

Guía de usuario de cliente de VPN

9235969

Edición 1

Copyright © 2004 Nokia. Reservados todos los derechos.

Queda prohibida la reproducción, la transferencia, la distribución o el almacenamiento de todo o parte del contenido de este documento bajo cualquier forma sin el consentimiento previo y por escrito de Nokia.

Nokia es una marca comercial registrada de Nokia Corporation. El resto de los productos y nombres de compañías aquí mencionados pueden ser marcas comerciales o registradas de sus respectivos propietarios.

Symbian and Symbian OS are trademarks of Symbian Ltd.

SecurID is a registered trademark of RSA Security INC.

Nokia opera con una política de desarrollo continuo y se reserva el derecho a realizar modificaciones y mejoras en cualquiera de los productos descritos en este documento sin previo aviso.

Nokia no se responsabilizará bajo ninguna circunstancia de la pérdida de datos o ingresos ni de ningún daño especial, incidental, consecuente o indirecto, independientemente de cuál sea su causa.

El contenido del presente documento se suministra tal cual. Salvo que así lo exija la ley aplicable, no se ofrece ningún tipo de garantía, expresa o implícita, incluida, pero sin limitarse a, la garantía implícita de comerciabilidad y adecuación a un fin particular con respecto a la exactitud, la fiabilidad y el contenido de este documento. Nokia se reserva el derecho de revisar o retirar este documento en cualquier momento sin previo aviso.

La disponibilidad de productos concretos puede variar de una región a otra. Consulte con su distribuidor Nokia más cercano.

Índice

Redes privadas virtuales.....	4
Instalación	6
Requisitos del sistema	6
Normativas de VPN.....	7
Instalación de normativas de VPN desde servidores de normativas de VPN.....	7
Instalación de normativas de VPN desde archivos SIS.....	8
Visualización de normativas de VPN	9
Estado de normativa	10
Estado del certificado	10
Creación de puntos de acceso de VPN con valores predeterminados	11
Actualización de normativas de VPN	11
Eliminación de normativas de VPN.....	11
Servidores de normativas de VPN	13
Conexión con los servidores de normativas de VPN ..	13
Instalación de ajustes desde archivos SIS	14
Visualización de los servidores de normativas de VPN.....	15
Adición de servidores de normativas de VPN	15
Edición de servidores de normativas de VPN.....	17
Sincronización de servidores de normativas de VPN..	17
Incorporación de certificados de VPN	18
Eliminación de servidores de normativas de VPN	18
Puntos de acceso de VPN.....	19
Visualización de puntos de acceso de VPN.....	19
Creación de puntos de acceso de VPN	19
Eliminación de puntos de acceso de VPN.....	20
Registro de VPN	21
Visualización del registro de VPN	21
Borrado del registro de VPN.....	21
Contraseñas de almacén de claves.....	22
Creación o modificación de una contraseña del almacén de claves	22
Introducción de contraseñas de almacén de claves..	23
VPN y aplicaciones	24
Autenticación de las pasarelas de VPN.....	24
Solución de problemas	26

1. Redes privadas virtuales

➔ Vaya a *Menú* y seleccione *Herrams.*
> *Ajustes* > *Ajustes de conexión* > *VPN*.

Con una **red privada virtual (VPN)**, puede crear conexiones cifradas para acceder a la información que necesite mientras esté fuera de la oficina. Estará en contacto y podrá controlar mediante un acceso cifrado la red de su empresa para consultar el correo electrónico, las aplicaciones de la base de datos y la intranet.

Para crear una VPN, una pasarela y el comunicador se autentican y negocian algoritmos de cifrado y autenticación para proteger la privacidad y la integridad de la información a la que accede el usuario.

Para crear conexiones VPN, cree en primer lugar puntos de acceso de VPN y, a continuación, seleccione los puntos de acceso de VPN cuando utilice aplicaciones para conectarse a la red de su empresa. Una conexión VPN con la red de la empresa se crea mediante otro tipo de conexión

a Internet. La conexión VPN se crea y los datos se cifran de acuerdo con una normativa de VPN que se carga cuando el usuario se conecta a un punto de acceso de VPN.

 **Nota:** Para utilizar redes VPN, debe recibir los ajustes del servidor de normativas de VPN de los administradores. Los administradores pueden enviarle los ajustes en un archivo del **Sistema de instalación Symbian (SIS)**.

Para utilizar redes privadas virtuales

1 Instalación de cliente de VPN.

Para obtener más información, véase "Instalación" en la página 6.

2 Especifique una conexión a un servidor de normativas de VPN.

Puede especificar los ajustes para un servidor de normativas de VPN o instalarlos desde un archivo SIS.

Para obtener más información, véase "Conexión con servidores de normativas de VPN" en la página 12.

 **Nota:** Si instala normativas de VPN desde archivos SIS, no tendrá que crear conexiones a los servidores de normativas de VPN.

3 Instale normativas de VPN desde el servidor de normativas de VPN.

Para obtener más información, véase "Instalación de normativas de VPN desde servidores de normativas de VPN" en la página 7.

4 Cree puntos de acceso de VPN.

Los puntos de acceso de VPN especifican un punto de acceso de Internet y una normativa de VPN.

Para obtener más información, véase "Creación de puntos de acceso de VPN" en la página 17.

 **Nota:** Los puntos de acceso de VPN combinan las normativas de VPN con puntos de acceso de Internet. Cuando se sincroniza un servidor de normativas de VPN por primera vez, se crean puntos de acceso de VPN para cada normativa que instale en el comunicador.

5 Seleccione un punto de acceso de VPN cuando utilice aplicaciones para conectarse a la red de la empresa.

Para obtener más información, véase "VPN y aplicaciones" en la página 21.

La conexión de VPN se crea encima de la conexión a Internet.

2. Instalación

El usuario recibe el cliente de VPN como un archivo del **Sistema de instalación Symbian (SIS)** estándar.

El cliente de VPN debe instalarse en un dispositivo móvil compatible del mismo modo en que se instalan otros tipos de software. Si desea obtener más información sobre la instalación de software en un dispositivo móvil, véase la documentación del dispositivo.

Cuando se haya completado la instalación, apague el dispositivo y vuelva a encenderlo para que los cambios se apliquen.

El archivo SIS de cliente de VPN no es necesario después de la instalación. Elimine el archivo SIS para liberar memoria.

Requisitos del sistema

Durante la instalación de El cliente de VPN necesita al menos 1,5 MB de memoria en el dispositivo móvil.

Después de la instalación, el cliente de VPN reserva 900 K de memoria en el dispositivo móvil o en una tarjeta de memoria. Cada normativa de VPN suele necesitar de 1 K a 16 K de memoria en el dispositivo móvil.

3. Normativas de VPN

Las **Normativas de VPN** definen el método que utilizan un dispositivo móvil y una pasarela de VPN para autenticarse entre sí, así como los algoritmos de cifrado que utilizan para cifrar los datos. Los administradores crean normativas de VPN y las almacenan en los servidores de normativas de VPN o las envían al usuario como archivos del **Sistema de instalación de Symbian (SIS)**. Puede instalar normativas de VPN desde un servidor de normativas de VPN o desde archivos SIS.

➡ Vaya a *Menú* y seleccione *Herrams.*
> *Ajustes* > *Ajustes de conexión* > *VPN* > *Gestión de VPN* > *Normativas de VPN*.

Instalación de normativas de VPN desde servidores de normativas de VPN.

Para instalar normativas de VPN

- 1 Pulse *Sí* cuando acceda a una vista *Normativas de VPN* vacía y se le solicite instalar normativas de VPN.
- 2 Pulse *Sí* cuando se le solicite agregar servidores de normativas de VPN.
- 3 Especifique los ajustes para conectarse con un servidor de normativas de VPN. Para obtener más información, véase "Conexión con servidores de normativas de VPN" en la página 12.
- 4 Pulse *Sí* cuando se le solicite sincronizar el servidor de normativas de VPN.

▶ **Glosario:** Los servidores de normativas de VPN son servidores de la red empresarial que contienen normativas de VPN.

 **Glosario:** La contraseña del almacén de claves ayuda a proteger las claves privadas en las conexiones de normativas de VPN y de servidores de normativas de VPN del uso no autorizado.

 **Glosario:** Un código de identidad de servidor de normativas de VPN es la identificación del certificado del servidor de normativas de VPN, que identifica el certificado.

 **Glosario:** La contraseña de importación de claves sirve para proteger las claves privadas del archivo de normativas de VPN.

- 5 Cree una **contraseña del almacén de claves**.
Para obtener más información, véase "Creación o modificación de una contraseña del almacén de claves" en la página 20.
Conéctese al servidor de normativas de VPN.
- 6 Compruebe el **código de identidad del servidor de normativas de VPN** para establecer una relación de confianza.
Puede saltarse este paso si instala los ajustes del servidor de normativas de VPN desde un archivo SIS.
Para obtener más información, véase "Agregación de servidores de normativas de VPN" en la página 13.
- 7 Introduzca información de autenticación para acceder al servidor de normativas de VPN y pulse [Aceptar](#).
El administrador del servidor de normativas de VPN le proporciona esta información.

Las normativas de VPN se instalarán en el dispositivo móvil.

 **Nota:** Si pulsa [Salir](#), las normativas de VPN no se instalarán. Pulse [Opciones](#) y seleccione [Instalar normativa](#) para instalar las normativas de VPN desde un servidor de normativas de VPN.

Instalación de normativas de VPN desde archivos SIS

Los administradores pueden proporcionarle normativas de VPN como archivos SIS. Si instala normativas de VPN desde archivos SIS, no tendrá que definir conexiones a los servidores de normativas de VPN. Después de instalar las normativas de VPN, puede crear puntos de acceso de VPN y asociarlos a las aplicaciones.

Si las normativas de VPN contienen claves privadas y sus certificados correspondientes, los administradores definirán las **contraseñas de importación de claves** para proteger las claves privadas. Los administradores deberían utilizar un método seguro para entregar al usuario la contraseña de importación de claves.

Para instalar normativas de VPN desde archivos SIS

- 1 Escriba la contraseña de importación de claves en *Contraseña importación de claves:* y pulse *Aceptar*.
- 2 Escriba la contraseña de almacenamiento de claves en *Contraseña almacenamiento de claves:* y pulse *Aceptar*.

Visualización de normativas de VPN

La vista *Normativas de VPN* enumera las normativas de VPN que instalará en el dispositivo móvil.

Si se muestra *(no hay normativas de VPN)* debe instalar las normativas de VPN. Pulse *Opciones* y seleccione *Instalar normativa* para instalar las normativas de VPN desde un servidor de normativas de VPN.

Seleccione una normativa de VPN para ver la siguiente información:

- *Descripción:* información adicional de la normativa de VPN. Los administradores definen la descripción cuando crean la normativa de VPN.
- *Estado de normativa:* indica si la normativa de VPN está lista para su uso o si ya se encuentra en uso.
- *Estado de certificado:* indica si hay certificados de usuario válidos disponibles en el dispositivo móvil.
- *Nombre de normativa:* el nombre que los administradores dan a la normativa de VPN cuando crean la normativa de VPN.
- *Servidor de normativas:* el nombre del servidor de normativas de VPN desde el que instaló la normativa de VPN. Se le asignan nombres a los servidores de normativas de VPN cuando se definen conexiones con los servidores de normativas de VPN. Este campo queda oculto si instaló la normativa de VPN desde un archivo SIS.
- *Actualizada:* fecha de la última vez que se actualizó la normativa de VPN desde el servidor de normativas de VPN. Este campo queda oculto si instaló la normativa de VPN desde un archivo SIS.

Estado de normativa



Nota: La vista de detalles de normativa de VPN no se actualiza si el estado de la normativa cambia mientras la vista está abierta.

Estado de normativa: puede tener los siguientes valores:

- *En uso:* ha creado una conexión a un punto de acceso de VPN asociado a la normativa de VPN. Cuando crea una conexión, la normativa de VPN se activa.
- *Asociada con punto de acceso de VPN:* ha asociado la normativa de VPN con uno o varios puntos de acceso de VPN. Puede seleccionar cualquier punto de acceso de VPN para activar la normativa de VPN.
- *No asociada con punto de acceso de VPN:* debe asociar la normativa de VPN a un punto de acceso de VPN para activar la normativa de VPN.

Estado del certificado

Estado de certificado: puede tener los siguientes valores:

- *Aceptar:* hay disponible al menos un certificado válido en el dispositivo móvil o no utiliza certificados para autenticarse en las pasarelas de VPN.
- *Caducado:* ha finalizado el periodo de validez de uno o más certificados.
Si no puede crear una conexión de VPN, intente actualizar la normativa de VPN para incorporar nuevos certificados.
- *No hay ningún certificado:* no puede encontrarse uno o más de los certificados necesarios en el dispositivo móvil.
Si no puede crear una conexión de VPN, intente actualizar la normativa de VPN para incorporar nuevos certificados.
- *No válido aún:* uno o más certificados son para uso futuro.
Este valor también puede significar que la fecha y la hora del dispositivo móvil no están actualizadas, que las zonas horarias no están definidas correctamente o que el ajuste de horario de verano está activado.

Pulse la tecla de selección para cerrar los detalles y volver a la vista [Normativas de VPN](#).

Creación de puntos de acceso de VPN con valores predeterminados

Para utilizar la normativa de VPN debe asociarla con un punto de acceso de VPN. Pulse [Opciones](#) y seleccione [Definir pto. acc. VPN](#) en la vista [Normativas de VPN](#).

El cliente de VPN móvil crea un punto de acceso de VPN con ajustes predeterminados. Puede crear y modificar puntos de acceso de VPN en la vista Puntos de acceso de VPN.

Esta opción no aparece disponible si ha instalado la normativa de VPN desde un archivo SIS.

Actualización de normativas de VPN

Al crear una conexión a un punto de acceso de VPN, el estado de la normativa de VPN se comprueba desde el servidor de normativas de VPN. Si los administradores han creado una nueva versión de la normativa de VPN, la nueva versión se instala en el dispositivo móvil. Si los administradores han eliminado la normativa de VPN desde el servidor de normativas de VPN, dicha normativa se elimina del dispositivo móvil.

Los cambios se aplicarán la próxima vez que se cree una conexión con el punto de acceso de VPN, por lo que no afectan a la conexión de VPN actual.

También puede actualizar una normativa de VPN en la vista [Normativas de VPN](#). Para actualizar una normativa de VPN, seleccione una, pulse [Opciones](#) y seleccione [Actualiz. normativa](#). El estado de la normativa de VPN se comprueba desde el servidor de normativas de VPN.

Eliminación de normativas de VPN

Las normativas de VPN se eliminan automáticamente al sincronizar un servidor de normativas de VPN después de que los administradores eliminen las normativas de VPN del servidor de normativas de VPN. Si elimina una normativa de VPN que aún existe en el

servidor de normativas de VPN, dicha normativa se volverá a instalar cuando sincronice las normativas de VPN desde el servidor de normativas de VPN.

Para eliminar una normativa de VPN, selecciónela y pulse la tecla Borrar.

No puede utilizar un punto de acceso de VPN si elimina una normativa de VPN asociada a él.

4. Servidores de normativas de VPN

Puede instalar normativas de VPN desde servidores de normativas de VPN. Al crear una conexión con un punto de acceso de VPN, la normativa de VPN asociada al punto de acceso de VPN se actualiza automáticamente desde un servidor de normativas de VPN. Para actualizar todas las normativas de VPN, sincronice los servidores de normativas de VPN con el dispositivo móvil. Para obtener más información, véase "Sincronización de servidores de normativas de VPN" on page 17.

➡ Vaya a *Menú* y seleccione *Herrams.*
> *Ajustes* > *Ajustes de conexión* > *VPN* > *Gestión de VPN* > *Servids. norms. VPN.*

Conexión con los servidores de normativas de VPN

Al instalar normativas de VPN desde un servidor de normativas de VPN, se crea una relación de confianza entre el dispositivo móvil y el servidor de normativas de VPN. Para crear la relación de confianza, debe autenticar el servidor de normativas de VPN y éste, a su vez, debe autenticar al usuario.

 **Sugerencia** Los administradores pueden entregarle un archivo SIS que contiene ajustes que especifican una conexión a un servidor de normativas de VPN o puede especificar los ajustes para el servidor de normativas de VPN.

Una vez que el servidor de normativas de VPN autentica al usuario, se genera una clave privada y se incorpora un certificado correspondiente. El certificado autentica al usuario en el servidor de normativas de VPN. La clave privada y el certificado se almacenan en un almacén de claves en el dispositivo móvil.

Instalación de ajustes desde archivos SIS

Puede instalar los ajustes del servidor de normativas de VPN en el servidor de normativas de VPN desde un archivo SIS. Instale los ajustes en un dispositivo móvil como si se tratara de cualquier otro software.

Los ajustes constan de la dirección y del certificado del servidor de normativas de VPN. El certificado del servidor hace que el dispositivo móvil confíe en el servidor de normativas de VPN, de modo que sólo necesita presentar un nombre de usuario y una contraseña para probar su identidad.

El archivo SIS no contiene los ajustes necesarios para que el punto de acceso de Internet se conecte al servidor de normativas de VPN. Para especificar el punto de acceso de Internet, edite los ajustes del servidor de normativas de VPN. También puede seleccionar el punto de acceso de Internet cuando se conecte al servidor de normativas de VPN.

Si los administradores no firman el archivo SIS, aparece una advertencia de seguridad al instalar el archivo SIS. Puede ignorar la advertencia si está seguro de que el administrador del servidor de normativas de VPN ha creado el archivo SIS y de que el archivo SIS no se ha modificado.

Salga de [VPN](#) antes de instalar los ajustes desde un archivo SIS o se produce algún error durante la instalación.

Visualización de los servidores de normativas de VPN

La vista *Servidores de normats. VPN* enumera los servidores de normativas de VPN que cree.

Si se muestra *(no hay servidores de normativas VPN)*, debe crear servidores de normativas de VPN. Para agregar un servidor de normativas, pulse *Opciones* y seleccione *Servidor nuevo*.

Adición de servidores de normativas de VPN

Si no instala los ajustes del servidor de normativas de VPN desde un archivo SIS, especifique los ajustes del servidor de normativas de VPN.

Al conectarse por primera vez a la dirección del servidor de normativas de VPN, debe autenticar el servidor de normativas de VPN. Recibirá de los administradores un código de identificación del servidor de normativas de VPN. Compruebe y complete el código de identidad del servidor de normativas de VPN.

Una vez completada la autenticación correctamente, se incorpora un certificado para la posterior autenticación del servidor de normativas de VPN.

Para agregar un servidor de normativas de VPN

- 1 Pulse *Opciones* y seleccione *Servidor nuevo* en la vista *Servidores de normats. VPN*.
- 2 Seleccione *Nombre serv. norms.* para introducir un nombre para el servidor de normativas de VPN y pulse *Aceptar*.

Puede elegir cualquier nombre de servidor de normativas, pero debe ser único en la vista *Servidores de normativas de VPN*.

Si deja este campo vacío, *Direcc. servid. norms.* aparece en este campo.

El nombre del servidor de normativas aparece en la lista de servidores de normativas de VPN y en la barra de título del cuadro de diálogo *Ajustes de servidor de normativas de VPN*.

 **Glosario:** La sincronización significa que un servidor de normativas de VPN comprueba la existencia de normativas de VPN nuevas, actualizadas o eliminadas.

 **Glosario:** El nombre de usuario y la contraseña del servidor de normativas sirven para proteger el servidor de normativas de VPN del acceso no autorizado.

- 3 Seleccione *Direcc. servid. norms.*, introduzca el nombre de host o la dirección IP del servidor de normativas de VPN desde el que desea instalar normativas de VPN y pulse *Aceptar*.
También puede especificar un número de puerto separado por dos puntos (:). Los administradores le deben proporcionar la dirección del servidor de normativas.
- 4 Seleccione *Punto acc. a Internet*, asocie el servidor de normativas de VPN a un punto de acceso y pulse *Aceptar*.
El punto de acceso se utiliza para conectarse a este servidor de normativas de VPN. Los administradores le informan de qué punto de acceso debe seleccionar.
- 5 Pulse *Atrás* para guardar los ajustes del servidor de normativas de VPN.
- 6 Pulse *Sí* cuando se le solicite **sincronizar** el servidor de normativas de VPN. Se le solicita verificar la identidad del servidor de normativas de VPN. Recibirá de los administradores un código de identificación del servidor de normativas de VPN.
- 7 Compare con cuidado el código de identidad del servidor de normativas de VPN que aparece con el código que recibe de los administradores, introduzca los caracteres que faltan en el campo y pulse *Aceptar*.
- 8 Introduzca su **nombre de usuario** en *Nombre de usuario de servidor norms.*; y la **contraseña** en *Contraseña servidor normativas*: para autenticarse en el servidor de normativas de VPN y pulse *Aceptar*.
Los administradores le informan del nombre de usuario y la contraseña que deberá introducir.

Se incorpora un certificado para las siguientes autenticaciones en el servidor de normativas de VPN y las normativas de VPN se instalan en el dispositivo móvil.

Ahora puede crear puntos de acceso de VPN y asociarlos a las aplicaciones. Para obtener más información, véase "Creación de puntos de acceso de VPN" en la página 17.

Edición de servidores de normativas de VPN

Seleccione un servidor de normativas de VPN en la vista [Servidores de normats. VPN](#) para ver o cambiar los ajustes para el servidor de normativas de VPN.

Seleccione [Nombre serv. norms.](#) para introducir un nuevo nombre para el servidor de normativas. La vista [Servidores de normats. VPN](#) muestra el nuevo nombre.

No puede cambiar [Direcc. servid. norms.](#) después de instalar normativas de VPN desde el servidor de normativas de VPN, ya que el servidor de normativas de VPN envía la dirección durante la primera conexión.

Si ha eliminado el punto de acceso asociado al servidor de normativas de VPN, [Punto acc. a Internet](#) muestra el texto (no seleccionado). Seleccione el punto de acceso de Internet para elegir un nuevo punto de acceso. Si ha eliminado todos los puntos de acceso, no puede guardar los ajustes.

Sincronización de servidores de normativas de VPN

Seleccione un servidor de normativas de VPN en la vista [Servidores de normats. VPN](#), pulse [Opciones](#) y seleccione [Sincroniz. servidor](#) para instalar y actualizar normativas desde el servidor de normativas de VPN. El servidor de normativas de VPN comprueba si se han agregado, actualizado o eliminado normativas de VPN.

Si el servidor de normativas de VPN contiene nuevas normativas de VPN o nuevas versiones de normativas de VPN, las normativas de VPN se instalan en el dispositivo móvil. Si los administradores han eliminado normativas de VPN del servidor de normativas de VPN, dichas normativas se eliminarán del dispositivo móvil.

Cuando se sincroniza un servidor de normativas de VPN por primera vez, se crea un punto de acceso de VPN para cada normativa de VPN que instale en el dispositivo móvil. Puede crear y editar puntos de acceso de VPN en la vista [Puntos de acceso de VPN](#).

Cuando se conecta a un servidor de normativas de VPN para instalar o actualizar normativas de VPN, puede que necesite incorporar certificados del servidor de normativas de VPN.

Incorporación de certificados de VPN

Se crea una solicitud de certificación para cada certificado necesario y se envía al servidor de normativas de VPN. El servidor de normativas de VPN incorpora cada certificado solicitado desde una **autoridad de certificación** (CA).

La solicitud de certificación y el certificado correspondiente contienen la identidad del usuario. Dependiendo de la configuración del servidor de normativas de VPN, la identidad de usuario del servidor de normativas de VPN puede utilizarse también como la identidad del usuario en los certificados de VPN. Si esto no es posible, se le solicita su identidad de usuario para un dominio específico.

Para crear solicitudes de certificación

- 1 Introduzca su identidad de usuario de certificado para el dominio especificado en *Identidad de usuario para* :
Los administradores le indicarán la información que debe introducir.
- 2 Pulse *Aceptar*.

Eliminación de servidores de normativas de VPN

Para eliminar un servidor de normativas de VPN, seleccione el servidor de normativas de VPN en la vista *Servidores de normats. VPN* y pulse la tecla Borrar.

Confirme la eliminación de las normativas de VPN que ha instalado desde el servidor de normativas de VPN.

5. Puntos de acceso de VPN

Un punto de acceso de VPN es un punto de acceso virtual que combina una normativa de VPN con un punto de acceso de Internet. Seleccione un punto de acceso de VPN en las listas de puntos de acceso de Internet para crear una conexión VPN.

➡ Vaya a *Menú* y seleccione *Herrams.*
> *Ajustes* > *Ajustes de conexión* > *VPN* > *Puntos de acceso de VPN*.

Visualización de puntos de acceso de VPN

La vista *Puntos de acceso de VPN* enumera los puntos de acceso de VPN que ha creado en el dispositivo móvil. El mensaje (*no hay puntos de acceso de VPN*) significa que no ha creado puntos de acceso de VPN. Para crear un nuevo punto de acceso de VPN, pulse *Opciones* y seleccione *Punto acceso nuevo*.

Seleccione un punto de acceso de VPN y, a continuación, seleccione *Opciones* > *Editar* para ver y editar la información siguiente:

- *Nombre de conexión*: identifica el punto de acceso de VPN en las listas de puntos de acceso.
- *Normativa de VPN*: nombre de la normativa de VPN asociada con el punto de acceso de VPN.
- *Punto acc. a Internet*: nombre del punto de acceso a través del cual se crea la conexión de VPN.
- *Direc. servidor proxy*: dirección de un servidor proxy en la red empresarial.
- *Nº puerto de proxy*: número de puerto para conectar al servidor proxy.

Creación de puntos de acceso de VPN

La primera vez que abra la vista *Puntos de acceso de VPN*, se le solicitará que cree puntos de acceso de VPN. Pulse *Sí*.

 **Sugerencia** Si especifica un servidor proxy en los ajustes de punto de acceso de VPN, no tendrá que especificar el servidor proxy en los ajustes del navegador de Internet.

Creación de puntos de acceso de VPN

- 1 Pulse *Opciones* y seleccione *Punto acceso nuevo*.
- 2 Seleccione *Nombre de conexión* para cambiar el nombre de la conexión. Puede elegir cualquier nombre de conexión.
- 3 Seleccione *Normativa de VPN* para definir el modo en que se ha cifrado la conexión. Si la lista está vacía, debe instalar normativas de VPN desde archivos SIS o servidores de normativas de VPN.
- 4 Seleccione *Punto acc. a Internet* para seleccionar el punto de acceso que desea utilizar para la conexión VPN. Si la lista está vacía, debe crear puntos de acceso.
- 5 Seleccione *Direc. servidor proxy* para introducir la dirección de un servidor proxy en la red empresarial.
- 6 Seleccione *Nº puerto de proxy* para cambiar el puerto predeterminado, 80.

Eliminación de puntos de acceso de VPN

Para eliminar un punto de acceso de VPN, seleccione un punto de acceso de VPN en la vista *Puntos de acceso de VPN* y pulse la tecla *Borrar*.

6. Registro de VPN

El registro de VPN contiene mensajes de registro que se almacenan cuando se actualizan y sincronizan normativas de VPN y se crean conexiones de VPN con pasarelas de VPN.

➡ Vaya a *Menú* y seleccione *Herrams.*
> *Ajustes* > *Ajustes de conexión* > *VPN* > *Gestión de VPN* > *Registro de VPN.*

Visualización del registro de VPN

La vista *Registro de VPN* muestra el número de versión del cliente de VPN.

Puede ver el tipo de mensaje, la hora de cada mensaje y el comienzo del mensaje de registro. Seleccione un mensaje de registro para ver el mensaje de registro completo.

La vista *Registro de VPN* clasifica los mensajes de registro por fecha y hora y pone el mensaje más reciente en primer lugar. Puede ver todos los mensajes hasta el momento en que haya abierto la vista *Registro de VPN*. Pulse *Opciones* y seleccione *Actualizar registro* para ver los mensajes de registro más recientes.

Los mensajes de registro pueden contener códigos de error, de estado y de motivo. Informe a los administradores de los códigos contenidos en los mensajes de registro cuando informe de la presencia de errores.

Iconos:  para indicar errores,  para indicar advertencias y  para indicar descripciones.

Borrado del registro de VPN

Los mensajes de registro se almacenan en un búfer circular. Cuando el tamaño del registro alcanza los 20 kilobytes, los nuevos mensajes de registro reemplazan a los mensajes de registro antiguos.

Para eliminar todos los mensajes de registro y borrar la vista *Registro de VPN*, pulse *Opciones* y seleccione *Borrar registro*.

7. Contraseñas de almacén de claves

➡ Vaya a *Menú* y seleccione *Herrams.*
> *Ajustes* > *Ajustes de conexión* > *VPN* > *Gestión de VPN* > *Contraseña almacenamiento de claves:*

▶ **Sugerencia** Una contraseña de almacén de claves puede contener letras y números y debe tener como mínimo seis caracteres.

La contraseña del almacén de claves ayuda a proteger las claves privadas en el dispositivo móvil y en las conexiones de servidores de normativas de VPN del uso no autorizado.

Creación o modificación de una contraseña del almacén de claves

Cree una contraseña del almacén de claves cuando instale la primera normativa de VPN. Si los atacantes averiguan una contraseña del almacén de claves, pueden utilizar el dispositivo móvil para acceder a la red empresarial que la red VPN contribuye a proteger. Por tanto, debe crear contraseñas del almacén de claves que sean lo suficientemente largas como para que resulte difícil averiguarlas. Asegúrese de mantener sus contraseñas en un lugar secreto. No las escriba.

Para crear o cambiar la contraseña del almacén de claves:

- 1 En *Contraseña almac. de claves nueva*; introduzca una contraseña que le resulte fácil de recordar, pero que resulte difícil de averiguar para cualquier otra persona.
- 2 Seleccione *Confirme contraseña*; y vuelva a introducir la contraseña para evitar errores de escritura.
- 3 Pulse *Aceptar* para crear la contraseña.

Introducción de contraseñas de almacén de claves

Se le solicitará que introduzca la contraseña de almacén de claves cuando:

- Instale normativas de VPN nuevas o actualizadas desde servidores de normativas de VPN.
- Utilice aplicaciones para conectar puntos de acceso de VPN que requieran autenticación de certificado.



Nota: Cuando se introducen contraseñas, la función de texto predictivo se desactiva. Introduzca los caracteres de uno en uno. Los caracteres se escriben en minúsculas de forma predeterminada.

8. VPN y aplicaciones

Cuando utilice una aplicación para crear una conexión VPN, el cliente de VPN lleva a cabo las siguientes tareas:

- Conecta con el punto de acceso de Internet asociado con el punto de acceso de VPN.
- Carga la normativa de VPN asociada con el punto de acceso de VPN.
- Se conecta con una pasarela de VPN para crear una conexión de VPN.

Autenticación de las pasarelas de VPN

Necesita probar su identidad cada vez que inicie sesión en la red empresarial. La normativa de VPN determina el método de autenticación que utiliza:

- Autenticación basada en certificados: debe tener un certificado firmado por una autoridad de certificación de confianza. Utilice una inscripción de certificados en línea para obtener el certificado o instalar certificados al instalar la normativa de VPN desde un archivo SIS.
- Autenticación anterior: debe utilizar nombres de usuario y contraseñas o códigos de acceso para autenticarse. Los administradores crean los nombres de usuario y las contraseñas o le conceden tokens para SecurID con el fin de generar códigos de acceso.

Si utiliza certificados de autenticación, introduzca la contraseña de almacén de claves.

Si utiliza la autenticación anterior, introduzca la información de autenticación de VPN cuando utilice aplicaciones para conectar puntos de acceso de VPN y el dispositivo móvil negocie las conexiones cifradas con la pasarela de VPN.

Para autenticarse en una pasarela de VPN

- 1 Introduzca su nombre de usuario de VPN en *Nombre de usuario de VPN*.
- 2 Introduzca su contraseña o código de acceso de VPN:
 - Introduzca su contraseña en *Contraseña de VPN*.
 - Cree un código de acceso de SecurID, introdúzcalo en *Código de VPN*; y pulse *Aceptar*.

- 3 Si el token de SecurID ya no está sincronizado con la hora del reloj de ACE/Server, se le solicita el siguiente código de acceso que ACE/Server utiliza como nueva referencia atendiendo a la hora del token.
Genere e introduzca una clave de acceso nueva en *Código siguiente*.
Si esto no funciona, póngase en contacto con los administradores.
- 4 Pulse *Aceptar*.

9. Solución de problemas

La siguiente tabla enumera mensajes de error en orden alfabético, describe las posibles causas de los errores e incluye sugerencias para recuperarse de estos errores.

Mensaje	Causa	Acción
<i>Fallo de autenticación. Verifique el nombre de usuario y la contraseña.</i>	<ul style="list-style-type: none"> • Ha introducido un nombre de usuario o una contraseña incorrecta al autenticarse en un servidor de normativas de VPN o iniciar sesión en una VPN. • Ha introducido una clave de acceso incorrecta cuando se le ha solicitado la Próxima clave de acceso. 	<ul style="list-style-type: none"> • Compruebe el nombre de usuario y la contraseña y vuelva a intentarlo. • Espere hasta que el código de acceso de la pantalla del token de SecurID cambie e introduzca el código de acceso.

Mensaje	Causa	Acción
<i>Contraseña incorrecta</i>	Ha introducido una contraseña de almacén de claves o contraseña de importación de claves incorrectas.	<ul style="list-style-type: none"> • Compruebe la contraseña y vuelva a intentarlo. • El usuario recibe la contraseña de importación de claves de los administradores. Cree la contraseña de almacén de claves.
<i>Código de identidad de servidor</i>	Ha introducido una cadena incorrecta cuando se le ha solicitado que introduzca el código de identidad del servidor de normativas de VPN.	Compare el código de identidad del servidor de normativas de VPN con el código que ha recibido de los administradores y vuelva a introducir los caracteres que faltan.
<i>El servidor de normativas está actualmente en uso. Imposible borrar.</i>	No puede eliminar un servidor de normativas de VPN mientras actualiza las normativas de VPN del servidor. Cuando se utiliza una aplicación para crear una conexión de VPN, las normativas de VPN se actualizan automáticamente.	Espere a que se actualicen las normativas de VPN y vuelva a intentarlo.

Mensaje	Causa	Acción
<p><i>Imposible activar conexión de VPN. Actualice antes la normativa de VPN.</i></p>	<ul style="list-style-type: none"> • Se ha producido un error en la autenticación anterior. • El certificado que ha utilizado para autenticarse en la pasarela de VPN falta, ha caducado o su periodo de validez no ha comenzado aún. 	<ul style="list-style-type: none"> • Compruebe el nombre de usuario y la contraseña y vuelva a intentarlo. • Seleccione una normativa de VPN en la vista <i>Normativas de VPN</i>, pulse <i>Opciones</i> y seleccione <i>Actualiz. normativa</i> para actualizar la normativa de VPN. • Compruebe los ajustes de fecha y hora en el dispositivo móvil.
<p><i>Imposible iniciar sesión en servidor de normativas. Borre el servidor y redefina los detalles.</i></p>	<p>El certificado del servidor del servidor de normativas de VPN ha caducado.</p>	<p>En la vista <i>Servidores de normats. VPN</i>:</p> <ol style="list-style-type: none"> 1 Pulse <i>Opciones</i> y seleccione <i>Borrar servidor</i> para eliminar el servidor de normativas de VPN. 2 Pulse <i>Opciones</i> y seleccione <i>Servidor nuevo</i> para volver a agregar el servidor de normativas de VPN o solicite al administrador un archivo SIS que contenga nuevos ajustes para el servidor de normativas de VPN.

Mensaje	Causa	Acción
<p><i>Imposible iniciar sesión en servidor de normativas. Introduzca nombre usuario&contraseña.</i></p>	<p>El certificado que le autentica en el servidor de normativas de VPN caduca o los administradores han revocado el certificado.</p>	<ul style="list-style-type: none"> • Informe a los administradores de este error. Ellos le proporcionarán una contraseña de un solo uso para el inicio de sesión. • Introduzca el nombre de usuario y la contraseña de un solo uso para autenticarse en el servidor de normativas de VPN. • Se incorpora un nuevo certificado.
<p><i>Imposible iniciar sesión en servidor de normativas. Vea el registro de VPN para detalles.</i></p>	<p>El periodo de validez del certificado que le autentica en el servidor de normativas de VPN no ha comenzado aún.</p>	<p>Compruebe los ajustes de fecha y hora o espere hasta que comience el periodo de validez del certificado.</p>

Mensaje	Causa	Acción
<ul style="list-style-type: none"> • <i>Imposible actualizar la normativa. Vea el registro de VPN para obtener detalles.</i> • <i>Imposible sincronizar. Vea el registro de VPN para obtener detalles.</i> 	<p>Se ha producido un error mientras las normativas de VPN se descargan del servidor de normativas de VPN o se instalan en el dispositivo móvil.</p>	<ul style="list-style-type: none"> • En la vista <i>Normativas de VPN</i>, seleccione una normativa de VPN, pulse <i>Opciones</i> y seleccione <i>Actualiz. normativa</i> para actualizar una normativa de VPN. • En la vista <i>Servidores de normats. VPN</i>, seleccione un servidor de normativas de VPN, pulse <i>Opciones</i> y seleccione <i>Sincroniz. servidor</i> para instalar normativas desde el servidor de normativas de VPN.
<p><i>Normativa de VPN borrada. Intente redefinir el punto de acceso de VPN.</i></p>	<p>La normativa de VPN asociada con el punto de acceso de VPN se ha eliminado porque estaba obsoleta.</p>	<p>En la vista <i>Puntos de acceso de VPN</i>, seleccione un punto de acceso de VPN, pulse <i>Opciones</i> y seleccione <i>Editar</i> para asociar otra normativa de VPN con el punto de acceso de VPN</p>

Índice alfabético

A

advertencias de seguridad 14
 almacén de claves 14
 autenticación anterior 24
 autenticación basada en certificados
 24

C

campo Actualizada 9
 campo Clave de acceso de VPN 24
 campo Contraseña de servidor de
 normativas 16
 campo Contraseña de VPN 24
 campo Descripción 9
 campo Dirección de servidor de
 normativas 16
 campo Dirección de servidor proxy 19
 campo Estado de certificado 9
 campo Estado de normativa 9, 10
 campo Nombre de conexión 19
 campo Nombre de normativa 9
 campo Nombre de servidor de
 normativas 15, 16
 campo Nombre de usuario de VPN 24
 campo Normativa de VPN 19
 campo Nueva contraseña de almacén
 de claves 22
 campo Número de puerto proxy 19

campo Próxima clave de acceso 24
 campo Punto de acceso
 de Internet 16, 19
 campo Servidor de normativa 9
 campos

Actualizada 9
 Clave de acceso de VPN 24
 contraseña de servidor de
 normativas 16
 Contraseña de VPN 24
 Descripción 9
 dirección de servidor de
 normativas 16
 Dirección de servidor proxy 19
 Estado de certificado 9
 Estado de normativa 9, 10
 Nombre de conexión 19
 Nombre de normativa 9
 Nombre de servidor de
 normativas 15
 Nombre de usuario de servidor de
 normativas 16
 Nombre de usuario de VPN 24
 Normativa de VPN 19
 Nueva contraseña de almacén de
 claves 22
 Número de puerto proxy 19

Próxima clave de acceso 24, 25
 Punto de acceso de Internet 16
 punto de acceso de Internet 19
 Servidor de normativa 9

certificados

autenticación de servidores de
 normativas de VPN 14
 estado 10
 identidad de usuario 18
 incorporación 18

certificados caducados 10

certificados no válidos aún 10

clave de acceso SecurID 24

cliente de VPN

requisitos del sistema 6

cliente VPN

uso 5

Código de identidad del servidor

incorrecto. 27

Contraseña incorrecta. 27

contraseñas del almacén de claves

acerca de 8, 22

creación 22

E

el 6

El servidor de normativas está en uso
 actualmente. No se puede

eliminar. 27

F
Fallo de autenticación. Verifique el nombre de usuario y la contraseña. 26

I
Imposible activar la conexión de VPN. Actualice antes la normativa de VPN. 28
Imposible actualizar la normativa. Vea el registro de VPN para obtener más información. 30
Imposible iniciar sesión en el servidor de normativas. Borre el servidor y redefina los detalles. 28
Imposible iniciar sesión en el servidor de normativas. Introduzca el nombre de usuario y la contraseña del servidor. 29
Imposible iniciar sesión en el servidor de normativas. Vea el registro de VPN para obtener más información. 29
Imposible sincronizar. Vea el registro de VPN para obtener más información. 30

instalación
ajustes del servidor de normativas de VPN desde archivos SIS 14
instalación de normativas de VPN 17

M
mensajes de error 26

N
no hay normativas de VPN 9
no hay puntos de acceso de VPN 19
no hay servidores de normativas de VPN 15
Normativa de VPN borrada. Intente redefinir el punto de acceso de VPN. 30
normativas de VPN
actualización 11
eliminación 11
estado 10
ver 9

O
opción de actualizar 21
opción de borrar registro 21
opción de edición 19
opción de eliminar normativa 12
opción de nuevo servidor 15
opción de punto de acceso nuevo 19
opción de sincronizar servidor 17

P
próxima clave de acceso 25
puntos de acceso de VPN
edición 19
ver 20
visualización 19

R
registro de VPN
visualización 21
requisitos de memoria 6
requisitos del sistema 6

S
Servidores de normativas de VPN
instalación de ajustes desde archivos SIS 14
servidores de normativas de VPN
adición 15
conexión 13
sincronización 17
visualización 15
sin certificado 10
sin certificados 10

U
Un 19

V
VPN
autenticación 24
uso con aplicaciones 24