Manual de Administración del Portal

Acceso Remoto Movistar

Telefónica Empresas

2023

Índice

1 Introducción

Este documento es una guía de uso dirigida a los administradores del servicio Acceso Remoto.

2 Portal de Administración del Servicio

El servicio de Acceso Remoto Movistar proporciona una Web de Administración que permite a los clientes gestionar y monitorizar los accesos en movilidad de sus usuarios a sus recursos corporativos.

Hace falta un nombre de usuario y clave para iniciar sesión en la Web de Administración. El nombre de usuario es un código del servicio único asignado por Movistar y la clave es generada de forma aleatoria por el sistema. Ambas credenciales se comunican al administrador por correo electrónico.

El administrador debe cambiar su clave de administración cuando acceda por primera vez a la Web de Administración.

La URL de acceso a la Web de Administración es

https://www.accesoremoto.movistar.es/admin

3 Estado

La página de Estado muestra el estado del conector VPN y los usuarios conectados en ese momento al servicio:

4 Configuración

4.1 Usuarios

Si selecciona “**Usuarios”** en menú de la izquierda puede ver los detalles de todos los usuarios creados en la cuenta del servicio.

4.1.1 Detalles y estado

Los datos de cada usuario se muestran al hacer clic en el nombre de usuario:

NOTA: El número máximo de usuarios que se pueden configurar está limitado por el número de licencias adquiridas. Este número máximo se puede incrementar o reducir desde el menú de “Mi cuenta”.

4.1.2 Política de acceso de red

En la sección de Política de acceso de red el administrador puede configurar lo siguiente:

Métodos de acceso

Los métodos de acceso cuyo uso tiene autorizado este usuario.

Horarios de acceso

Las horas durante las cuales el usuario se puede conectar.

Opciones de acceso (Cliente VPN):

- **Permitir el acceso a Internet durante la conexión ("split-tunnel")**

  Esta configuración solo se aplica al cliente Windows VPN.

  - **Si esta opción SÍ está marcada**: el tráfico de Internet se redirige desde la conexión de Internet del usuario, no hacia el túnel VPN.
  - **Si esta opción NO está marcada**: el tráfico de Internet se redirige hacia el túnel VPN.

- **Aplicar control de extremo final**

  El control de extremo final permite a los administradores controlar el nivel de acceso concedido a los usuarios del cliente VPN basándose en algunas pruebas. Las pruebas disponibles son las siguientes:

  - **Confirmación que el cliente VPN ha sido emitido a este usuario**: esta prueba verifica si el software del cliente VPN que está utilizando este usuario se emitió a su nombre de usuario.
  - **Confirmación que el equipo es miembro de un dominio de Windows conocido**: esta prueba verifica si el PC que se está utilizando es miembro del dominio de Windows de la empresa.

Si el usuario intenta acceder a la red mediante un PC/Portátil que no pasa las diferentes pruebas, el usuario se coloca automáticamente en Cuarentena, lo que significa que se aplican las reglas de Cuarentena. Para obtener más información sobre reglas de Cuarentena, consulte la sección 4.4.3 Control de extremo final/Cuarentena.

4.1.3 Autenticación/Política de bloqueo

En la sección Autenticación/Política de bloqueo el administrador puede configurar lo siguiente:

Autenticación

Controla si el usuario está autenticado por Acceso Remoto o Single Sign-On (por ejemplo, su propio RADIUS o dominio de Windows). La opción SSO solo está disponible si se ha marcado desde Red.

Política de bloqueo

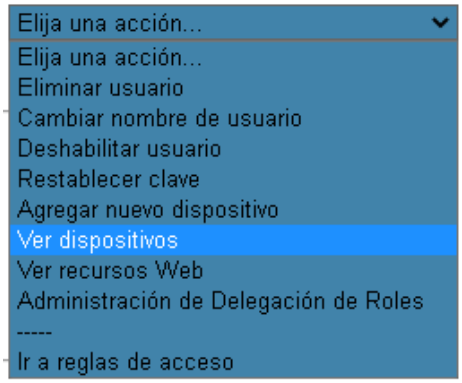
Define la configuración de la política de bloqueo que incluye Denegaciones máximas, el máximo número de denegaciones permitidas antes de que se bloquee a un usuario, así

como Restablecer después el periodo de tiempo tras el cual el usuario se desbloquea automáticamente.

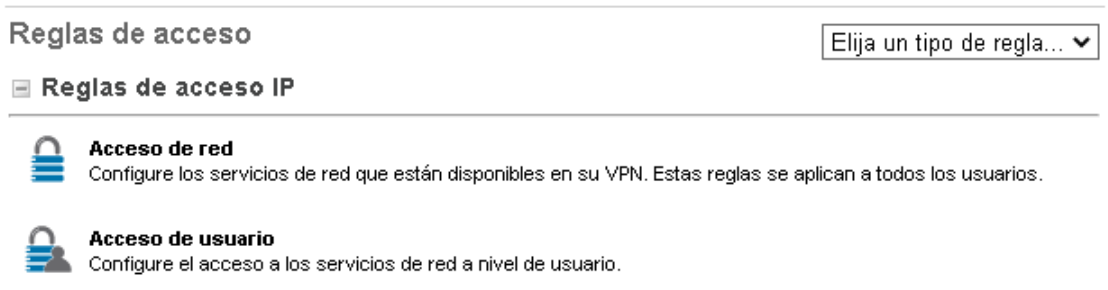
4.1.4 Acciones de usuarios

El desplegable “Elija una opción” permite realizar las siguientes acciones sobre los usuarios habilitados:

- Eliminar usuario
- Cambiar nombre de usuario
- Deshabilitar usuario
- Restablecer clave
- Agregar nuevo dispositivo
- Ver dispositivos
- Ver recursos Web
- Administración de Delegación de Roles



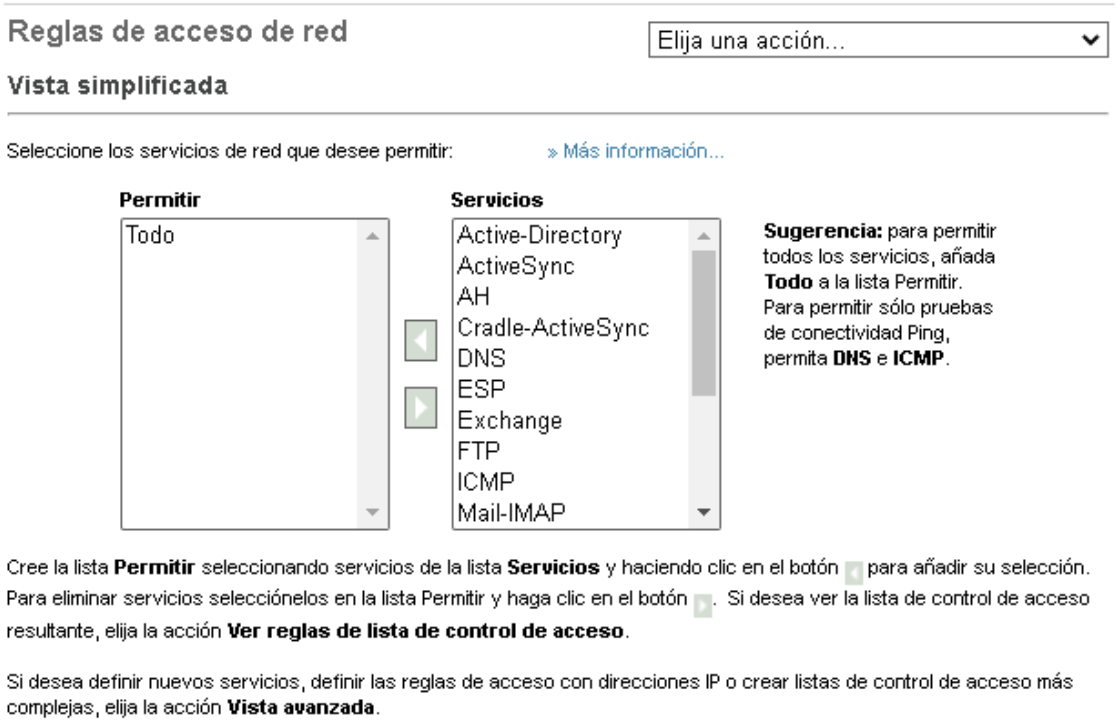
4.2 Reglas de acceso



4.2.1 Acceso de red

Las reglas de acceso de red controlan el tipo de tráfico que se permite a los usuarios transmitir hacia la red corporativa. La configuración por defecto es permitir todos los tipos de tráfico. Se pueden añadir reglas para restringir el tráfico solo a servicios / protocolos específicos.

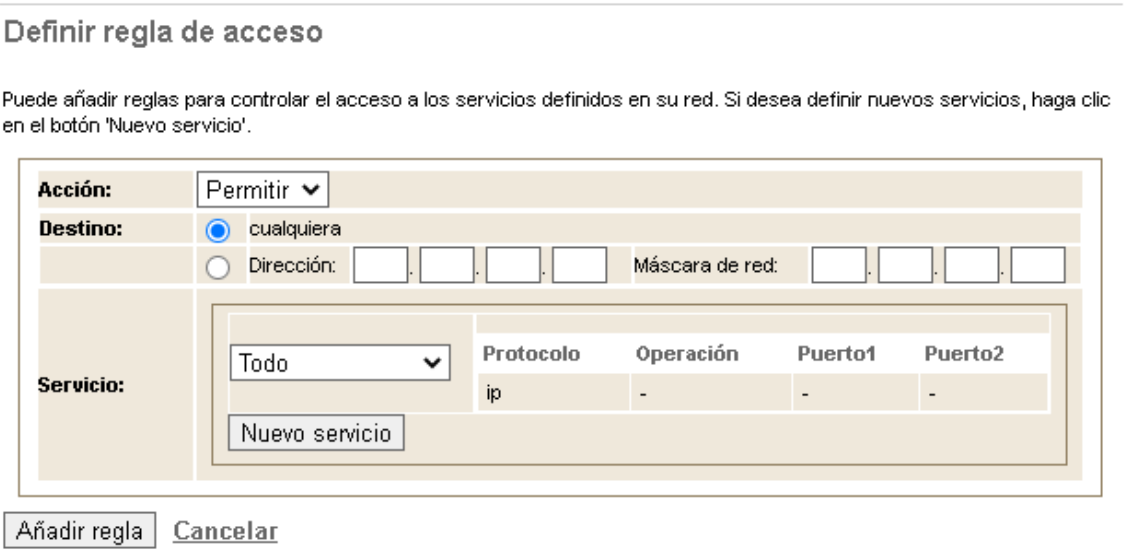
NOTA: Tenga en cuenta que cuando la funcionalidad de split-tunnel este deshabilitada, para dispositivos conectados mediante APN móvil, el tráfico de navegación a internet será a través del conector VPN. En este caso las reglas de acceso de red deberán permitir también el tráfico de navegación web (es decir, en general protocolos HTTP y HTTPs y otros específicos que pudieran hacer falta como Mail-IMAP o similares).



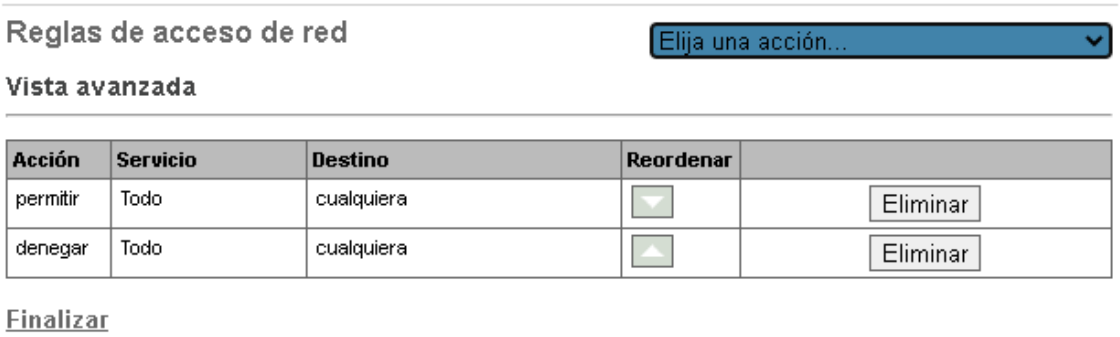
Seleccione **Elija una acción > Vista Avanzada > Insertar regla** para insertar una nueva regla.

Especifique el rango o la dirección IP y el tipo de tráfico al que se debe **Permitir** o **Denegar** el acceso.

A continuación, seleccione **Añadir regla**:

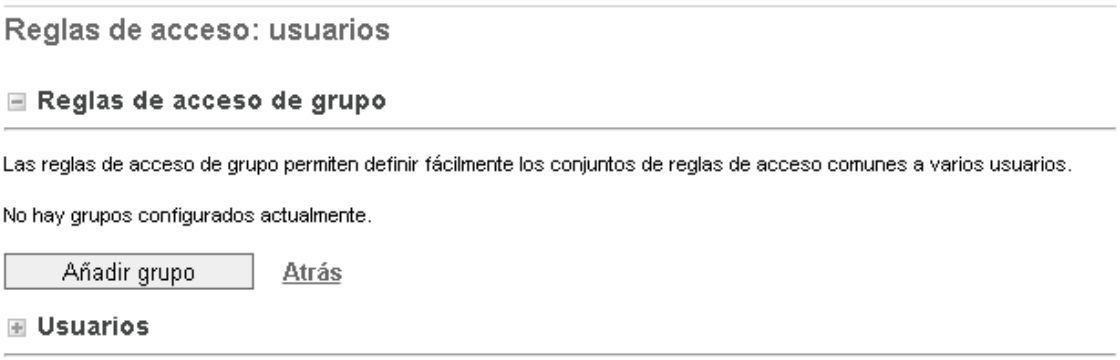


Para ordenar la lista de reglas, utilice los botones **Reordenar**:



4.2.2 Acceso de usuario

Las reglas de acceso de usuario permiten añadir restricciones para un solo usuario. El tráfico puede restringirse de forma individua, o se puede configurar para grupos y asignar al usuario a estos grupos.



Para configurar un nuevo grupo y definir reglas de grupo, seleccione **Añadir grupo**.

Utilice las opciones **Mostrar todo** o **Buscar** de la sección Usuarios para seleccionar a un usuario individual y definir una regla individual para ellos.

4.2.3 Acceso de cuarentena

Las reglas de acceso de cuarentena son las reglas que se aplicarán a un usuario con cliente VPN que no supere las pruebas de control de extremo final. Esta sección solo es visible si el “Control de extremo final” se ha habilitado en la cuenta de cliente. Para obtener más información, consulte la sección 4.4.3 Control de extremo final/Cuarentena.

4.3 Dispositivos

Seleccionar **Dispositivos** del menú de la izquierda para ver los detalles de todos los dispositivos de su cuenta de servicio:

Haga clic en el tipo de dispositivo para ver una lista de todos los dispositivos de ese tipo.

4.3.1 Clientes VPN

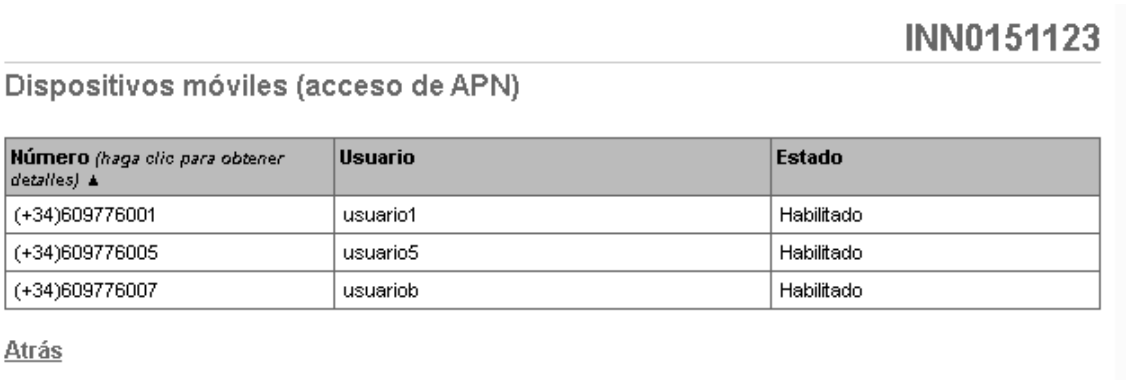
Detalles de todos dispositivos de tipo clientes VPN (PC/Portátiles Windows) que se han instalado. Se muestran el nombre de PC y el sistema operativo. Si un usuario desinstala su cliente VPN, los detalles aparecerán aquí. Actualmente no existe un modo para quitar un dispositivo de cliente VPN de esta lista.

Clientes VPN (IPSec/L2TP)

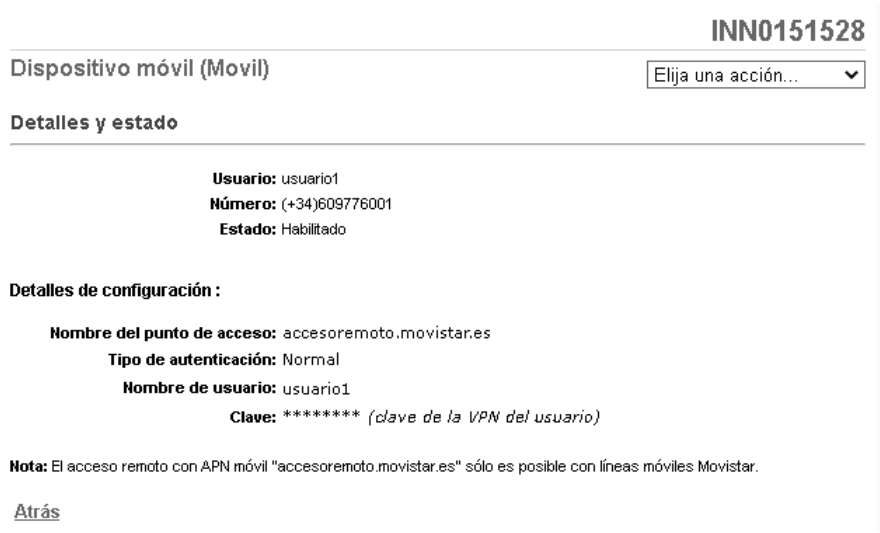
Nombre	**Descripción**	**Certificado** *(haga clic para obtener detalles)*
AS-LT-07	Windows Vista	*Descargar*
AS-LT-711	Windows Vista	*Descargar*
DESKTOP-72O8K7E	Windows Vista	*Descargar*
AS-LT-702	Windows Vista	*Descargar*

4.3.2 Dispositivos APN

Detalles de todos los dispositivos APN móvil de la cuenta. Se muestran el estado, usuario y número (MSISDN) del dispositivo.

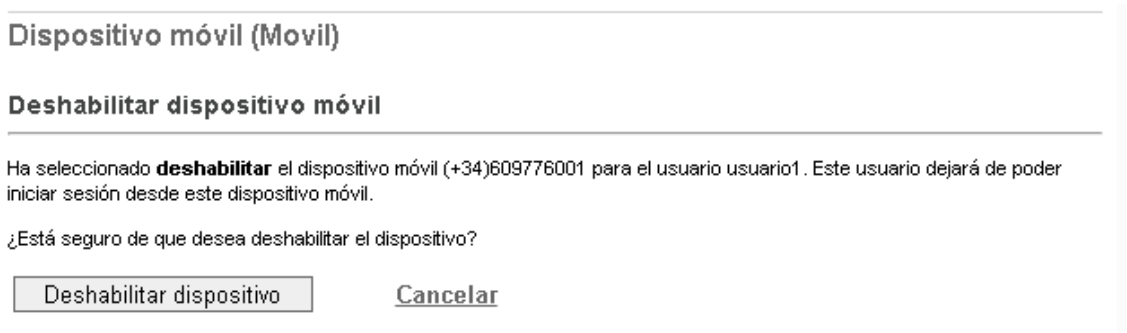


Haga clic en el número para ver más detalles:

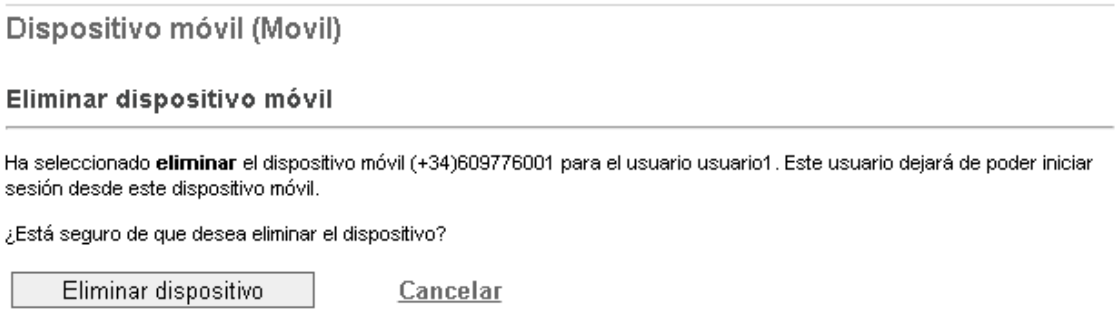


Se muestran los detalles del dispositivo APN móvil, incluidos el nombre del APN y las credenciales requeridas para su autenticación.

Para deshabilitar el dispositivo APN móvil, haga clic en **Elija una acción > Deshabilitar dispositivo**:

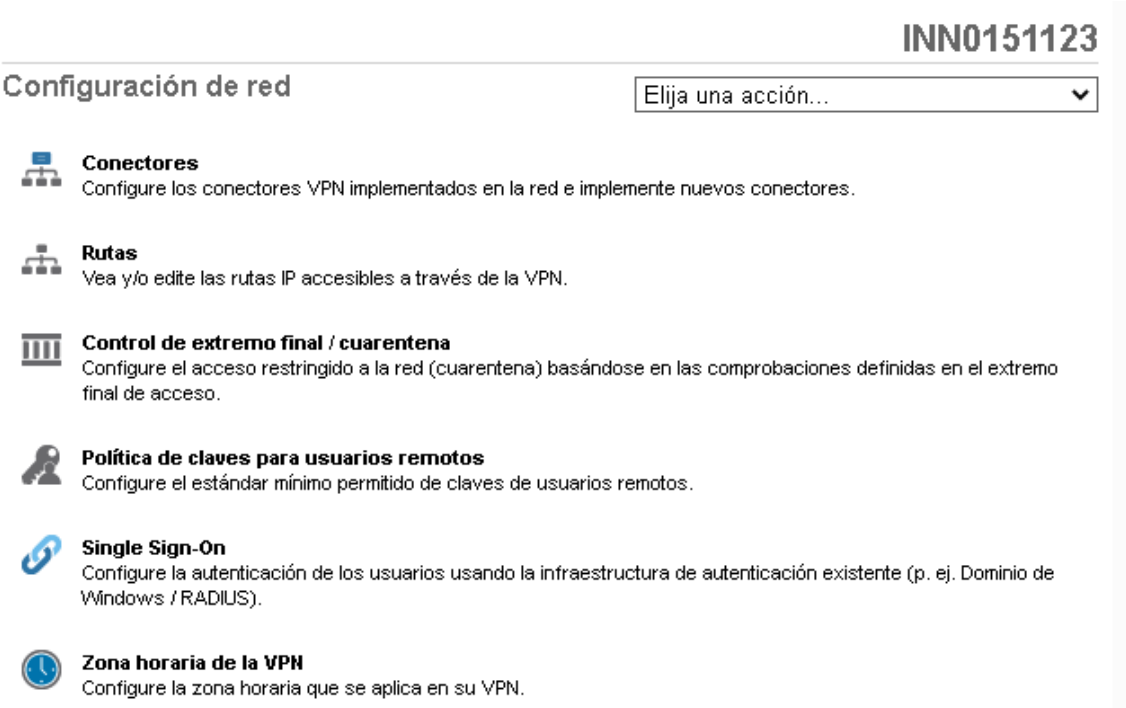


Para eliminar el cliente APN móvil, haga clic en **Elija una acción > Eliminar dispositivo**:



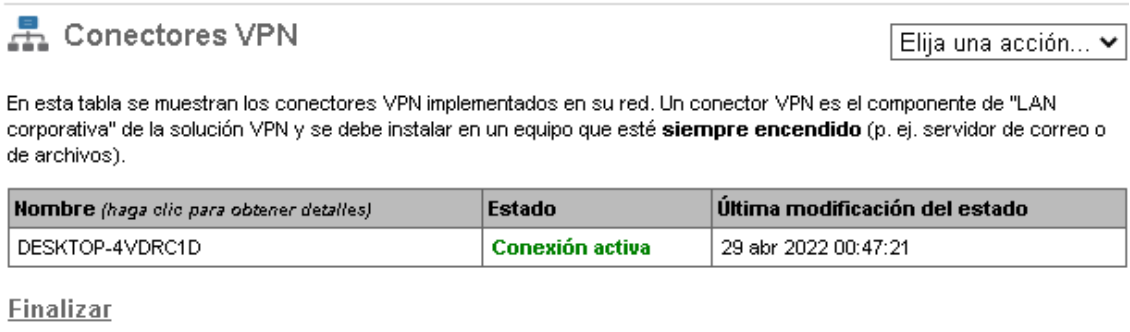
4.4 Red

Opciones de configuración de red:

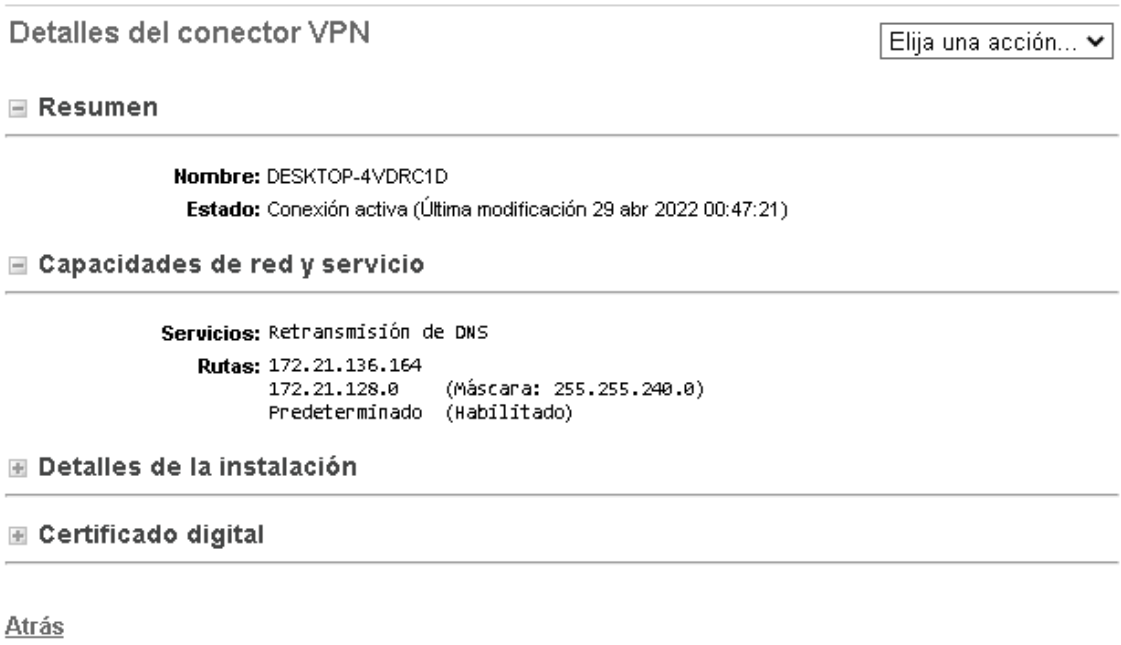


4.4.1 Conectores

Proporciona detalles del conector VPN de la cuenta de servicio:

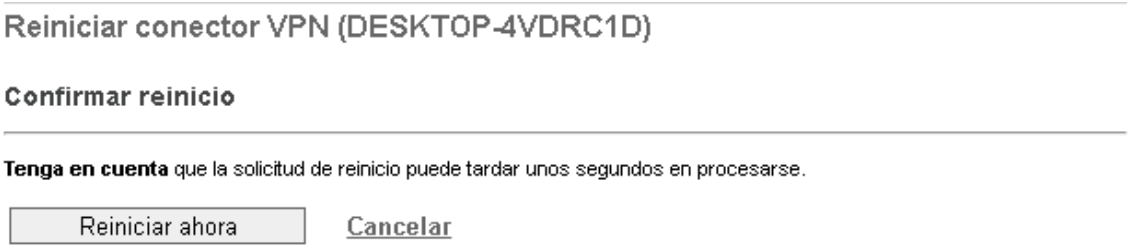


Los datos de cada conector se muestran al hacer clic en el nombre del conector:



4.4.1.1 Acciones de conectores

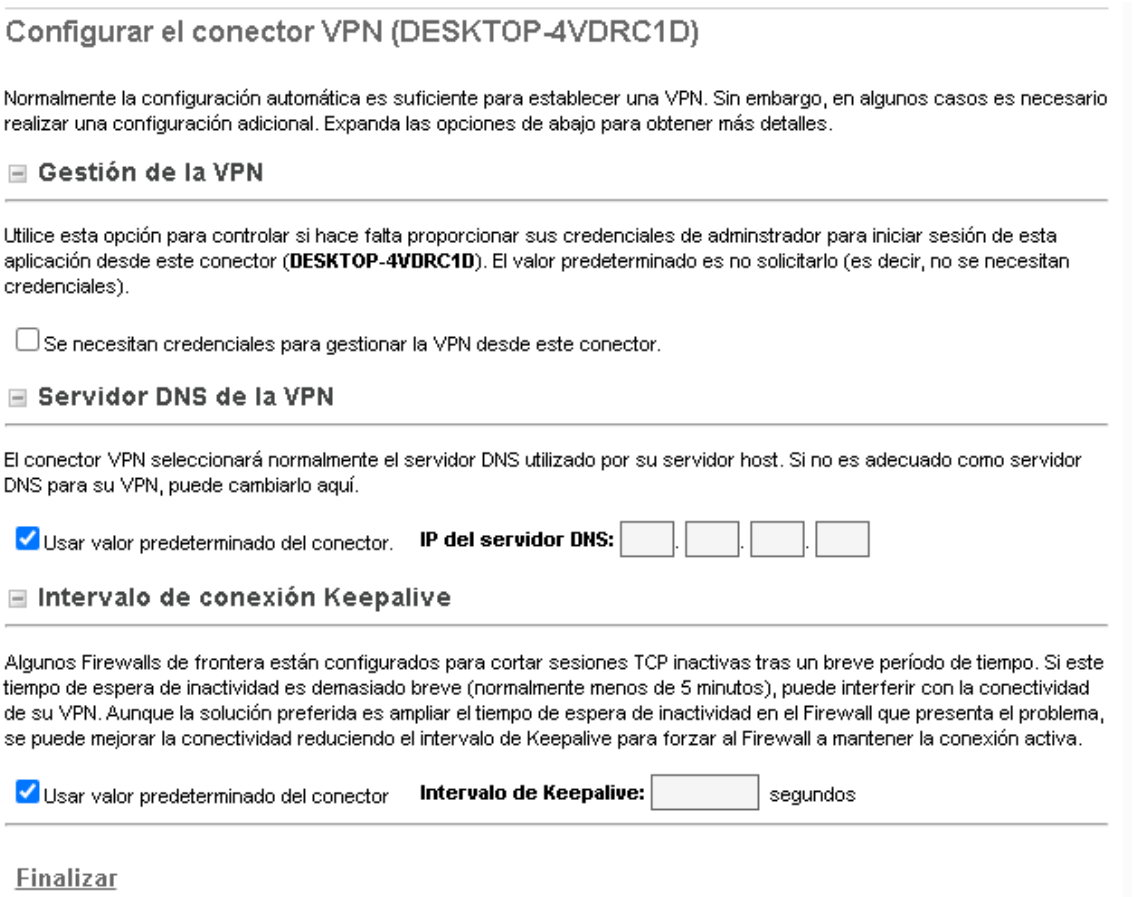
Para reiniciar un conector, haga clic en **Elija una acción > Reiniciar**



Para deshabilitar un conector, haga clic en **Elija una acción > Deshabilitar**

Para eliminar un conector, haga clic en **Elija una acción > Eliminar**

Para configurar un conector, haga clic en **Elija una acción > Configurar**

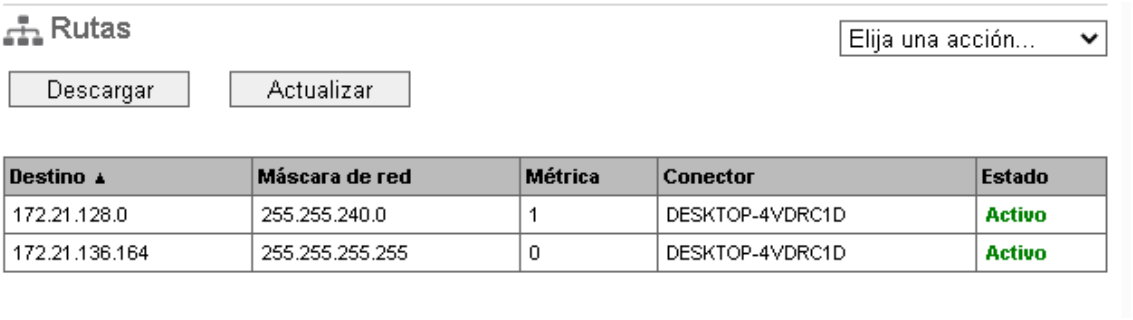


En la página de configuración del conector, el administrador puede configurar los siguientes ajustes:

- **Gestión de la VPN:** Controla si son necesarios un nombre de usuario y clave de administrador para abrir el portal de administración desde este conector.
- **Servidor DNS de VPN:** Normalmente un conector utilizará el servidor DNS utilizado por su servidor host. Aquí puede especificarse otro servidor DNS. 46
- **Intervalo de conexión Keepalive:** Se configura el intervalo Keepalive del conector para evitar que la conexión del conector sea revocada por un firewall que desactiva las conexiones TCP transcurrido un breve espacio de tiempo.

4.4.2 Rutas

Aquí se muestran las rutas que están disponibles en la red de Acceso Remoto. Estas rutas se insertan automáticamente cuando se instala el conector. Para configurar una cuenta estándar de Acceso Remoto no debería ser necesario que el administrador hiciera cambios aquí



4.4.3 Control de extremo final/Cuarentena

El control de extremo final permite a los administradores controlar el nivel de acceso concedido a los usuarios con cliente VPN basándose en algunas pruebas.

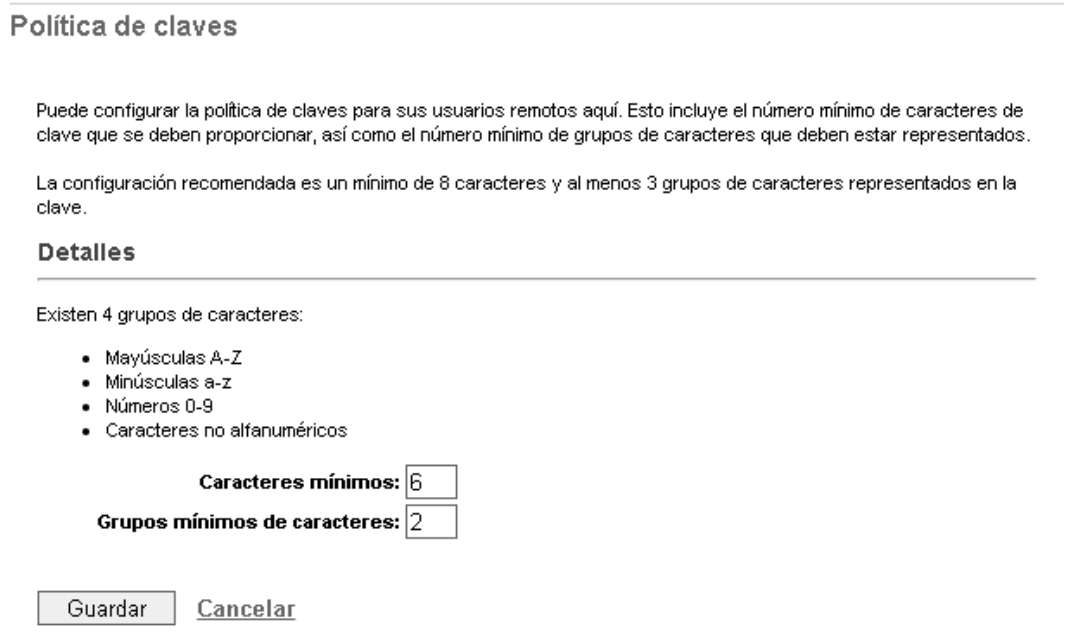
Si un usuario para el que el control de extremo final se ha habilitado intenta acceder a la red mediante un PC que no pasa las diferentes pruebas, el usuario se coloca automáticamente en Cuarentena.

Las pruebas que se deben pasar para dejar la cuarentena se definen por usuario en su Política de acceso de red. Durante la cuarentena, el usuario solamente puede acceder a un conjunto limitado de recursos. La política de cuarentena se define como un conjunto de reglas ACL. Estas reglas se pueden definir al través del portal de administración, al seleccionar **Reglas, Acceso desde la cuarentena**.

4.4.4 Política de claves para usuarios remotos

El administrador puede cambiar la política de claves para los usuarios aquí. Esta política especifica el número mínimo de caracteres que se deben proporcionar, así como el número mínimo de grupos de caracteres que deben incluir en las claves de acceso.

La política predeterminada especifica un mínimo de 6 grupos de caracteres y 2 grupos de caracteres:

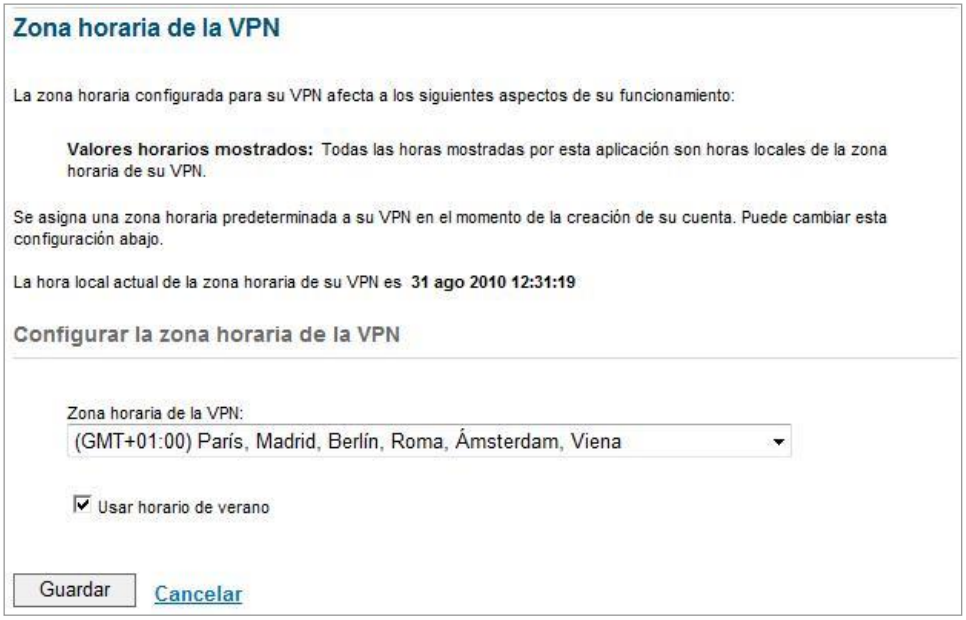


4.4.5 Single Sign-On

Esta sección permite al administrador habilitar, configurar y gestionar Single Sign-On (SSO). SSO permite a los usuarios autenticarse frente al dominio de Windows de una empresa o el servidor interno Radius.

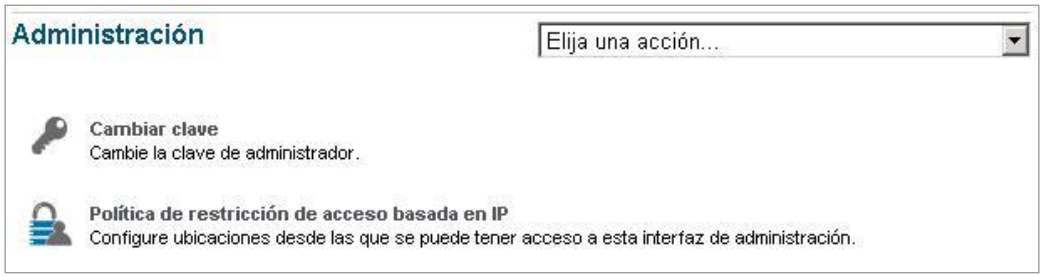
4.4.6 Zona horaria de la VPN

Aquí se puede modificar la zona horaria de la VPN. Esta configuración afecta a los horarios mostrados en la sección “Informes”.



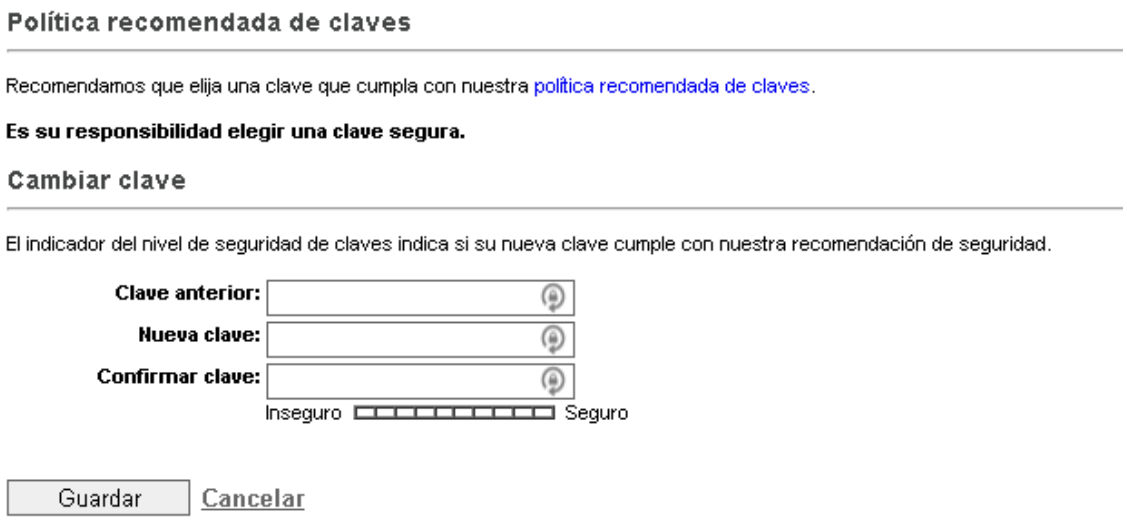
5 Administración

El administrador de la cuenta puede cambiar su clave aquí, restringir desde dónde puede visualizarse esta página web de administración, así como asignar a los usuarios derechos de administrador delegado.



5.1 Cambiar Clave

Para cambiar la clave del administrador, este debe introducir la antigua clave en el primer cuadro, seguida de la nueva clave en los dos cuadros siguientes

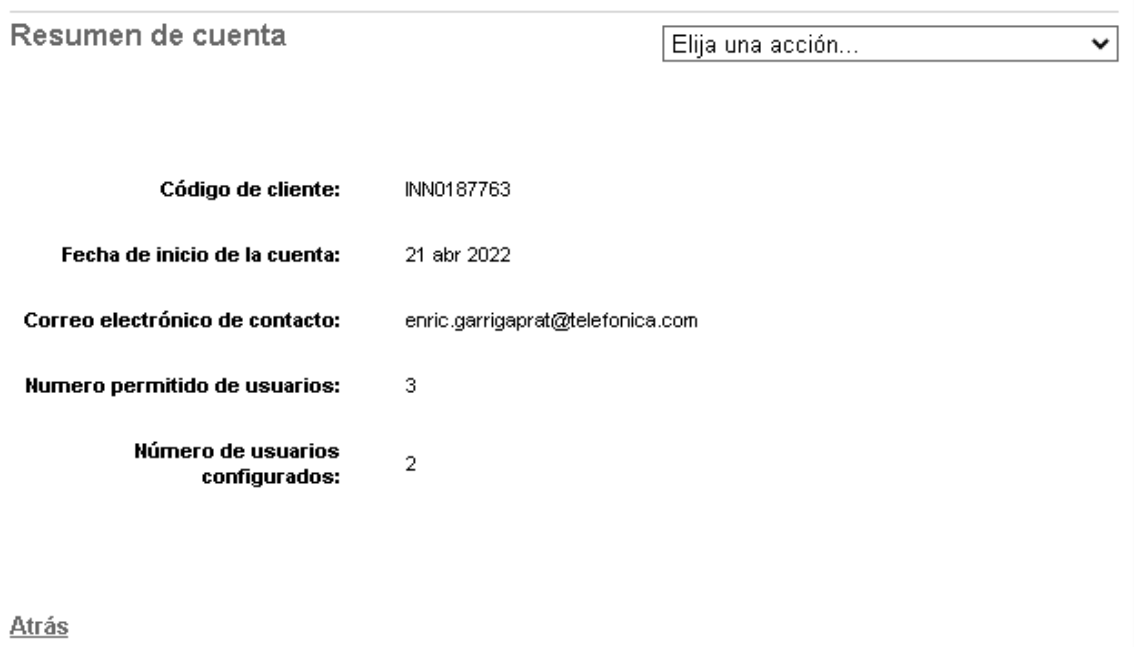


5.2 Política de restricción de acceso basada en IP

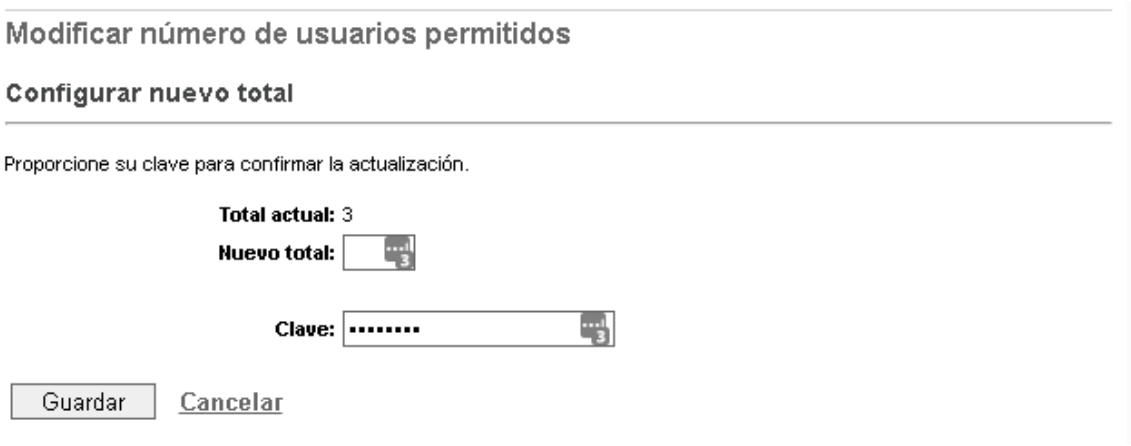
En esta sección el administrador puede restringir el acceso a este sitio web de administración. El administrador puede configurar una lista de direcciones IP y subredes desde las que puede conectarse a esta web de administración. Si no se especifica ninguna dirección IP, se permitirá el acceso al sitio web de administración desde cualquier ubicación.

6 Mi cuenta

Esta sección muestra los números de licencia asociados con esta cuenta.



Para cambiar el número de usuarios permitidos, haga clic en **Elija una acción > Modificar número permitido de usuarios**



NOTA: El número permitido de usuarios, es el número de usuarios contratado y es el número de usuarios que se factura. Su valor tiene que ser mayor que el número de usuarios dados de alta. Si tienen dados de alta más usuarios de los permitidos, deberá que darlos de baja antes.

7 Mensajes

En esta página se muestran todos los mensajes generados por el sistema que van dirigidos al administrador. Por ejemplo, si el administrador no ha podido iniciar sesión, se registrará un mensaje en la sección de mensajes.

8 Informes

En esta sección se puede acceder y descargar informes sobre conectividad de líneas y conectores.

8.1 Conexiones de usuarios

Se muestra un registro de las conexiones efectuadas que muestra la hora de inicio, la hora de finalización y la cantidad de tráfico que ha pasado. La vista predeterminada corresponde a las últimas 24 horas de actividad de todos los usuarios. El informe muestra las conexiones finalizadas, sin incluir las activas en ese momento

Para personalizarla, haga clic en el botón **Personalizar**:

8.2 Inicios de sesión fallidos

Se muestra un registro de los errores de inicio de sesión que muestra el dispositivo, la causa y la hora del error. La vista predeterminada corresponde a las últimas 24 horas de actividad y puede personalizarse a cualquier fecha de los últimos seis meses

8.3 Conectividad de conectores

Se muestra un log de las conexiones de conectores al VPN que incluye las horas de inicio y finalización. Este registro puede utilizarse para evaluar la estabilidad de la conexión de conectores. La vista predeterminada corresponde a las últimas 24 horas de actividad y puede personalizarse a cualquier fecha de los últimos seis meses.

Informes

Sesiones de conectores

Sesiones de conector en las últimas 24 horas

Descargar | Actualizar | Personalizar

Conector	Hora de inicio ▼	Hora fin
DESKTOP-4VDRC1D	28 abr 2022 18:05:39	28 abr 2022 20:48:34

Todas las horas mostradas son locales a la zona horaria configurada para su VPN. Haga clic aquí para obtener más detalles.

Atrás

www.telefonica.com