Servicio de Informática

Vicerrectorado de Estrategia y Universidad Digital

Servicio de conexión remota mediante VPN-SSL
Guía de usuario

Edición: 08
Última Actualización 18 de enero de 2024

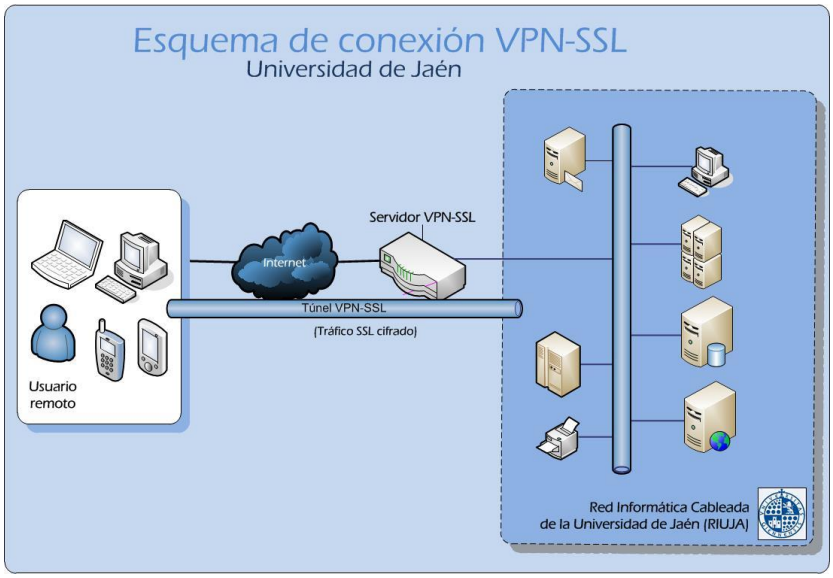
Histórico de cambios

Fecha	Descripción	Autor
24/06/13	Primera edición	Servicio de Informática
02/12/15	Revisión y actualización	Servicio de Informática
01/02/17	Revisión y actualización	Servicio de Informática
29/01/19	Actualización de nuevos plugins	Servicio de Informática
20/05/20	Actualizaciones conexión con Android	Servicio de Informática
25/05/20	Actualizaciones conexión mediante MacOS X	Servicio de Informática
07/07/23	Doble factor de autenticación (2FA)	Servicio de Informática
12/09/23	Conexión VPN-SSL desde el extranjero	Servicio de Informática

Tabla de contenido

1.- Introducción

El servicio de Red Privada Virtual (***V**irtual **P**rivate **N**etwork*) permite integrar un dispositivo externo (PC/portátil de casa, Tablet o Smartphone) en la Red Informática cableada de la Universidad de Jaén (RIUJA), posibilitando el acceso a recursos y servicios que sólo están disponibles a los equipos internos.



El sistema establece una conexión segura específica (túnel virtual) entre su ordenador y un servidor o sistema situado en la Universidad de Jaén. Una vez establecida la conexión VPN-SSL, todo el tráfico de red destinado a las redes internas de la UJA se encaminará a través del túnel. El resto del tráfico será encaminado a través de su conexión habitual a Internet (generalmente mediante ADSL, fibra óptica o similar).

Esta comunicación a través del túnel VPN-SSL está cifrada por lo que no es posible ver el contenido de la información mientras viaja por Internet. Antes de establecer el túnel se requiere la autenticación del usuario, mediante usuario y contraseña y posteriormente, por seguridad, mediante un segundo factor (2FA). Previamente se realizan una serie de comprobaciones de seguridad en el equipo del usuario, siendo por tanto un medio de conexión robusto y seguro.

El sistema VPN empleado en la Universidad de Jaén usa para el cifrado de los datos el protocolo estándar SSL (*Secure Socket Layer*, Capa de Socket Segura) lo que hace que este sistema sea extremadamente sencillo de utilizar, siendo necesario en la mayoría de los casos un simple navegador web.

IMPORTANTE: El servicio VPN-SSL se limita a integrar el ordenador del usuario (por ejemplo: ordenador de casa) en RIUJA y no realiza ninguna configuración para el acceso a los servicios anteriormente indicados. La configuración correcta de estos servicios es responsabilidad del usuario.

2.- ¿Quién puede hacer uso del servicio VPN-SSL?

Actualmente, el sistema VPN-SSL está destinado únicamente al **PTGAS y al PDI de la Universidad de Jaén**.

3.- Servicios y recursos disponibles mediante VPN-SSL

El servicio de conexión remota VPN-SSL de la Universidad de Jaén es un medio seguro para acceder desde Internet a los servicios proporcionados por la Red Informática Cableada de la Universidad de Jaén (RIUJA). La principal utilidad es el acceso a servicios y recursos de la UJA que no están accesibles públicamente.

La conexión VPN-SSL ofrece acceso a los siguientes servicios:

- **Navegación web HTTP y HTTPS** a sitios web dentro y fuera de la UJA.
- Acceso al software Panda Antivirus en la UJA: https://www.ujaen.es/servicios/sinformatica/virus-y-antivirus
- **Acceso a determinadas páginas restringidas dentro del sitio web de la UJA**
  Ej: Servicio de Informática – Oficina de Atención al Usuario: https://www.ujaen.es/servicios/sinformatica/atencion-usuario
- **Conexión segura a equipos de la Universidad** mediante Conexión a Escritorio Remoto de Windows (RDP) y mediante SSH (Secure Shell).
- **Acceso a servidores FTP** internos y externos a la UJA.
- **Universidad Virtual:** acceso a opciones restringidas, sólo accesibles desde dentro de la UJA.
- **Publicación de páginas web personales en** http://www4.ujaen.es

Este catálogo de servicios puede ser ampliado en un futuro en función de las peticiones y necesidades de los usuarios.

El acceso mediante VPN-SSL a los sistemas de Gestión Económica y Académica de la Universidad (Sorolla, Universitas XXI, etc) está explícitamente cerrado.

4.- Requisitos necesarios para acceder al sistema VPN-SSL

IMPORTANTE: CONEXIÓN VPN-SSL DESDE EL EXTRANJERO

Debido a las últimas tendencias en ciberataques que están usando las conexiones VPN como vía de acceso, por seguridad se ha limitado el acceso VPN-SSL únicamente a España y ciertos países puntuales solicitados a demanda por algunos de nuestros usuarios.

Si estás en el extranjero o tienes previsto viajar fuera de España y necesitas el acceso VPN-SSL de la UJA, debes comunicarlo previamente al Servicio de Informática para comprobar si tu país de destino está entre los permitidos. En caso contrario, una vez estudiado el caso y si no representa ningún potencial problema de seguridad, procederemos a añadirlo al conjunto de países de origen permitidos.

Para poder usar este servicio son necesarios los siguientes requisitos:

- **Un dispositivo (PC, portátil, tablet, smartphone) con conexión a Internet.** Están soportados equipos de sobremesa/portátiles con Windows, MacOS o Linux, así como plataformas móviles (tablets y Smartphones) con Apple iOS y Android.
- **Una cuenta TIC.** Su nombre de usuario y contraseña de la cuenta TIC, además del segundo factor de autenticación (2FA) serán los que le permitan la conexión remota VPN-SSL. Utilice contraseñas robustas y renuévelas de forma periódica. No reutilice la contraseña de su

cuenta TIC de la UJA en otros servicios o aplicaciones. Asimismo, en general, guardar las contraseñas en el navegador no es una buena práctica.

- **Un navegador web estándar.** Se han realizado pruebas satisfactorias con los siguientes navegadores: Google Chrome, Microsoft Edge, Mozilla Firefox, Safari y Opera. En las plataformas móviles es necesario instalar un cliente específico, que también está disponible para MacOS.
- **En sistemas Microsoft Windows** es necesario, además:
  - **Tener instalado algún antivirus estándar.** La plataforma de conexión VPN-SSL soporta un gran número de antivirus gratuitos y de pago que existen en el mercado.
  - Tener configurado el **protector de pantalla,** protegido por contraseña y con un tiempo de activación inferior a 30 minutos.

5.- Conexión desde un navegador web en un equipo portátil o sobremesa

La conexión al sistema VPN-SSL se realiza con un navegador web. A continuación, se detallan los pasos necesarios para realizar la conexión. En algunos pasos se necesitará instalar un complemento o plugin para el navegador web. El proceso de instalación del complemento suele ser automático, pero si necesita realizar la instalación manual puede consultar el procedimiento en nuestro servicio de Preguntas y Respuestas de la UJA (http://faq.ujaen.es).

Pasos para la conexión VPN-SSL:

1) Iniciar conexión al servidor de VPN-SSL

a. Abra un navegador web y teclee la dirección:

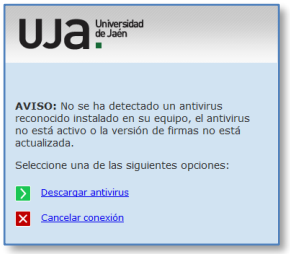
https://vpnssl.ujaen.es

b. Introduzca el nombre de usuario **(sin el dominio @ujaen.es**) y contraseña de su cuenta TIC:

2) (Sólo en sistemas Windows) Comprobar si existe un antivirus instalado y la fecha de última actualización:

- El navegador mostrará el mensaje **"Comprobando el software de seguridad…"** y descargará e instalará un complemento encargado de realizar la comprobación del

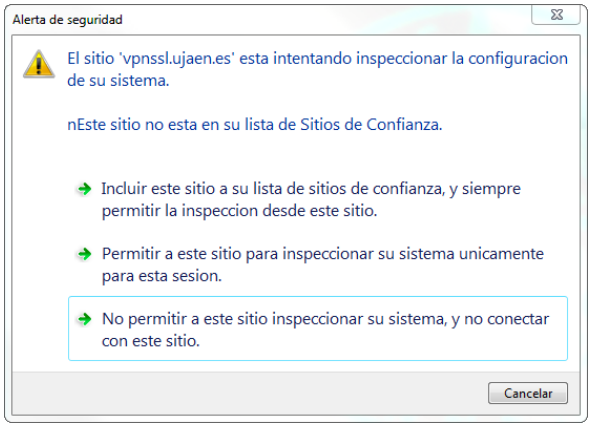
antivirus (**en sistemas Windows solicitará permiso para la ejecución del complemento).** Si todas las comprobaciones son correctas se continuará con las comprobaciones. En caso contrario, se le encaminará a una página donde se proponen varios antivirus gratuitos. Si llega a este último paso, instale un antivirus, actualícelo y repita los pasos desde el apartado 1.



NOTA: aunque durante este paso podrá instalar un antivirus gratuito, se recomienda, en cuanto pueda, instalar el antivirus corporativo de la UJA.

3) **(Sólo en sistemas Windows) Comprobar si está activado el protector de pantalla con contraseña de acceso:**
   - El sistema comprobará si tiene protegido su PC con un protector de pantalla con contraseña y un tiempo máximo de activación de 30 minutos. Esta medida permite que, en periodos de ausencia superiores a 30 minutos, por seguridad, se bloquee la sesión del PC.

4) **Instalación automática del complemento para el navegador (F5 Big-IP Edge Client):**
   - El navegador instalará el complemento **F5 Big-IP Edge Client**, necesario para completar la conexión VPN-SSL. En determinados navegadores es posible que la configuración de seguridad nos muestre la siguiente ventana:



Para evitar que se muestre en el futuro, debemos hacer clic sobre la primera opción (**Incluir este sitio a su lista de sitios de confianza, y siempre permitir la inspección desde este sitio**).

5) **Conexión establecida:**
   - Una vez establecida la conexión, aparecerá una pantalla informando de que la conexión se ha realizado (Conectado). A partir de este momento, se podrá acceder a los recursos internos de la UJA.

6) **Comprobar el estado de la conexión:**
   - En sistemas Windows, pulsando en el icono  situado en la parte inferior derecha.

7) **Cerrar la conexión:**

- En sistemas Windows, pulsando en el icono  situado en la parte inferior derecha y luego en "Finalizar conexiones" o bien, pulsando el botón:

- En sistemas MacOS y Linux, pulsando en el botón

que aparece en el propio navegador en la parte superior derecha de la cabecera.

NOTA IMPORTANTE: el icono  que se usa para la desconexión y la visualización de la sesión puede estar escondido. Para mostrarlo, tiene dos opciones:

- Pulsar en la flecha **^** que aparece abajo a la derecha en la bandeja de Windows para mostrar los iconos ocultos.

- Hacer que ese icono sea visible de forma permanente: pulsando en la flecha **^** indicada anteriormente, y entrando en el enlace **"Personalizar"**. Localice el icono  (puede aparecer varias veces), y active la opción **"Mostrar icono y notificaciones".**

Para obtener información más detallada sobre la conexión con los distintos sistemas, navegadores y clientes puede acceder a este enlace:

http://faq.ujaen.es/index.php?action=show&cat=93

6.- Conexión desde MacOS X

El sistema VPN-SSL funciona sobre el protocolo estándar SSL y el único requisito es un navegador web (todos los navegadores actuales soportan SSL). En principio, la conexión VPN-SSL debería funcionar correctamente con cualquier versión de MacOS. En cuanto a navegadores, actualmente están soportados Safari (el navegador estándar de MacOS), Mozilla Firefox y Google Chrome.

IMPORTANTE:

- En el caso de MacOS **NO** se realiza la comprobación de software antivirus en el sistema.
- En MacOS no existe un icono que permita la desconexión. Para desconectarnos de la sesión VPN-SSL debemos pulsar en el botón **"Cerrar sesión"** que aparece en el propio navegador en la parte superior derecha de la cabecera.

Hay dos formas de conexión VPN-SSL en MacOS:

- **Mediante navegador web**. El método es muy similar al descrito anteriormente para otras plataformas como Windows, y se describe con detalle en el siguiente enlace:

http://faq.ujaen.es/index.php?action=artikel&cat=93&id=830&artlang=es

- **Mediante el cliente F5 Access**. Este método se describe a continuación.

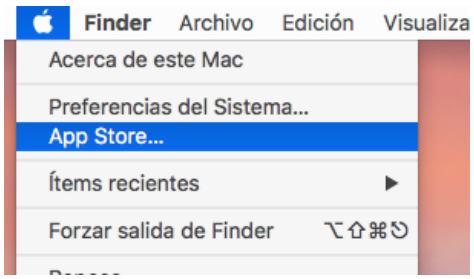
Conexión VPN-SSL desde MacOS con App F5 Access

En MacOS, existe una alternativa de conexión VPN-SSL mediante una App (**F5 Access**) disponible en la Mac App Store de Apple.

NOTA IMPORTANTE: Estas instrucciones, así como la App que se indica, son válidas **ÚNICAMENTE para la versión 10.12 (Sierra) o posterior de MacOS.**

Los pasos a seguir son los siguientes:

- Instalación de la App F5Access. El primer paso es la descarga e instalación de la App F5Access accesible desde la Mac App Store. Podemos acceder a ella mediante el icono de la manzana en la barra de menú:



Dentro de la **Mac App Store**, buscaremos **F5Access**:

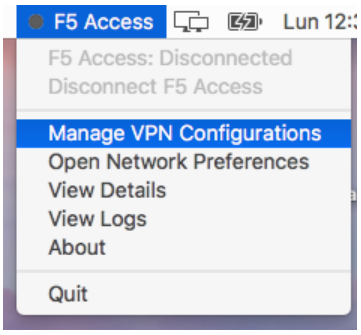
Una vez localizada la aplicación, haremos clic en el botón **Obtener** (o **Instalar** si ya se instaló alguna vez) que aparece junto a esta:

Tras finalizar la instalación, buscaremos el icono de **F5Access** en Aplicaciones y haremos doble clic sobre el mismo:

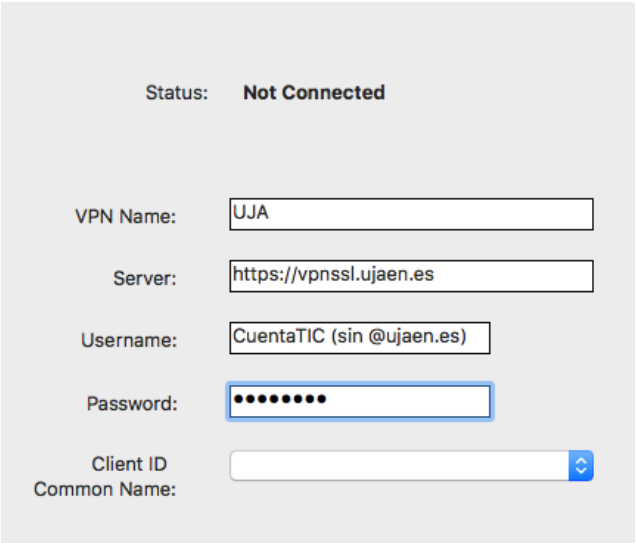
Opcionalmente, podemos buscar con el Finder **F5Access** y una vez aparezca el icono, lo arrastraremos al escritorio para tenerlo más accesible.

NOTA: la primera vez que instalamos la App, debemos aceptar una pantalla de Términos y Condiciones.

- Conexión VPN-SSL con F5 Access. En la barra de menú, próximo al reloj, aparecerá una nueva opción **F5 Access.** Si hacemos clic se desplegarán una serie de opciones. Seleccionando **Manage VPN Configurations** accedemos a las conexiones VPN configuradas:



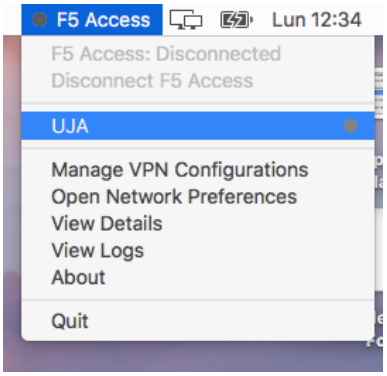
Podemos crear una nueva configuración haciendo clic en **+** rellenando los siguientes parámetros:



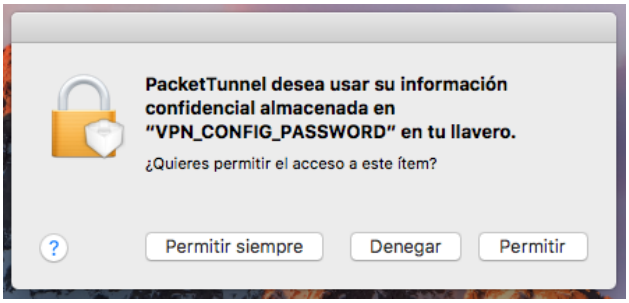
Es importante indicar que en **Username**, hay que escribir únicamente nuestro nombre de usuario (**nuestra Cuenta TIC sin @ujaen.es).** Se recomienda dejar en este paso la password en blanco. De esta forma, por seguridad, no se almacena y nos la pedirá en cada conexión.

Una vez configurada la nueva conexión VPN, saldremos del gestor de configuraciones haciendo clic en **OK**.

En el menú F5 Access antes utilizado, ahora aparecerá una nueva opción con la conexión que se ha creado, llamada en este ejemplo **UJA**:

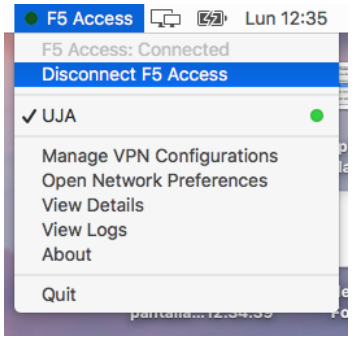


Si lanzamos dicha conexión, a continuación, nos aparecerá una solicitud de permiso de acceso al Llavero del Sistema:



Haciendo clic en **Permitir siempre**, se establecerá la conexión a la red VPN-SSL de la UJA.

Podemos comprobar que se ha establecido correctamente observando el cambio del icono en **F5 Access** a un **color verde:**



Para finalizar la conexión VPN correctamente, haremos clic en **Disconnect F5 Access** y esperaremos a que termine por completo el proceso, momento en el que el icono verde cambiará de nuevo de color, pasando a **amarillo-ambar**.

7.- Conexión desde dispositivos móviles (iOS y Android)

Además de los diferentes sistemas operativos de sobremesa, el sistema VPN-SSL de la Universidad de Jaén permite la conexión desde dispositivos móviles, básicamente Tablets y Smartphones, funcionando con los sistemas operativos iOS (en el caso del iPhone/iPad de Apple) y Android (en el caso de Smartphones y Tablets de numerosos fabricantes).

En el caso de estas plataformas móviles, el acceso se hace mediante un cliente VPN-SSL específico que se debe descargar desde el repositorio de aplicaciones correspondiente: Apple Store en el caso de iPhone/iPad, o Google Play en el caso de Android.

A continuación, se muestran las fases de la conexión:

1) **Descargar e instalar el cliente VPN-SSL** desde Apple Store o Google Play, según el sistema operativo de su dispositivo. Deberá buscar la aplicación **F5 Access.**

2) **Configurar un perfil de conexión**, donde se indica:
   - Nombre del servidor: `vpnssl.ujaen.es`
   - Nombre de usuario: `su usuario de cuenta TIC (sin @ujaen.es)`
   - Contraseña: `su contraseña de cuenta TIC`

3) **Conectar**
   - Pulse en el botón "**Conectar/Connect**" para iniciar la conexión.

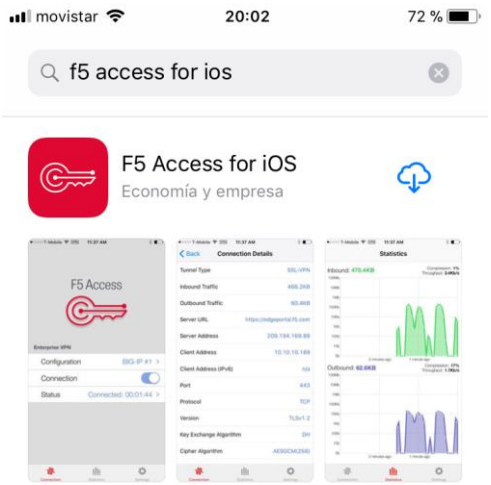
4) **Conexión establecida.**
   - Una vez establecida la conexión, aparecerá una pantalla informando de que la conexión se ha realizado (Conectado). En este momento, se podrá acceder a los recursos internos de la UJA.

5) **Cerrar la conexión.**
   - Pulse en "**Desconectar/Disconnect**" para cerrar la conexión.

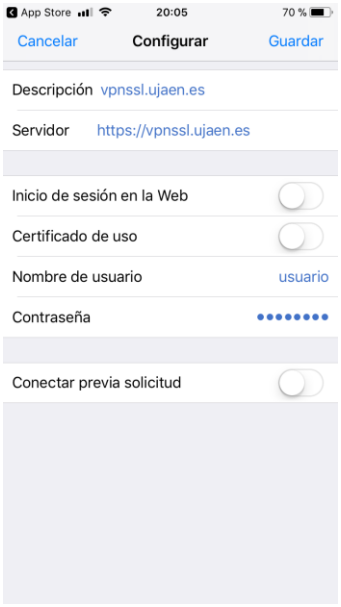
6.1. Conexión desde iPhone (Apple iOS)

Los pasos para realizar la conexión VPN-SSL a la Universidad de Jaén mediante un dispositivo móvil Apple (iPhone, iPad o similar) son los siguientes:

1. Descargar el cliente VPN-SSL **F5 Access for iOS** desde Apple Store:



2. Configurar un perfil de conexión. Para ello, entramos en **Configuración > Agregar nueva.**



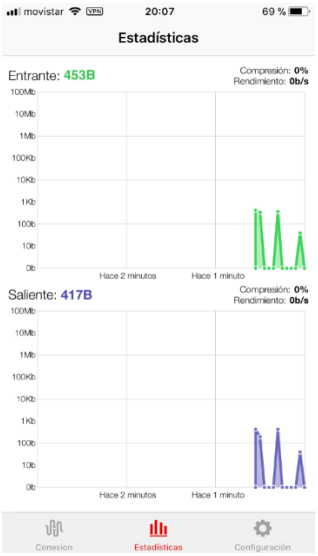
y configuramos la conexión con los siguientes datos:

- **Descripción:** `vpnssl.ujaen.es`
- **Servidor:** `https://vpnssl.ujaen.es`
- **Inicio de sesión en la web:** este campo no es necesario. Se desactiva
- **Certificados de uso:** este campo no es necesario. Se desactiva
- **Nombre de usuario:** nombre de usuario de nuestra cuenta TIC (**sin @ujaen.es**)
- **Contraseña:** la contraseña de nuestra cuenta TIC

Una vez completados todos los datos, salvamos el perfil pulsando el botón **Guardar**. En cualquier momento, podemos acceder a la configuración del perfil y modificarla mediante el botón **Configuración**.

- Tras configurar el perfil, basta con pulsar el botón de conexión para establecer la conexión VPN. Si todo es correcto, la conexión se realizará en pocos segundos:

- Una vez conectados, podemos ver el tiempo de conexión en **Estado**, además de gráficas detalladas mediante el botón **Estadísticas**:

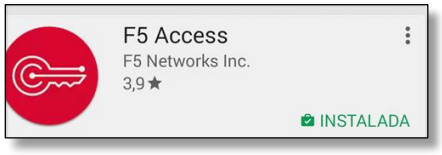


- **Cerrar la conexión:** Podemos cerrar una conexión establecida, desactivando el botón "**Conexión**"

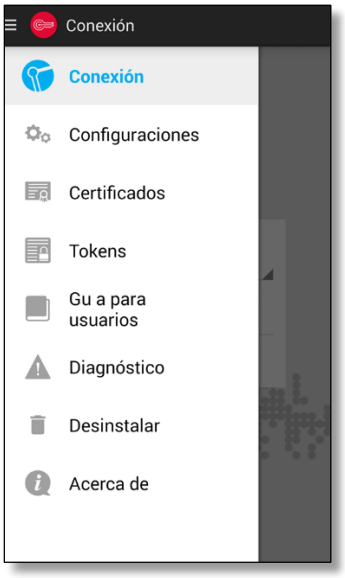
6.2. Conexión desde Android

Los pasos para realizar la conexión VPN-SSL a la Universidad de Jaén mediante un dispositivo móvil basado en Android (smartphone o tableta) son los siguientes:

1. Descargar el cliente VPN-SSL **F5 Connect** (anteriormente **F5 Big-IP Edge Client**) desde Google Play:

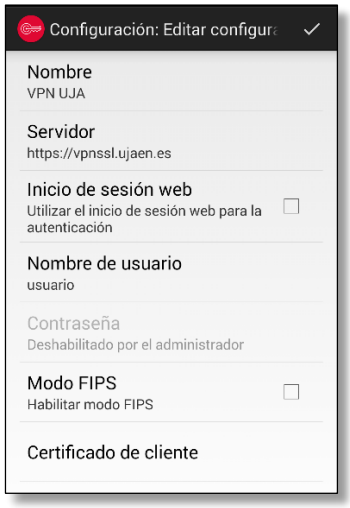


2. Configurar un perfil de conexión. Para ello, pulsamos en el menú superior izquierdo y entraremos en **Conexión > Configuraciones:**



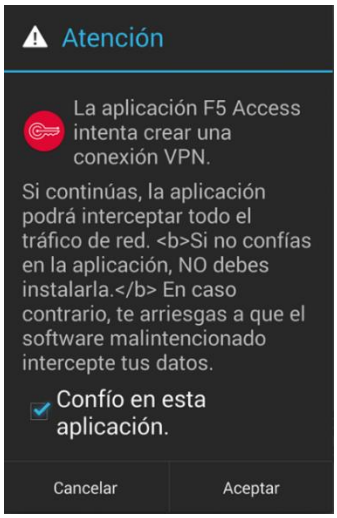
y lo configuramos con los siguientes datos:

- **Nombre:** `vpnssl.ujaen.es`
- **Servidor:** `https://vpnssl.ujaen.es`
- **Nombre de usuario:** nombre de usuario de nuestra cuenta TIC (**sin @ujaen.es**)
- **Contraseña:** la contraseña de nuestra cuenta TIC. No se rellena, se introduce cada vez que se realiza una nueva conexión.
- **Certificado de cliente:** este campo no es necesario. Se desactiva.



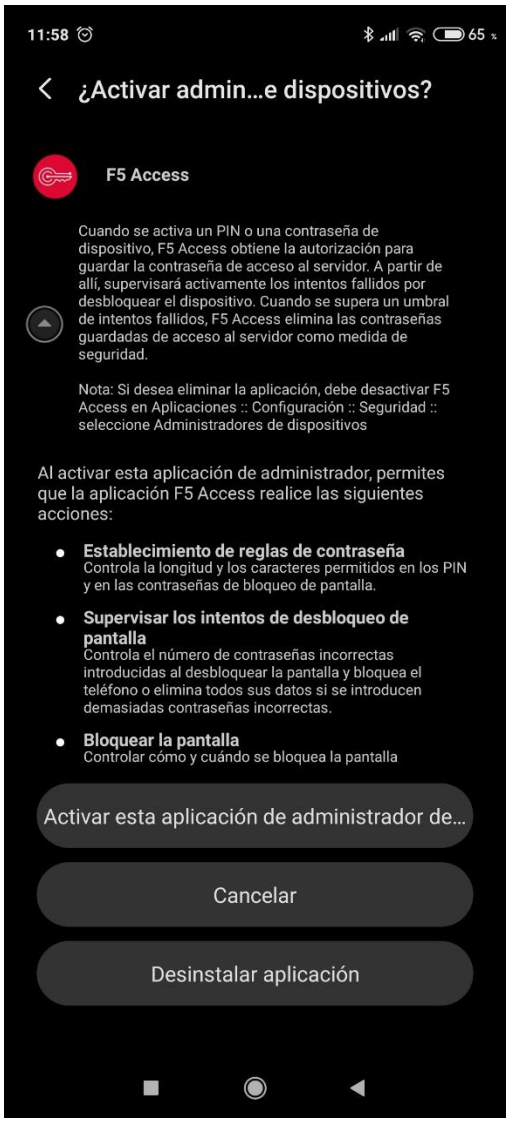
- **Conectar:** basta con pulsar el botón "**Conectar**" para establecer la conexión VPN. Si todo es correcto, la conexión se realizará en pocos segundos:

Es posible que nos avise de posibles riesgos de seguridad con el siguiente mensaje:



La conexión VPN es totalmente confiable, por lo que debemos marcar la casilla **"Confío en esta aplicación"** y **Aceptar.**

Con las versiones más recientes de Android, posiblemente se nos solicite activar la aplicación de Administrador de dispositivos, informándonos de forma detallada de todo lo que ello implica:



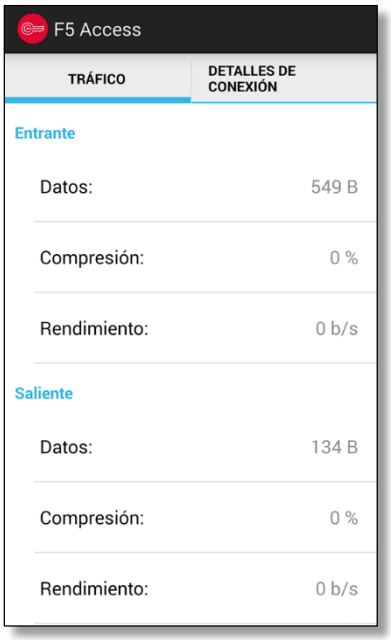
En este paso, debemos pulsar el botón **Activar esta aplicación de administrador de dispositivos.**

Por último, si detecta que nuestro teléfono no está protegido por PIN o contraseña, nos indicará que lo hagamos, definiendo una de las dos (PIN o contraseña)

IMPORTANTE: al definir un PIN o contraseña, debemos estar muy seguros de recordarla y/o anotarla en un sitio seguro, ya que, sin ella, no podremos desbloquear el teléfono, y en caso de olvido puede ser necesario volverlo a los valores de fábrica.

Si todo es correcto, llegados a este paso, nuestra conexión VPN-SSL se habrá establecido y veremos un contador de tiempo que indica el tiempo que lleva activa:

- Una vez conectados, podemos ver el tiempo de conexión en **Estado** e información detallada mediante los botones **Tráfico** y **Detalles de conexión**:



- **Cerrar la conexión:** Podemos cerrar una conexión establecida, pulsando el botón "**Desconectar**"

8.- Doble factor de autenticación (2FA)

La Universidad de Jaén refuerza de manera continua la seguridad en sus servicios. Las recomendaciones del Esquema Nacional de Seguridad (ENS), unidas a los continuos ciberataques que están sufriendo las instituciones públicas, hacen necesario incorporar nuevas medidas.

Es obligatorio **autenticarse con doble factor** (2FA) en las conexiones remotas VPN-SSL desde equipos externos a la UJA. Esta medida protege el inicio de sesión con el **usuario/contraseña** tradicional (primer factor) con **un segundo código de verificación** aleatorio de 6 dígitos (2º factor).

Si usas el servicio VPN-SSL, en Universidad Virtual e indicar dónde quieres recibir el código de verificación: correo electrónico, SMS o en una app móvil (Google Authenticator).

El código de verificación cambia en cada inicio de sesión. Si alguien roba tu usuario/contraseña, no conseguirá acceder, porque no habrá recibido el código de verificación.

¿Qué ocurre si no he configurado ningún método para recibir los códigos de verificación?

Si no has configurado ningún método de contacto no podrás utilizar el servicio VPN-SSL. Sigue estos pasos para configurarlo:

- Desde un PC en la Universidad, accede a Universidad Virtual (https://uvirtual.ujaen.es).
- Entra en **Servicios administrativos > Datos Personales.** En este apartado es fundamental tener rellenos los campos "Correo electrónico alternativo" y "Teléfono móvil" para recibir los códigos de verificación.
- Entra en **Operaciones > Seguridad** cuenta TIC y activa el doble factor de autenticación con la casilla ([x] Autorizo la activación de la autenticación de doble factor y al tratamiento de los datos de contacto personal necesarios para ello).
- El método recomendado para recibir códigos es instalar en el móvil una app de OTP como Google Authenticator (hay versiones para iOS y Android).

En Universidad Virtual

- Activa **[x] Permitir uso app móvil**, para ver el código QR de vinculación con tu móvil.

En el móvil:

- Descarga la app Google Authenticator, según el sistema operativo del dispositivo.
- Elige "usa Google Authenticator sin iniciar sesión en la cuenta".
- Abre la app y escanea el código QR de Universidad Virtual para vincularla a la app.
- Después de activar el doble factor de autenticación en Universidad Virtual, el Servicio de Identidad de la UJA (SIDUJA) incorporará la nueva protección de seguridad.

¿Tengo que introducir siempre el código de verificación?

El doble factor sólo se pedirá para equipos externos a la UJA. Además, en los PCs/dispositivos de tu domicilio, puedes marcar la casilla "[x] equipo de confianza" para que no se pida continuamente. **No se recomienda activar esta opción en equipos compartidos.**

9.- Solución de problemas

Todas las soluciones a las diferentes incidencias detectadas en el funcionamiento del servicio VPN-SSL están recogidas y documentadas en nuestro sistema de Preguntas y Respuestas de la UJA (http://faq.ujaen.es). Puede consultarlas seleccionando la categoría **Red Privada Virtual SSL (VPN-SSL)**, o accediendo al siguiente enlace:

http://faq.ujaen.es/index.php?action=show&cat=93