



# Manual de Administración del Portal

Acceso Remoto Movistar

Telefónica Empresas

2023

# Índice

<b>1</b>	<b>Introducción</b>	<b>3</b>
<b>2</b>	<b>Portal de Administración del Servicio</b>	<b>3</b>
<b>3</b>	<b>Estado</b>	<b>3</b>
<b>4</b>	<b>Configuración</b>	<b>4</b>
4.1	Usuarios	4
4.2	Reglas de acceso	6
4.3	Dispositivos	8
4.4	Red	11
<b>5</b>	<b>Administración</b>	<b>16</b>
5.1	Cambiar Clave	16
5.2	Política de restricción de acceso basada en IP	16
<b>6</b>	<b>Mi cuenta</b>	<b>17</b>
<b>7</b>	<b>Mensajes</b>	<b>18</b>
<b>8</b>	<b>Informes</b>	<b>19</b>
8.1	Conexiones de usuarios	19
8.2	Inicios de sesión fallidos	20
8.3	Conectividad de conectores	20

# 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:



The screenshot shows the 'Acceso Remoto' administration interface. The header includes the title 'Acceso Remoto' and the Movistar logo. The user ID 'INN0187763' is displayed in the top right. A sidebar on the left contains navigation options: Estado, Configuración (with sub-items: Usuarios, Reglas, Dispositivos, Red), Administración (with sub-item: Mi cuenta), Mensajes, Informes, Centro de ayuda, and Cerrar sesión. The main content area is titled 'Estado del sistema' and shows 'Conexiones activas: 0' and 'Conector VPN: Conectado'. Below this is a table with the following data:

Nombre <small>(haga clic para detalles)</small>	Versión	Estado	Rutas
DESKTOP-4VDR01D	3.7.9.1903	✓	172.21.136.164 172.21.128.0 (Máscara: 255.255.240.0)

## 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.

**Acceso Remoto**

INN0114152

Usuarios remotos Elija una acción...

Nombre de usuario <i>(haga clic para detalles)</i>	Autenticado por	Estado
alartesting	Acceso Remoto	Habilitado
asavie-1ftest	Acceso Remoto	Habilitado
cathaltesting	Acceso Remoto	Habilitado
ftest	Acceso Remoto	Habilitado
sre_test_mac_f1	Acceso Remoto	Habilitado
w11	Acceso Remoto	Habilitado

[Añadir usuario](#) [Finalizar](#)

#### 4.1.1 Detalles y estado

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

**Acceso Remoto**

INN0114152

Configuración de usuario remoto (w11) Elija una acción...

**Detalles y estado**

**Nombre de usuario :** w11 Agregar nuevo dispositivo

**Estado :** Habilitado

**Autenticado por :** Acceso Remoto

**Denegaciones :** 0

**Última denegación :** -

**Política de acceso de red**

**Autenticación/Política de bloqueo**

[Guardar](#) [Cancelar](#)

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**

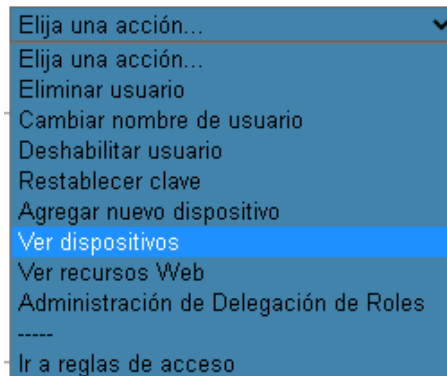
Define la configuración de la política de bloqueo que incluye Denegaciones máximas, el máximo número de denegaciones permitidas antes de que se bloquee a un usuario, así

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


### Reglas de acceso

Elija un tipo de regla... ▼

Reglas de acceso IP

---

 **Acceso de red**  
Configure los servicios de red que están disponibles en su VPN. Estas reglas se aplican a todos los usuarios.

 **Acceso de usuario**  
Configure el acceso a los servicios de red a nivel de usuario.

### 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).

## Reglas de acceso de red

Elija una acción...

### Vista simplificada

Seleccione los servicios de red que desee permitir:

[» Más información...](#)



#### Permitir

Todo

#### Servicios

Active-Directory  
ActiveSync  
AH  
Cradle-ActiveSync  
DNS  
ESP  
Exchange  
FTP  
ICMP  
Mail-IMAP

**Sugerencia:** para permitir todos los servicios, añada **Todo** a la lista Permitir. Para permitir sólo pruebas de conectividad Ping, permita **DNS** e **ICMP**.

Cree la lista **Permitir** seleccionando servicios de la lista **Servicios** y haciendo clic en el botón  para añadir su selección. Para eliminar servicios selecciónelos en la lista Permitir y haga clic en el botón . Si desea ver la lista de control de acceso resultante, elija la acción **Ver reglas de lista de control de acceso**.

Si desea definir nuevos servicios, definir las reglas de acceso con direcciones IP o crear listas de control de acceso más complejas, elija la acción **Vista avanzada**.

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**:

### Definir regla de acceso

Puede añadir reglas para controlar el acceso a los servicios definidos en su red. Si desea definir nuevos servicios, haga clic en el botón 'Nuevo servicio'.

<b>Acción:</b>	Permitir ▼				
<b>Destino:</b>	<input checked="" type="radio"/> cualquiera <input type="radio"/> Dirección: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> Máscara de red: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>				
<b>Servicio:</b>	<input type="text" value="Todo"/> ▼ <input type="button" value="Nuevo servicio"/>	<b>Protocolo</b>	<b>Operación</b>	<b>Puerto1</b>	<b>Puerto2</b>
		ip	-	-	-

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

---

Reglas de acceso de red Elija una acción... ▾

Vista avanzada

---

Acción	Servicio	Destino	Reordenar	
permitir	Todo	cualquiera	▾	Eliminar
denegar	Todo	cualquiera	▴	Eliminar

[Finalizar](#)

#### 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 individual, o se puede configurar para grupos y asignar al usuario a estos grupos.

---

Reglas de acceso: usuarios

▣ Reglas de acceso de grupo

---

Las reglas de acceso de grupo permiten definir fácilmente los conjuntos de reglas de acceso comunes a varios usuarios.

No hay grupos configurados actualmente.

[Atrás](#)

▣ Usuarios

---

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:



- [Estado](#)
- [Configuración](#)
  - Usuarios
  - Reglas
  - Dispositivos
  - Red
- [Administración](#)
- [Mi cuenta](#)
- [Mensajes \(16\)](#)
- [Informes](#)
- [Centro de ayuda](#)
- [Cerrar sesión](#)

INN0114152

**Dispositivos de acceso remoto** Elija un tipo de dispositivo... ▾

-  **Cliente VPN**  
Los PC con clientes VPN IPSec aprovisionados actualmente en su VPN.
-  **Dispositivos de APN móvil**  
Dispositivos que usan acceso de APN móvil (incluidos smartphones y PDA) aprovisionados actualmente en su VPN.

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)

Hombre	Descripción	Certificado <small>(haga clic para obtener detalles)</small>
AS-LT-07	Windows Vista	<a href="#">Descargar</a>
AS-LT-711	Windows Vista	<a href="#">Descargar</a>
DESKTOP-7208K7E	Windows Vista	<a href="#">Descargar</a>
AS-LT-702	Windows Vista	<a href="#">Descargar</a>

### 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.

## Dispositivos móviles (acceso de APN)

Número <i>(haga clic para obtener detalles)</i> ▲	Usuario	Estado
(+34)609776001	usuario1	Habilitado
(+34)609776005	usuario5	Habilitado
(+34)609776007	usuariob	Habilitado

[Atrás](#)

Haga clic en el número para ver más detalles:

**INN0151528**

---

Dispositivo móvil (Movil) Elija una acción... ▼

---

**Detalles y estado**

---

**Usuario:** usuario1  
**Número:** (+34)609776001  
**Estado:** Habilitado

**Detalles de configuración :**

**Nombre del punto de acceso:** accesoremoto.movistar.es  
**Tipo de autenticación:** Normal  
**Nombre de usuario:** usuario1  
**Clave:** \*\*\*\*\* *(clave de la VPN del usuario)*

**Nota:** El acceso remoto con APN móvil "accesoremoto.movistar.es" sólo es posible con líneas móviles Movistar.

[Atrás](#)

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**:

---

**Dispositivo móvil (Movil)**

---

**Deshabilitar dispositivo móvil**

---

Ha seleccionado **deshabilitar** el dispositivo móvil (+34)609776001 para el usuario usuario1. Este usuario dejará de poder iniciar sesión desde este dispositivo móvil.

¿Está seguro de que desea deshabilitar el dispositivo?

[Cancelar](#)

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

## Dispositivo móvil (Movil)

### Eliminar dispositivo móvil

Ha seleccionado **eliminar** el dispositivo móvil (+34)609776001 para el usuario usuario1 . Este usuario dejará de poder iniciar sesión desde este dispositivo móvil.

¿Está seguro de que desea eliminar el dispositivo?

Eliminar dispositivo

Cancelar







## 4.4 Red

Opciones de configuración de red:

**INN0151123**


---

**Configuración de red** Elija una acción... ▼

-  **Conectores**  
Configure los conectores VPN implementados en la red e implemente nuevos conectores.
-  **Rutas**  
Vea y/o edite las rutas IP accesibles a través de la VPN.
-  **Control de extremo final / cuarentena**  
Configure el acceso restringido a la red (cuarentena) basándose en las comprobaciones definidas en el extremo final de acceso.
-  **Política de claves para usuarios remotos**  
Configure el estándar mínimo permitido de claves de usuarios remotos.
-  **Single Sign-On**  
Configure la autenticación de los usuarios usando la infraestructura de autenticación existente (p. ej. Dominio de Windows / RADIUS).
-  **Zona horaria de la VPN**  
Configure la zona horaria que se aplica en su VPN.

### 4.4.1 Conectores

Proporciona detalles del conector VPN de la cuenta de servicio:

 **Conectores VPN** Elija una acción... ▼

En esta tabla se muestran los conectores VPN implementados en su red. Un conector VPN es el componente de "LAN corporativa" de la solución VPN y se debe instalar en un equipo que esté **siempre encendido** (p. ej. servidor de correo o de archivos).

Nombre <i>(haga clic para obtener detalles)</i>	Estado	Última modificación del estado
DESKTOP-4VDRC1D	<b>Conexión activa</b>	29 abr 2022 00:47:21

Finalizar

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

## Detalles del conector VPN

Elija una acción... ▼

### Resumen

**Nombre:** DESKTOP-4VDRC1D

**Estado:** Conexión activa (Última modificación 29 abr 2022 00:47:21)

### Capacidades de red y servicio

**Servicios:** Retransmisión de DNS

**Rutas:** 172.21.136.164

172.21.128.0 (Máscara: 255.255.240.0)

Predeterminado (Habilitado)

### Detalles de la instalación

### Certificado digital

[Atrás](#)

#### 4.4.1.1 Acciones de conectores

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

### Reiniciar conector VPN (DESKTOP-4VDRC1D)

#### Confirmar reinicio

**Tenga en cuenta** que la solicitud de reinicio puede tardar unos segundos en procesarse.

Reiniciar ahora

[Cancelar](#)

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

### ¿Deshabilitar Conector VPN DESKTOP-4VDRC1D?

Sí

No

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

### Conectores VPN

### ¿Está seguro de que desea eliminar el conector VPN (DESKTOP-4VDRC1D)?

Sí

No

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

## Configurar el conector VPN (DESKTOP-4VDRC1D)

Normalmente la configuración automática es suficiente para establecer una VPN. Sin embargo, en algunos casos es necesario realizar una configuración adicional. Expanda las opciones de abajo para obtener más detalles.

### **Gestión de la VPN**

Utilice esta opción para controlar si hace falta proporcionar sus credenciales de administrador para iniciar sesión de esta aplicación desde este conector (**DESKTOP-4VDRC1D**). El valor predeterminado es no solicitarlo (es decir, no se necesitan credenciales).

Se necesitan credenciales para gestionar la VPN desde este conector.

### **Servidor DNS de la VPN**

El conector VPN seleccionará normalmente el servidor DNS utilizado por su servidor host. Si no es adecuado como servidor DNS para su VPN, puede cambiarlo aquí.

Usar valor predeterminado del conector. **IP del servidor DNS:**  .  .  .

### **Intervalo de conexión Keepalive**

Algunos Firewalls de frontera están configurados para cortar sesiones TCP inactivas tras un breve periodo de tiempo. Si este tiempo de espera de inactividad es demasiado breve (normalmente menos de 5 minutos), puede interferir con la conectividad de su VPN. Aunque la solución preferida es ampliar el tiempo de espera de inactividad en el Firewall que presenta el problema, se puede mejorar la conectividad reduciendo el intervalo de Keepalive para forzar al Firewall a mantener la conexión activa.

Usar valor predeterminado del conector **Intervalo de Keepalive:**  segundos

### Finalizar

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

## Rutas

Elija una acción... ▼

Descargar

Actualizar

Destino ▲	Máscara de red	Métrica	Conector	Estado
172.21.128.0	255.255.240.0	1	DESKTOP-4VDRC1D	Activo
172.21.136.164	255.255.255.255	0	DESKTOP-4VDRC1D	Activo

### 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:

#### Política de claves

Puede configurar la política de claves para sus usuarios remotos aquí. Esto incluye el número mínimo de caracteres de clave que se deben proporcionar, así como el número mínimo de grupos de caracteres que deben estar representados.

La configuración recomendada es un mínimo de 8 caracteres y al menos 3 grupos de caracteres representados en la clave.

#### Detalles

Existen 4 grupos de caracteres:

- Mayúsculas A-Z
- Minúsculas a-z
- Números 0-9
- Caracteres no alfanuméricos

Caracteres mínimos:

Grupos mínimos de caracteres:

Guardar

Cancelar

#### 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.

##### Single Sign-On (SSO)

Single Sign-On (SSO) permite autenticar los inicios de sesión de usuarios remotos con su infraestructura de autenticación privada propia.

Solo puede haber un método de SSO habilitado a la vez. La autenticación de un usuario mediante SSO o no se especifica de forma individual. Si se selecciona SSO, su infraestructura de autenticación interna DEBE reconocer el nombre de usuario. Tenga en cuenta que los dispositivos móviles configurados para usar credenciales autogeneradas **no** se autentican mediante SSO.

##### Dominio de autenticación de Windows

Seleccione esta opción si desea usar sus credenciales del dominio de Windows para Single-Sign-On.

[» Más información...](#)

Habilitar SSO (dominio de Windows)

##### Autenticación RADIUS

Seleccione esta opción si desea usar su servidor RADIUS interno existente para Single-Sign-On.

[» Más información...](#)

Habilitar SSO (RADIUS)

Servidor RADIUS:

Puerto:

Secreto:

#### 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".

### Zona horaria de la VPN

La zona horaria configurada para su VPN afecta a los siguientes aspectos de su funcionamiento:

**Valores horarios mostrados:** Todas las horas mostradas por esta aplicación son horas locales de la zona horaria de su VPN.

Se asigna una zona horaria predeterminada a su VPN en el momento de la creación de su cuenta. Puede cambiar esta configuración abajo.

La hora local actual de la zona horaria de su VPN es **31 ago 2010 12:31:19**

#### Configurar la zona horaria de la VPN

Zona horaria de la VPN:



Usar horario de verano

## 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.

### Administración

Elija una acción...

-  **Cambiar clave**  
Cambie la clave de administrador.
-  **Política de restricción de acceso basada en IP**  
Configure ubicaciones desde las que se puede tener acceso a esta interfaz de administración.

### 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

#### Política recomendada de claves

Recomendamos que elija una clave que cumpla con nuestra [política recomendada de claves](#).

**Es su responsabilidad elegir una clave segura.**

#### Cambiar clave

El indicador del nivel de seguridad de claves indica si su nueva clave cumple con nuestra recomendación de seguridad.

**Clave anterior:**

**Nueva clave:**

**Confirmar clave:**

Inseguro  Seguro

[Cancelar](#)

### 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.



## Política de restricción de acceso basada en IP

### Detalles

Se puede configurar una lista de direcciones IP y subredes desde las cuales está permitido el acceso a ésta web de administración. Si no se especifica ninguna dirección IP, el acceso a la web de administración será permitido desde CUALQUIER ubicación.

Dirección IP:  .  .  .       Máscara de red: 255.255.255.255 ▼

Dirección IP	Máscara IP	

[Finalizar](#)

## 6 Mi cuenta

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

### Resumen de cuenta

Elija una acción... ▼

**Código de cliente:** INNO187763

**Fecha de inicio de la cuenta:** 21 abr 2022

**Correo electrónico de contacto:** enric.garrigaprat@telefonica.com

**Numero permitido de usuarios:** 3

**Número de usuarios configurados:** 2

[Atrás](#)

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

## Modificar número de usuarios permitidos

### Configurar nuevo total

Proporcione su clave para confirmar la actualización.

**Total actual:** 3

**Nuevo total:**

**Clave:**

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.



The screenshot shows the Movistar administrator interface. At the top right is the Movistar logo and the user ID 'INNCOR28083'. On the left is a navigation menu with options: Estado, Configuración (with sub-items: Usuarios, Reglas, Dispositivos, Red), Administración (with sub-item: Mi cuenta), Mensajes (2), Informes, Centro de ayuda, and Cerrar sesión. The main content area is titled 'Mensajes (2)' and includes a 'Marcar todo como leído' button and an 'Elegir vista...' dropdown. Below this is a table with the following data:

Fecha de creación	Asunto	Mensaje	Estado de lectura
12 sep 2014 19:17:14	corourke@movistar.es	Se ha aceptado la invitación. <a href="#">Haga clic aquí para ver los detalles del usuario</a>	

## 8 Informes

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

# Acceso Remoto



INN0187763

- Estado
- Configuración
  - Usuarios
  - Reglas
  - Dispositivos
  - Red
- Administración
  - Mi cuenta
- Mensajes
- Informes
- Centro de ayuda
- Cerrar sesión

### Informes

Elija un informe...

- Conexiones de usuarios**  
Un log de auditoría de conexiones correctas de usuarios remotos a la VPN. Este log contiene las horas de inicio y finalización de conexiones, además de estadísticas de tráfico.
- Inicios de sesión fallidos**  
Un log de auditoría de los intentos fallidos de inicio de sesión de usuarios remotos, incluyendo el motivo del fallo y la hora en que ocurrió.
- Sesiones de conector**  
Un log de auditoría de las conexiones de conectores VPN, incluyendo las horas de inicio y finalización. La VPN solamente está disponible cuando los conectores VPN están conectados.
- Logs W3C**  
Existen logs en formato W3C para toda actividad VPN. Dado que estos logs suelen ser muy grandes, **no están disponibles aquí**, sino en el servidor donde se ubica el conector VPN.

### 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

### Informes

Conexiones de usuarios

Conexiones de usuario en las últimas 24 horas

Descargar Actualizar Personalizar

Usuario	Dispositivo	Hora de inicio ▼	Hora fin	Bytes de transmisión	Bytes de recepción
nreville@movistar.es	(+34) 1234567890	15 sep 2014 12:16:15	15 sep 2014 12:16:33	1956	35645
nreville@movistar.es	(+34) 1234567890	15 sep 2014 12:16:03	15 sep 2014 12:16:11	1123	24634
nreville@movistar.es	(+34) 1234567890	15 sep 2014 11:54:33	15 sep 2014 12:15:12	1046	22973

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

Atrás

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

**Informes** Conexiones de usuarios ▾

**Personalizar el informe**

Mostrar conexiones de usuario desde:

hasta:

**Opciones avanzadas**

---

< **ene 2022** >

dom	lun	mar	mié	jue	vie	sáb
						<b>1</b>
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

## 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

**Informes** Inicios de sesión fallidos ▾

Inicios de sesión erróneos en las últimas 24 horas

Usuario	Dispositivo	Causa	Hora ▼
nreville@movistar.es	(+34)1234567890	Intento de inicio de sesión fuera del horario permitido	15 sep 2014 13:00:46
nreville@movistar.es	(+34)1234567890	Usuario no habilitado	15 sep 2014 12:40:27
nreville@movistar.es	(+34)1234567890	Usuario no habilitado	15 sep 2014 12:40:26

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

[Atrás](#)

## 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](http://www.telefonica.com)