://www.iisfaq.com/default.aspx?View=A136&P=109\)](http://www.iisfaq.com/default.aspx?View=A136&P=109)
- ♦ [Uso del filtrado de paquetes de IIS \(http://www.15seconds.com/issue/011227.htm\)](http://www.15seconds.com/issue/011227.htm)

Por motivos de seguridad, se recomienda encarecidamente eliminar las siguientes carpetas por defecto de la instalación de IIS:

- ♦ IISHelp
- ♦ IISAdmin
- ♦ Guiones
- ♦ Printers

También es aconsejable utilizar IIS Lockdown Tool 2.1, disponible en [microsoft.com \(http://www.microsoft.com/technet/security/tools/locktool.mspix\)](http://www.microsoft.com/technet/security/tools/locktool.mspix).

La versión 2.1 está controlada por las plantillas proporcionadas para los principales productos de Microsoft que dependen de IIS. Seleccione la plantilla que coincida en mayor medida con la función de este servidor. En caso de duda, se recomienda utilizar la plantilla dinámica del servidor Web.

---

Antes de empezar la instalación, asegúrese de que se cumplan los siguientes requisitos:

- ❑ Asegúrese de que dispone de acceso a un Servicio de directorio admitido (eDirectory™, Active Directory o los dominios NT). Los dominios NT se admiten sólo cuando un Servicio de servidor único se instala en Microsoft Windows 2000 Advanced Server (SP4).
- ❑ Si realiza la implantación con el servicio eDirectory, asegúrese de que Novell Client™ se haya instalado en el servidor y pueda autenticarse correctamente en eDirectory. Cree una contraseña de cuenta no modificable para utilizarla en la autenticación de la consola de gestión (consulte [Sección 7.2.1, “Adición de servicios de eDirectory”, en la página 49](#)).
- ❑ Para la resolución del nombre del servidor único para Endpoint Security Client, asegúrese de que los equipos de destino (en los que se instalará Endpoint Security Client) puedan hacer "ping" en el nombre del servidor de SSI. De lo contrario, debe solucionar este problema antes de continuar con la instalación. (Cambie el nombre del servidor de SSI por el nombre FQDN/NETBIOS, modifique AD para que utilice el nombre FQDN/NETBIOS, cambie las configuraciones de DNS modificando el archivo de host local en los equipos de destino para que incluya la información de MS correcta, etc.).
- ❑ Habilite o instale los Servicios de Internet Information Server (IIS) de Microsoft y configúrelos para que acepten los certificados SSL (enlace de zócalo seguro).

---

**Importante:** No habilite el recuadro de verificación *Requerir canal seguro (SSL)* en la página Comunicaciones seguras (en la utilidad Administración de equipos de Microsoft, expanda *Servicios y aplicaciones > Administrador de Internet Information Services (ISS) >* , a continuación, expanda también *Sitios web >* haga clic con el botón derecho en *Sitio web predeterminado >* haga clic en *Propiedades >* a continuación, en la pestaña *Seguridad de directorios >* y, por último, en el botón *Editar* en el recuadro del grupo de Comunicaciones seguras). Al habilitar esta opción, se interrumpe la comunicación entre el servidor de ZENworks Endpoint Security Management y el cliente de ZENworks Endpoint Security en el puesto final.

---

- ❑ Si utiliza sus propios certificados SSL, asegúrese de que el certificado del servicio Web y la CA raíz se hayan cargado en el equipo y de que el nombre del servidor validado en los pasos anteriores (independientemente de que sea NETBIOS o FQDN) coincida con el valor de *Emitido para* del certificado configurado en IIS.
- ❑ Si utiliza sus propios certificados o ya ha instalado el certificado autofirmado de Novell, puede validar también SSL introduciendo la siguiente URL en el equipo en el que se instalará Endpoint Security Client: `https://SSI_SERVER_NAME/AuthenticationServer/UserService.asmx` (donde *SSI\_SERVER\_NAME* es el nombre del servidor). Esta acción debería devolver datos válidos (una página html) y no advertencias sobre los certificados. Todas las advertencias sobre los certificados deben solucionarse antes de realizar la instalación, a menos que decida usar certificados autofirmados de Novell en su lugar.
- ❑ Asegúrese de que dispone de acceso a un RDBMS admitido (Microsoft SQL Server 2000 SP4, SQL Server Standard o SQL Server Enterprise). Defina la base de datos en el modo Mixto.

## 3.1 Pasos de instalación

Seleccione *Instalación en un único servidor* en el menú del programa de instalación principal. Esta instalación combina las instalaciones del Servicio de distribución de directivas y del Servicio de gestión. Para obtener más información, consulte [Capítulo 5, “Instalación del Servicio de distribución de directivas”, en la página 23](#) y [Capítulo 6, “Instalación del Servicio de gestión”, en la página 33](#).

Al igual que en las instalaciones individuales, la opción *Típica* instala los valores por defecto de los servicios y los certificados SSL autofirmados de Novell. La *Instalación personalizada* permite al administrador determinar las vías de directorios y el uso de una autoridad certificadora de la empresa.

## 3.2 Iniciar el servicio

El Servicio de distribución y gestión combinado se lanza inmediatamente después de completarse la instalación; no es necesario reiniciar el servidor. La consola de gestión se utiliza para gestionar los servicios de distribución y de gestión a través de la función Configuración. Para obtener más información, consulte *Guía de administración de ZENworks Endpoint Security Management*.

Tras completar la instalación, tanto la consola de gestión como el Servicio de seguridad de ubicación de clientes se pueden instalar en el servidor. Si desea instalar la consola de gestión en otro equipo, copie la carpeta de archivos de configuración de ZENworks Endpoint Security Management en el equipo designado para la consola con el fin de completar la instalación.

Continúe con la [Capítulo 5, “Instalación del Servicio de distribución de directivas”](#), en la [página 23](#).



# Instalación en varios servidores

# 4

La instalación en varios servidores es aconsejable para las implantaciones de gran tamaño, así como en el caso de que el Servicio de distribución de directivas deba ubicarse fuera del cortafuegos corporativo para garantizar que los usuarios reciban frecuentemente las actualizaciones de directivas si se encuentran fuera del perímetro. Este tipo de instalaciones se deben realizar, al menos, en dos servidores independientes. Si intenta instalar el Servicio de distribución de directivas y el Servicio de gestión en el mismo servidor, la instalación fallará. Para obtener más información, consulte [Capítulo 3, “Instalación en un único servidor”, en la página 17](#) en el caso de la instalación en un único servidor.

En una instalación de este tipo, en primer lugar debe instalarse el Servicio de distribución de directivas en un servidor protegido, ubicado fuera o dentro del cortafuegos corporativo. Para obtener más información, consulte la [Capítulo 5, “Instalación del Servicio de distribución de directivas”, en la página 23](#).

Tras instalar el Servicio de distribución de directivas, debe instalarse el Servicio de gestión. Para obtener más información, consulte la [Capítulo 6, “Instalación del Servicio de gestión”, en la página 33](#).

Se recomienda instalar la consola de gestión también en este servidor. Para obtener más información, consulte la [Capítulo 7, “Instalación de la consola de gestión”, en la página 45](#).

Continúe con la [Capítulo 5, “Instalación del Servicio de distribución de directivas”, en la página 23](#).



# Instalación del Servicio de distribución de directivas

# 5

Sus usuarios deben poder acceder en todo momento al servidor que aloja el Servicio de distribución de directivas de ZENworks® Endpoint Security Management, tanto desde dentro de la red como fuera, en la DMZ. Asegúrese de que el software necesario se haya instalado en el servidor antes de realizar la instalación (consulte “Requisitos del sistema” en la página 10). Tras seleccionar el servidor, anote su nombre: tanto el nombre de dominio completo (FQDN) como NETBIOS.

La implantación del Servicio de distribución de directivas en un controlador de dominio primario (PDC) no se admite por motivos de seguridad y funcionalidad.

---

**Nota:** Se recomienda configurar (reforzar) el servidor de SSI para que desactive todas las aplicaciones, los servicios, las cuentas y las demás opciones que no sean necesarias para la funcionalidad del servidor que se desea usar. Los pasos relacionados con esta tarea dependen de las características específicas del entorno local, por lo que no se pueden describir de antemano. Se recomienda a los administradores que consulten la sección adecuada de la [página Web de seguridad de Microsoft Technet](http://www.microsoft.com/technet/security/default.mspx) (<http://www.microsoft.com/technet/security/default.mspx>). En *Guía de administración de ZENworks Endpoint Security Management*, se proporcionan recomendaciones adicionales para el control de acceso.

Para restringir el acceso sólo a los equipos de confianza, el directorio virtual e IIS se pueden configurar para que dispongan de ACL. Consulte los artículos siguientes:

- ♦ [Concesión y denegación de acceso a equipos](http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx) (<http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx>)
- ♦ [Restricción de acceso al sitio por dirección IP o nombre de dominio](http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066) (<http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066>)
- ♦ [Preguntas más frecuentes de IIS: restricciones de nombres de dominio y direcciones IP 2000](http://www.iisfaq.com/default.aspx?View=A136&P=109) (<http://www.iisfaq.com/default.aspx?View=A136&P=109>)
- ♦ [Uso del filtrado de paquetes de IIS](http://www.15seconds.com/issue/011227.htm) (<http://www.15seconds.com/issue/011227.htm>)

Por motivos de seguridad, se recomienda encarecidamente eliminar las siguientes carpetas por defecto de la instalación de IIS:

- ♦ IISHelp
- ♦ IISAdmin
- ♦ Guiones
- ♦ Printers

También es aconsejable utilizar IIS Lockdown Tool 2.1, disponible en [microsoft.com](http://www.microsoft.com/technet/security/tools/locktool.mspx) (<http://www.microsoft.com/technet/security/tools/locktool.mspx>).

La versión 2.1 está controlada por las plantillas proporcionadas para los principales productos de Microsoft que dependen de IIS. Seleccione la plantilla que coincida en mayor medida con la función de este servidor. En caso de duda, se recomienda utilizar la plantilla dinámica del servidor Web.

---

Compruebe que se cumplan los siguientes requisitos previos antes de comenzar a realizar la instalación:

- ❑ Asegurar la resolución del nombre del servidor del Servicio de gestión (MS) en el Servicio de distribución de directivas (DS): asegúrese de que el equipo de destino en el que se haya instalado MS puede hacer "ping" en el nombre del servidor de DS (NETBIOS si DS se ha configurado dentro del cortafuegos de red o FQDN si se ha instalado fuera, en la DMZ).
- ❑ Si se realiza este paso correctamente, éste será el nombre del servidor que deberá introducir en la instalación. De lo contrario, debe solucionar este problema antes de continuar con la instalación.
- ❑ Para garantizar la resolución del nombre del servidor de Endpoint Security Client en DS, compruebe que los clientes finales (en los que Endpoint Security Client está instalado) puedan hacer "ping" en el mismo nombre del servidor de DS utilizado anteriormente. De lo contrario, debe solucionar este problema antes de continuar con la instalación.
- ❑ Habilite o instale los Servicios de Internet Information Server (IIS) de Microsoft; asegúrese de que ASP.NET esté habilitado y configúrelo para que acepte certificados SSL (enlace de zócalo seguro).

---

**Importante:** No habilite el recuadro de verificación *Requerir canal seguro (SSL)* en la página Comunicaciones seguras (en la utilidad Administración de equipos de Microsoft, expanda *Servicios y aplicaciones > Administrador de Internet Information Services (ISS) >* , a continuación, expanda también *Sitios web >* haga clic con el botón derecho en *Sitio web predeterminado >* haga clic en *Propiedades >* a continuación, en la pestaña *Seguridad de directorios >* y, por último, en el botón *Editar* en el recuadro del grupo de Comunicaciones seguras). Al habilitar esta opción, se interrumpe la comunicación entre el servidor de ZENworks Endpoint Security Management y el cliente de ZENworks Endpoint Security en el puesto final.

---

- ❑ Si utiliza sus propios certificados SSL, asegúrese de que el certificado del servicio Web se haya cargado en el equipo y que el nombre del servidor validado en los pasos anteriores (independientemente de que sea NETBIOS o FQDN) coincida con el valor de *Emitido para* del certificado configurado en IIS.
- ❑ Si utiliza sus propios certificados SSL, valide SSL desde el servidor de MS al servidor de DS: abra un navegador Web en el Servicio de gestión e introduzca la siguiente URL: `https://NOMBRES` (donde *NOMBRES* es el nombre de servidor del DS). Esta acción debería devolver datos válidos y no advertencias sobre los certificados (entre los datos válidos se puede incluir el mensaje "Página en construcción"). Todas las advertencias sobre los certificados deben solucionarse antes de realizar la instalación, a menos que decida usar certificados autofirmados de Novell en su lugar.
- ❑ Asegúrese de que dispone de acceso a un RDBMS admitido (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise o SQL Server 2005). Defina la base de datos en el modo Mixto. Esta base de datos debería alojarse en el servidor del Servicio de gestión o en un servidor compartido protegido tras el cortafuegos empresarial.

## 5.1 Pasos de instalación

Haga clic en *Instalación del Servicio de distribución de directivas* en el menú de interfaz de instalación. Comienza la instalación del Servicio de distribución de directivas.



Al lanzarse, el programa de instalación verifica si todo el software necesario se encuentra en el servidor. Si falta algún componente de software, se instala automáticamente antes de que la instalación pase a la pantalla de bienvenida (es posible que sea necesario aceptar los acuerdos de licencia del software adicional). Si hay que instalar Microsoft Data Access Components (MDAC) 2.8, el servidor se debe reiniciar después de dicha instalación para que la instalación de ZENworks Endpoint Security Management pueda continuar. Si usa Windows 2003 Server, ASP.NET 2.0 se configura para que lo ejecute el programa de instalación.

Una vez que comience la instalación del Servicio de distribución de directivas, realice los siguientes pasos:

---

**Nota:** En los siguientes pasos se describe lo que el administrador debe realizar para completar el proceso de instalación. Los procesos internos se mostrarán a lo largo de la instalación, pero no aparecerán documentados aquí, salvo que haya una acción o información específica necesaria para realizar satisfactoriamente la instalación.

---

- 1 Haga clic en *Siguiente* en la pantalla de bienvenida para continuar.
- 2 Acepte el acuerdo de licencia y, a continuación, haga clic en *Siguiente*.
- 3 Seleccione la instalación *Típica* o *Personalizada*.

**Figura 5-1** Seleccione la instalación típica o personalizada



A continuación se muestran ambas vías de instalación:

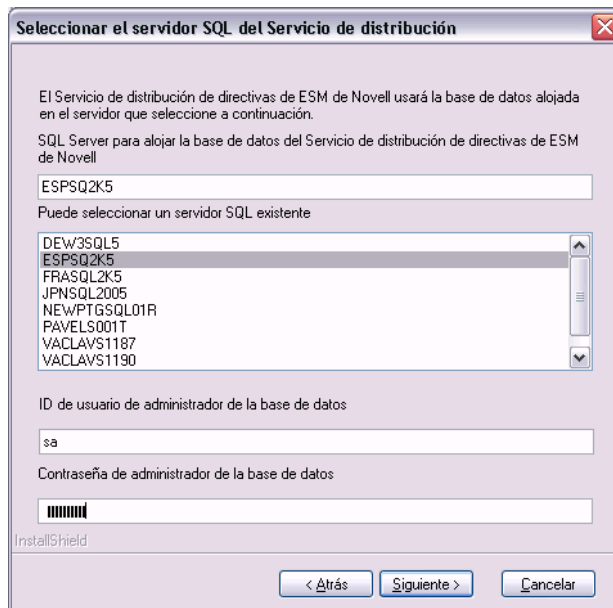
- ♦ [Sección 5.1.1, “Instalación típica”, en la página 26](#)
- ♦ [Sección 5.1.2, “Instalación personalizada”, en la página 28](#)

## 5.1.1 Instalación típica

La instalación típica ubica los archivos de software del Servicio de distribución de directivas en el directorio por defecto: `\Archivos de programa\Novell\ESM Policy Distribution Service`. A la base de datos SQL se le asigna el nombre `STDSDB`. Los tres archivos de la base de datos SQL (datos, índice y registro) se colocan en: `\Archivos de programa\Microsoft SQL Server\mssql\Data`.

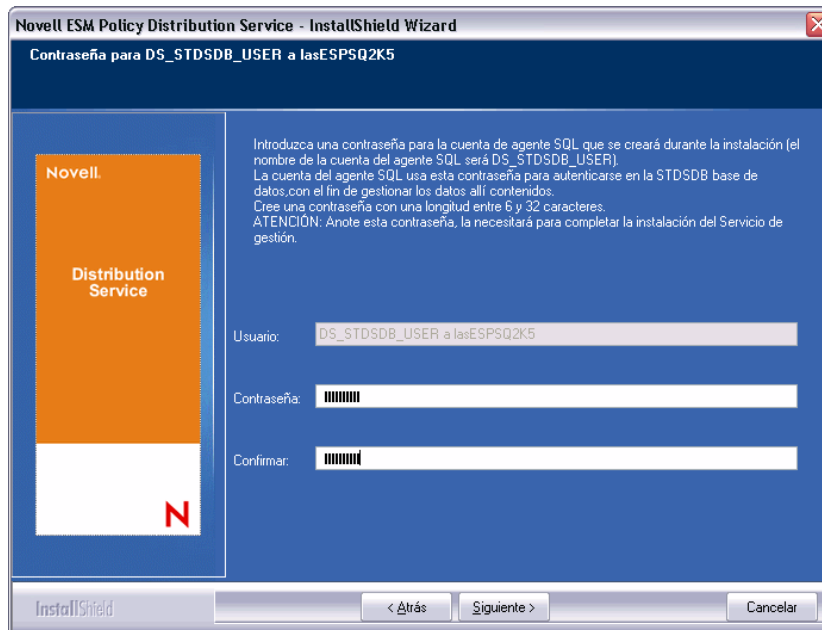
- 1 Se crean los certificados de SSL de Novell para la instalación. Si desea utilizar sus propios certificados SSL, utilice **Instalación Personalizada**. Estos certificados deben distribuirse a todos los usuarios.
- 2 El programa de instalación detecta las bases de datos SQL disponibles en el equipo y en la red. Seleccione una base de datos SQL protegida para el Servicio de distribución de directivas e introduzca el nombre y la contraseña del administrador de la base de datos (si la contraseña no tiene ningún carácter, el programa de instalación le avisará de un posible problema de seguridad). El nombre de usuario y la contraseña no pueden hacer referencia a un usuario de dominio; debe ser un usuario SQL con derechos de administración del sistema.

**Figura 5-2** Seleccione SQL Server



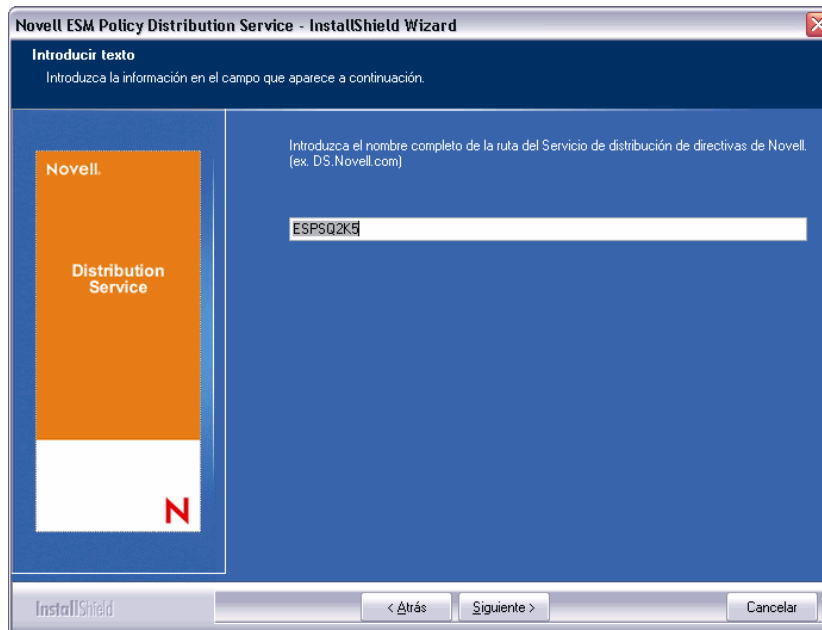
- 3 Especifique la contraseña del agente del Servicio de distribución de directivas. Se trata del nombre de usuario y la contraseña que el servicio utiliza para entrar en la base de datos SQL.

**Figura 5-3** Contraseña de SQL del servicio de distribución



- 4 Especifique el nombre de dominio del Servicio de distribución de directivas. Si el servidor va a residir fuera del cortafuegos corporativo, debe utilizarse un nombre de dominio completo. De lo contrario, sólo se necesita el nombre NETBIOS para el servidor.

**Figura 5-4** Introduzca el nombre de dominio del Servicio de distribución de directivas



- 5 En la pantalla Copiar archivos, haga clic en *Siguiente* para empezar la instalación.
- 6 Se crea la carpeta de archivos de configuración de ESM en el directorio de instalación. Ésta contiene un archivo de d. de configuración y el archivo ESM-DS.cer (el certificado SSL autofirmado de Novell), ambos necesarios para el Servicio de

gestión. Copie directamente este archivo en el equipo designado como host del Servicio de gestión mediante netshare o guardándolo en un disco o una unidad de almacenamiento portátil, y cargándolo manualmente en el directorio de instalación del servidor.

- 7 El Servicio de distribución de directivas ya se ha instalado. Haga clic en *Finalizar* para cerrar el programa de instalación y lanzar el monitor de rendimiento.

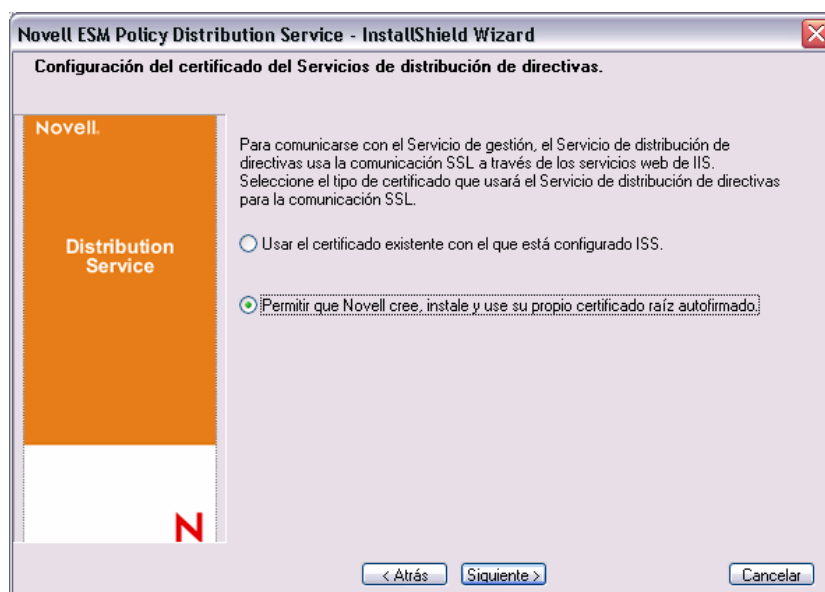
## 5.1.2 Instalación personalizada

La instalación personalizada muestra los valores por defecto utilizados en la instalación típica y permite al administrador especificar o desplazarse a un directorio diferente en el que ubicar los archivos de software.

El administrador puede instalar un certificado SSL autofirmado de Novell o utilizar uno propio.

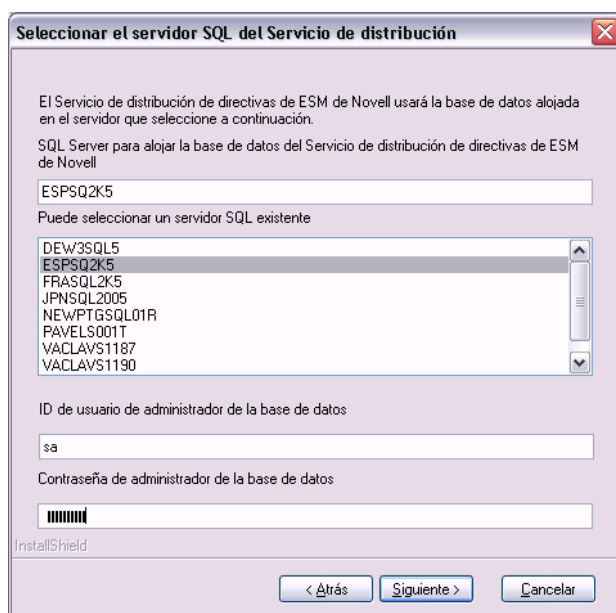
- 1 Se necesita un certificado de SSL para la comunicación segura entre el Servicio de distribución de directivas y el Servicio de gestión, y entre DS y todos los clientes de seguridad de Novell. Si ya tiene una autoridad certificadora, haga clic en *Utilice el certificado existente para el que IIS está configurado*. Si necesita un certificado, haga clic en *Permitir que Novell cree, instale y use su propio certificado raíz autofirmado*. El programa de instalación crea los certificados y la autoridad firmante. Independientemente de su tipo, los certificados deben distribuirse a todos los usuarios.

**Figura 5-5** Configuración de la raíz de confianza



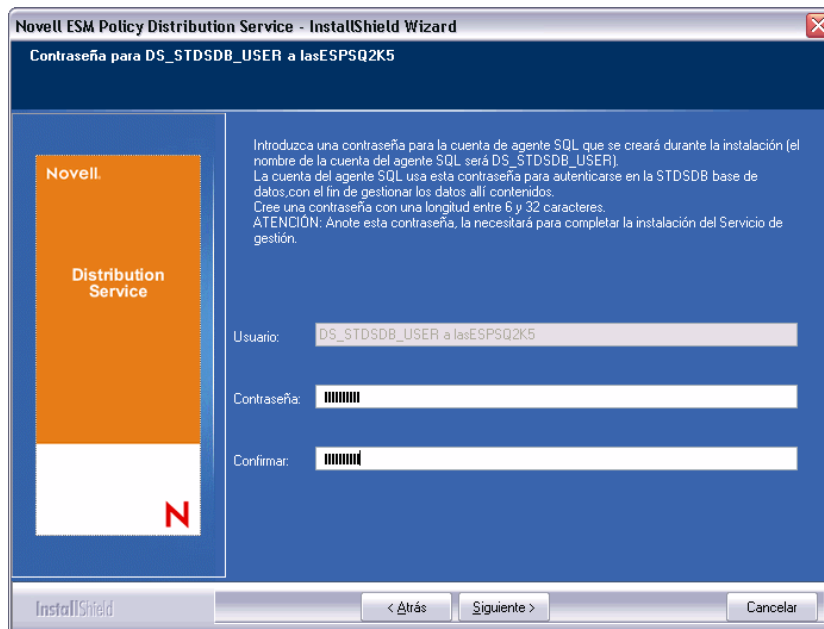
- 2 El programa de instalación detecta las bases de datos SQL disponibles en el equipo y en la red. Seleccione la base de datos SQL protegida para el Servicio de distribución de directivas e introduzca el nombre y la contraseña del administrador de la base de datos (si la contraseña no tiene ningún carácter, el programa de instalación le avisará de un posible problema de seguridad). El nombre de usuario y la contraseña no pueden hacer referencia a un usuario de dominio; debe ser un usuario SQL con derechos de administración del sistema.

Figura 5-6 Selección de SQL Server



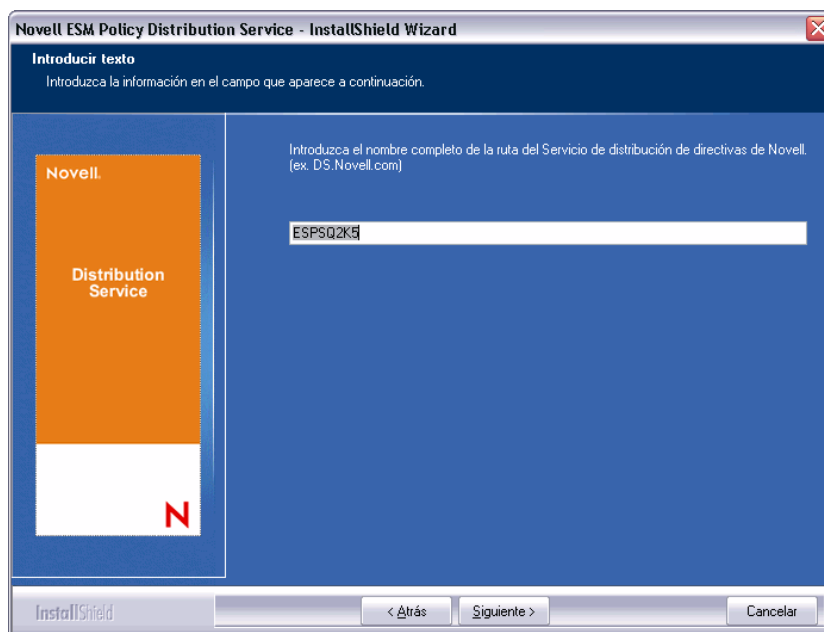
- 3 Defina el nombre de la base de datos (por defecto, se le asigna el nombre STDSDB).
- 4 Especifique la contraseña del agente del Servicio de distribución de directivas. Se trata del nombre de usuario y la contraseña que el servicio utiliza para entrar en la base de datos SQL.

Figura 5-7 Contraseña de SQL del servicio de distribución



- 5 Especifique el nombre de dominio del Servicio de distribución de directivas. Si el servidor va a residir fuera del cortafuegos corporativo, debe utilizarse un nombre de dominio completo. De lo contrario, sólo se necesita el nombre NETBIOS para el servidor.

**Figura 5-8** Introduzca el nombre de dominio del Servicio de distribución de directivas



- 6 En la pantalla Copiar archivos, haga clic en *Siguiete* para empezar la instalación.
- 7 Especifique las vías para los archivos de datos, índice y registro.
- 8 Se crea la carpeta de archivos de configuración de ESM en el directorio de instalación. Ésta contiene un archivo de Id. de configuración y el archivo ESM-DS.cer (el certificado de SSL autofirmado de Novell), ambos necesarios para el Servicio de gestión. Utilice Examinar para buscar la ubicación del servidor en la que debe guardarse el archivo (valor por defecto = directorio de instalación).

**Figura 5-9** Guardar los archivos de configuración



- 9 Si decide utilizar un certificado SSL de empresa, introduzca una copia de este archivo en la carpeta de `archivos de configuración de ESM`.
- 10 Copie directamente todos los `archivos de configuración de ESM` en el equipo designado como host del Servicio de gestión mediante netshare, o bien guardándolos en un disco o una unidad de almacenamiento portátil, y cargándolos manualmente en el directorio de instalación del servidor.
- 11 El Servicio de distribución de directivas ya se ha instalado. Haga clic en *Finalizar* para cerrar el programa de instalación y lanzar el monitor de rendimiento.

## 5.2 Iniciar el servicio

Una vez realizada la instalación, el Servicio de distribución de directivas se inicia inmediatamente sin que sea necesario reiniciar el sistema. La consola de gestión puede ajustar los tiempos de carga del Servicio de distribución mediante la herramienta de configuración. Para obtener más información, consulte *Guía de administración de ZENworks Endpoint Security Management*.

Continúe con la [Capítulo 6, “Instalación del Servicio de gestión”, en la página 33](#).





# Instalación del Servicio de gestión

# 6

El Servicio de gestión debe instalarse en un servidor seguro detrás de un cortafuegos y no puede compartir el mismo servidor que el Servicio de distribución de directivas (excepto en la instalación en un único servidor; consulte [Capítulo 3, “Instalación en un único servidor”, en la página 17](#)). Por motivos de seguridad, el Servicio de gestión no debe instalarse fuera del cortafuegos de red. Tras seleccionar el servidor, anote su nombre: tanto el nombre de dominio completo (FQDN) como NETBIOS. La implantación del Servicio de gestión en un controlador de dominio primario (PDC) no se admite por motivos de seguridad y funcionalidad.

---

**Nota:** Se recomienda configurar (reforzar) el servidor de SSI para que desactive todas las aplicaciones, los servicios, las cuentas y las demás opciones que no sean necesarias para la funcionalidad del servidor que se desea usar. Los pasos relacionados con esta tarea dependen de las características específicas del entorno local, por lo que no se pueden describir de antemano. Se recomienda a los administradores que consulten la sección adecuada de la [página Web de seguridad de Microsoft Technet \(http://www.microsoft.com/technet/security/default.mspx\)](#). En la [Guía de administración de ZENworks Endpoint Security Management](#), se proporcionan recomendaciones adicionales para el control de acceso.

Para restringir el acceso sólo a los equipos de confianza, el directorio virtual e IIS se pueden configurar para que dispongan de ACL. Consulte los artículos siguientes:

- ♦ [Concesión y denegación de acceso a equipos \(http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx\)](http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- ♦ [Restricción de acceso al sitio por dirección IP o nombre de dominio \(http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066\)](http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- ♦ [Preguntas más frecuentes de IIS: restricciones de nombres de dominio y direcciones IP 2000 \(http://www.iisfaq.com/default.aspx?View=A136&P=109\)](http://www.iisfaq.com/default.aspx?View=A136&P=109)
- ♦ [Uso del filtrado de paquetes de IIS \(http://www.15seconds.com/issue/011227.htm\)](http://www.15seconds.com/issue/011227.htm)

Por motivos de seguridad, se recomienda encarecidamente eliminar las siguientes carpetas por defecto de la instalación de IIS:

- ♦ IISHelp
- ♦ IISAdmin
- ♦ Guiones
- ♦ Printers

También es aconsejable utilizar IIS Lockdown Tool 2.1, disponible en [microsoft.com \(http://www.microsoft.com/technet/security/tools/locktool.mspx\)](http://www.microsoft.com/technet/security/tools/locktool.mspx).

La versión 2.1 está controlada por las plantillas proporcionadas para los principales productos de Microsoft que dependen de IIS. Seleccione la plantilla que coincida en mayor medida con la función de este servidor. En caso de duda, se recomienda utilizar la plantilla dinámica del servidor Web.

---

Antes de empezar la instalación, asegúrese de que se cumplan los siguientes requisitos:

- ❑ Asegúrese de que dispone de acceso a un servicio de directorio admitido (eDirectory, Active Directory o los dominios NT\*). \*= Sólo se admite cuando el Servicio de gestión se ha instalado en Microsoft Windows 2000 Advanced Server (SP4).
- ❑ Si realiza la implantación con el Servicio eDirectory™, asegúrese de que Novell Client™ se haya instalado en el servidor y pueda autenticarse correctamente en eDirectory. Cree una contraseña de cuenta no modificable para utilizarla en la autenticación de la consola de gestión (consulte [Sección 7.2.1, “Adición de servicios de eDirectory”](#), en la página 49).
- ❑ Para garantizar la resolución del nombre del servidor de Endpoint Security Client en MS, compruebe que los equipos de destino (en los que Endpoint Security Client está instalado) puedan hacer "ping" en el nombre del servidor de MS. Si se realiza correctamente, éste será el valor que se introduzca en la instalación. De lo contrario, debe solucionar este problema antes de continuar con la instalación.
- ❑ Habilite o instale los Servicios de Internet Information Server (IIS) de Microsoft, asegúrese de que ASP.NET esté habilitado y configúrelo para que acepte certificados SSL (enlace de zócalo seguro).

---

**Importante:** No habilite el recuadro de verificación *Requerir canal seguro (SSL)* en la página Comunicaciones seguras (en la utilidad Administración de equipos de Microsoft, expanda *Servicios y aplicaciones > Administrador de Internet Information Services (ISS)* > , a continuación, expanda también *Sitios web* > haga clic con el botón derecho en *Sitio web predeterminado* > haga clic en *Propiedades* > a continuación, en la pestaña *Seguridad de directorios* > y, por último, en el botón *Editar* en el recuadro del grupo de Comunicaciones seguras). Al habilitar esta opción, se interrumpe la comunicación entre el servidor de ZENworks Endpoint Security Management y el cliente de ZENworks Endpoint Security en el puesto final.

---

- ❑ Si utiliza sus propios certificados SSL, asegúrese de que la CA raíz se haya cargado en el equipo y de que el nombre del servidor validado en los pasos anteriores (independientemente de que sea NETBIOS o FQDN) coincida con el valor de *Emitido para* del certificado configurado en IIS.
- ❑ Si utiliza sus propios certificados o ya ha instalado el certificado autofirmado de Novell, puede validar también SSL introduciendo la siguiente URL en el equipo en el que se instalará Endpoint Security Client: `https://MS_SERVER_NAME/AuthenticationServer/UserService.asmx` (donde *MS\_SERVER\_NAME* es el nombre del servidor). Esta acción debería devolver datos válidos (una página html) y no advertencias sobre los certificados. Cualquier advertencia sobre los certificados debe solucionarse antes de realizar la instalación.
- ❑ Asegúrese de que dispone de acceso a un RDBMS admitido (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise o SQL 2005). Defina la base de datos en el modo mixto.
- ❑ Copie el directorio de los archivos de configuración de ESM, que contiene el Id. de configuración y el certificado raíz de SSL del Servicio de distribución de directivas, en el directorio de instalación de este servidor.

## 6.1 Pasos de instalación

Haga clic en *Instalación del Servicio de gestión* en el menú de interfaz de instalación. Comienza la instalación del Servicio de gestión.

Al lanzarse, el programa de instalación verifica si todo el software necesario se encuentra en el servidor. Si falta algún componente de software, se instala automáticamente antes de que la instalación pase a la pantalla de bienvenida (es posible que sea necesario aceptar los acuerdos de licencia del software adicional). Si hay que instalar Microsoft Data Access Components (MDAC) 2.8, el servidor se debe reiniciar después de dicha instalación para que la instalación de ZENworks Endpoint Security Management pueda continuar. Si usa Windows 2003 Server, se debe configurar ASP.NET 2.0 para que lo ejecute el programa de instalación.

Tras comenzar la instalación del Servicio de gestión, realice los siguientes pasos:

---

**Nota:** En los siguientes pasos se describe lo que el administrador debe realizar para completar el proceso de instalación. Los procesos internos se mostrarán a lo largo de la instalación, aunque no aparecerán documentados aquí a menos que haya una acción o información específica necesaria para realizar satisfactoriamente la instalación.

---

- 1 Haga clic en *Siguiente* en la pantalla de bienvenida para continuar.
- 2 Acepte el acuerdo de licencia y, a continuación, haga clic en *Siguiente*.
- 3 Seleccione la instalación *Típica* o *Personalizada*.

**Figura 6-1** Seleccione la instalación típica o personalizada



A continuación se muestran ambas vías de instalación:

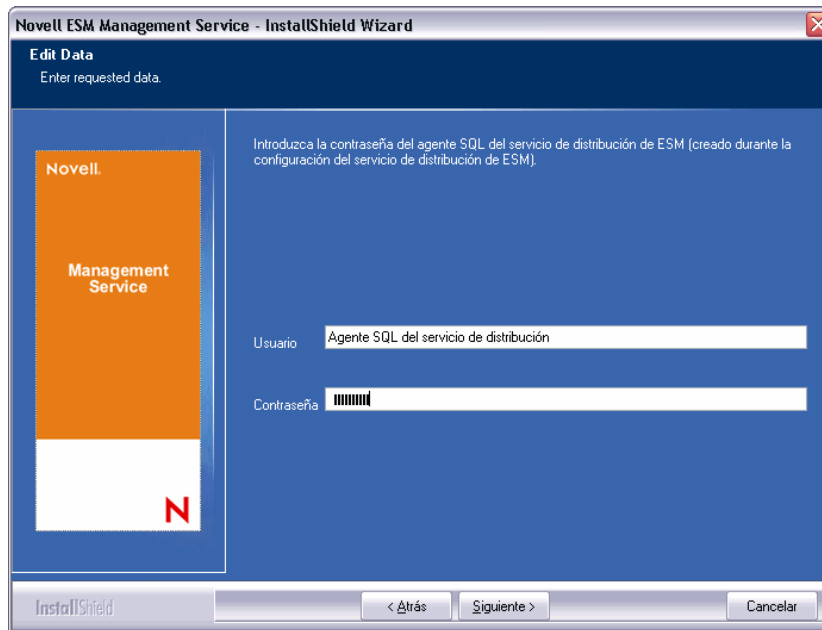
- ♦ [Sección 6.1.1, “Instalación típica”, en la página 36](#)
- ♦ [Sección 6.1.2, “Instalación personalizada”, en la página 39](#)

## 6.1.1 Instalación típica

La instalación típica ubica los archivos de software del Servicio de gestión en el directorio por defecto: \Archivos de programa\Novell\ESM Management Service. A la base de datos SQL se le asigna el nombre STMSDB. Los tres archivos de la base de datos SQL (datos, índice y registro) se colocan en: \Archivos de programa\Microsoft SQL Server\mssql\Data.

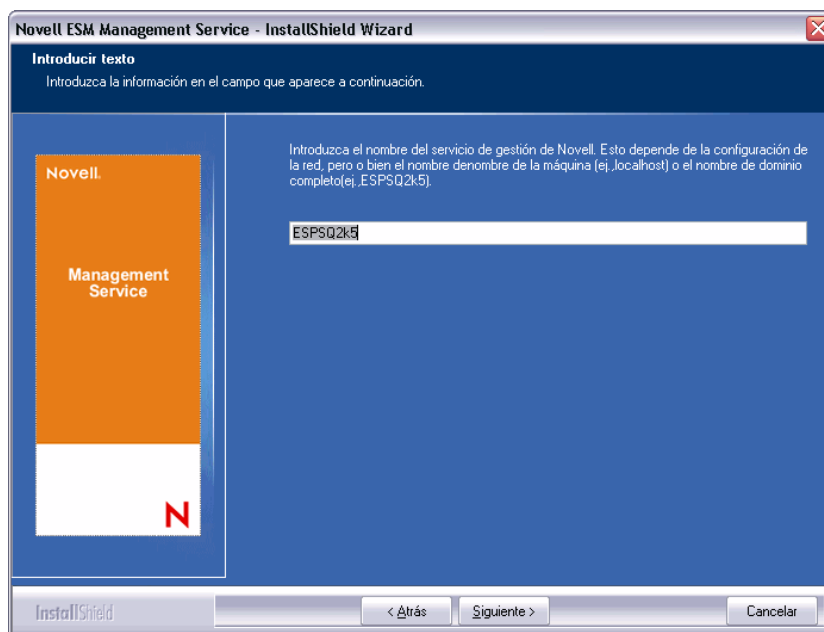
- 1 Especifique la contraseña del agente del Servicio de distribución de directivas que se creó durante la instalación de la distribución de directivas.

**Figura 6-2** Introduzca la contraseña de SQL



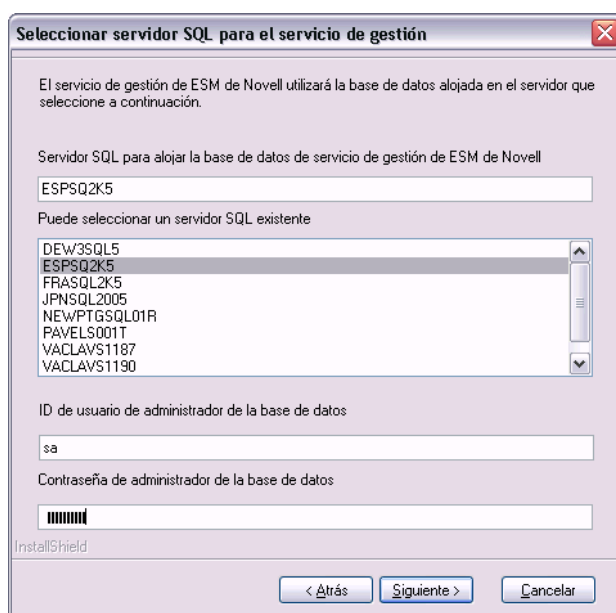
- 2 Especifique el nombre del servidor que va a alojar el Servicio de gestión.

Figura 6-3 Introduzca el nombre del servidor de MS



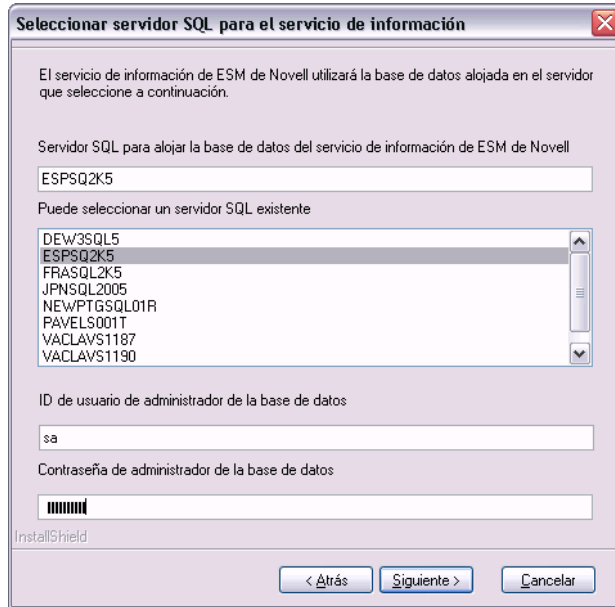
- 3 Se crean los certificados de SSL de Novell para la instalación. Si desea utilizar sus propios certificados SSL, realice una **instalación personalizada**. Estos certificados deben distribuirse a todos los usuarios.
- 4 El programa de instalación detecta las bases de datos SQL disponibles en el equipo y en la red. Seleccione la base de datos SQL protegida para el Servicio de gestión y especifique el nombre y la contraseña del administrador de la base de datos (si la contraseña no tiene ningún carácter, el programa de instalación avisará de un posible problema de seguridad). El nombre de usuario y la contraseña no pueden hacer referencia a un usuario de dominio; debe ser un usuario SQL con derechos de administración del sistema.

Figura 6-4 Seleccione la base de datos SQL de MS



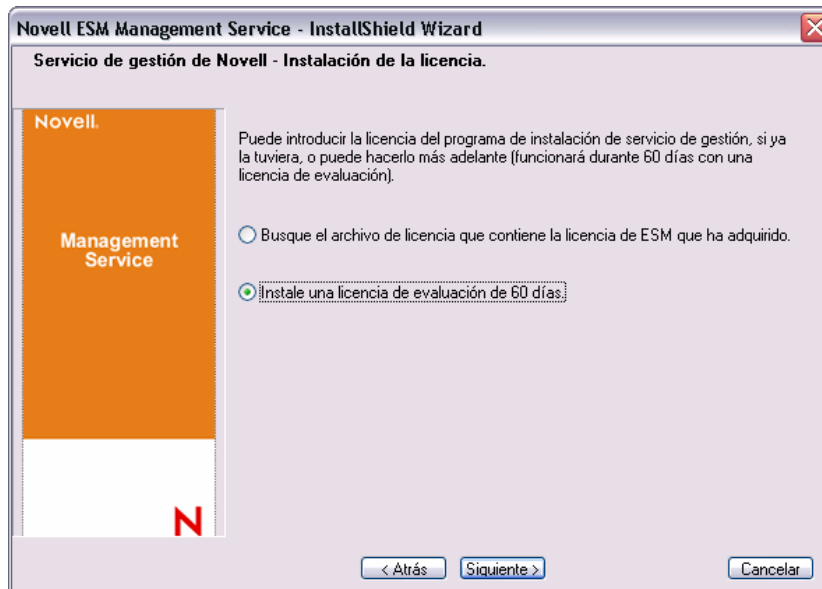
- 5 Seleccione la base de datos SQL para el Servicio de informes y especifique la contraseña del administrador para esa base de datos. Si desea capturar y almacenar un gran número de informes, se recomienda conceder su propio servidor SQL a la base de datos del servicio de elaboración de informes.

Figura 6-5 Seleccione la base de datos del servicio de elaboración de informes



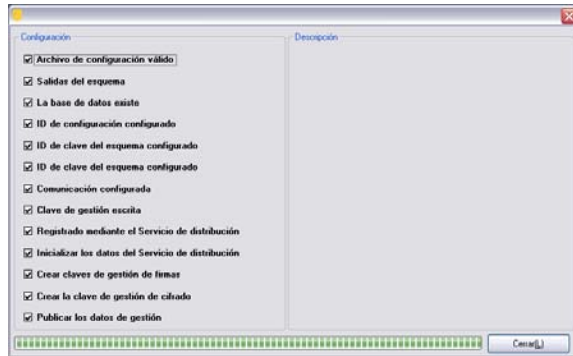
- 6 Si ZENworks Endpoint Security Management ya se ha adquirido, se proporciona un archivo de licencia independiente. Copie el archivo de licencia en este servidor y búsquelo (consulte la página de instrucciones incluida con el archivo de licencia para obtener más información). Si aún no ha adquirido ninguna licencia de ZENworks Endpoint Security Management, seleccione *Licencia de evaluación de 60 días* para continuar.

Figura 6-6 Busque el archivo de licencia de Novell



- 7 En la pantalla Copiar archivos, haga clic en *Siguiente* para empezar la instalación.
- 8 El Servicio de gestión ejecuta una comprobación de la comunicación tanto en las bases de datos SQL como en el Servicio de distribución de directivas. Si no se puede verificar la comunicación, el programa de instalación le informará de este problema. Para que la instalación se realice correctamente, deben marcarse todas las casillas.

**Figura 6-7** Verificación de la comunicación



- 9 Omite los pasos **Paso 10** y **Paso 11** si va a instalar eDirectory como servicio de directorio.
- 10 Si la instalación se va a realizar en un servidor miembro de un dominio que tenga el Servicio de directorio de Active Directory o de dominios NT, el programa de instalación lo detectará automáticamente y añadirá los siguientes datos a la instalación mediante una conexión segura de sólo lectura:
  - ♦ El nombre del equipo o el nombre de dominio raíz
  - ♦ El nombre del administrador del dominio o una cuenta de recursos con los permisos de lectura adecuados
- 11 Especifique la contraseña del administrador en el espacio proporcionado y haga clic en *Probar para verificar que se pueda establecer una conexión*. Si la prueba se realiza correctamente, haga clic en *Guardar*. Si, por el contrario, la prueba falla o no se detecta el dominio correcto, deberá añadirlo manualmente mediante la consola de gestión (consulte **Sección 7.2.1, “Adición de servicios de eDirectory”**, en la página 49).

---

**Nota:** La contraseña que se introduzca debe ajustarse para que no caduque. Además, esta cuenta nunca se debe inhabilitar.

---

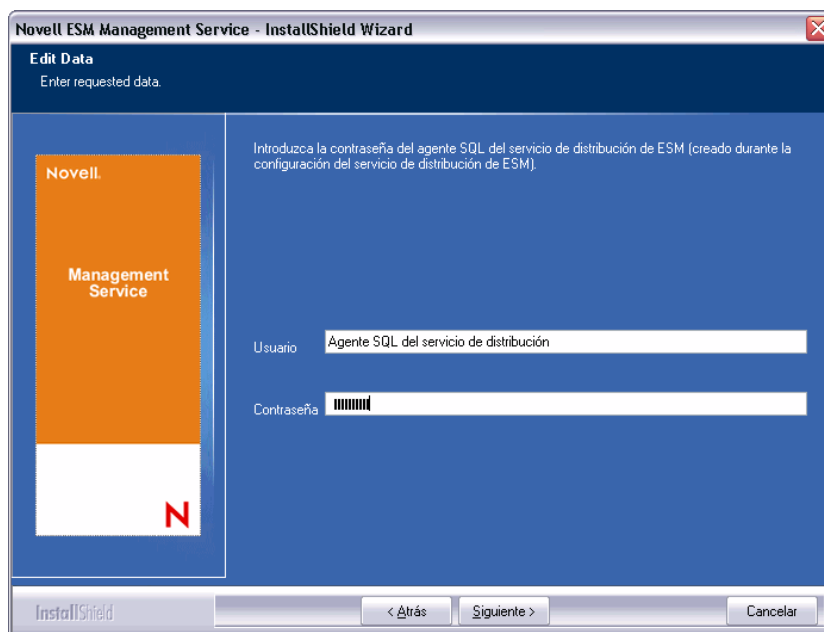
- 12 Ya se ha instalado el Servicio de gestión. Haga clic en *Listo* para cerrar las comprobaciones de comunicación y, a continuación, en *Finalizar* para cerrar el programa de instalación.

## 6.1.2 Instalación personalizada

La instalación personalizada muestra los valores por defecto utilizados en la instalación típica y permite al administrador acceder o desplazarse a una ubicación diferente.

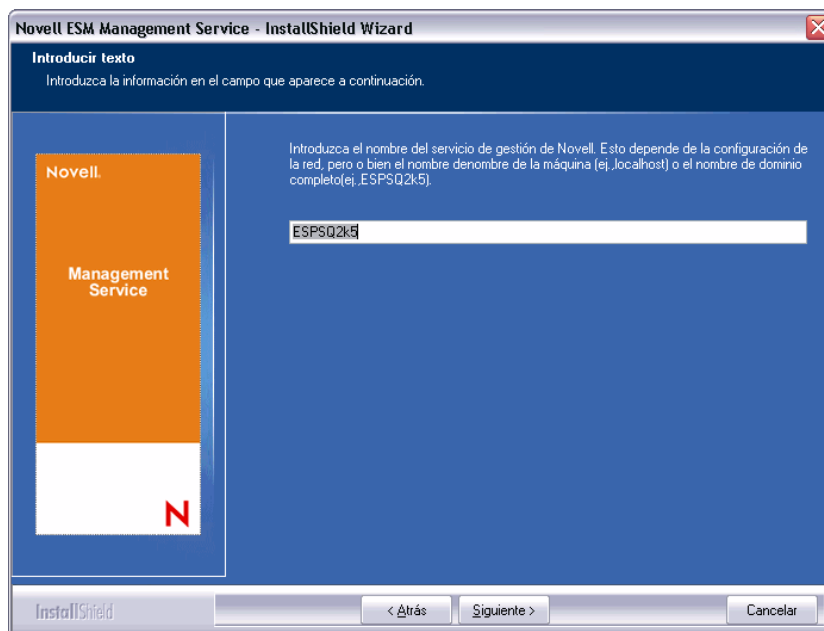
- 1 Especifique la contraseña del agente del Servicio de distribución de directivas que se creó durante la instalación de la distribución de directivas.

**Figura 6-8** Introduzca la contraseña de SQL



- 2 Seleccione el tipo de certificado de SSL utilizado para la instalación del Servicio de distribución de directivas. Si ha usado una autoridad certificadora (empresarial) existente, haga clic en *El Servicio de distribución de Novell ha utilizado un certificado con el que ya se había configurado IIS*. Si el Servicio de distribución ha creado un certificado de Novell, haga clic en *El Servicio de distribución de Novell ha instalado un certificado raíz autofirmado de Novell*.
- 3 Especifique el nombre del servidor que va a alojar el Servicio de gestión.

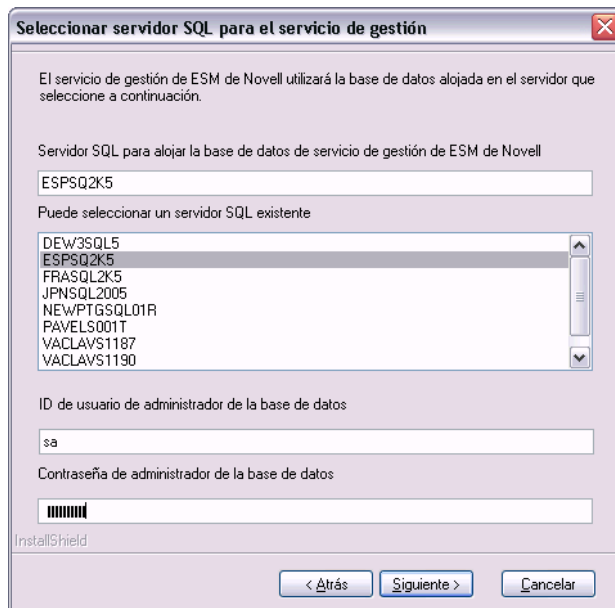
**Figura 6-9** Introduzca el nombre del servidor de MS





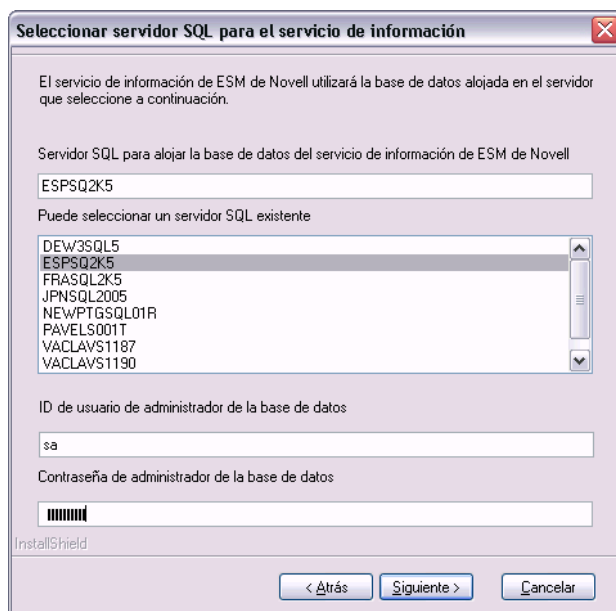
- 4 Se necesita un certificado de SSL para la comunicación segura entre el servicio de gestión y todos los clientes de Endpoint Security Client. Si ya dispone de una autoridad certificadora, haga clic en *Utilizar el certificado existente para el que está configurado IIS*. Si necesita un certificado, haga clic en *Permitir a Novell crear, instalar y utilizar su propio certificado raíz autofirmado*. El programa de instalación crea los certificados y la autoridad firmante. Independientemente de su tipo, los certificados deben distribuirse a todos los usuarios.
- 5 Al seleccionar los certificados de Novell, seleccione la ubicación en la que se puede guardar el certificado para una distribución sencilla (el valor por defecto es el directorio de instalación).
- 6 El programa de instalación detecta las bases de datos SQL disponibles en el equipo y en la red. Seleccione la base de datos SQL protegida para el Servicio de gestión y especifique el nombre y la contraseña del administrador de la base de datos (si la contraseña no tiene ningún carácter, el programa de instalación avisará de un posible problema de seguridad). El nombre de usuario y la contraseña no pueden hacer referencia a un usuario de dominio; debe ser un usuario SQL con derechos de administración del sistema.

**Figura 6-10** Seleccione la base de datos SQL de MS



- 7 Defina el nombre de la base de datos (por defecto, se le asigna el nombre STMSDB).
- 8 Seleccione la base de datos SQL para el Servicio de informes y especifique la contraseña del administrador para esa base de datos.

**Figura 6-11** Seleccione la base de datos del servicio de elaboración de informes



- 9 Defina el nombre de la base de datos (por defecto, se le asigna el nombre STRSDB).
- 10 Si ZENworks Endpoint Security Management ya se ha adquirido, se proporciona un archivo de licencia independiente. Copie el archivo de licencia en este servidor y búsquelo (consulte la página de instrucciones incluida con el archivo de licencia para obtener más información). Si aún no ha adquirido ninguna licencia de ZENworks Endpoint Security Management, seleccione *Licencia de evaluación de 60 días* para continuar.

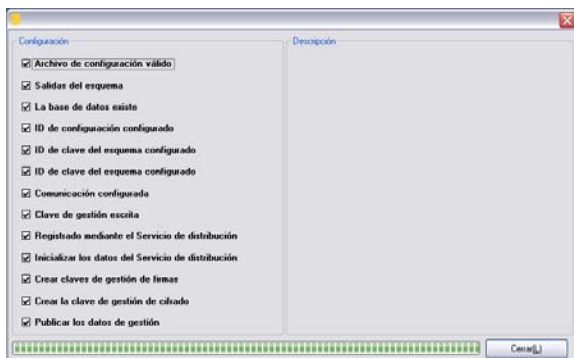
**Figura 6-12** Busque el archivo de licencia de Novell



- 11 En la pantalla Copiar archivos, haga clic en *Siguiente* para empezar la instalación.
- 12 Seleccione las vías para los archivos de datos, índice y registro de la base de datos del Servicio de gestión.

- 13 Seleccione las vías para los archivos de datos, índice y registro de la base de datos del Servicio de informes.
- 14 El Servicio de gestión ejecuta una comprobación de la comunicación tanto en las bases de datos SQL como en el Servicio de distribución de directivas. Si no se puede verificar la comunicación, el programa de instalación le informará de este problema. Para que la instalación se realice correctamente, deben marcarse todas las casillas.

**Figura 6-13** Verificación de la comunicación



- 15 Omita los pasos Paso 16 y Paso 17 si va a instalar eDirectory como servicio de directorio.
- 16 Si la instalación se va a realizar en un servidor miembro de un dominio que tenga el Servicio de directorio de Active Directory o de dominios NT, el programa de instalación lo detectará automáticamente y añadirá los siguientes datos a la instalación mediante una conexión segura de sólo lectura:
  - ♦ El nombre del equipo o el nombre de dominio raíz
  - ♦ El nombre del administrador del dominio o una cuenta de recursos con los permisos de lectura adecuados
- 17 Especifique la contraseña del administrador en el espacio proporcionado y haga clic en *Probar para verificar que se pueda establecer una conexión*. Si la prueba se realiza correctamente, haga clic en *Guardar*. Si, por el contrario, la prueba falla o no se detecta el dominio correcto, deberá añadirlo manualmente mediante la consola de gestión (consulte Sección 7.2.1, “Adición de servicios de eDirectory”, en la página 49).

---

**Nota:** La contraseña especificada debe definirse para que no caduque. Además, no se debe inhabilitar nunca esta cuenta.

---

- 18 Ya se ha instalado el Servicio de gestión. Haga clic en *Listo* para cerrar las comprobaciones de comunicación y, a continuación, en *Finalizar* para cerrar el programa de instalación.

## 6.2 Iniciar el servicio

Una vez realizada la instalación, el Servicio de gestión se inicia inmediatamente sin que sea necesario reiniciar el sistema. La consola de gestión se utiliza para gestionar los datos del servicio de gestión (consulte *Guía de administración de ZENworks Endpoint Security Management*).

Novell recomienda instalar la consola de gestión en este servidor. Si instala la consola de gestión en otro equipo, copie el directorio de archivos de configuración de ESM mediante netshare o guardando el archivo en un disco o una unidad de almacenamiento portátil en el equipo que alojará la consola de gestión.

Continúe con la [Capítulo 7, “Instalación de la consola de gestión”](#), en la página 45.

# Instalación de la consola de gestión

# 7

La consola de gestión puede instalarse en el servidor del Servicio de gestión o en un equipo seguro que tenga comunicación directa con dicho servidor. Pueden configurarse varias instalaciones de la consola de gestión para que se comuniquen con un único Servicio de gestión; sin embargo, se recomienda limitar el acceso a la consola de gestión a usuarios seleccionados.

Por motivos de seguridad, es aconsejable instalar la consola de gestión directamente en el servidor del Servicio de gestión.

Si desea instalar la consola de gestión en una estación de trabajo independiente, asegúrese de que se cumplan los siguientes requisitos antes de empezar la instalación:

- Asegúrese de que el dispositivo en el que desea instalar la consola de gestión cumpla los siguientes requisitos:
  - ♦ Windows XP SP1, Windows XP SP2 o Windows 2000 SP4.
  - ♦ Se recomienda utilizar un procesador de 1 GHz con un mínimo de 256 MB de RAM y disponer de 100 MB de espacio en el disco.
- Copie en el equipo la carpeta de los archivos de configuración ESM que contiene los certificados raíz SSL del Servicio de distribución de directivas y el Servicio de gestión, junto con el archivo `STInstParam.id`.
- Si va a instalar la consola de gestión en el servidor del Servicio de gestión, compruebe que dispone de la versión 5.5, o superior, de Microsoft Internet Explorer.

## 7.1 Pasos de instalación

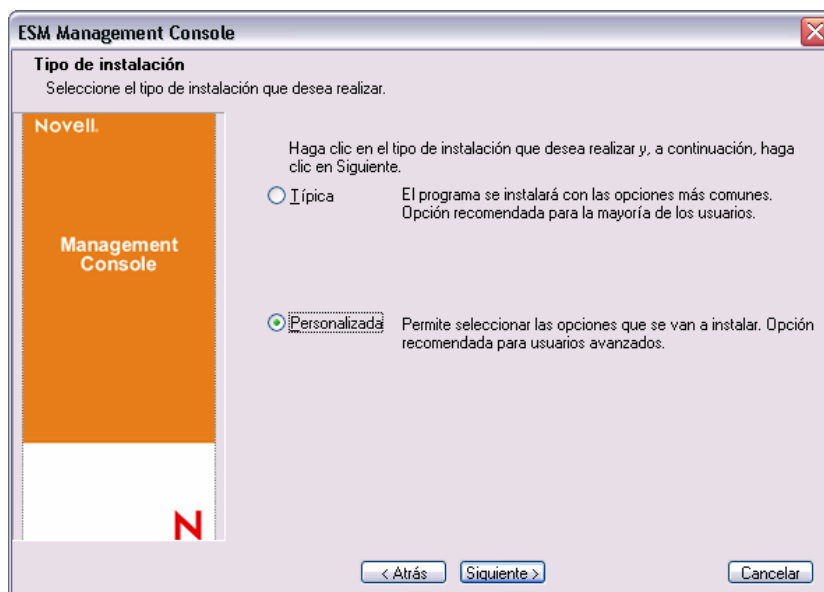
Haga clic en *Instalación de la consola de gestión* en el menú de interfaz de instalación.

Durante el inicio, el programa de instalación verifica que tanto NET Framework 3.5 como WSE 2.0 SP2 se encuentren en el equipo. Si alguno de ellos o ambos no estuvieran presentes, se instalarán automáticamente antes de que la instalación pase a la pantalla de bienvenida (deberá aceptarse el acuerdo de licencia de .NET 3.5).

Para instalar las consolas de gestión:

- 1** Haga clic en *Next* (Siguiente) para continuar.
- 2** Acepte el acuerdo de licencia y, a continuación, haga clic en *Siguiente*.
- 3** Seleccione la instalación *Típica* o *Personalizada*.

Figura 7-1 Seleccione la instalación típica o personalizada



A continuación se muestran ambas vías de instalación:

- ♦ [Sección 7.1.1, “Instalación típica”, en la página 46](#)
- ♦ [Sección 7.1.2, “Instalación personalizada”, en la página 46](#)

## 7.1.1 Instalación típica

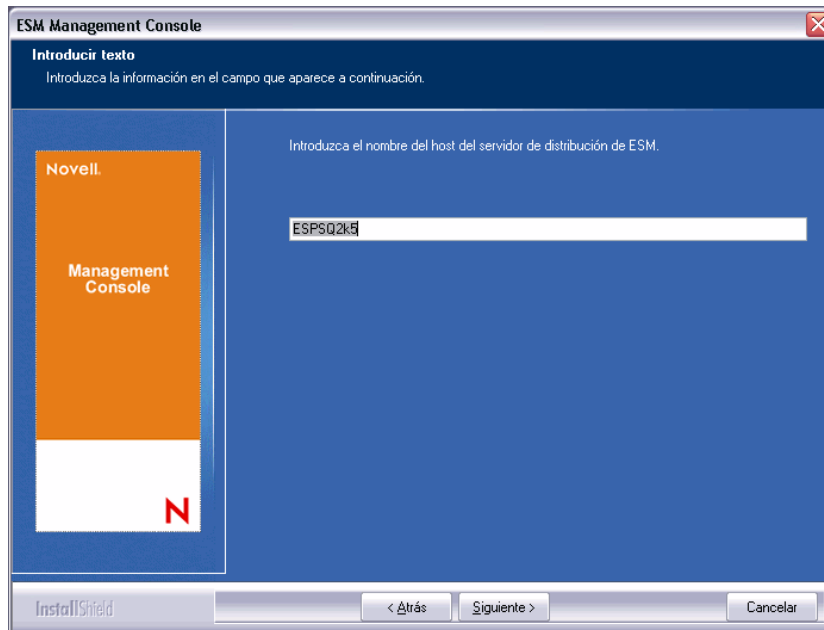
La instalación típica utiliza toda la información del servidor por defecto y de SSL que se incluye en el archivo `STInstParam.id` y utiliza el directorio por defecto: `\Archivos de programa\Novell\ESM Management Console`. No es necesario realizar ninguna selección adicional para la instalación de la consola de gestión, siempre que el directorio de los archivos de configuración de ESM se encuentre en el equipo.

## 7.1.2 Instalación personalizada

La instalación personalizada muestra los valores por defecto de `STInstParam.id` utilizados en la instalación típica y permite al administrador cambiar esta información.

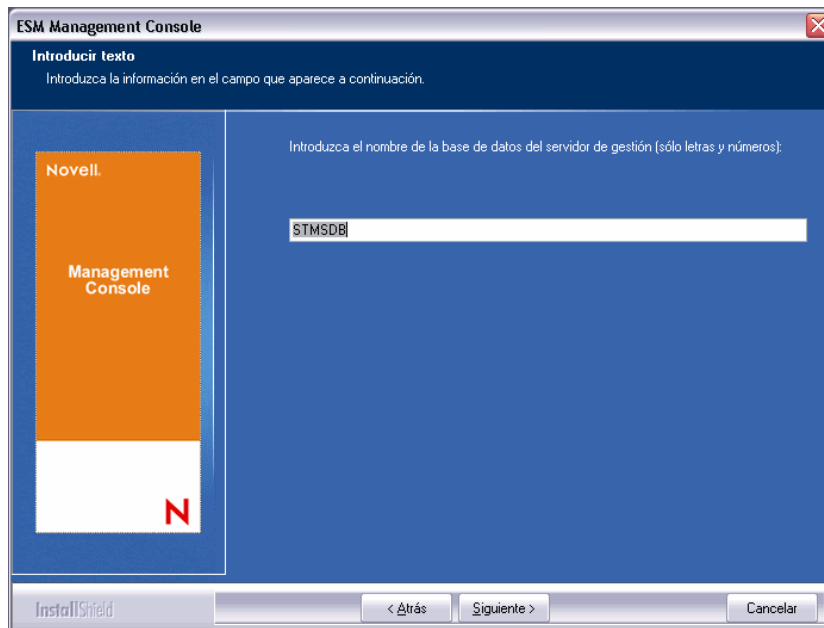
- 1 Especifique el nombre de host del Servicio de distribución de directivas (debe tratarse de un nombre de dominio completo si el servidor de distribución se ha implantado fuera del cortafuegos empresarial).

**Figura 7-2** Introduzca el nombre de host del Servicio de distribución



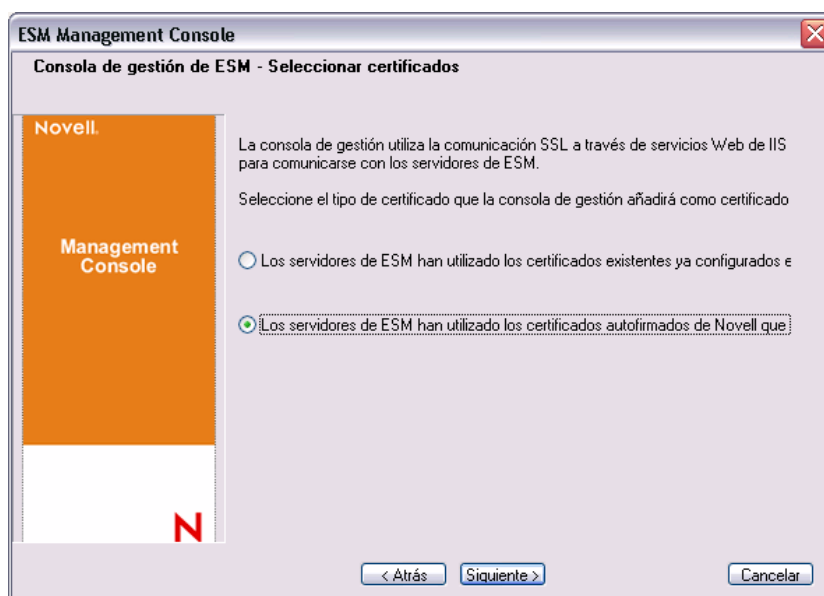
- 2 Especifique el nombre de host del Servicio de gestión.
- 3 Especifique el nombre de host de la base de datos SQL del Servicio de gestión.
- 4 Introduzca el nombre de la base de datos SQL del Servicio de gestión.

**Figura 7-3** Introduzca el nombre de la base de datos MS SQL



- 5 Especifique el nombre de usuario y la contraseña de SQL SA identificados durante la instalación del Servicio de gestión.
- 6 Seleccione el tipo de certificado de SSL instalado en el Servicio de distribución de directivas y el Servicio de gestión.

**Figura 7-4** Seleccione los certificados del servidor



- 7 Seleccione el directorio en el que se ha instalado la consola de gestión. La ubicación por defecto es `\Archivos de programa\Novell\ESM Management Console`.

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 de Endpoint Security Client 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. Para obtener más información sobre la creación y configuración del servicio de directorio, consulte [“Configuración del servicio de directorio”](#) en *Guía de administración de ZENworks Endpoint Security Management*.

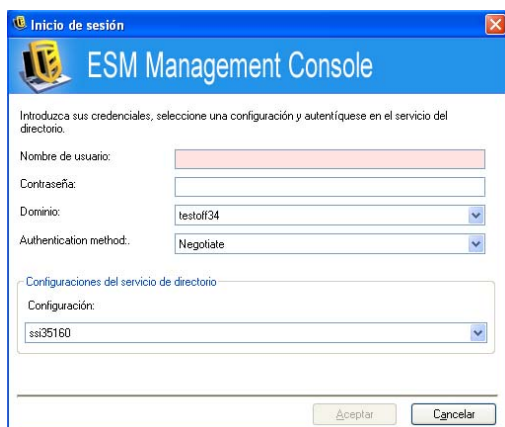
## 7.2 Inicio de la consola

Para lanzar la ventana de entrada a la consola de gestión, haga clic en *Inicio > Todos los programas > Novell > Consola de gestión de ESM > Consola de gestión*.

Para entrar en la consola, introduzca el nombre y la contraseña del administrador. Antes de poder introducir el nombre de usuario y la contraseña, debe estar conectado al dominio del servicio de directorio (consulte [Sección 7.2.1, “Adición de servicios de eDirectory”, en la página 49](#)). El nombre de usuario debe hacer referencia a un usuario que se encuentre en el dominio del Servicio de gestión.



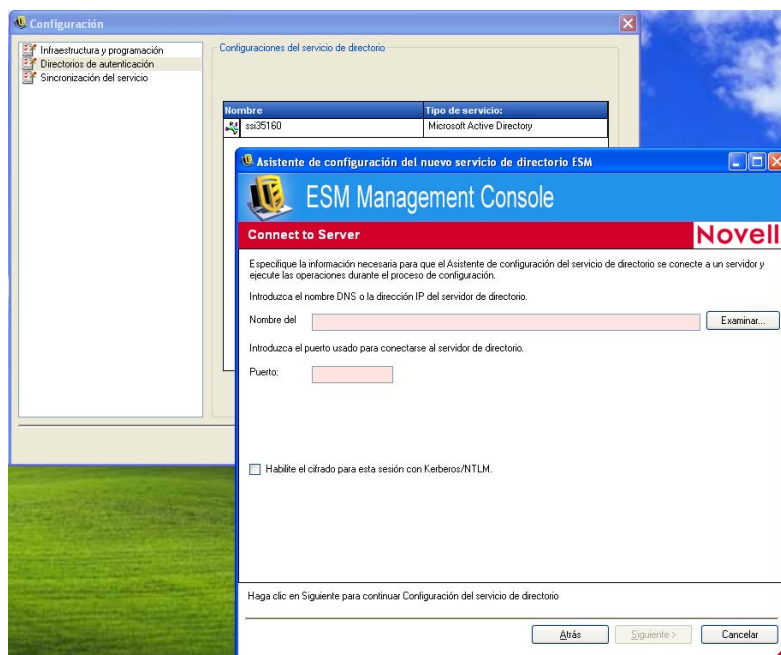
Figura 7-5 Acceda a la consola de gestión de ZENworks Endpoint Security Management



## 7.2.1 Adición de servicios de eDirectory

- 1 Haga clic en el botón *Opciones* de la pantalla de entrada para mostrar la ventana de configuración.

Figura 7-6 Autenticación de directorios



- 2 Introduzca un nombre descriptivo para el Servicio de directorio y seleccione eDirectory en la lista desplegable *Tipo de servicio*.
- 3 En el campo *Host/DN*, especifique la dirección IP del servidor de eDirectory y el nombre del árbol en *Dominio*.
- 4 Marque *Disponible para la autenticación de usuarios* para mostrar el menú desplegable de entrada.
- 5 Desactive la casilla *Autenticación segura* en las opciones de *Conexión de servicio*.

- 6 Especifique el nombre de la cuenta con el formato LDAP. Por ejemplo, en "cn=admin,o=acmeserver" "cn" es el usuario y "o" es el objeto en que está almacenada la cuenta del usuario.
- 7 Especifique la contraseña de la cuenta.

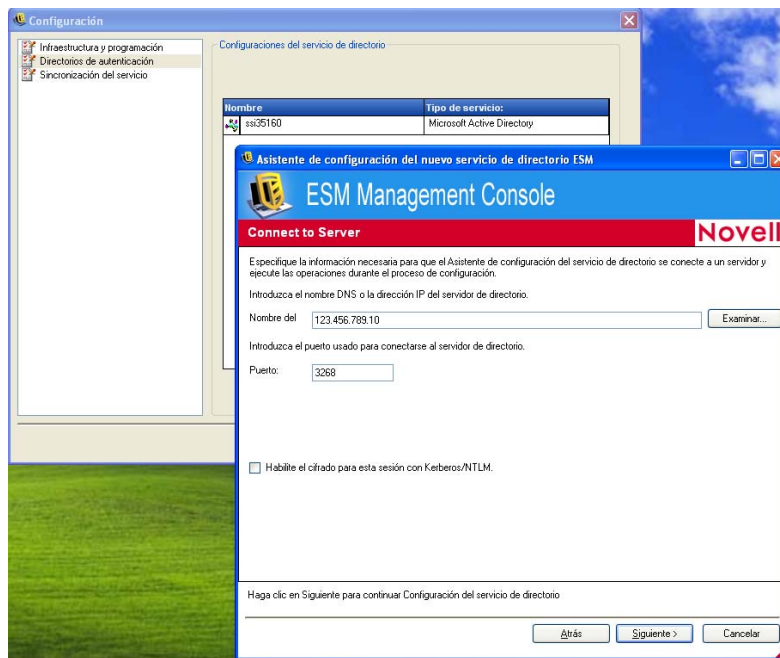
---

**Nota:** La contraseña se debe ajustar de forma que no caduque y esta cuenta nunca se debe inhabilitar.

---

- 8 Haga clic en *Probar* para verificar la comunicación con este servicio de directorio. Si no es posible establecer comunicación con él, el usuario recibe notificación del error. Siempre que sea posible, la interfaz corregirá durante la prueba toda la información que no sea precisa.

**Figura 7-7** Pantalla de directorio completado



- 9 Haga clic en *Guardar* para añadir este servicio de directorio a la base de datos y, seguidamente, haga clic en *Nuevo* para añadir otro servicio de directorio a la base de datos.
- 10 Haga clic en *Aceptar* o en *Cancelar* para salir de la ventana de configuración y volver a la pantalla de entrada.

Para obtener información sobre cómo configurar la escucha de servicios de directorio adicionales, entre los que se incluyen los servicios de Active Directory y los dominios NT compatibles, consulte *la Guía de administración de ZENworks Endpoint Security Management*.

## 7.2.2 Configuración de los ajustes de los permisos de la consola de gestión

La opción *Permisos* se encuentra en el menú *Herramientas* de la consola de gestión y sólo puede acceder a ella el administrador principal del Servicio de gestión y cualquier otro usuario al que dicho administrador haya otorgado permisos. Este control no está disponible al ejecutar la consola de gestión independiente. Para obtener más información, consulte [Capítulo 11, “Instalación no gestionada de ZENworks Endpoint Security Management”](#), en la página 81.

Los parámetros de configuración de los permisos definen el usuario o el grupo de usuarios que tiene permiso de acceso a la consola de gestión para publicar directivas y cambiar estos parámetros.

Durante la instalación del servidor de gestión, se debe introducir el nombre del administrador o la cuenta de recursos en el formulario de configuración. Una vez que se haya realizado una prueba satisfactoria y se haya guardado la información de usuario, se conceden automáticamente los permisos a dicho usuario.

Tras instalar la consola de gestión, se conceden permisos totales a todos los grupos de usuarios del dominio. El usuario del recurso debe eliminar los permisos de todos los grupos y usuarios, excepto de aquéllos que deben tener acceso. El usuario del recurso puede definir permisos adicionales para los usuarios designados. Los permisos que se otorgan tienen el siguiente resultado:

- ♦ **Acceso a la consola de gestión:** El usuario puede ver las directivas y los componentes, y editar las directivas existentes. A los usuarios a los que sólo se les haya otorgado este privilegio no se les permite añadir o suprimir directivas; y las opciones de publicación y permisos no están disponibles.
- ♦ **Publicar directiva:** El usuario puede publicar directivas sólo para los usuarios y grupos asignados.
- ♦ **Cambiar permiso:** El usuario puede acceder y cambiar los ajustes de los permisos de otros usuarios que ya se hayan definido, o bien conceder permisos a los usuarios nuevos.
- ♦ **Crear directivas:** El usuario puede crear directivas nuevas en la consola de gestión.
- ♦ **Suprimir directivas:** El usuario puede suprimir cualquier directiva de la consola de gestión.

---

**Nota:** Por motivos de seguridad, los permisos para cambiar y suprimir directivas sólo se deben otorgar al usuario del recurso o a muy pocos administradores.

---

Las secciones siguientes contienen más información sobre:

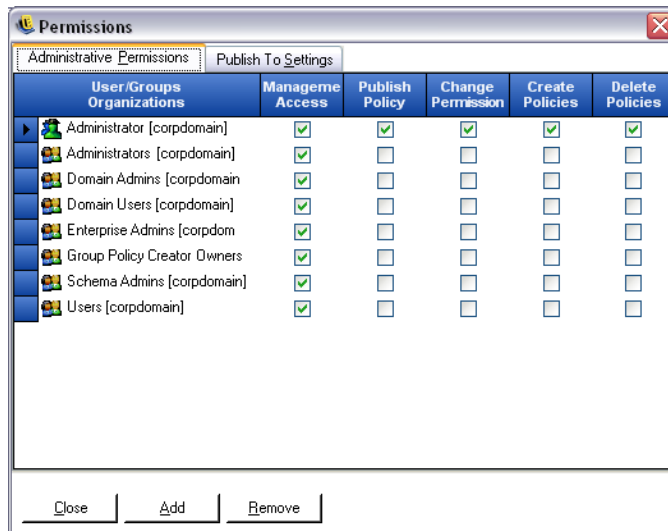
- ♦ [“Configuración de permisos administrativos” en la página 51](#)
- ♦ [“Configuración de los ajustes de Publicar en” en la página 53](#)

### Configuración de permisos administrativos

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

Se mostrarán los grupos asociados a este dominio.

**Figura 7-8** Ventana de parámetros de configuración de los permisos de la consola de gestión



**Nota:** A todos los grupos se les conceden por defecto permisos totales en la consola de gestión. Los administradores deberían desactivar la casilla de cualquiera de las tareas de directivas (o de todas) de los grupos no autorizados. Para impedir el acceso a la consola, desactive la casilla de ese permiso.

**2** (Opcional) Para cargar usuarios y grupos nuevos a esta lista:

**2a** Haga clic en el botón *Añadir* en la parte inferior de la pantalla para mostrar la tabla Organización.

**Figura 7-9** Tabla Organización de los parámetros de configuración de permisos



- 2b** Seleccione los usuarios y grupos pertinentes en la lista. Use las teclas Ctrl o Mayús para seleccionar varios usuarios.
- 2c** Cuando se hayan seleccionado todos los grupos y usuarios, haga clic en el botón *Aceptar* para añadirlos a la cuadrícula del formulario de permisos.
- 3** Asignar permisos a los usuarios y grupos disponibles.

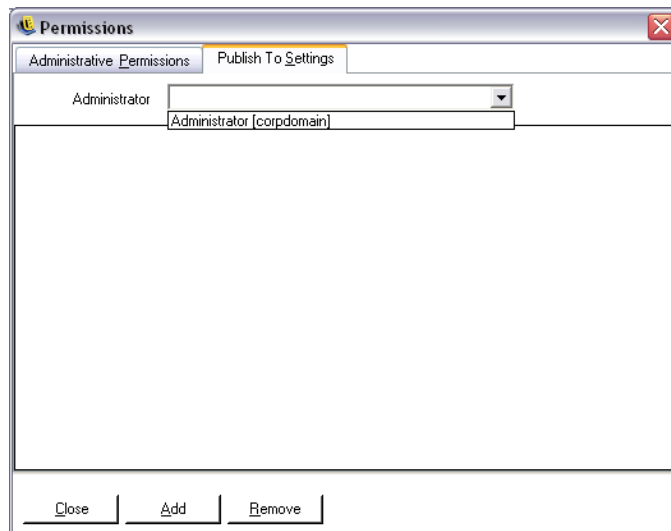
Para eliminar un usuario o grupo seleccionado, seleccione el nombre y haga clic en *Eliminar*.

### Configuración de los ajustes de Publicar en

A los usuarios y grupos que tengan la casilla *Publicar directiva* marcada se les debe asignar usuarios o grupos en los que publicar. Para definir los ajustes de Publicar en:

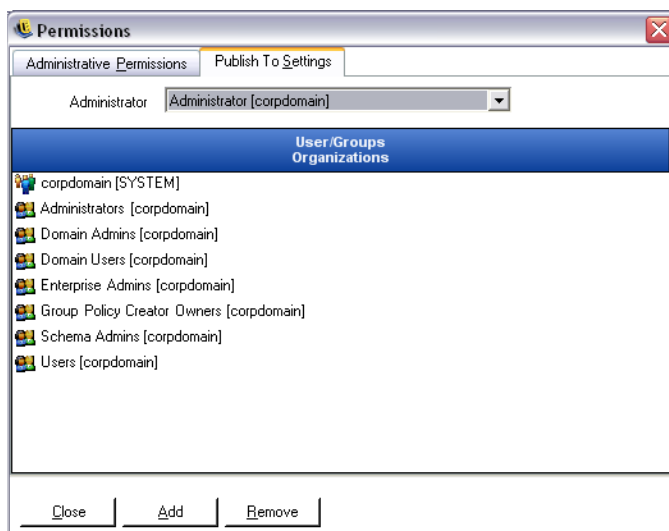
- 1** Haga clic en la pestaña *Ajustes de Publicar en*.
- 2** En la lista desplegable, seleccione los usuarios y grupos a los que se les ha otorgado el permiso de publicación.

**Figura 7-10** Parámetros de configuración de la publicación



- 3** Para asignar usuarios o grupos a este usuario o grupo:
  - 3a** Haga clic en el botón *Añadir* en la parte inferior de la pantalla para mostrar la tabla Organización.
  - 3b** Seleccione los usuarios y grupos pertinentes en la lista. Use las teclas Ctrl y Mayús para seleccionar varios usuarios.
  - 3c** Cuando se hayan seleccionado todos los usuarios/grupos, haga clic en el botón *Aceptar*.

**Figura 7-11** Lista de publicación



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

Los conjuntos de permisos se implementan de inmediato, por lo que el administrador sólo tiene que hacer clic en *Cerrar* y aceptar los cambios para volver al editor.

Al añadir un nuevo servicio de directorio, se le conceden permisos totales a la cuenta de recursos, como se describe anteriormente.

### 7.2.3 Publicación de una directiva

Para publicar una directiva de seguridad con los ajustes por defecto:

- 1 Haga clic en *Crear nueva directiva*.
- 2 Especifique un nombre para la directiva y haga clic en *Crear*.
- 3 Guarde la directiva y haga clic en la pestaña *Publicar*.
- 4 Dado que los usuarios de Endpoint Security Client deben realizar un control de entrada para aparecer en el árbol, seleccione la parte superior del árbol a la izquierda y haga doble clic para rellenar el campo de publicación con todos los grupos y usuarios actuales.
- 5 Haga clic en *Publicar* para enviar la directiva al Servicio de distribución de directivas.

La directiva generada mediante este método presenta las siguientes características:

- ♦ Se crea una única ubicación (desconocida).
- ♦ Se permite el uso de unidades de CD/DVD ROM.
- ♦ Se permite el uso de dispositivos de almacenamiento extraíbles.
- ♦ Se permiten todos los puertos de comunicaciones (incluido Wi-Fi).
- ♦ Se incluyen los parámetros de configuración del cortafuegos y la opción Todo adaptado (se permite todo el tráfico saliente a través de los puertos de red, pero no se permite el tráfico entrante no solicitado a través de los puertos de red).

Para obtener información sobre cómo crear una directiva de seguridad más sólida, consulte [la Guía de administración de ZENworks Endpoint Security Management](#).

Continúe con la [Capítulo 8, “Instalación del Servicio de seguridad de ubicación de clientes”](#), en la [página 57](#).

## 7.3 Instalación del lector USB

El lector USB de Novell que se incluye en el paquete de instalación ayuda al administrador a crear listas de dispositivos USB permitidos.

Para instalar el lector:

- 1 Para empezar la instalación, haga clic en *Configuración*
- 2 En la pantalla de bienvenida, haga clic en *Siguiente* para continuar.
- 3 Acepte la licencia y, a continuación, haga clic en *Siguiente*.
- 4 En la pantalla de información del cliente, especifique el nombre de usuario y la información de la organización pertinentes, y seleccione si a cualquiera que use ese equipo se le permite acceder al software, o bien si sólo puede acceder el usuario especificado.
- 5 Haga clic en *Instalar*.
- 6 Haga clic en *Finalizar*.

Para obtener más información sobre el uso del lector USB, consulte [la Guía de administración de ZENworks Endpoint Security Management](#).





# Instalación del Servicio de seguridad de ubicación de clientes

# 8

Este servidor sólo debería estar accesible cuando los usuarios entren en un entorno de red controlado para garantizar que se encuentran realmente en el entorno que ZENworks® Security Client ha identificado. A continuación se encuentran las instrucciones de las configuraciones de conmutación por error y las réplicas. Si se desea, el Servicio de seguridad de ubicación de clientes (CLAS) se puede implantar en el mismo servidor que aloja la instalación en un servidor único o la instalación del Servicio de gestión en varios servidores.

Instale CLAS un servidor cuyos puntos finales sólo se puedan detectar cuando se encuentren en un entorno de red que requiera una verificación criptográfica.

La implantación de CLAS en un controlador de dominio primario (PDC) no se admite por motivos de seguridad y funcionalidad.

---

**Nota:** Se recomienda configurar (reforzar) el servidor de SSI para que desactive todas las aplicaciones, los servicios, las cuentas y las demás opciones que no sean necesarias para la funcionalidad del servidor que se desea usar. Los pasos relacionados con esta tarea dependen de las características específicas del entorno local, por lo que no se pueden describir de antemano. Se recomienda a los administradores que consulten la sección adecuada de la [página Web de seguridad de Microsoft Technet](http://www.microsoft.com/technet/security/default.mspx) (<http://www.microsoft.com/technet/security/default.mspx>). En *la Guía de administración de ZENworks Endpoint Security Management*, se proporcionan recomendaciones adicionales para el control de acceso.

Para restringir el acceso sólo a los equipos de confianza, el directorio virtual e IIS se pueden configurar para que dispongan de ACL. Consulte los artículos siguientes:

- ♦ [Concesión y denegación de acceso a equipos](http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx) (<http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx>)
- ♦ [Restricción de acceso al sitio por dirección IP o nombre de dominio](http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066) (<http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066>)
- ♦ [Preguntas más frecuentes de IIS: restricciones de nombres de dominio y direcciones IP 2000](http://www.iisfaq.com/default.aspx?View=A136&P=109) (<http://www.iisfaq.com/default.aspx?View=A136&P=109>)
- ♦ [Uso del filtrado de paquetes de IIS](http://www.15seconds.com/issue/011227.htm) (<http://www.15seconds.com/issue/011227.htm>)

Por motivos de seguridad, se recomienda encarecidamente eliminar las siguientes carpetas por defecto de la instalación de IIS:

- ♦ IISHelp
- ♦ IISAdmin
- ♦ Guiones
- ♦ Printers

También es aconsejable utilizar IIS Lockdown Tool 2.1, disponible en [microsoft.com \(http://www.microsoft.com/technet/security/tools/locktool.mspx\)](http://www.microsoft.com/technet/security/tools/locktool.mspx).

La versión 2.1 está controlada por las plantillas proporcionadas para los principales productos de Microsoft que dependen de IIS. Seleccione la plantilla que coincida en mayor medida con la función de este servidor. En caso de duda, se recomienda utilizar la plantilla dinámica del servidor Web.

---

Asegúrese de que se hayan cumplido los siguientes requisitos previos antes de comenzar la instalación:

- ❑ Asegurar la resolución del nombre del servidor del Servicio de gestión (MS) en el Servicio de distribución de directivas (DS): asegúrese de que el equipo de destino en el que se haya instalado MS puede hacer "ping" en el nombre del servidor de DS (NETBIOS si DS se ha configurado dentro del cortafuegos de red o FQDN si se ha instalado fuera, en la DMZ).
- ❑ Habilite o instale los Servicios de Internet Information Server (IIS) de Microsoft y asegúrese de que ASP.NET esté habilitado.

---

**Importante:** No habilite el recuadro de verificación *Requerir canal seguro (SSL)* en la página Comunicaciones seguras (en la utilidad Administración de equipos de Microsoft, expanda *Servicios y aplicaciones > Administrador de Internet Information Services (ISS) >* , a continuación, expanda también *Sitios web >* haga clic con el botón derecho en *Sitio web predeterminado >* haga clic en *Propiedades >* a continuación, en la pestaña *Seguridad de directorios >* y, por último, en el botón *Editar* en el recuadro del grupo de Comunicaciones seguras). Al habilitar esta opción, se interrumpe la comunicación entre el servidor de ZENworks Endpoint Security Management y el cliente de ZENworks Endpoint Security en el puesto final.

---

Haga clic *Instalación del Servicio de seguridad de ubicación de clientes* en el menú de interfaz de instalación. Comienza la instalación de CLAS.

Al lanzarse, el programa de instalación verifica si todo el software necesario se encuentra en el servidor. Si falta algún componente de software, se instala automáticamente antes de que la instalación pase a la pantalla de bienvenida (es posible que sea necesario aceptar los acuerdos de licencia del software adicional). Si Microsoft Data Access Components 2.8 no está instalado, el servidor se tiene que reiniciar después de dicha instalación para que la instalación de ZENworks Endpoint Security Management pueda continuar. Si usa Windows 2003 Server, ASP.NET 2.0 se configura para que lo ejecute el programa de instalación.

## 8.1 Pasos de instalación

Para instalar CLAS y generar una clave de licencia:

- 1 Haga clic en *Siguiente* en la pantalla de bienvenida para continuar.
- 2 Acepte el acuerdo de licencia y, a continuación, haga clic en *Siguiente*.
- 3 La instalación copia los archivos en el directorio por defecto: `\Archivos de programa\Novell\ESM CLAS`.

- 4 La instalación del Servicio de seguridad de ubicación del cliente genera dos claves: una pública y otra privada. El archivo de clave pública se puede almacenar en el escritorio o en otro directorio. Si desea almacenar el archivo de clave pública en otro directorio, haga clic en *Sí* y desplácese a la carpeta que desee. Haga clic en *No* para aceptar el valor por defecto y almacenar el archivo de clave pública junto con el de clave privada.
- 5 Haga clic en *Finalizar* para cerrar el programa de instalación.

El Servicio de gestión debe poder acceder a la clave pública.

## 8.2 Instalaciones de conmutación por error de CLAS

Se pueden instalar varias iteraciones de CLAS en los servidores de toda la empresa, bien para proteger de forma criptográfica varias ubicaciones empresariales, bien para garantizar que, en caso de que el servidor de CLAS principal deje de funcionar, aún se pueda proteger la ubicación.

En el caso de la segunda situación, la clave privada se ubica en función de la URL, en lugar de la dirección IP. Por tanto, se puede configurar un bloque de servidores para compartir una única URL. CLAS se puede instalar en un único servidor; a continuación y, a continuación, la imagen de ese servidor se puede copiar en cada servidor adicional, o bien instalarse en cada servidor de forma independiente, y las claves pública y privada se pueden copiar en otros servidores. Todos los servidores de un bloque de URL deben tener las mismas claves públicas y privadas.

## 8.3 Transferencia de la clave pública al Servicio de gestión

Una vez completada la instalación, la clave pública generada, que se transfiere mediante la directiva de seguridad a Endpoint Security Client, se encuentra en el directorio `\Archivos de programa\Novell\Novell ESM CLAS` del servidor. La clave pública se identifica mediante el nombre de archivo `publickey`. Este nombre de archivo se puede cambiar a cualquier nombre deseado.

A continuación, el archivo de clave pública debe copiarse y transferirse al servicio de gestión (en cualquier parte del servicio), lo que permite que la consola de gestión acceda a la clave y la distribuya a todos los clientes de Endpoint Security Client mediante una directiva de seguridad. El archivo de clave pública también se puede cargar en un equipo que utilice una consola de gestión de ZENworks Endpoint Security Management.

Continúe con la [Capítulo 9, “Instalación de Endpoint Security Client 3.5”](#), en la página 61.



# Instalación de Endpoint Security Client 3.5

# 9

Use Novell ZENworks Endpoint Security Client 3.5 para clientes de Windows XP (SP1 y SP2) y de Windows 2000 SP4. Haga clic en el programa de instalación de *ZENworks Security Client* apropiado en el menú de interfaz de la instalación. Comienza la instalación de Endpoint Security Client. En las siguientes páginas, se describe el proceso de instalación básico y de MSI.

- La instalación básica sólo instala Endpoint Security Client 3.5 en el equipo actual.
- En la instalación de MSI, se lanza el programa de instalación en el modo administrativo (/a) y se crea un paquete de software MSI. A continuación, este paquete puede transferirse o ponerse a disposición de los usuarios en una ubicación de red específica con las entradas de usuario necesarias configuradas previamente. De esta forma, se permitirá a los usuarios instalar el software con los valores predefinidos del servidor.

## 9.1 Instalación básica de Endpoint Security Client 3.5

Este procedimiento sólo instala Endpoint Security Client 3.5 en el equipo actual.

Compruebe que todas las revisiones de seguridad para Microsoft y el software antivirus estén instaladas y actualizadas.

Instale los certificados raíz SSL del Servicio de gestión en el equipo local (ESM-MS.cer o el certificado empresarial).

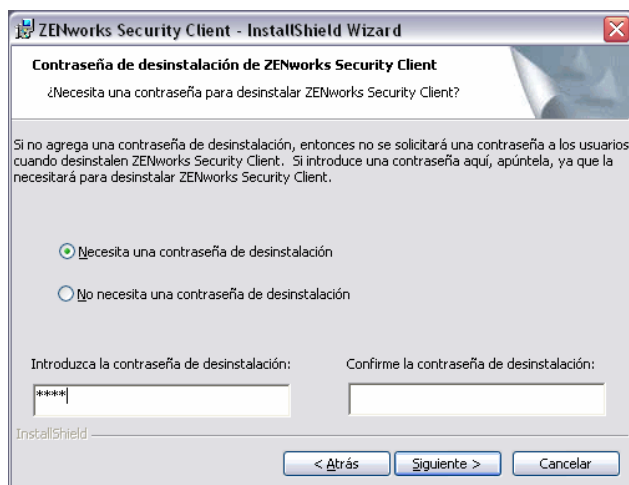
---

**Nota:** Durante la instalación de Endpoint Security Client 3.5, se recomienda cerrar el software antivirus y los programas espía que interactúen con las funciones del registro válidas.

---

- 1 Haga clic en *Siguiente* en la pantalla de bienvenida para continuar.
- 2 Acepte el acuerdo de licencia y, a continuación, haga clic en *Siguiente*.
- 3 Introduzca una contraseña de instalación. De esta forma, se impide que el usuario desinstale Endpoint Security Client 3.5 mediante la opción *Agregar o quitar programas* (opción recomendada).

**Figura 9-1** Contraseña de desinstalación



- 4 Seleccione cómo se recibirán las contraseñas: desde el Servicio de distribución para los clientes administrados o, de forma local, para una configuración no administrada (consulte [Capítulo 11, “Instalación no gestionada de ZENworks Endpoint Security Management”](#), en la página 81 para obtener información sobre la opción no administrada).

**Figura 9-2** Parámetros de configuración de gestión



- 5 Especifique la información del Servicio de gestión.
- 6 Seleccione si se deben recibir directivas para los usuarios o para el equipo (directivas basadas en equipos).

**Figura 9-3** Directivas basadas en usuarios o equipos



7 Haga clic en *Instalar*.

Una vez instalado el software, se solicita al usuario que reinicie el equipo.

---

**Nota:** Puede copiar de forma opcional el certificado del Servicio de gestión en una carpeta, junto al archivo `setup.exe`, antes de ejecutar la instalación. Esto instala automáticamente el certificado en el equipo (por ejemplo, para todos los usuarios). Este proceso también se puede llevar a cabo con la licencia de Novell.archivo `dat`.

---

## 9.2 Instalación de MSI

Este procedimiento crea un paquete de MSI para Endpoint Security Client 3.5. Este paquete lo utiliza un administrador del sistema para publicar la instalación en un grupo de usuarios mediante una directiva de Active Directory o mediante otros métodos de distribución de software.

Para crear el paquete MSI:

Si va a realizar la instalación desde el programa de instalación principal ISO o del CD y no tiene intención de ejecutar ninguna variable de la línea de comando (consulte [Sección 9.2.1, “Variables de línea de comando”](#), en la página 66):

- 1 Inserte el CD y espere a que se lance el programa de instalación principal.
- 2 Haga clic en *Instalación del producto*.
- 3 Haga clic en *Cliente de seguridad*.
- 4 Haga clic en *Crear paquete MSI para ZSC*.

Si sólo utiliza el archivo `setup.exe` para la instalación (el archivo ejecutable se puede encontrar en el siguiente directorio del CD: `D:\ESM32\ZSC`), realice, en primer lugar, lo siguiente:

- 1 Haga clic con el botón derecho del ratón en `setup.exe`.
- 2 Seleccione *Crear acceso directo*.
- 3 Haga clic con el botón derecho en el acceso directo y, a continuación, haga clic en *Propiedades*.

- 4 Al final del campo Destino, después de las comillas, haga clic en la barra espaciadora una vez y escriba /a.

Por ejemplo: "C:\Documents and Settings\euser\Desktop\CL-Release-3.2.455\setup.exe" /a

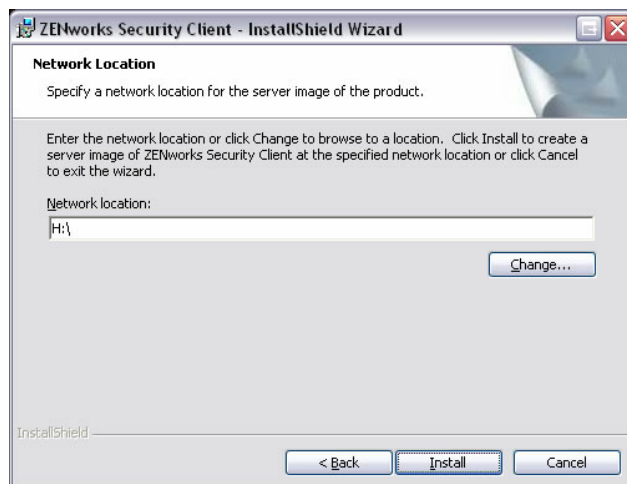
Hay varias variables de línea de comandos disponibles para la instalación de MSI; para obtener más información al respecto, consulte [Sección 9.2.1, "Variables de línea de comando"](#), en la [página 66](#).

- 5 Haga clic en *Aceptar*.
- 6 Haga doble clic en el acceso directo para lanzar el programa de instalación de MSI.

Cuando la instalación comience:

- 1 Para continuar, haga clic en *Siguiente* en la pantalla de bienvenida.
- 2 Acepte el acuerdo de licencia y, a continuación, haga clic en *Siguiente*.
- 3 Seleccione si es necesaria una contraseña de desinstalación (opción recomendada) e introduzca la contraseña.
- 4 Seleccione cómo se recibirán las contraseñas: desde el Servicio de distribución para los clientes administrados o, de forma local, para una configuración no administrada. Si se selecciona la configuración administrada:
  - ♦ Especifique la información del Servicio de gestión (FQDN o NETBIOS, según el método de entrada durante la instalación del Servicio de gestión).
  - ♦ Seleccione si se utilizarán directivas basadas en usuarios o equipos.
- 5 (Opcional) Especifique una dirección de correo electrónico en el campo que se proporciona con el fin de recibir una notificación si la instalación no se realiza correctamente.
- 6 Especifique la ubicación de red en la que se crea la imagen de MSI o desplácese a dicha ubicación haciendo clic en el botón *Cambiar*.

**Figura 9-4** Seleccione la ubicación de red para la imagen de MSI

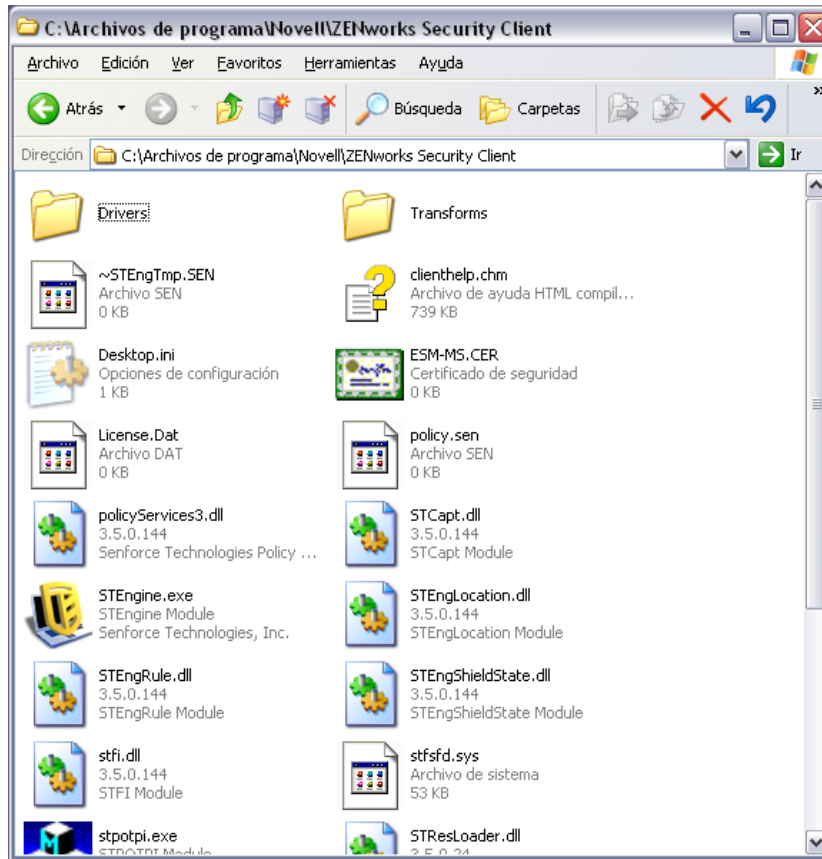


- 7 Para crear la imagen de MSI, haga clic en *Instalar*.



- 8 Desplácese a la imagen de MSI creada y abra la carpeta "`\Archivos de programa\Novell\ZENworks Security Client\`"
- 9 Copie el certificado SSL del Servicio de gestión (ESM-MS.cer o el certificado empresarial y la clave de licencia de Novell en esta carpeta, sustituyendo los archivos de 0 kb por defecto que se encuentran actualmente en ella. El certificado SSL de ESM-MS está disponible en la carpeta de los archivos de configuración de ZENworks Endpoint Security Management. La clave de licencia se le enviará por separado por correo electrónico (si está utilizando la versión de evaluación de 30 días de duración, no es necesario que utilice ninguna clave de licencia).

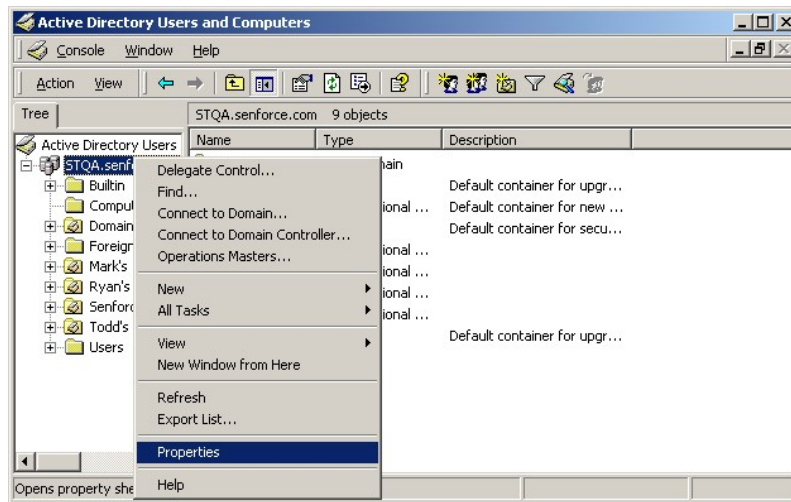
**Figura 9-5** *Sustituya los archivos por defecto del paquete de MSI*



Para definir el paquete MSI para que se transfiera a los grupos de usuarios como una directiva de grupo:

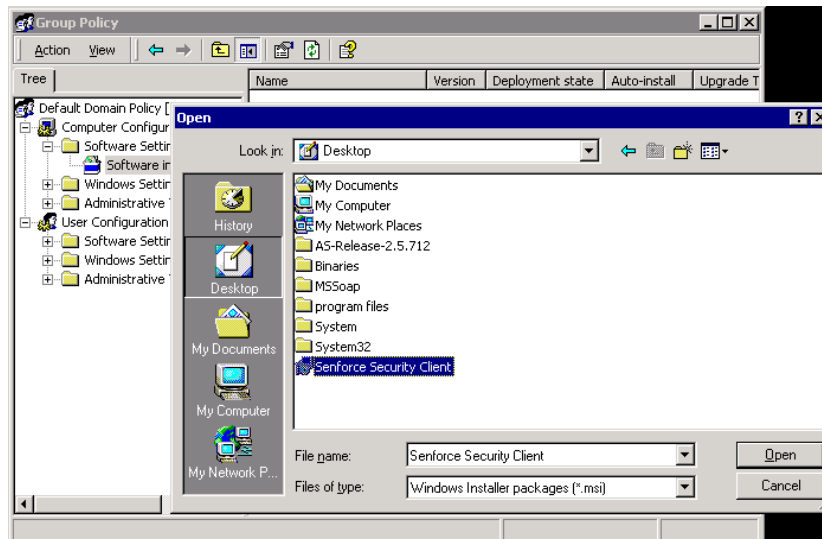
- 1 Abra *Herramientas administrativas (Usuarios y equipos de Active Directory)* y abra *Dominio raíz* o *Propiedades de OU*.

Figura 9-6 Abra la opción Propiedades en OU o Dominio raíz



- 2 Haga clic en la pestaña *Directiva de grupo* y haga clic en *Editar*.
- 3 Añada el paquete de MSI a la configuración del equipo.

Figura 9-7 Seleccione el paquete de MSI que desea añadir



## 9.2.1 Variables de línea de comando

Hay disponibles opciones de variables de línea de comando para la instalación de MSI. Estas variables deben definirse en el acceso directo del archivo ejecutable que se configura para ejecutarse en el modo de administrador. Para utilizar una variable, debe escribirse la siguiente línea de comando en el acceso directo de MSI:

"...\setup.exe" /a /V"variables". Introduzca entre comillas cualquiera de los comandos mostrados a continuación. Separe las diversas variables con un único espacio.

Ejemplo: `setup.exe /a /V"STDRV=stateful STBGL=1"` crea un paquete de MSI en el que Endpoint Security Client 3.5 se arrancará en el modo Con estado y con la aplicación estricta de una lista blanca.

**Nota:** El arranque con estado puede provocar ciertos problemas de interoperabilidad (retrasos de las direcciones DHCP, problemas de interoperabilidad con la red Novell, etc.).

Están disponibles las siguientes variables de línea de comando:

**Tabla 9-1** Variables de línea de comando

Variable de línea de comando	Descripción	Notas
STDRV=con estado	El controlador NDIS presenta el modo Con estado durante el arranque.	Cambie el estado por defecto del controlador NDIS de "Todo abierto" a "Con estado", permitiendo el tráfico de red durante el arranque hasta que Endpoint Security Client 3.5 haya determinado su ubicación.
/qn	Instalación silenciosa.	Utilice esta opción para suprimir el proceso de instalación típica de MSI. Endpoint Security Client 3.5 se activará la próxima vez que el usuario reinicie el sistema.
STRBR=ReallySuppress	No es necesario reiniciar el sistema una vez completada la instalación.	La aplicación de seguridad y la autodefensa del cliente serán completamente funcionales después reiniciar por primera vez.
STBGL=1	Ejecución estricta de la lista blanca en el control de aplicaciones.	DEBE crearse una directiva que identifique la aplicación en la lista blanca y distribuirse con esta directiva.
STUPGRADE=1	Actualizar Endpoint Security Client 3.5.	Se usa al actualizar Endpoint Security Client 3.5.
STUNINSTALL=1	Desinstalar Endpoint Security Client 3.5.	Se usa al desinstalar Endpoint Security Client 3.5.
STUIP="la contraseña"	Permite realizar una desinstalación con contraseña.	Utilice esta opción cuando la contraseña de desinstalación esté activa.
STNMS="Nombre de MS"	Permite cambiar el nombre del Servicio de gestión.	Cambia el nombre del servicio de gestión de Endpoint Security Client 3.5.
POLICYTYPE=1	Cambiar Endpoint Security Client 3.5 a directivas basadas en equipos.	Use esta opción para que los clientes de Endpoint Security Client instalados en MSI acepten las directivas basadas en equipos en lugar de las basadas en usuarios.

Variable de línea de comando	Descripción	Notas
POLICYTYPE=2	Cambiar Endpoint Security Client 3.5 a directivas basadas en usuarios.	Use esta opción para que los clientes de Endpoint Security Client instalados en MSI acepten las directivas basadas en usuarios en lugar de las basadas en equipos.
STVA="Nombre del adaptador"	Permite añadir un adaptador virtual.	Utilice esta opción para activar el control de directivas a través de un adaptador virtual
/L*v c:\log.txt	Permite activar el registro.	Utilice esta opción para activar el registro durante la instalación. De lo contrario, este proceso tendrá que realizarse mediante las herramientas de diagnóstico de Endpoint Security Client (consulte el Manual del administrador).

## 9.2.2 Distribución de una directiva con el paquete de MSI

La directiva por defecto incluida en la instalación de MSI puede sustituirse por una directiva configurada en la empresa. Para transferir una directiva concreta con la imagen de MSI:

- 1 Cree una directiva que se vaya a distribuir a todos los usuarios a través de la consola de gestión (para obtener más información sobre la creación de directivas, consulte *la Guía de administración de ZENworks Endpoint Security Management*).
- 2 Exporte la directiva y guárdela como `policy.sen`.

---

**Nota:** A todas las directivas distribuidas de esta forma (no gestionada) se les debe asignar el nombre `policy.sen` para que Endpoint Security Client 3.5 las acepte. Endpoint Security Client 3.5 no implementa las directivas a las que no se les haya asignado el nombre `policy.sen`.

---

- 3 Abra la carpeta a la que se ha exportado la directiva y copie los archivos `policy.sen` y `setup.sen`.
- 4 Desplácese a la imagen de MSI creada y abra la carpeta "`\Archivos de programa\Novell\ZENworks Security Client\`".
- 5 Pegue los archivos `policy.sen` y `setup.sen` en la carpeta. Esto sustituirá los archivos por defecto `policy.sen` y `setup.sen`.

## 9.2.3 Instalación de usuario de Endpoint Security Client 3.5 desde MSI

Cuando el usuario vuelva a autenticarse en el dominio (mediante el reinicio del equipo), el paquete de instalación MSI se ejecutará antes de entrar a la sesión. Una vez que la instalación de MSI haya finalizado, el equipo se reiniciará y al usuario podrá entrar en él. Endpoint Security Client 3.5 está instalado y ejecutándose en el equipo.

## 9.3 Ejecución de Endpoint Security Client 3.5

Endpoint Security Client 3.5 se ejecuta automáticamente durante el inicio del sistema. Para obtener más información sobre Endpoint Security Client 3.5, consulte *la Guía de usuario de ZENworks Endpoint Security Client 3.5*.

La Guía de usuario puede distribuirse a todos los usuarios para ayudarles a conocer de forma más precisa el funcionamiento de su nuevo software de seguridad final.



# Instalación de ZENworks Endpoint Security Client 4.0

# 10

Novell® ZENworks® Endpoint Security Client 4.0 es la nueva versión cliente compatible con los sistemas operativos Microsoft Windows Vista con Service Pack 1 y Windows Server 2008 que se ejecutan en modo de 32 bits. Endpoint Security Client 4.0 utiliza la consola de gestión y el servidor de ZENworks Endpoint Security Management 3.5. Ahora puede gestionar Windows XP con el cliente 3.5 y Windows Vista con el cliente 4.0.

En las siguientes páginas, se describe el proceso de instalación básico y de MSI.

La instalación básica sólo instala Endpoint Security Client 4.0 en el equipo actual.

En la instalación de MSI, se lanza el programa de instalación en el modo administrativo (/a) y se crea un paquete de software MSI. A continuación, este paquete puede transferirse o ponerse a disposición de los usuarios en una ubicación de red específica con las entradas de usuario necesarias configuradas previamente. De esta forma, los usuarios podrán instalar el software con los valores predefinidos del servidor.

- ♦ [Sección 10.1, “Instalación básica de Endpoint Security Client 4.0”, en la página 71](#)
- ♦ [Sección 10.2, “Instalación de MSI”, en la página 74](#)
- ♦ [Sección 10.3, “Ejecución de Endpoint Security Client 4.0”, en la página 78](#)
- ♦ [Sección 10.4, “Funciones incompatibles con Endpoint Security Client 4.0”, en la página 79](#)

## 10.1 Instalación básica de Endpoint Security Client 4.0

Este procedimiento sólo instala ZENworksEndpoint Security Client 4.0 en el equipo actual.

### Antes de empezar:

- ♦ Compruebe que todas las revisiones de seguridad para Microsoft y el software antivirus estén instaladas y actualizadas. El software Endpoint Security Client 4.0 se puede instalar en los sistemas operativos Windows Vista con Service Pack 1 y Windows Server 2008 que se ejecutan en modo de 32 bits.
- ♦ Durante la instalación de Endpoint Security Client 4.0, Novell recomienda cerrar cualquier antivirus y programas antispyware a que interactúen con las funciones del registro válidas.
- ♦ El cliente gestionado de Endpoint Security Client necesita comunicarse mediante SSL con el componente del servicio de gestión de ZENworks Endpoint Security. Si, durante la instalación del servidor único o del servicio de gestión, ha seleccionado "certificados autofirmados", el puesto final que se ejecuta en Security Client debe tener instalado el certificado en el contexto adecuado (preferiblemente en el contexto del equipo local).

Para realizarlo de forma automática, coloque el archivo `ESM-MS.cer` en la carpeta en la que se encuentra el archivo `Setup.exe` del programa de instalación de Endpoint Security Client. De manera opcional, puede copiar la carpeta completa `archivos de configuración de ESM` de la instalación del servicio de gestión (o de la instalación del servidor único) en la

carpeta con el programa de instalación de Endpoint Security Client Setup.exe (asegúrese de que ESM-MS.cert se encuentra en la carpeta archivos de configuración de ESM y de que se llama archivos de configuración de ESM). Esto instala automáticamente el certificado en el equipo (por ejemplo, para todos los usuarios). Este proceso también se puede llevar a cabo con la licencia de Novell.archivo dat.

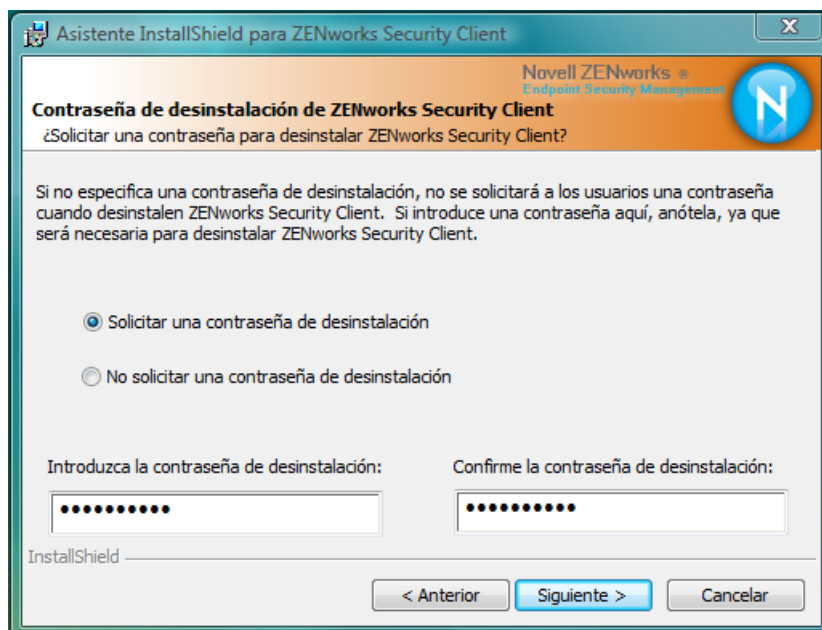
Seleccione el directorio del programa de instalación de *ZENworks Security Client* apropiado en el menú de interfaz de la instalación.

- 1** Para comenzar con el proceso de instalación, haga doble clic en Setup.exe.
- 2** Seleccione el idioma que desea para la instalación y después haga clic en *Aceptar*.

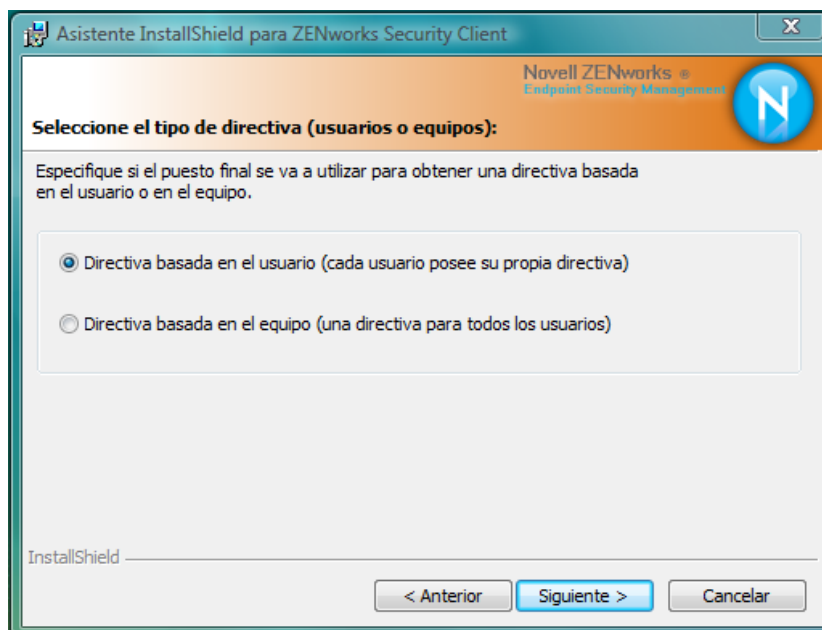
Puede elegir entre los siguientes idiomas:

- ♦ Chino simplificado
  - ♦ Chino tradicional
  - ♦ Inglés (por defecto)
  - ♦ Francés
  - ♦ Alemán
  - ♦ Italiano
  - ♦ Japonés
  - ♦ Portugués
  - ♦ Español tradicional
- 3** Endpoint Security Client 4.0 necesita que tenga instalado en su equipo Microsoft Web Services Enhancements (WSE) 2.0 con Service Pack 3 y Microsoft Visual C++ 2008 antes de comenzar con la instalación del cliente. Si, durante el proceso de instalación, no se detectan estos componentes, verá esta pantalla. Haga clic en *Instalar* para instalar estos requisitos.
  - 4** Si todavía no los ha instalado, cierre el software antivirus y los programas espía antes de presionar *Siguiente* en la pantalla de bienvenida.
  - 5** Acepte el acuerdo de licencia y, a continuación, haga clic en *Siguiente*.





- 6 Seleccione *Requerir contraseña de desinstalación*. De esta manera, se impide que el usuario desinstale Endpoint Security Client 4.0 (opción recomendada).
- 7 Agregue una contraseña de desinstalación, confirmela y, a continuación, haga clic en *Siguiete*.

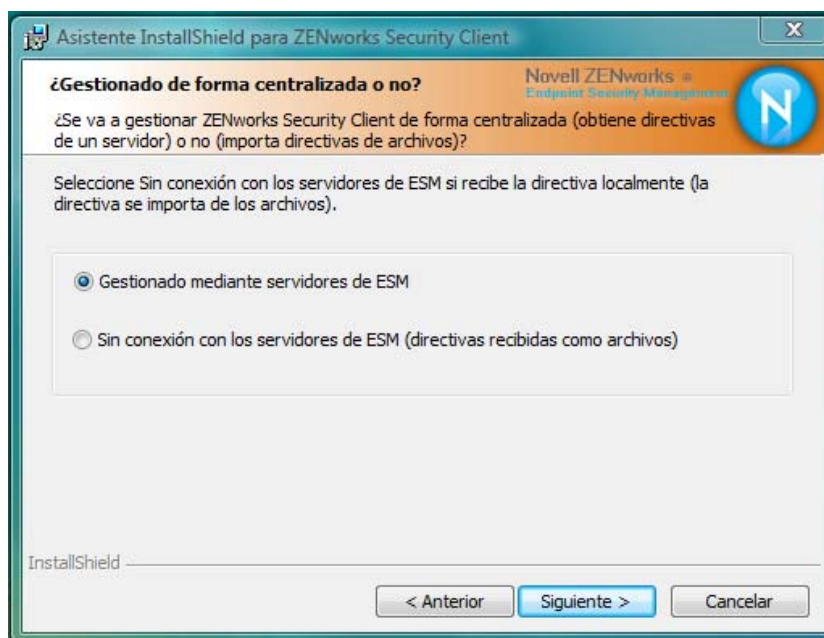


- 8 Seleccione un tipo de directiva (ya sea una directiva basada en usuarios, donde cada usuario tiene una directiva individual, o basada en equipos, donde todos los usuarios utilizan la misma directiva). Haga clic en *Siguiete*.

---

**Nota:** Seleccione la directiva basada en usuarios si su red utiliza eDirectory como su servicio de directorio. eDirectory no es compatible con las directivas basadas en equipos.

---



- 9 Seleccione de qué manera se recibirán las directivas (gestionada a través de servidores de ESM para clientes gestionados o recuperada localmente para una configuración (independiente) no gestionada. Haga clic en *Siguiente*.

Para obtener más información sobre una instalación no gestionada, consulte [Capítulo 11, “Instalación no gestionada de ZENworks Endpoint Security Management”](#), en la página 81.

- 10 (Opcional) Si ha seleccionado *Gestionar a través de servidores de ESM* en [Paso 9](#), escriba el nombre del servidor compatible con el servicio de gestión.

El nombre del servidor introducido debe coincidir con el nombre incluido en "Emitido para" en el certificado de raíz de confianza utilizado en el servidor en el que instaló el servidor único o el servicio de gestión de ZENworks Endpoint. Debe ser el nombre NETBIOS o el nombre de dominio completo (FQDN) del servidor que ejecuta el componente del servicio de gestión de ZENworks Endpoint. Una vez introducido el nombre, haga clic en *Siguiente*.

- 11 Haga clic en *Instalar* para comenzar la instalación.

- 12 Una vez instalado el software, reinicie el equipo cuando se le solicite.

Para obtener una lista de las funciones del cliente 4.0 que no están disponibles para Vista, consulte [Sección 10.4, “Funciones incompatibles con Endpoint Security Client 4.0”](#), en la página 79.

## 10.2 Instalación de MSI

Este procedimiento crea un paquete de MSI para Endpoint Security Client 4.0. Este paquete lo utiliza un administrador del sistema para publicar la instalación en un grupo de usuarios mediante una directiva de Active Directory o mediante otros métodos de distribución de software.

- ♦ [Sección 10.2.1, “Uso del programa de instalación principal”](#), en la página 75
- ♦ [Sección 10.2.2, “Uso del archivo Setup.exe”](#), en la página 75
- ♦ [Sección 10.2.3, “Finalización de la instalación”](#), en la página 75

- ♦ [Sección 10.2.4, “Variables de línea de comando”, en la página 77](#)
- ♦ [Sección 10.2.5, “Distribución de una directiva con el paquete de MSI”, en la página 78](#)

## 10.2.1 Uso del programa de instalación principal

Si va a realizar la instalación desde el programa de instalación principal ISO o desde el CD, y no tiene intención de ejecutar ninguna variable de la línea de comando:

- 1 Inserte el CD y espere a que se lance el programa de instalación principal.
- 2 Haga clic en *Instalación del producto*.
- 3 Haga clic en *Cliente de seguridad*.
- 4 Haga clic en *Crear paquete MSI para ZSC*.
- 5 Continúe con [Sección 10.2.3, “Finalización de la instalación”, en la página 75](#).

## 10.2.2 Uso del archivo Setup.exe

Si sólo utiliza el archivo `setup.exe` para la instalación:

- 1 Haga clic con el botón derecho del ratón en `setup.exe`.  
El archivo ejecutable se puede encontrar en el CD en `D:\ESM32\ZSC`.
- 2 Seleccione *Crear acceso directo*.
- 3 Haga clic con el botón derecho en el acceso directo y, a continuación, haga clic en *Propiedades*.
- 4 Al final del campo *Destino*, después de las comillas, presione la barra espaciadora una vez y escriba `/a`.  
Por ejemplo: `"C:\Documents and Settings\user\Desktop\CL-Release-3.2.455\setup.exe" /a`  
Hay varias variables de línea de comandos disponibles para la instalación de MSI. Consulte [Sección 9.2.1, “Variables de línea de comando”, en la página 66](#) para obtener más información.
- 5 Haga clic en *Aceptar*.
- 6 Haga doble clic en el acceso directo para lanzar el programa de instalación de MSI.
- 7 Continúe con [Sección 10.2.3, “Finalización de la instalación”, en la página 75](#).

## 10.2.3 Finalización de la instalación

Finalice [Uso del programa de instalación principal](#) o [Uso del archivo Setup.exe](#) y después utilice este procedimiento para terminar de instalar el cliente.

- 1 Para continuar, haga clic en *Siguiente* en la pantalla de bienvenida.
- 2 Seleccione *Requerir contraseña de desinstalación* (opción recomendada) e introduzca la contraseña. Haga clic en *Siguiente*.

---

**Nota:** Si desinstala Endpoint Security Client con un paquete de MSI, debe especificar la contraseña de desinstalación mediante las propiedades de MSI (consulte [Tabla 10-1 en la página 77](#)).

---

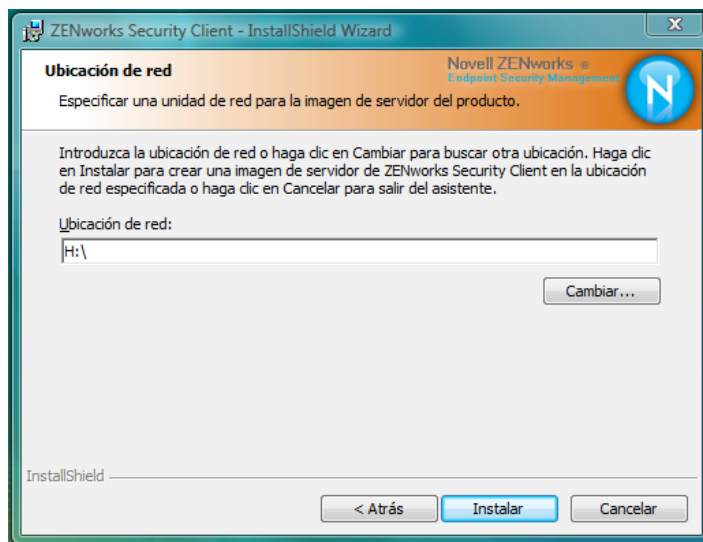
- 3 Seleccione un tipo de directiva (ya sea una directiva basada en usuarios, donde cada usuario tiene una directiva individual, o basada en equipos, donde todos los usuarios utilizan la misma directiva). Haga clic en *Siguiente*.

---

**Nota:** Seleccione la directiva basada en usuarios si su red utiliza eDirectory como su servicio de directorio. eDirectory no es compatible con las directivas basadas en equipos.

---

- 4 Seleccione de qué manera se recibirán las directivas (gestionada a través de servidores de ESM para clientes gestionados o recuperada localmente para una configuración (independiente) no gestionada).
- 5 (Opcional) Si ha seleccionado *Gestionar a través de servidores de ESM* en **Paso 4**:
  - ♦ El nombre del servidor introducido debe coincidir con el nombre incluido en "Emitido para" en el certificado de raíz de confianza utilizado en el servidor en el que instaló el servidor único o el servicio de gestión de ZENworks Endpoint. Debe ser el nombre NETBIOS o el nombre de dominio completo (FQDN) del servidor que ejecuta el componente del servicio de gestión de ZENworks Endpoint.
- 6 (Opcional) Especifique una dirección de correo electrónico en el campo que se proporciona con el fin de recibir una notificación si la instalación no se realiza correctamente.
- 7 Especifique la ubicación de red en la que desea que se cree la imagen de MSI o desplácese a dicha ubicación haciendo clic en el botón *Cambiar*.



- 8 Para crear la imagen de MSI, haga clic en *Instalar*. Haga clic en *Finalizar* para cerrar el programa de instalación.
- 9 Desplácese a la ubicación donde se ha creado la imagen de MSI y abra la carpeta \Archivos de programa\Novell ZENworks\Endpoint Security Client\.
- 10 Copie el certificado SSL del servicio de gestión (ESM-MS .cer o el certificado empresarial) y la clave de licencia de Novell en esta carpeta, sustituyendo los archivos de 0 KB por defecto que se encuentran actualmente en ella.

El certificado SSL de ESM-MS está disponible en la carpeta de los archivos de configuración de ZENworks Endpoint Security Management. La clave de licencia se envía por separado mediante correo electrónico. Si está utilizando la versión de evaluación de 60 días, no es necesario que utilice ninguna clave de licencia.

## 10.2.4 Variables de línea de comando

Hay disponibles opciones de variables de línea de comando para la instalación de MSI. Estas variables deben definirse en el acceso directo del archivo ejecutable que se configura para ejecutarse en el modo de administrador. Para utilizar una variable, debe escribirse la siguiente línea de comando en el acceso directo de MSI:

```
"...\setup.exe" /a /V"variables". Introduzca entre comillas cualquiera de los comandos mostrados a continuación. Separe las diversas variables con un único espacio.
```

Están disponibles las siguientes variables de línea de comando:

**Tabla 10-1** Variables de línea de comando

Variable de línea de comando	Descripción	Notas
/qn	Instalación silenciosa.	Suprime el proceso de instalación típico de MSI. Endpoint Security Client se activará la próxima vez que el usuario reinicie el sistema.
SESMMSG=1	Muestra un mensaje al usuario final en el que se indica que no se pueden eliminar automáticamente cifrados de los archivos en "Safe Harbors" (puertos seguros) si se ha implementado una directiva de cifrado.	El valor por defecto es 0 (no se muestran mensajes) para que se pueda realizar la desinstalación "silenciosa".
STRBR=ReallySuppress	No es necesario reiniciar el sistema una vez completada la instalación.	La aplicación de seguridad y la autodefensa del cliente no funcionarán completamente hasta que no reinicie el sistema por primera vez.
STUPGRADE=1	Actualizar Endpoint Security Client 4.0.	Actualiza Endpoint Security Client 4.0.
STUNINSTALL=1	Desinstalar Endpoint Security Client 4.0.	Desinstala Endpoint Security Client 4.0.
STUIP="la contraseña"	Permite realizar una desinstalación con contraseña.	Utilice esta variable cuando la contraseña de desinstalación esté activa.
STNMS="Nombre de MS"	Permite cambiar el nombre del Servicio de gestión.	Cambia el nombre del servicio de gestión de Endpoint Security Client 4.0.
POLICYTYPE=1	Cambiar Endpoint Security Client 4.0 a directivas basadas en equipos.	Cambia los clientes de Endpoint Security Client instalados en MSI para que acepten las directivas basadas en equipos en lugar de las basadas en usuarios.

Variable de línea de comando	Descripción	Notas
POLICYTYPE=2	Cambiar Endpoint Security Client 4.0 a directivas basadas en usuarios.	Cambia los clientes de ZENworks Security 4.0 para Vista instalados en MSI para que acepten las directivas basadas en usuarios en lugar de las basadas en equipos.
STVA="Nombre del adaptador"	Agregar un adaptador virtual.	Activa un control de directivas sobre un adaptador virtual.
/L*v c:\log.txt	Permite activar el registro.	Activa el registro durante la instalación. Si no utiliza esta variable, el registro debe realizarse mediante las herramientas de diagnóstico de Endpoint Security Client.

### 10.2.5 Distribución de una directiva con el paquete de MSI

La directiva por defecto incluida en la instalación de MSI puede sustituirse por una directiva configurada en la empresa. Para transferir una directiva concreta con la imagen de MSI:

- 1 Cree una directiva que se vaya a distribuir a todos los usuarios a través de la consola de gestión (para obtener más información sobre la creación de directivas, consulte [la Guía de administración de ZENworks Endpoint Security Management](#)).
- 2 Exporte la directiva y, a continuación, renómbrela como `policy.sen`.  
A todas las directivas distribuidas de esta forma (no gestionada) se les debe asignar el nombre `policy.sen` para que Endpoint Security Client 4.0 las acepte. Endpoint Security Client 4.0 no implementa las directivas a las que no se les haya asignado el nombre `policy.sen`.
- 3 Abra la carpeta a la que se ha exportado la directiva y copie los archivos `policy.sen` y `setup.sen`.
- 4 Desplácese a la imagen de MSI creada y abra la carpeta `\Archivos de programa\Novell ZENworks\Endpoint Security Client\`.
- 5 Pegue los archivos `policy.sen` y `setup.sen` en la carpeta. Esto sustituirá los archivos por defecto `policy.sen` y `setup.sen`.

## 10.3 Ejecución de Endpoint Security Client 4.0

Endpoint Security Client 4.0 se ejecuta automáticamente durante el inicio del sistema. Para obtener más información sobre Endpoint Security Client 4.0, consulte [la Guía de usuario de ZENworks Endpoint Security Management Security Client 4.0](#).

La Guía de usuario puede distribuirse a todos los usuarios para ayudarles a conocer de forma más precisa el funcionamiento de su nuevo software de seguridad final.

## 10.4 Funciones incompatibles con Endpoint Security Client 4.0

Las funciones total o parcialmente incompatibles con Endpoint Security Client 4.0 incluyen:

- ♦ Autodefensa del cliente.
- ♦ Soporte de módem.
- ♦ Creación de guiones.
- ♦ Cambio manual de los cortafuegos de una ubicación determinada.
- ♦ Distintos cortafuegos visibles en una ubicación. Sólo está disponible el cortafuegos por defecto.
- ♦ Reglas de integridad.
- ♦ Bloqueo de una aplicación.
- ♦ La información del icono del área de notificación sobre la que se desplaza el ratón ha cambiado. El icono sólo muestra la información relacionada con la directiva y la ubicación.
- ♦ Conectividad USB.
- ♦ Gestión de la clave de Wi-Fi.
- ♦ Las conexiones con cable no están sobrevaloradas con respecto a las inalámbricas.
- ♦ Actualizaciones de Endpoint Security Client (por directiva).
- ♦ Tiempo límite de la autenticación VPN.
- ♦ Reproducción automática del control del dispositivo de almacenamiento.
- ♦ Entradas de la agenda telefónica en el entorno de red.





# Instalación no gestionada de ZENworks Endpoint Security Management

Una empresa puede ejecutar ZENworks® Security Client y la consola de gestión en el modo no gestionado (sin conexión al Servicio de distribución de directivas o al Servicio de gestión). Este tipo de instalación está disponible como opción y está diseñada principalmente para la configuración de evaluaciones sencillas. Esta opción es también ideal para las empresas que dispongan de muy poco espacio en el servidor o ninguno, o con necesidades básicas de seguridad. Sin embargo, con esta configuración, no están disponibles las actualizaciones rápidas de directivas ni la elaboración de informes de conformidad.

## 11.1 Instalación de un cliente Endpoint Security Client no gestionado

Para instalar un cliente Endpoint Security Client no gestionado, siga las instrucciones de [Capítulo 9, “Instalación de Endpoint Security Client 3.5”](#), en la [página 61](#) y seleccione la opción *No conectado a los servidores de ZENworks Endpoint Security Management (directivas recibidas como archivos)*. La instalación omite las cuestiones relativas a los nombres de los servidores e instala Endpoint Security Client en este equipo (también se puede crear un paquete de MSI para Endpoint Security Client no gestionado).

**Figura 11-1** Seleccione “No conectado a los servidores de ZENworks Endpoint Security Management”



## 11.2 Consola de gestión independiente

Esta configuración permite instalar una consola de gestión de ZENworks Endpoint Security Management y crear directivas sin necesidad de conectarse a un Servicio de gestión exterior o distribuir directivas mediante el Servicio de distribución de directivas. Seleccione *Instalación de la*

*consola de gestión independiente* en el menú Programa de instalación principal y siga las instrucciones de **Capítulo 7, “Instalación de la consola de gestión”, en la página 45** para realizar la instalación.

Al comienzo de la instalación, se instala una base de datos SQL (si ya existe una en el equipo, el programa de instalación configurará en su lugar las bases de datos adecuadas). Una vez que la base de datos esté instalada, la instalación se detendrá. El equipo tiene que reiniciarse para activar la base de datos SQL. Después de que reinicie, active de nuevo la instalación para continuar.

La mayor parte de las funciones de directivas están disponibles para la implantación, a excepción de la función de elaboración de informes. Todos los archivos de directivas exportados se deben distribuir al directorio `\Archivos de programa\Novell\ZENworks Security Client\` de Endpoint Security Client.

## 11.3 Distribución de directivas no gestionadas

Para distribuir directivas no gestionadas:

- 1** Busque el archivo `setup.sen` de la consola de gestión y cópielo en una carpeta independiente.  
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 Guía de administración de ZENworks Endpoint Security Management*).
- 3** Utilice el comando *Exportar* para exportar la directiva a la misma carpeta que contiene el archivo `setup.sen`. A todas las directivas distribuidas se les debe asignar el nombre `policy.sen` para que Endpoint Security Client las acepte.
- 4** Distribuya los archivos `policy.sen` y `setup.sen`. Estos archivos deben copiarse en el directorio `\Archivos de programa\Novell\ZENworks Security Client\` para todos los clientes no gestionados.  
El archivo `setup.sen` sólo debe copiarse en los dispositivos no gestionados una vez, con la primera directiva. Posteriormente, sólo se deben distribuir nuevas directivas.

Si el cliente Endpoint Security Client no gestionado se instala en el mismo equipo que la consola de gestión independiente, el archivo `setup.sen` se copiará también en el directorio `\Archivos de programa\Novell\ZENworks Security Client\`. Si el cliente Endpoint Security Client no gestionado se instala en el equipo después del editor independiente, el archivo se debe transferir de forma manual, como se ha indicado anteriormente.

Al hacer clic en el botón *Publicar*, se publica inmediatamente la directiva en el cliente de Endpoint Security Client no gestionado del equipo. Para proporcionar directivas a varios usuarios no gestionados, utilice la función *Exportar*, como se ha descrito anteriormente.

# Actualizaciones de la documentación

# A

En esta sección, se incluye información relativa a los cambios realizados en el contenido de la documentación de *la Guía de instalación de Novell ZENworks Endpoint Security Management* después de su lanzamiento inicial para la versión 3.5. Los cambios se muestran según la fecha de publicación.

La documentación de este producto está disponible en Web en dos formatos: HTML y PDF. La documentación HTML y PDF está actualizada con los cambios que aparecen en esta sección.

Si necesita saber si la copia de la documentación en PDF que está usando es la más reciente, consulte la fecha de publicación que aparece en la página del título.

La documentación se ha actualizado en las siguientes fechas:

- ♦ **Sección A.1, “5 de enero de 2009”, en la página 83**

## A.1 5 de enero de 2009

Se han realizado actualizaciones en las siguientes secciones:

Ubicación	Actualización
Todas las secciones	El nombre del cliente se ha cambiado en toda la guía. Ahora se le denomina formalmente Novell ZENworks Endpoint Security Client. En sus capítulos respectivos, los clientes se denominan Endpoint Security Client 3.5 (para Windows XP) y Endpoint Security Client 4.0 (para Windows Vista).
<b>Sección 1.1, “Requisitos del sistema”, en la página 10</b>	Se han añadido requisitos del sistema para el cliente nuevo Vista y la consola de gestión independiente.
<b>Capítulo 9, “Instalación de Endpoint Security Client 3.5”, en la página 61</b>	Se ha añadido el cambio del nombre e información indicando que Endpoint Security Client 3.5 está diseñado para Windows XP.
<b>Capítulo 10, “Instalación de ZENworks Endpoint Security Client 4.0”, en la página 71</b>	Se ha añadido un capítulo sobre Endpoint Security Client 4.0 (para Windows Vista).