Acceso Remoto Unificado

Manual de Usuario

ÍNDICE

1 INTRODUCCIÓN 1
2 DESCRIPCIÓN DEL SERVICIO 2
3 ACCESO A LOS RECURSOS/APLICACIONES CORPORATIVAS 3
4 ACCESO DESDE UN NAVEGADOR 4
4.1 Autenticación 4
4.1.1 Acceso desde Internet Explorer 4
4.1.2 Acceso con Mozilla-FireFox 7
5 ACCESO DESDE JUNOS PULSE (SMARTPHONES Y TABLETAS) 8
5.1 Pulse-Secure para Android 8
5.1.1 Descarga e Instalación 8
5.1.2 Configuración 8
5.1.3 Uso de Pulse-Secure 9
5.2 Junos Pulse para Android con Dispostivos Samsung 10
5.3 Junos Pulse para iOS Apple 10
5.3.1 Descarga e Instalación 10
5.3.2 Configuración 10
5.3.3 Uso de Junos Pulse 11
Incluye las siguientes funciones: 11
5.4 Inicio de Conexiones 13

1 INTRODUCCIÓN

El presente documento es una guia de uso dirigida a los usuarios del servicio Acceso Remoto Unificado, en adelante ARU.

El objeto es describir de manera breve en qué consiste el servicio y cómo el usuario final hace uso del mismo.

En concreto:

2. Descripción del servicio: Qué ofrece, qué elementos lo componen, etc
3. Acceso a lor recursos/aplicaciones corporativas: A qué puedo acceder en función del dispositivo/SO y cómo lo llevo a cabo.
4. Acceso desde un navegador: Uno de los métodos de acceso al servicio. Cuándo es el método más indicado y qué pasos deben darse.
5. Acceso desde Junos Pulse (smartphones y tabletas). El método de acceso más indicado para smartphones y tabletas. Se detalla el procedimiento de descarga del software, instalación, configuración y uso.

2 DESCRIPCIÓN DEL SERVICIO

El servicio ARU proporciona a los usuarios del cliente (empleados, proveedores, colaboradores) acceso remoto seguro a los recursos informáticos que el cliente decide para cada perfil de usuario. De esta manera los usuarios del servicio podrán acceder a aplicaciones corporativas (Correo electrónico, intranet, documentación, aplicaciones empresariales, etc) desde fuera de la oficina (teletrabajo, movilidad, etc).

Los requisitos son:

1. Disponer de un dispositivo desde el que acceder (PC, tableta, smartphone). El servicio no incluye la provisión de dicho dispositivo. Debe además cumplir con lo siguiente:
    - Que cumpla con los requisitos fijados por el propio cliente. Ejemplo: corporativo, con al antiviruas actualizado, etc
    - Qué esté configurado y/o que disponga del software necesario para el acceso.
2. Tener acceso a Internet
3. Estar dado de alta en el servicio. (usuario y contraseña válidos).
4. Pertenecer a un perfil de usuario para el que se ha habilitado el acceso a los recursos a los que se precisa acceder

El acceso se podrá llevar a cabo desde cualquier red de datos (ADSL, 3G, 4G, etc) que facilite el acceso a Internet.

Asimismo podrá acceder tanto desde PCs, notebooks, etc como de dispositivos móviles

De manera previa, los usuarios del servicio deberán estar dados de alta o habilitados para su uso.

Una vez que el usuario ha sido habilitado en el servicio, el acceso a los recursos informáticos del cliente se hará de manera diferente en función del dispositivo/sistema operativo desde el que se acceda.

- A través de Internet y de un navegador instalado en el dispositivo de usuario, se accederá al Portal de Usuario donde tras autenticarse, el usuario encontrará los enlaces a las aplicaciones a las que se le ha permitido el acceso.
- En el caso de dispositivos móviles (iOS, Android) , puede ocurrir que el Portal de Usuario no permita el acceso a todos los recursos y sea necesario el uso de un software que podrá descargarse de los repositorios habituales: Android Market, Apple Store

El servicio además contempla la figura del Responsable Técnico del cliente, que será la persona/grupo designada como interlocutora del cliente para el servicio. En este sentido llevará la interlocución única entre los usuarios del servicio y Telefónica para incidencias y peticiones de servicio entre las que se encuentran:

- Incidencias en el acceso debidas al servicio ARU
- Consultas técnicas de modificación de la configuración.
- Peticiones de cambios en la configuración no habilitados para el cliente. Entre ellos, la creación de un nuevo perfil de usuarios.
- Etc.

3 ACCESO A LOS RECURSOS/APLICACIONES CORPORATIVAS

En la fase de provisión del servicio se habrá llevado a cabo una parametrizacion del mismo según los requerimientos acordados entre el cliente y Telefónica.

Se agrupan los usuarios en perfiles y se determina para cada uno de estos perfiles los recursos a los que se permite el acceso.

Asimismo, podrán aplicarse políticas de acceso según el dispositivo desde el que el usuario remoto acceda. Es decir, cabe la posibilidad de que los recursos a los que un mismo usuario tiene acceso dependan del dispositivo (PC corporativo, smartphone, etc) desde el que estén accediendo

El acceso al servicio puede llevarse a cabo:

- Accediendo al Portal de Usuario desde un dispositivo con acceso a Internet y un navegador (Internet Explorer, Chrome, Firefox, Safari, etc)
- A través de una aplicación, Junos Pulse, que deberá ser descargada y configurada de los repositorios correspondientes (Apple Store, Android Market). Esta opción aplica principalmente al acceso desde **smartphones y tabletas**.

4 ACCESO DESDE UN NAVEGADOR

El acceso puede ser mediante:

- Enlaces directos en el Portal de Usuario. Esto aplica a recursos/aplicaciones tipo:
  - Aplicaciones WEB
  - Ficheros Compartidos en Servidores Windows ó Unix
  - Terminal Service para conexión remota a Servidores Windows
  - Telnet y SSH para conexión remota a Servidores Unix
  - Outlook
  - Etc
- Acceso mediante la ejecución previa de un software. En el portal de usuario aparece un icono. En este caso se asigna una IP virtual al PC del usuario, dentro de un rango predeterminado, de forma que se puede llegar a la Red Privada del Cliente como si se estuviera directamente conectado a ella.

4.1 Autenticación

En este caso es necesario disponer de un navegador que entienda el protocolo web cifrado: HTTPS, que es lo normal en todos los navegadores hoy en día.

Este protocolo permite que toda la comunicación entre el dispositivo del usuario y la plataforma de servicio circule cifrada y así se puede garantizar la confidencialidad de la información transmitida.

De este modo, el usuario solo necesita conocer la URL ó Dirección Web a la que debe apuntar su navegador, un usuario válido y su contraseña.

Si el cliente hubiera solicitado que la autenticación de los usuarios remotos fuera mediante un certificado electrónico, los usuarios deberían además de disponer en lso dispositivos de acceso de un certificado válido.

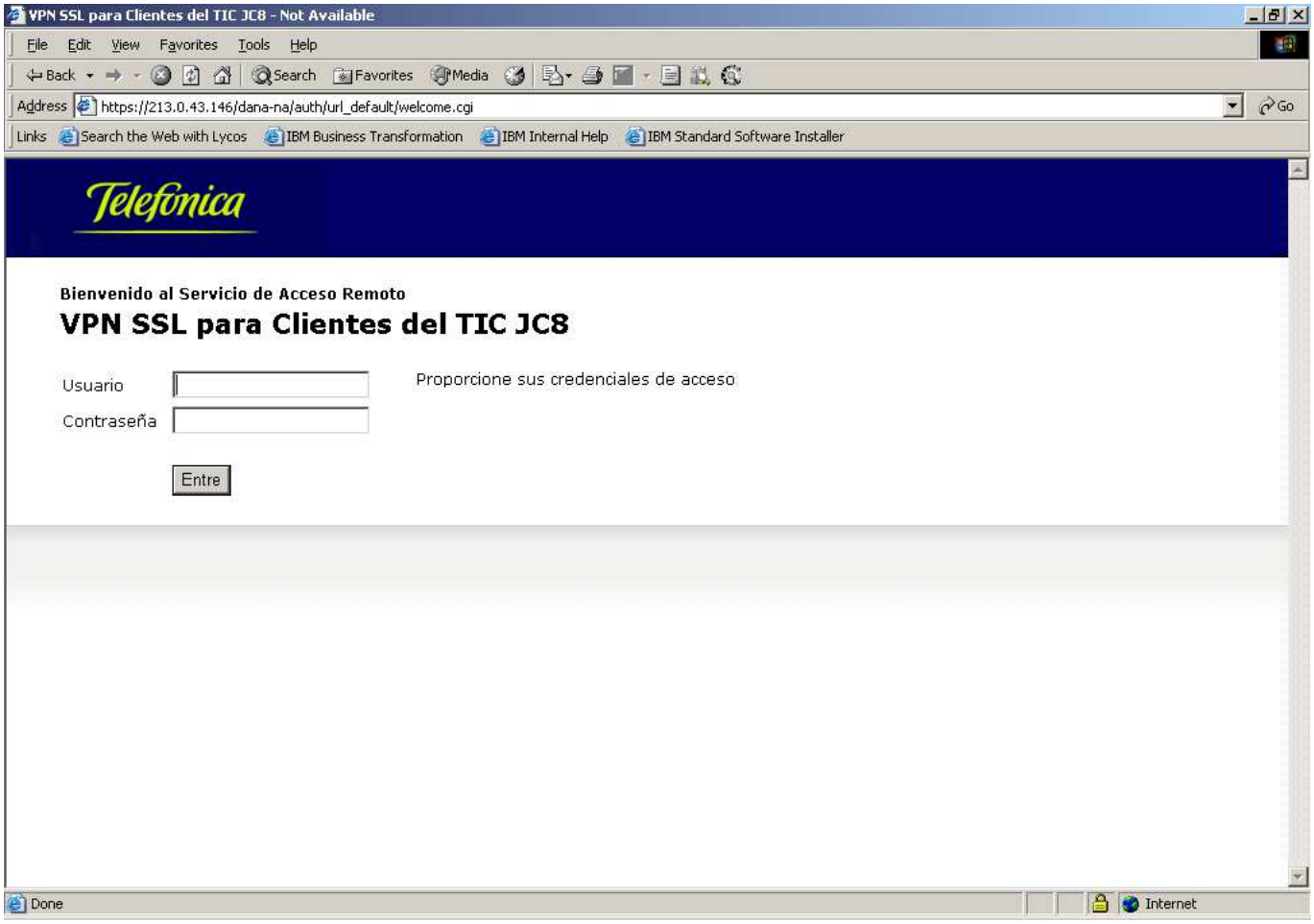
4.1.1 Acceso desde Internet Explorer

Una vez tecleada la URL en la barra de navegación, se pulsa "ENTER" y el equipo del usuario conecta con la plataforma de servicio.

Si es la primera vez que se accede, se le presenta el Certificado del Servidor HTTPS, para que se acepte. Esto también puede ocurrir cada vez que se acceda.

Respondemos "Yes" para aceptar el certificado y seguir con el proceso de acceso y autenticación.

En la figura se muestra una página de acceso típica, donde se pide al usuario que proporcione sus credenciales de autenticación.



Una vez autenticado correctamente, el usuario accede a un portal donde se le ofrecen los enlaces para acceder a los recursos que tenga permitidos.

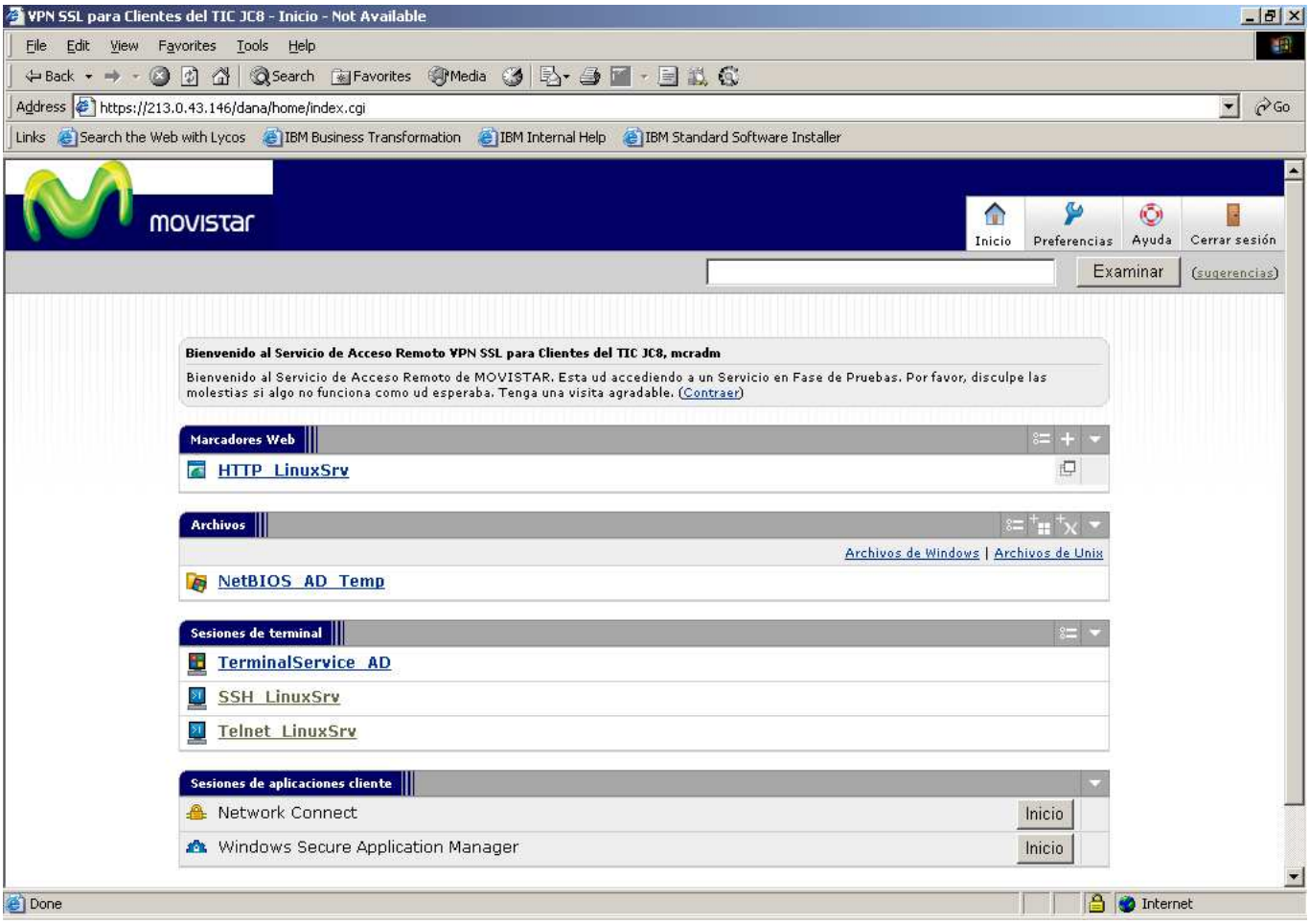
A continuación se muestra a modo de ejemplo el Portal de Usuarios de Demos de Telefónica

Examinando la página, los elementos activos de mayor importancia son:

- Zona Superior Derecha: Los iconos de la zona superior derecha, permiten realizar operaciones simples:
  - Inicio: Regresa al usuario a esta misma página.
  - Preferencias: Permite reordenar la apariencia de la zona central.
  - Ayuda: Da paso a un manual de ayuda.
  - Cerrar sesión: Termina la sesión.

- Zona Central:
  - Enlaces directos a cierto tipo de recursos (aplicaciones web, Ficheros Compartidos en Servidores Windows ó Unix, aplicación "Terminal Service" para conexión remota a Servidores Windows, Telnet y SSH para conexión remota a Servidores Unix, Cliente Lotus Notes, etc.

  - Botones de comando para acceder a recursos que requieren la ejecución previa de un software en el dispositivo del usuario ("Sesiones de aplicaciones cliente": Network Connect, Windows Secure Application Manager)



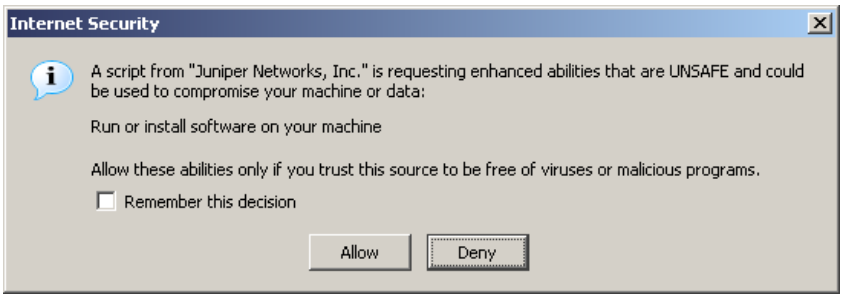
Es posible que el cliente haya decidido que de manera automática, una vez el usuario se haya autenticado, se ejecute el software "network connect" y/o WSAM sin necesidad de que el usuario remoto deba pulsar ningún botón de comando.

4.1.2 Acceso con Mozilla-FireFox

Todo el proceso es similar:

- Se nos pide aceptar el certificado del Servidor HTTPS.
- Se nos pide proporcionar las credenciales de autenticación.

La diferencia estriba en que antes de darnos paso al portal con los enlaces a servicios, se nos pide aceptar un applet que se descarga desde el Servicio de Acceso Remoto al PC de usuario:



Se debe responder "Allow":

Se puede seleccionar la casilla "Remember this decision" para evitar que se nos pida esta confirmación en cada acceso al servicio.

5 ACCESO DESDE JUNOS PULSE (SMARTPHONES Y TABLETAS)

En el caso de smartphones y tabletas, aunque algunos de los recursos pueden ser accedidos según lo explicado en el apartado anterior, se recomienda llevar a cabo el acceso mediante el software Junos Pulse a fin de optimizar la usabilidad y funcionalidad del servicio para este tipo de dispositivos.

En este apartado se desarrollará de forma clara y concisa los pasos necesarios para proceder con la instalación del software Junos Pulse en los dispositivos móviles de usuario final. Se han contemplado tres escenarios distintos dependiendo del tipo de dispositivo final:

- **Pulse-Secure para Android.**
- **Pulse-Secure para Android con dispositivos Samsung.**
- **Pulse-Secure para IOS Apple.**

5.1 Pulse-Secure para Android

El primer escenario corresponde a dispositivos con Sistemas Operativos Android que no sean Samsung.

5.1.1 Descarga e Instalación

El software Pulse-Secure está disponible en la tienda de aplicaciones de Android. El software se deberá descargar e instalar en el dispositivo móvil final. En la tienda de aplicaciones aparecerán varias opciones de descarga, entre ellas se deberá elegir "**Junos Pulse for Android**".

Cuando se ha descargado el software se deberá aceptar el acuerdo de licencia de usuario final para poder configurarlo.

Una vez se ha descargado y aceptado el acuerdo de licencia aparecerá un acceso directo de esta aplicación desde el dispositivo móvil. Para poder acceder al software Junos Pulse será necesario seleccionar o cliquear sobre el acceso directo.

5.1.2 Configuración

Una vez se ha accedido al software, aparecerán varias opciones que se deberán configurar:

Conexiones: Es la parte fundamental de configuración de Pulse-Secure. Con esta opción se configura la URL del portal del servicio. Por consiguiente, si seleccionamos la opción de **Conexiones→Agregar Conexión**, aparecerán 2 campos a rellenar:

1. **Nombre de la Conexión:** Es el nombre local que identifica la Conexión. En este caso se podrá poner cualquier nombre que sea amigable e identificativo para el usuario final. Por ejemplo: Acceso Empresa.
2. **URL:** En este campo se deberá de introducir la dirección IP o nombre (siempre que esté dado de alta en DNS) que tendrá el extremo donde termina el túnel (plataforma de servicio). Por tanto, este campo se tendrá que rellenar con la IP o Nombre donde acabe la conexión VPN. A modo de ejemplo: https://81.47.206.193.

En aquellos casos en los que se haya optado por la autenticación de usuarios mediante certificado electrónico, deberá configurarse seleccionando la opción "**usa certificado**". Aparecerán dos campos extras para poder indicarle al software la ruta del certificado y la Ruta de la Clave. El certificado se importará en el dispositivo móvil a través de un E-mail como adjunto o a través de un adjunto en SMS.

Además, indicar que para generar la conexión y guardarla en memoria será necesario seleccionar la opción de **Crear Conexión**. De esta forma, se guardará el perfil de conexión que será utilizado por el usuario final cada vez que requiera acceder.

5.1.3 Uso de Pulse-Secure

Las funciones disponibles dependerán de la configuración llevada a cabo en la fase de provisión de acuerdo a los requerimientos especificados por el cliente.

Según los ajustes de configuración, Junos Pulse puede incluir las siguientes funciones:

- **Conexiones:** Le permite agregar, editar y eliminar conexiones de red.
- **Intranet:** Proporciona vínculos Web configurados por el administrador.
- **Email (Correo electrónico):** Inicia la aplicación de correo electrónico.
- **Estado:** Le permite ver, borrar y enviar por correo electrónico los archivos de registro de Pulse, lo que puede ser necesario para operaciones de solución de problemas.

5.2 Junos Pulse para Android con Dispostivos Samsung

El segundo escenario corresponde a Sistemas Operativos Android y Hardware Samsung. Los pasos son idénticos al primer escenario pero el software que se debe de descargar desde la tienda de aplicaciones de Android es "Junos Pulse For Samsung".

5.3 Junos Pulse para iOS Apple

5.3.1 Descarga e Instalación

El software Junos Pulse está disponible desde la tienda de aplicaciones de Apple. También se puede instalar desde iTunes.

Para instalar Pulse desde iTunes:
1.Copie Junos **Pulse.ipa** a su carpeta Apps en iTunes.
2.Sincronice su dispositivo iOS con iTunes.

El icono de Pulse-Secure aparecerá en el escritorio.

Nota: Junos Pulse es compatible con iOS Apple 4.1 y posterior.

Cuando se intente abrir Junos Pulse por primera vez se le solicitará activarlo en su dispositivo iOS. Para activarlo, se debe de cliquear en Enable.

5.3.2 Configuración

Una vez se ha accedido al software mediante un cliqueo del acceso directo generado, aparecerán varias opciones que se deberán configurar:

Agregar Conexiones: Para iOS Apple existen 2 posibilidades:

- El administrador de red puede enviar la información requerida. Si ha recibido un perfil de configuración por medio del correo electrónico o como un archivo adjunto a un mensaje, procese ese archivo después de instalar el Software.
- Se puede agregar conexiones manualmente. En este caso, para definir una conexión:
    1. Inicie **Pulse**.
    2. Toque **Configuration**.
    3. Si ya tiene un perfil de conexión configurado y está agregando un perfil adicional, haga clic en **Edit**.
    4. Toque en **Add New Connection**. Se abrirá la ventana Agregar.
    5. Especifique las propiedades del perfil de conexión.

        Name: El nombre o la descripción que se la va dar a este perfil de conexión.

        URL: La dirección Web proporcionada por el administrador de red.

        Certificate: Si el administrador de red le proporcionó un certificado digital (normalmente por medio de un correo electrónico o un archivo adjunto a un mensaje), toque Certificate. Cuando se abra la pantalla Identidades, seleccione el certificado que desea usar con este perfil. Si no usa un certificado, debe proporcionar un nombre de usuario y contraseña al activar esta conexión.
    6. Toque en **Configuration > Junos Pulse** para volver a la pantalla principal de Pulse.

5.3.3 Uso de Junos Pulse

Incluye las siguientes funciones:

Configuration: Muestra el nombre de la conexión activa cuando Pulse está conectado o de la conexión predeterminada cuando Pulse no tiene una conexión activa. Le permite agregar, editar y eliminar conexiones de red.

Intranet: Proporciona acceso a vínculos Web configurados por el administrador.

Email: Inicia la aplicación de correo electrónico.

Status: Le permite mostrar las estadísticas de la conexión y le envía por correo electrónico los archivos de registro de Pulse para la resolución de problemas.

About: Muestra la información de la versión del software Pulse.

Nota: Las funciones disponibles en Pulse dependen de la configuración y los ajustes de VPN que realice el administrador.

5.4 Inicio de Conexiones

En todos los escenarios descritos anteriormente el Software Pulse usa conectividad de 3G o Wifi. Por ello, para conectarse por VPN será necesario seguir los siguientes pasos:

1. Inicie **Pulse**.
2. Toque en **Connect**.
3. Cuando aparezca la pantalla Conectar, introduzca su nombre de usuario y contraseña y toque en **Sign In**.

Una vez conectado ya se podrá acceder a los recursos de la Red Interna que el Administrador de Red le haya asociado a dicho perfil.