Manual de Usuario

Servicio Access Remoto Básico (ARB)

Telefónica Empresas

29 de abril de 2022

Índice

1. Introducción

Este documento es una guía de uso orientada a los usuarios del servicio Acceso Remoto de Movistar. Este servicio consta de 2 métodos de acceso diferentes:

- **Cliente VPN**

  El método de acceso con cliente VPN se utiliza cuando quiera conectarse a la red corporativa desde un PC/Portátil Windows o MAC. En su PC/Portátil será necesario instalar un software cliente (Cliente VPN).

- **APN móvil**

  El método de acceso con APN móvil se utiliza para establecer una conexión directa con la LAN corporativa del cliente mediante la llamada al APN del servicio:

  Para utilizar este método de acceso necesitará una SIM movistar. Con este método de acceso, todo el tráfico procedente de su dispositivo móvil (Smartphone/Tablet/PC-Portátil con pincho USB Movistar) se entrega a la red corporativa del cliente.

2. Cliente VPN

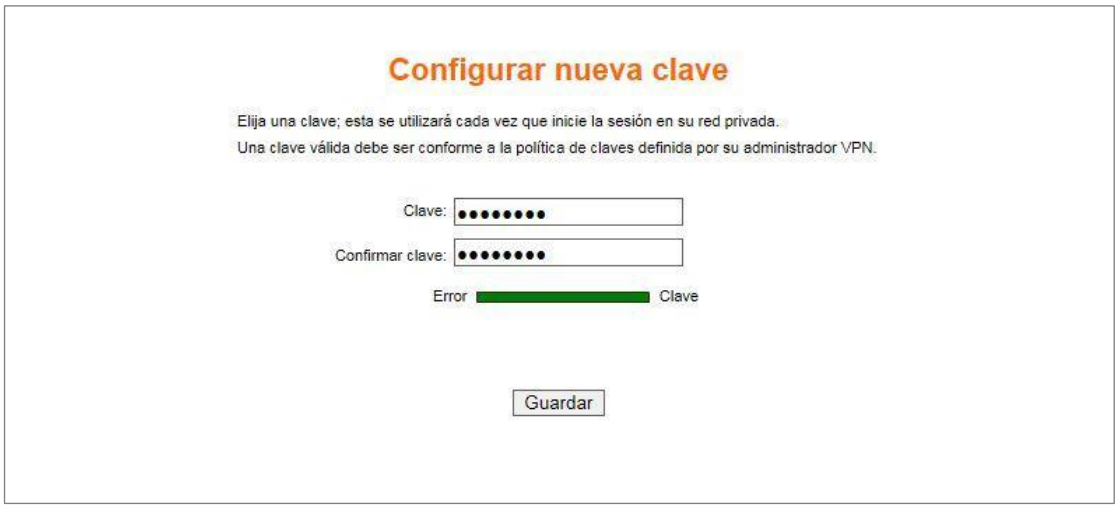
2.1. Instalación del cliente VPN para Windows

Si su administrador le habilita este método de acceso recibirá un email con las instrucciones para la instalación del cliente VPN en su PC/Portátil Windows:

> Estimado usuario,
>
> El administrador del servicio de su empresa le ha habilitado el acceso remoto a la oficina a través del servicio Movistar Acceso Remoto.
> Para completar el proceso de activación y poder disfrutar del servicio, por favor siga las instrucciones del siguiente enlace:
>
> https://www.accesoremoto.movistar.es/UserPortal/Login.aspx?type=reg&reqid=ZFapyokGYboG1zJB%2bHS3vQ%3d%3d&chcode=5450
>
> Si la dirección no funciona, inténtelo copiando la dirección completa en la barra de direcciones de su navegador web. La dirección no debe contener saltos de línea.
>
> Gracias,
>
> Movistar
>
> Este correo ha sido generado automáticamente. Por favor no responda a este correo.

Deberá hacer clic en el enlace del correo electrónico a fin de iniciar el proceso de configuración del cliente VPN.

Es posible que su administrador haya configurado una clave de acceso que le habrá enviado por separado. Si no dispone de la clave de acceso solicítesela a su administrador. Esta clave la deberá cambiar en el primer acceso.



Configure la nueva clave y haga clic en **Guardar**:

A partir de aquí puede iniciar el proceso de instalación del conector. Tras leer los requisitos haga clic in **Descargar:**

Esto hará que se abra una nueva ventana en la que tendrá la posibilidad de seleccionar entre la versión del software de 32 o 64 bits:

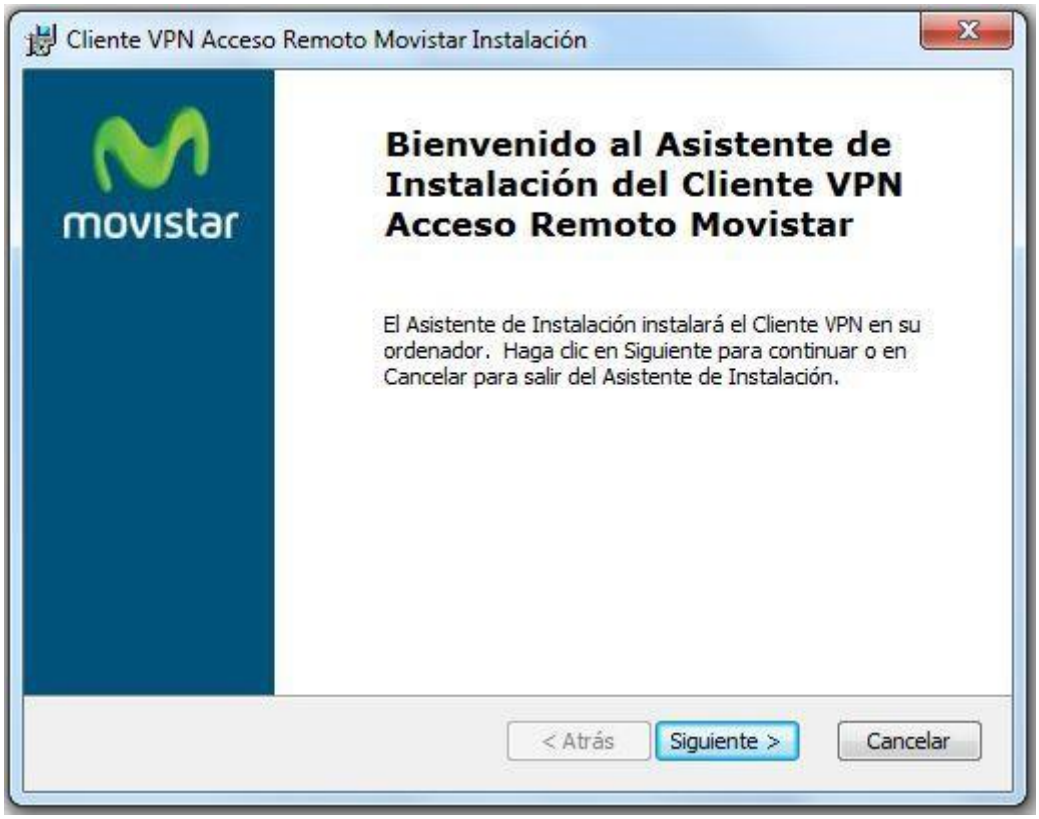
Seleccione la versión correcta del software y haga clic en **Descargar.**

La instalación en requiere privilegios de administrador. En función de su versión y configuración de Windows, durante la instalación tendrá que aceptar los mensajes de Control de cuentas de usuario (UAC).

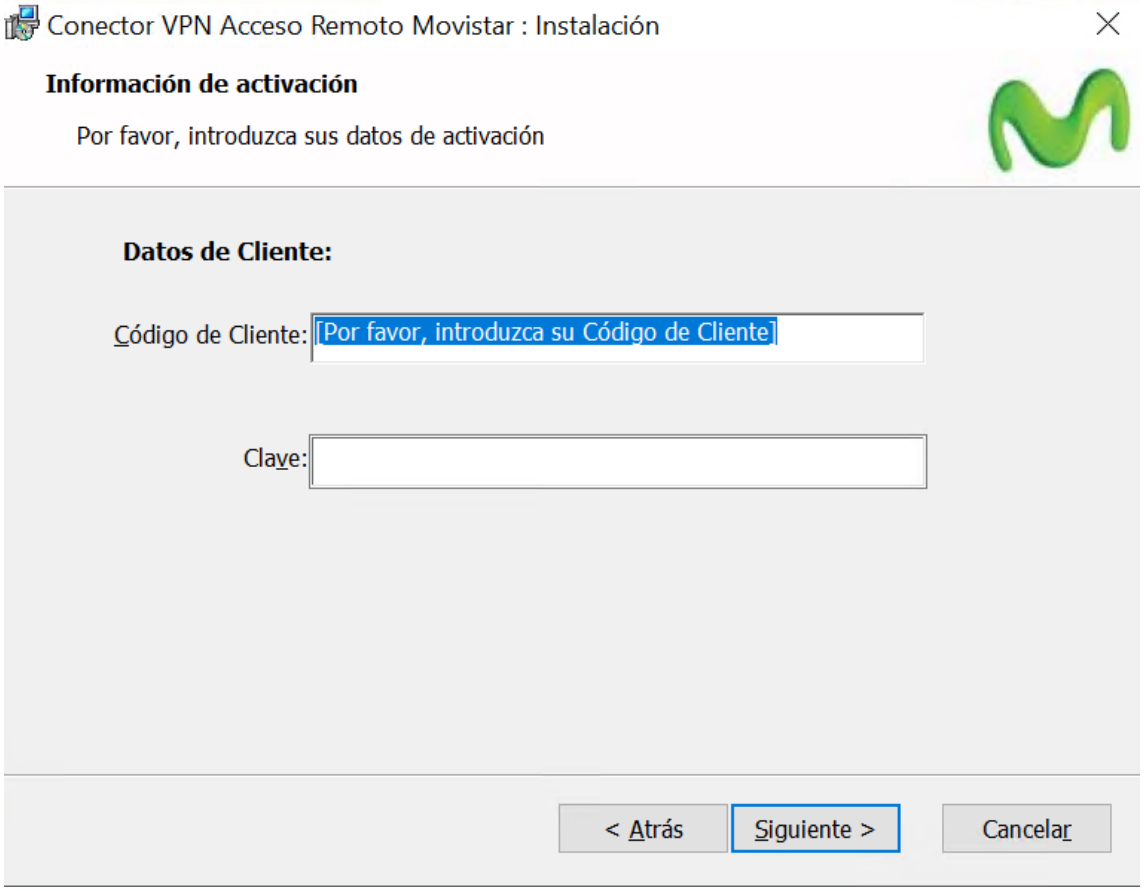
Si no tiene permisos suficientes sobre su PC, póngase en contacto con su administrador.

Una vez finalizada la descarga, haga doble clic en el archivo del instalador para iniciar la instalación.

Haga clic en **Siguiente >** para iniciar la instalación.



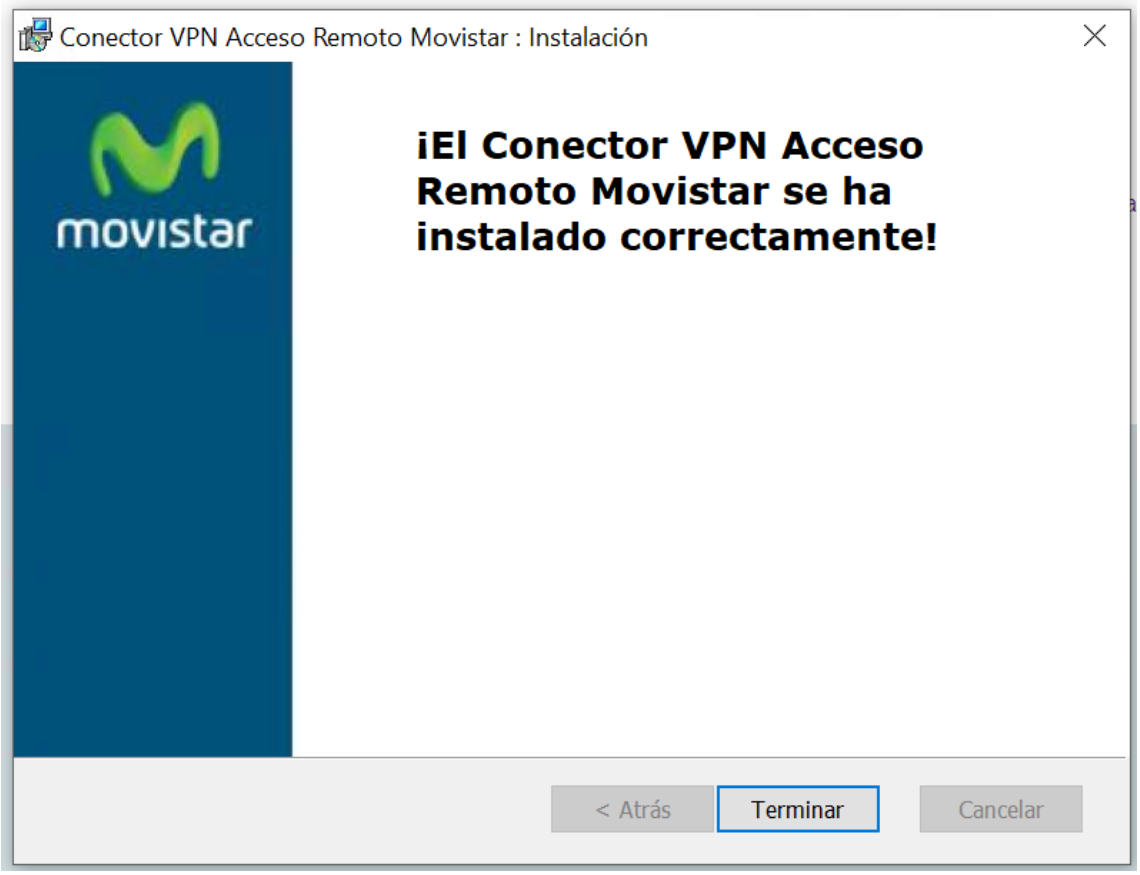
Introduzca el **Código de cliente** (habitualmente un código que comienza por INN + 6 dígitos) y la **Clave de acceso a portal**, y haga clic en **Siguiente >.**



Haga clic en **Instalar**:

Una vez comprobados los detalles de la activación, el instalador inscribirá el PC Windows en su cuenta de servicio de Acceso Remoto.

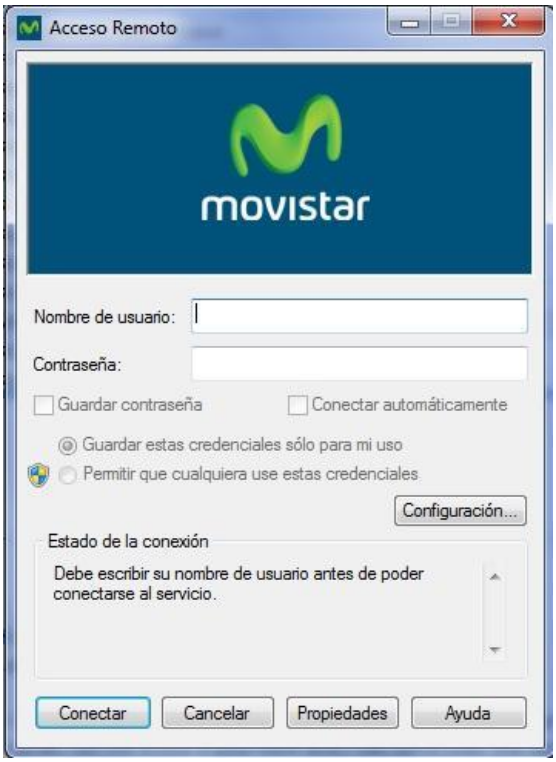
Cuando el proceso se haya completado, marque la casilla "**Iniciar Acceso Remoto**" y haga clic en **Terminar**:



El cliente VPN se integra directamente en el centro de redes y recursos compartidos de Windows. Además, se instala un icono en el escritorio y podrá encontrar el cliente VPN del servicio *Acceso Remoto* en el menú de inicio de Windows.

2.2. Utilización del cliente VPN en Windows

Para conectarse a su red corporativa inicie el cliente VPN, haciendo doble clic en el icono del escritorio, o bien seleccione **Programas -> Telefónica Acceso Remoto -> Acceso Remoto**.



Introduzca el **Nombre de usuario y la contraseña** y haga clic en **Conectar**.

Cuando la conexión VPN se haya establecido con éxito, el cuadro de diálogo se cerrará automáticamente.

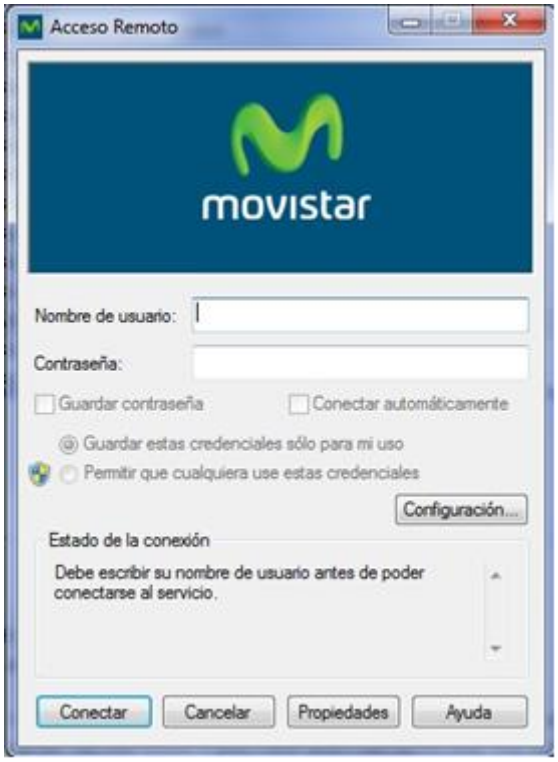
Para desconectarse, inicie de nuevo el cliente. Se solicitará que confirme si desea desconectarse.

Mientras el Cliente VPN esté conectado, todo el tráfico que genere desde su PC/Portátil se enviará a su red corporativa a través del túnel VPN creado. Esto significa que cualquier aplicación corporativa (correo electrónico, SharePoint, archivos y carpetas, etc.) debería funcionar exactamente de la misma manera que si estuviera en su oficina.

Si su administrador le habilita la funcionalidad “split-tunnel”, el tráfico hacia Internet no se enviará a su red corporativa, sino que va directamente a Internet desde su PC/Portátil.

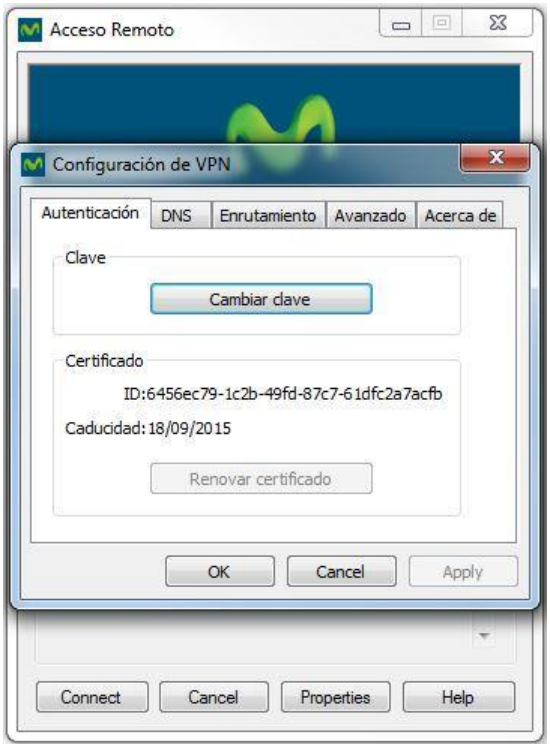
- Ajustes avanzados:

Haga clic en **Configuración** para acceder a los ajustes avanzados:



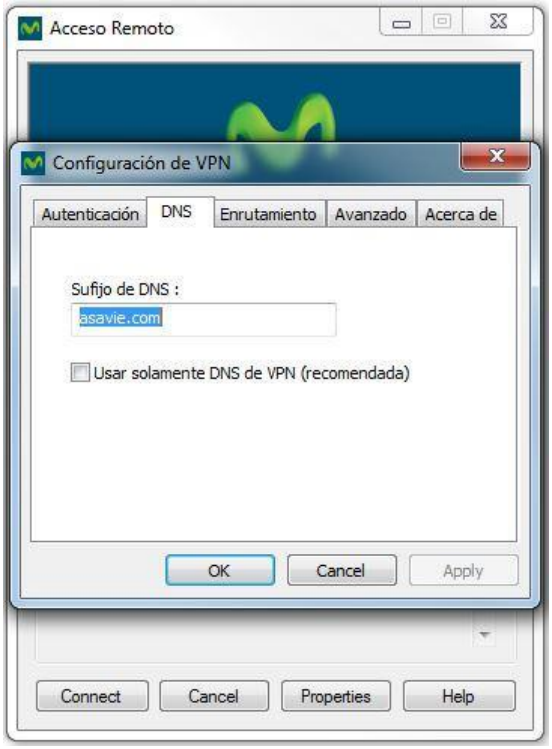
Pestaña de Autenticación

Desde esta pestaña podrá cambiar su clave de acceso remoto:



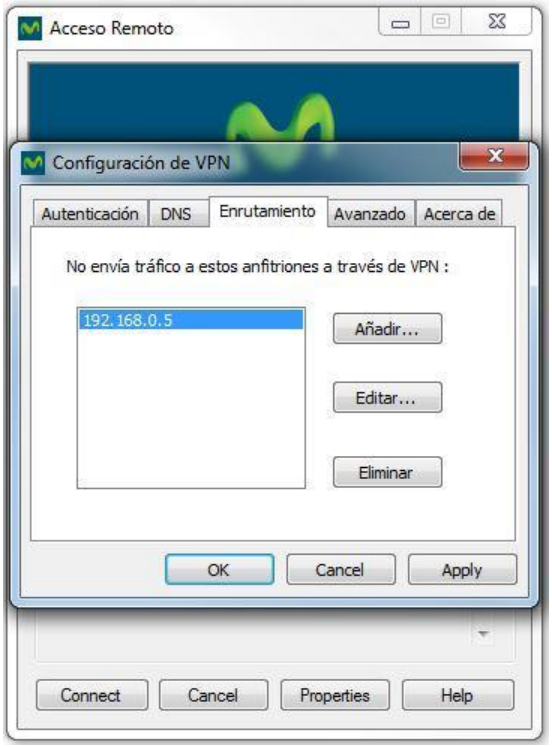
Pestaña de DNS

Desde esta pestaña podrá cambiar el sufijo DNS de su VPN:



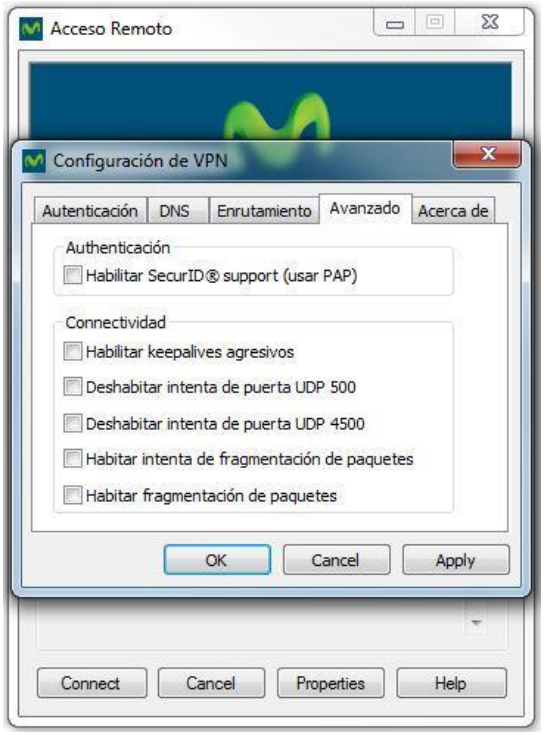
Pestaña de Enrutamiento

Desde esta pestaña, podrá añadir los destinos que no deben enrutarse a través del túnel VPN (por ejemplo, la dirección IP de su impresora local):



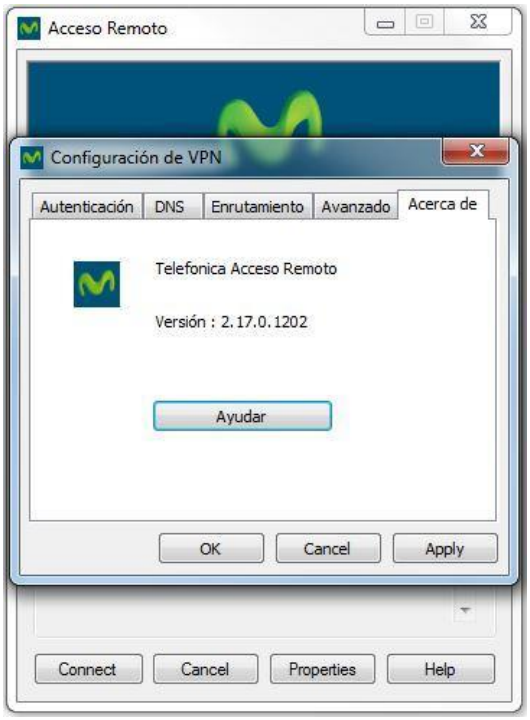
Pestaña Avanzado

Desde esta pestaña, podrá habilitar/deshabilitar distintas pruebas de conectividad y configurar otras opciones avanzadas. No se recomienda hacer modificaciones en esta pestaña:



Pestaña ‘Acerca de’

En esta pestaña se muestra información sobre la versión del cliente VPN:

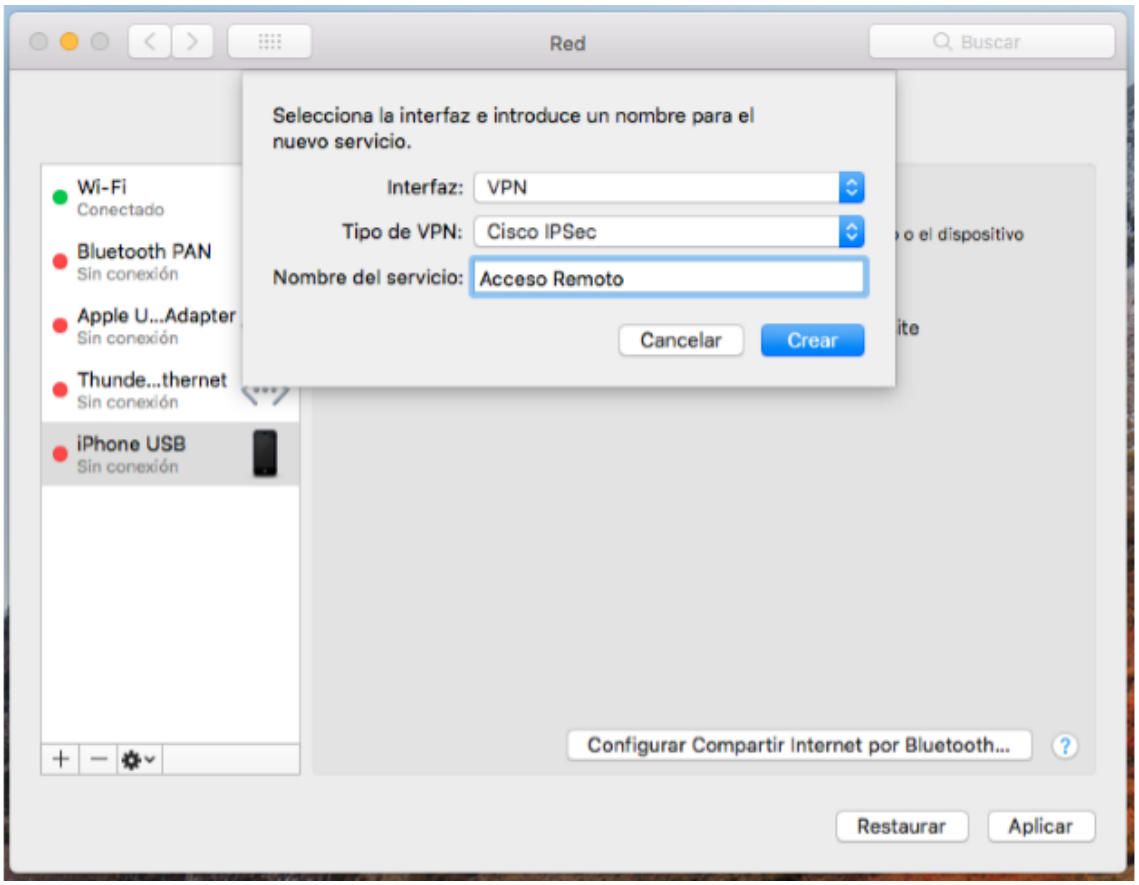


2.3. Configuración del cliente VPN para MAC

En este caso, el Administrador de la cuenta de Acceso Remoto deberá proporcionar al usuario el nombre de cuenta y la contraseña que ha creado en el portal de ARB, para que el usuario los pueda introducir durante el proceso de configuración. A diferencia de Windows, no es necesario instalar un cliente VPN en el dispositivo MAC para poder realizar la conexión a Acceso Remoto mediante este dispositivo.

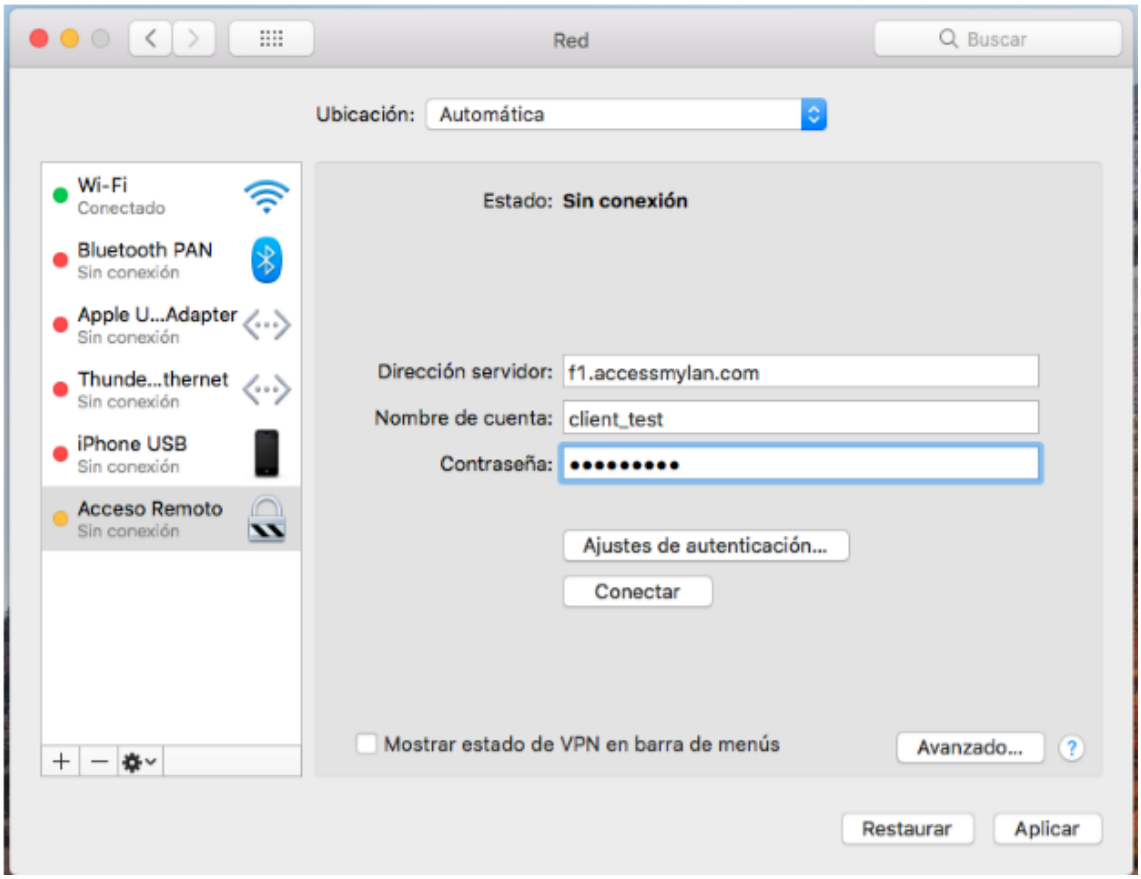
Para crear un nuevo cliente VPN en un dispositivo MAC, los pasos a realizar son los siguientes:

1. En su dispositivo Mac, vaya a Preferencias de Sistema y escoja Red. Haga clic sobre Anadir “+” debajo de la lista de servicios a la izquierda. Para el apartado **Interfaz**, elija “VPN”, y para **Tipo de VPN** elija “Cisco IPSec”. Designe un **Nombre del servicio**, en este caso Acceso Remoto. Cuando haya finalizado, haga clic en Crear.



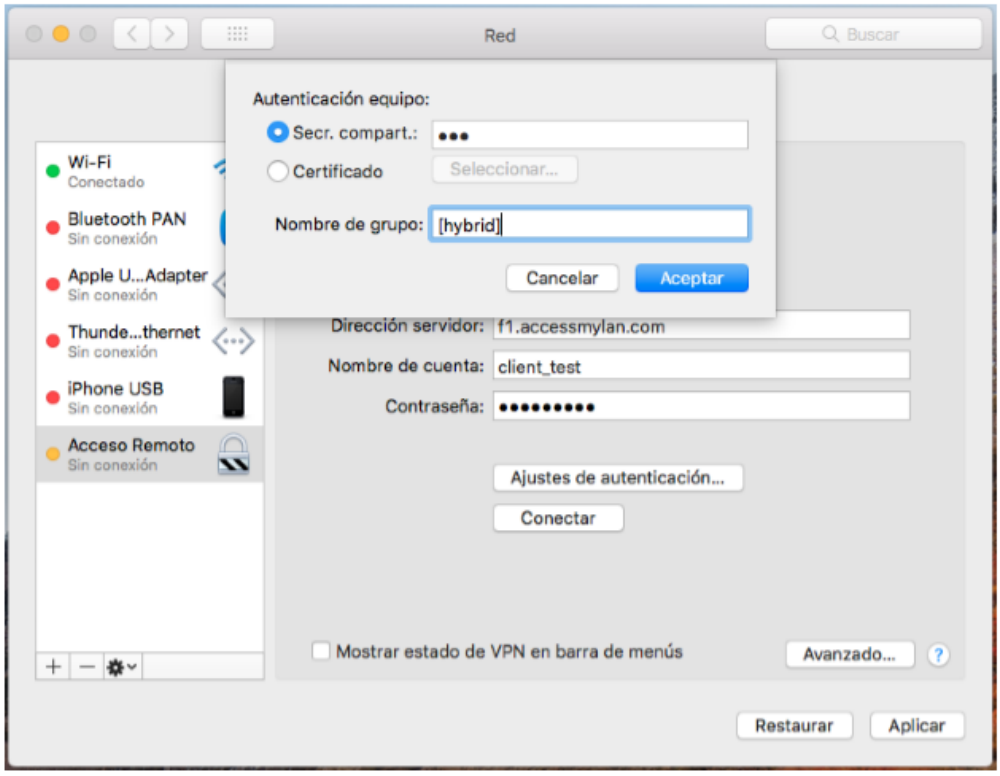
2. Tras crear el cliente VPN, tendrá que ingresar los datos para poder establecer la conexión de Acceso Remoto en los apartados siguientes:

- **Dirección de Servidor:** f1.accessmylan.com
- **Nombre de cuenta:** Introduzca el nombre de usuario Cliente VPN de Acceso Remoto.
- **Contraseña:** Introduzca la contraseña del usuario de Acceso Remoto, que le tendrá que proporcionar el Administrador de la cuenta.

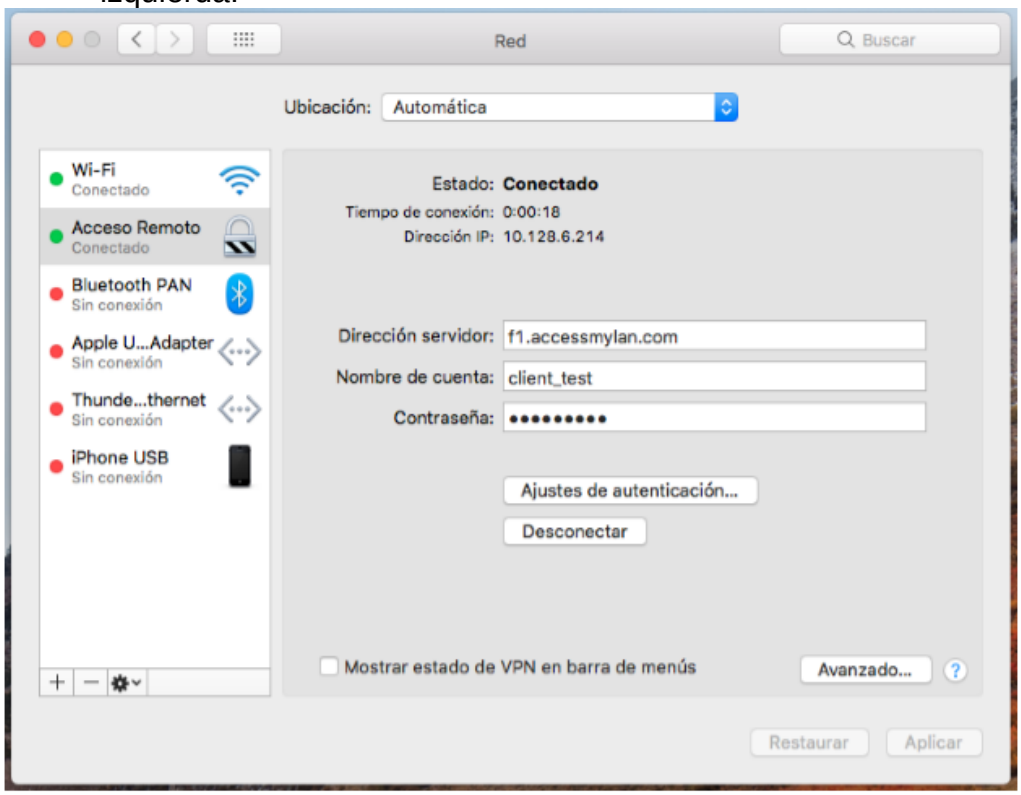


3. Tras introducir los datos, el usuario tendrá que dirigirse a Ajustes de Autenticación e introducir los siguientes datos y realizar las siguientes acciones:

- En **Secreto compartido**, podrá introducir una palabra cualquiera.
- **Nombre de grupo:** [hybrid]
- Haga clic en Aceptar.
- Haga clic en Conectar.
- Haga clic en Aplicar.



4. Tras finalizar, vera el servicio de Acceso Remoto en el listado en la parte izquierda:



3. APN móvil (ordenadores y dispositivos móviles)

3.1. Utilización del acceso mediante APN móvil

Con este método de acceso todo el tráfico procedente del dispositivo móvil (Smartphone/Tablet/PC-Portátil con pincho USB Movistar) se entrega a la red corporativa del cliente.

El acceso mediante APN privado no permite *split-tunnelling* (todo el tráfico se entrega a la red privada de su empresa, por lo que **para acceder a Internet el móvil usara el proxy de navegación de su empresa).**

3.2. Configuración accesos con APN móvil

Para utilizar este método de acceso necesitará una línea de contrato movistar. Para iniciar sesión con el APN móvil del servicio, debe configurar una conexión nueva en su escritorio Movistar (Accesos desde PC/Portátil) o en los ajustes de su Smartphone para utilizar el APN privado del servicio: **accesoremoto.movistar.es.**

El procedimiento para configurar el APN móvil depende del tipo de terminal. Por otro lado, si dispone de un MDM/UEM puede seguir una guía especifica que permite una configuración más rápida.

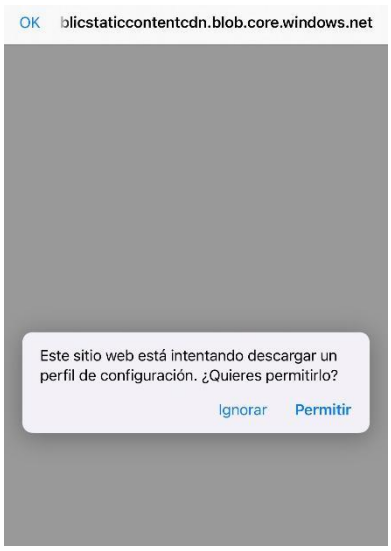
3.2.1. Configuración del APN en iPhone/iPad

La configuración del APN móvil para terminales iOS / iPadOS se realiza mediante la instalación de un perfil en el terminal siguiendo unos sencillos pasos

Cómo instalar el perfil de APN

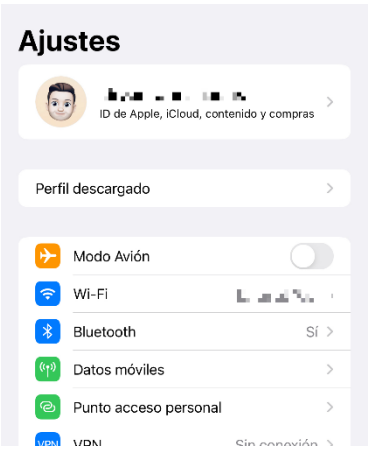
- El perfil del APN móvil está disponible en este enlace o en este código QR

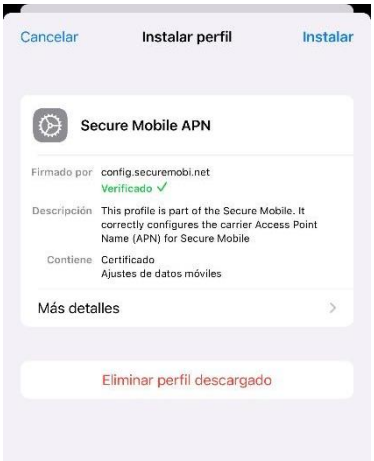
- Descárguelo, escanee el código QR o copie la URL y envíelo por SMS o correo electrónico a los terminales que necesiten ser configurados



Una vez que el archivo de configuración se haya recibido en el terminal iOS/iPadOS, selecciona las siguientes opciones de menú:

- Ajustes
- General
- Perfiles
- APN en PERFIL DESCARGADO
- Instala y sigue los pasos. Si se requiere un código de acceso, éste será el código de pantalla de desbloqueo del terminal.





Una vez completado, su terminal móvil se podrá conectar al servicio.

El *ESTADO DE LA CONEXIÓN* ahora debería mostrar Conectado en el panel de Conexiones Activas del menú de ESTADO del portal ARB.

Sugerencia: si el dispositivo no muestra un estado de Conectado en el portal:

- Asegúrese de que el dispositivo no esté conectado a Wi-Fi.
- Actualice la página del portal (tecla F5)

3.2.2. Despliegue en iPhone/iPad mediante Microsoft Intune

Nota: Microsoft Intune no admite la configuración de APN móvil para dispositivos Android de Samsung. Consulte a su contacto de soporte de Microsoft Intune para más información

Cómo crear un nuevo perfil de APN

1. Primero, descargue el perfil de configuración de iOS adecuado de este enlace (.mobileconfig)
2. En el centro de administración de Microsoft Endpoint Manager, cree un "perfil de configuración" de dispositivos iOS/iPadOS de Microsoft Intune. Ver Cómo crear un perfil de dispositivo en Microsoft Intune
   - Platform: iOS/iPadOS
   - Tipo de perfil: Personalizado
   - Nombre personalizado: nombre descriptivo para el perfil, como Perfil APN
3. En los ajustes de configuración:
   - Nombre de perfil de configuración personalizado: establecer como requerido
   - Archivo de perfil de configuración: Importar el iOS Perfil de configuración descargado en el primer paso. Verá el contenido del perfil de configuración que se muestra en Contenidos del archivo.

4. Cuando termine, regrese a la hoja Crear perfil y seleccione Crear.
5. Para instalar el perfil de configuración, debe asignarlo a los grupos de dispositivos a los que desea aplicar esta configuración. Ver Cómo asignar perfiles de usuario y dispositivo en Microsoft Intune.
    - Elija el perfil de dispositivo iOS de Microsoft Intune que creó en el segundo paso y, en la hoja Informes de perfil de APN, seleccione:
        - ADMINISTRAR
        - Asignaciones.
        - Elija: Incluir
        - Asignar a: Grupos a los que desea aplicar el perfil.
6. Guardar.
7. Microsoft Intune indicará a los dispositivos afectados que se registren con el servicio de Intune. La próxima vez que el dispositivo se registre, se aplicará el perfil del dispositivo y el dispositivo debería configurarse automáticamente para usar el APN. El proceso suele tardar menos de cinco minutos.

Ver Solución de problemas de perfiles de dispositivos en Microsoft Intune para obtener información adicional.

3.2.3. Despliegue en iPhone/iPad mediante UEM VMware Workspace ONE

Implemente la configuración de APN correcta para sus dispositivos iOS/iPadOS elegidos definiendo el perfil de dispositivo adecuado dentro de su portal de VMware Workspace ONE UEM.

En esta guía se utiliza un perfil de dispositivo separado para dispositivos iOS/iPadOS. Puede optar por modificar los perfiles de dispositivos existentes o agregar otros nuevos. Una vez que haya definido su perfil, puede aplicarlo a dispositivos individuales o a grupos.

Cómo crear un perfil

1. Vaya a:
    - Dispositivos
    - Perfiles y recursos
    - Perfiles
2. Seleccione:
    - AÑADIR
    - Añadir perfil.
3. Seleccione Apple iOS y el perfil del dispositivo

4. Configure los ajustes generales del perfil. Esta configuración determina cómo se implementa el perfil y quién lo recibe, y debe configurarse de acuerdo con las necesidades de su organización. Algunas recomendaciones incluyen:
    - *Nombre:* nombre descriptivo de la política. Por ejemplo “Perfil APN”
    - *Descripción* opcional
    - *Despliegue*: gestionado o manual de acuerdo con las preferencias del administrador
    - *Ámbito*: producción. Puede seleccionar Ambos si desea probar el perfil en el entorno de pruebas
    - *Tipo de asignación*: automático
    - *Permitir eliminación*: según las preferencias del administrador
    - *Grupos asignados:* Establezca los grupos a los que desea enviar este perfil. En este caso, asumimos que los dispositivos que deben recibir la configuración del perfil APN se agrupan a través de un grupo estándar o inteligente
    - *Excepciones:* según las necesidades del administrador
    - *Instalar solo en dispositivos dentro de las áreas seleccionadas*: no seleccionado
    - *Habilitar programación e instalar solo durante los periodos seleccionados:* no seleccionado
    - *Fecha de eliminación*: en blanco
5. Elija Payload móvil y seleccione Configurar.
6. En la lista APN (dejando los campos Adjuntar APN en blanco) configura los siguientes campos APN:
    - *APN: accesoremoto.movistar.es*
    - *Nombre de usuario: datos*
    - *Contraseña: datos*
    - *Tipo de autenticación: PAP*

Deja el resto de los campos vacíos

Selecciona Guardar y publicar.

Tras este proceso VMware Workspace ONE UEM aplicará este perfil a los dispositivos seleccionados.

Fuente: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/iOS_Platform/GUID-AWT-PROFILECELLULAR.html

3.2.4. Despliegue en iPhone/iPad mediante IBM MaaS360

Implemente el Configuración de APN para sus dispositivos iOS/iPadOS seleccionados definiendo la política MDM adecuada dentro de su portal IBM MaaS360. En esta guía se usa una política separada para dispositivos iOS. Puede optar por modificar las Políticas existentes o agregar nuevas.

Una vez que haya definido su política, puede aplicarla a individuos o grupos de dispositivos.

Cómo crear una política

1. Para agregar una nueva política desde su portal IBM MaaS360:
   - Seleccione Seguridad
   - Políticas
   - Seleccione Agregar política.
2. Introduzca las siguientes configuraciones:
   - *Nombre: Nombre* descriptivo de la política. Por ejemplo “Política de APN móvil”.
   - *Descripción*: descripción opcional
   - *Tipo:* iOS MDM
   - Plantilla*:* seleccione una política de iOS MDM existente como plantilla para su nueva política.
3. Seleccione Continuar
4. Expanda Ajustes Avanzados y seleccione Celular
5. Seleccione Editar
6. Seleccione: Configurar Ajustes Avanzados
7. Configure los siguientes campos APN:
   - *APN: accesoremoto.movistar.es*
   - *Nombre de Usuario: datos*
   - *Contraseña: datos*
   - *Tipo de Autenticación: PAP*
8. Dejar el resto de los campos vacíos

Guardar y Publicar.

Para publicar la política, introduzca:

- Descripción opcional para revisiones futuras
- Contraseña

Seleccione Continuar.

Su nueva política MDM de iOS ahora se puede aplicar a dispositivos individuales o a grupos.

3.2.5. Despliegue en Samsung Knox mediante UEM VMware Workspace ONE

Implemente la configuración de APN móvil para sus dispositivos Samsung Knox elegidos definiendo el perfil de dispositivo apropiado dentro de su portal de VMware Workspace ONE.

En esta guía se utiliza un perfil separado para los dispositivos Samsung Knox. Puede optar por modificar los perfiles de dispositivos existentes o agregar otros nuevos. Una vez que haya definido su perfil, puede aplicarlo a individuos o grupos de dispositivos.

Cómo crear un perfil

1. Vaya a:
    - Dispositivos
    - Perfiles y recursos
    - Perfiles

.Haga clic en AÑADIR

i.Añadir perfil.

2. Seleccione Android.

    Configure los ajustes generales del perfil. El perfil de APN solo se muestra cuando el campo Configuración de OEM está activado y se selecciona Samsung en el campo Seleccionar OEM. Esta configuración determina cómo se implementa el perfil y quién lo recibe, que debe establecerse de acuerdo con las necesidades de su organización. Algunas recomendaciones incluyen:

    - *Nombre:* nombre descriptivo de la política. Por ejemplo “Perfil APN”
    - *Descripción* opcional
    - *Despliegue*: gestionado o manual de acuerdo con las preferencias del administrador
    - *Ámbito*: producción. Puede seleccionar Ambos si desea probar el perfil en el entorno de pruebas
    - *Tipo de asignación*: automático

- *Permitir eliminación*: según las preferencias del administrador
- *Grupos asignados:* Establezca los grupos a los que desea enviar este perfil. En este caso, asumimos que los dispositivos que deben recibir la configuración del perfil APN se agrupan a través de un grupo estándar o inteligente
- *Excepciones:* según las necesidades del administrador
- *Instalar solo en dispositivos dentro de las áreas seleccionadas*: no seleccionado
- *Habilitar programación e instalar solo durante los periodos seleccionados:* no seleccionado
- *Fecha de eliminación*: en blanco

3. Elija el payload de APN y configure los siguientes campos del APN:
   - *APN: accesoremoto.movistar.es*
   - *Nombre de usuario: datos*
   - *Contraseña: datos*
   - *Tipo de autenticación: PAP*

   Deje todos los demás campos vacías
4. Seleccione Guardar y publicar.

   Tras este proceso VMware Workspace ONE UEM aplicará este perfil a los dispositivos seleccionados.

Fuente: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/Android_Platform/GUID-AWT-PROFILEAPN.html

3.2.6. Despliegue en Samsung Knox mediante IBM MaaS360

Implemente la configuración APN correcta para sus dispositivos Samsung Knox seleccionados definiendo la política MDM adecuada dentro de su portal IBM MaaS360. En esta guía se usa una política separada para dispositivos Android. Puede optar por modificar las Políticas existentes o agregar nuevas.

Una vez que haya definido su política, puede aplicarla a individuos o grupos de dispositivos.

Cómo crear una política

1. Para agregar una nueva política desde su IBM MaaS360 Portal:
   - Seleccione
     - Políticas

- Haga clic en Agregar política.

2. Introduzca las siguientes configuraciones:
   - *Nombre: Nombre* descriptivo de la política. Esta puede ser la política de APN.
   - *Descripción*: descripción opcional
   - *Tipo:* MDM de Android
   - Comenzar desde*:* una política de MDM de Android existente como plantilla para su nueva política.
3. Seleccione Continuar
4. Expanda Ajustes Avanzados y selecciona APN
5. Seleccione Editar
6. Seleccione: Configurar Ajustes APN
7. Introduzca los siguientes campos APN:
   - *APN: accesoremoto.movistar.es*
   - *Nombre de Usuario: datos*
   - *Contraseña: datos*
   - *Tipo de Autenticación: PAP*
8. Deje el resto de áreas vacías

Guardar y Publicar.

Para publicar la política

1. Introduzca:
   - Descripción opcional para revisiones futuras
   - Contraseña
2. Seleccione Continuar.

Su nueva política de MDM de Android ahora se puede aplicar a dispositivos individuales o grupos.

3.2.7. Configuración de otros terminales Android

Para que el dispositivo se conecte a la plataforma y acceder a la red privada se deberá configurar el punto de acceso móvil (APN) en el dispositivo. Esto se puede hacer de forma manual siguiendo los siguientes pasos.

Cómo configurar su dispositivo

Desde la pantalla de inicio, toque el botón Menú.

1. Navegue hasta:
    - Aplicaciones
    - Configuración
    - Redes móviles (toque Más si es necesario)
    - Nombres de puntos de acceso.
2. Toque el botón AÑADIR que normalmente se encuentra en la parte superior derecha de la pantalla.
3. Localice los siguientes campos y configurarlos con los siguientes valores:
    - *APN: accesoremoto.movistar.es*
    - *Nombre de usuario: data*
    - *Contraseña: data*
    - *Tipo de autenticación: PAP*

Deje todos los demás campos vacíos

4. Guarde la nueva configuración de APN.

Una vez completado, su dispositivo móvil debería mostrar Conectado en la pestaña Dispositivos del portal.

Sugerencia: si el dispositivo no muestra un estado de Conectado en el portal:

- Asegúrese de que el dispositivo no esté conectado a Wi-Fi.
- Actualice la página del portal (tecla F5)

www.telefonica.com