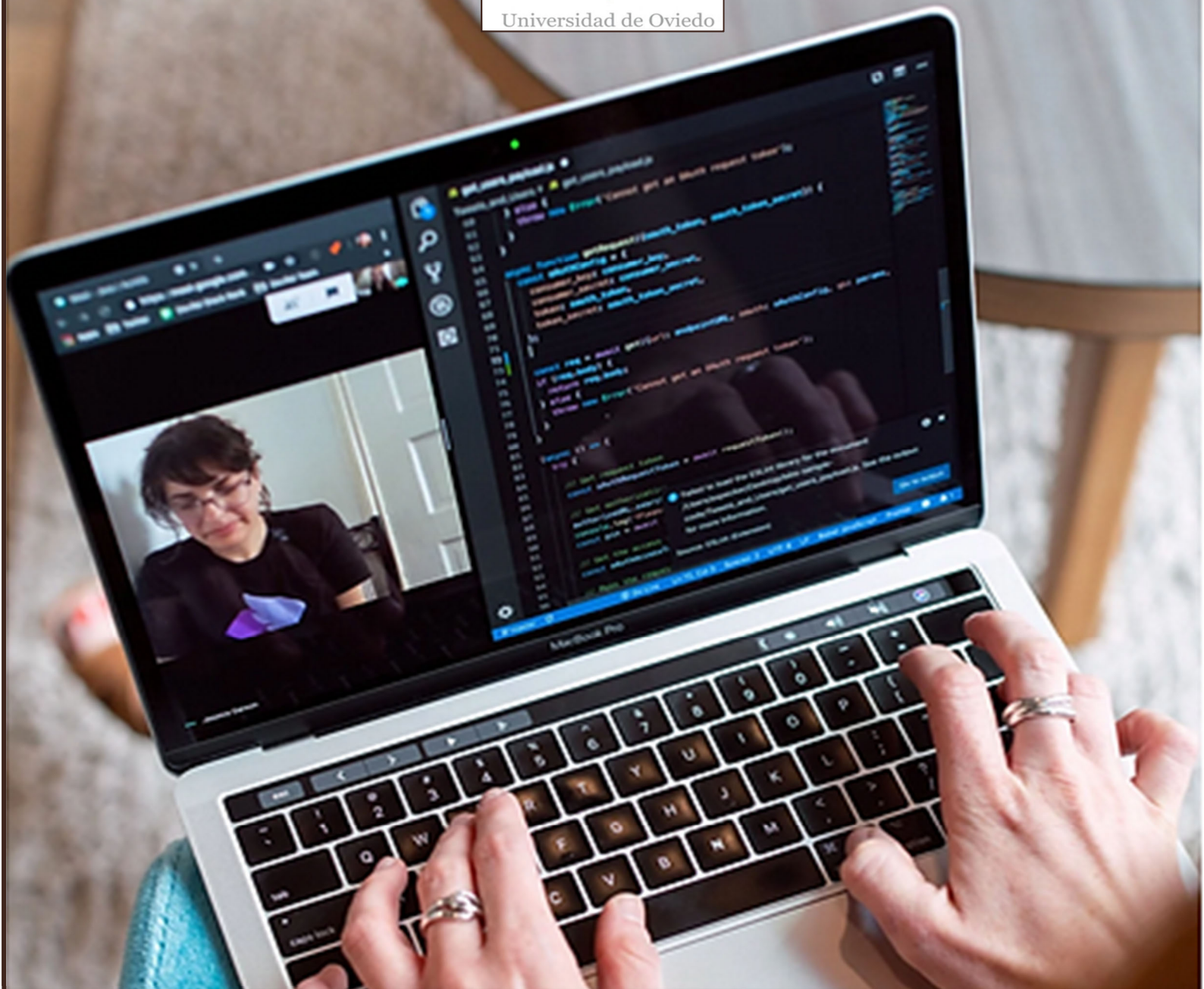




Universidad de Oviedo



ESTRATEGIAS DE PROTECCIÓN INDIVIDUAL FRENTE A CIBERATAQUES

MANUAL DE USO DE FORTINET (DISTRIBUCIÓN
INDEPENDIENTE)

José Manuel Redondo López (Departamento de Informática)
Universidad de Oviedo

"Nautilus" v1.0 (2022)

CONTENIDO

Usando la VPN de Uniovi desde cualquier sistema operativo (Nivel 2)	2
<i>Instalación</i>	2
<i>Configuración inicial</i>	6
<i>Conexión</i>	8
<i>Posibles errores</i>	10

Usando la VPN de Uniovi desde cualquier sistema operativo

El servicio de *Acceso Remoto* (VPN) de nuestra universidad nos permite acceder desde Internet a recursos que hay conectados en la red corporativa. **Una vez establecida la conexión, el ordenador de usuario estará virtualmente ubicado en la red de la Universidad.** Adicionalmente, todo el tráfico generado por el dispositivo del usuario cuyo destino esté dentro de la red de la Universidad, se enviará en un formato cifrado, de manera que nadie podrá ver su contenido, aunque estemos enviándolo por Internet. La conexión de acceso remoto (VPN) permite:

- Conectarse desde Internet a ordenadores situados en la red de la Universidad de Oviedo.
- Acceder a las *Bases de Datos* de la *Biblioteca Universitaria* (dichas *Bases de Datos* son de uso restringido y sólo se puede acceder a ellas desde dentro de la red de la Universidad).
- Acceder a *Publicaciones Periódicas*, también restringidas al uso dentro de la Universidad.

¿Por qué es mejor usar VPN que otras soluciones que son más sencillas de entender como exponer a Internet un escritorio remoto o RDP (puerto 3389)? Porque con escritorios remotos se han dado multitud de problemas de seguridad e intrusiones en el pasado principalmente debidos a dos motivos:

1. **Debilidad de las claves de entrada en sesión**, que las hace vulnerables a ataques de fuerza bruta, por ejemplo. Con esto cualquier persona ajena a la universidad podrá entrar a nuestra máquina y usarla para atacar otros sistemas internos o robar nuestra información.
2. **Vulnerabilidades conocidas**: No hace demasiado tiempo RDP tuvo una vulnerabilidad conocida muy grave que permitía a cualquiera ejecutar comandos en la máquina destino sin ni siquiera entrar en sesión de esta, quedando la máquina completamente expuesta. La única forma de librarse de estas vulnerabilidades es estar muy al día con las actualizaciones y que no seamos víctima de una antes de que el parche se pueda instalar.

Por estos motivos, requerir una conexión a la VPN de Uniovi antes de poder acceder al escritorio remoto de nuestros equipos es una medida de seguridad adicional que nos garantiza que solo personas autorizadas por la Universidad para entrar en la VPN podrán hacer intentos de conexión al mismo. Gracias a la incorporación del 2FA, la probabilidad de que sea una cuenta robada ha disminuido muy significativamente. En general esta política debe aplicarse no solo con el escritorio remoto, sino con cualquier servicio que necesitemos ofrecer desde alguna máquina de la Universidad. Esto quiere decir que debemos limitar al máximo (o no usar) las solicitudes de *apertura perimetral* que ofrece la Universidad a máquinas de su red: <https://sic.uniovi.es/atencionusuario/administradores>

El servicio VPN necesita la instalación de un cliente específico, y ésta se encuentra documentada aquí: <https://unioviedo.sharepoint.com/sites/PortaldeSoftwareCorporativo/SitePages/Acceso-Remoto.aspx>. No obstante, en esta actividad vamos a describir el uso del cliente *Fortinet VPN*, que es el que se necesita para utilizar sistemas operativos distintos de Windows o MacOS, como *Android*, *IOS* o *Linux*.

Instalación













Lo primero que debemos hacer es descargarnos el cliente correspondiente a nuestro sistema operativo de esta dirección: <https://www.fortinet.com/support/product-downloads>. De todos los productos disponibles, es necesario elegir *FortiClient VPN*.

FortiClient VPN

The VPN-only version of FortiClient offers SSL VPN and IPsecVPN, but does not include any support. Download the best VPN software for multiple devices.

Remote Access

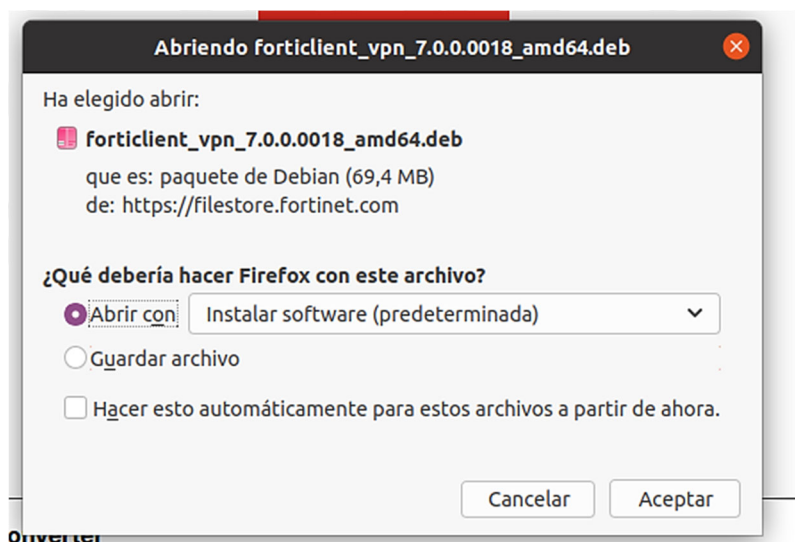
- ✓ SSL VPN with MFA
- ✓ IPSEC VPN with MFA

 Download VPN for Windows 	 Download VPN for MacOS 	 Download VPN for Linux 
 Download VPN for iOS 	 Download VPN for Android 	 Download VPN for Linux 

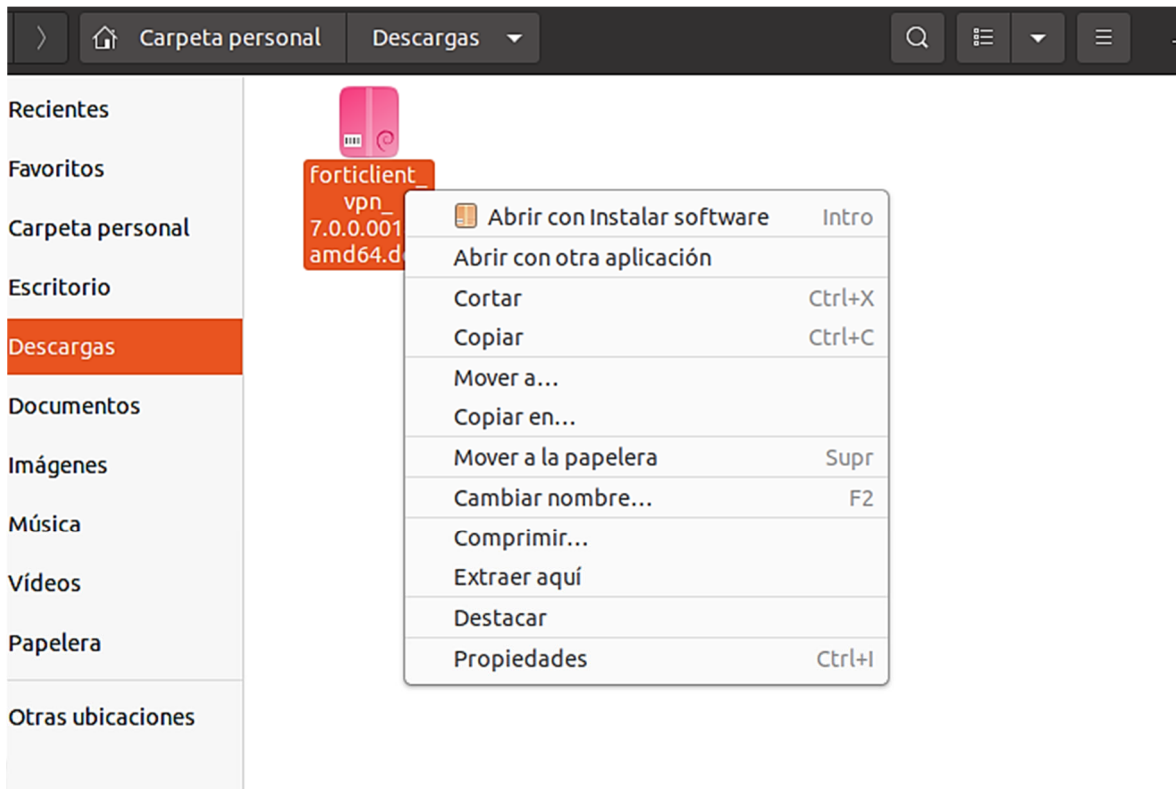
Aquí el comportamiento cambiará en función del sistema operativo que tengamos. Para *Windows*, por ejemplo, simplemente debemos instalar el cliente y reiniciar el sistema operativo para comenzar a usarlo. En el caso de *Linux*, todo depende del sistema gráfico que tengamos instalado y las funcionalidades que tenga implementadas.

Instalación con un GUI “completo” como Gnome

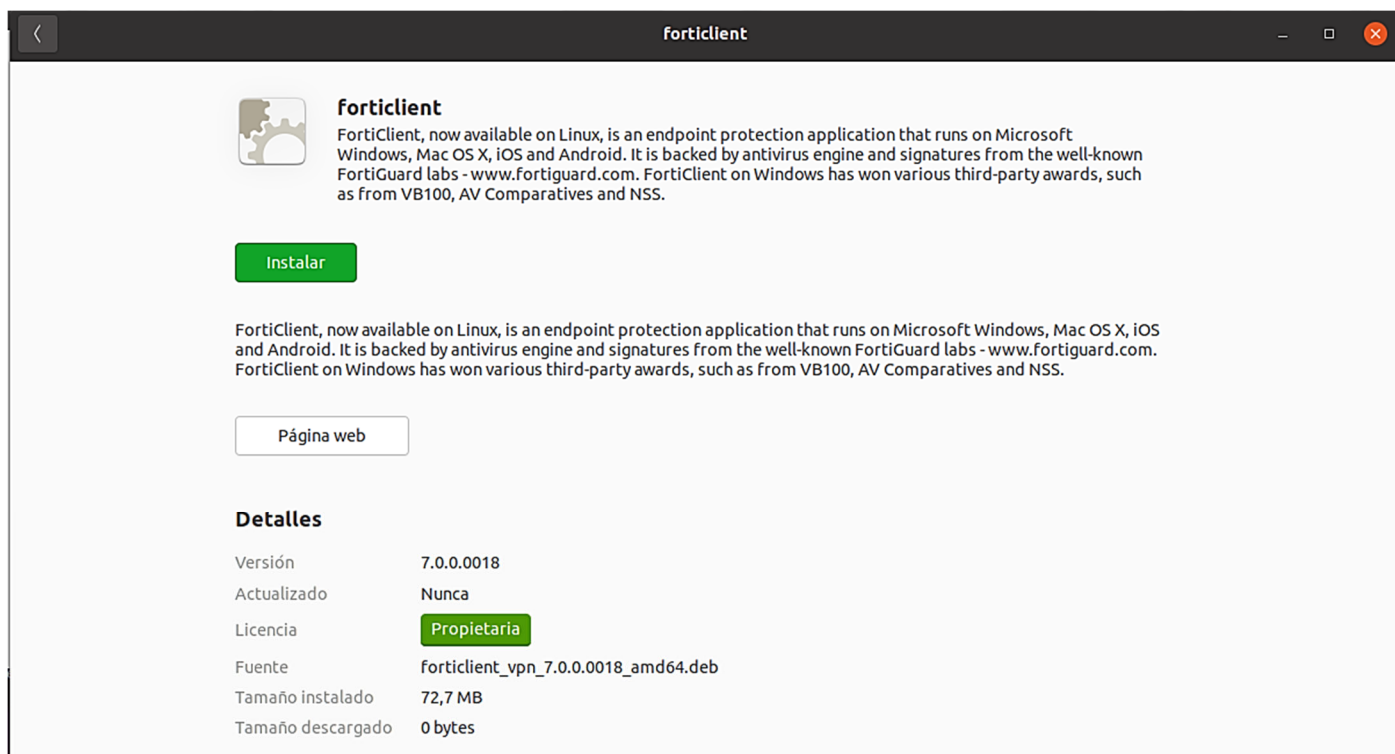
Por ejemplo, en el caso de *Gnome* (GUI por defecto de *Ubuntu 18.04+*) veremos este dialogo al descargar. En el vemos que se nos ofrece la opción de instalar el software directamente o la de guardarlo para instalarlo posteriormente. Se recomienda la segunda, puesto que se han detectado casos en los que la instalación directa da un error relativo al formato del fichero descargado.



Hecha la descarga, simplemente haciendo clic derecho sobre el archivo podremos usar la opción de “Abrir con instalar software”.



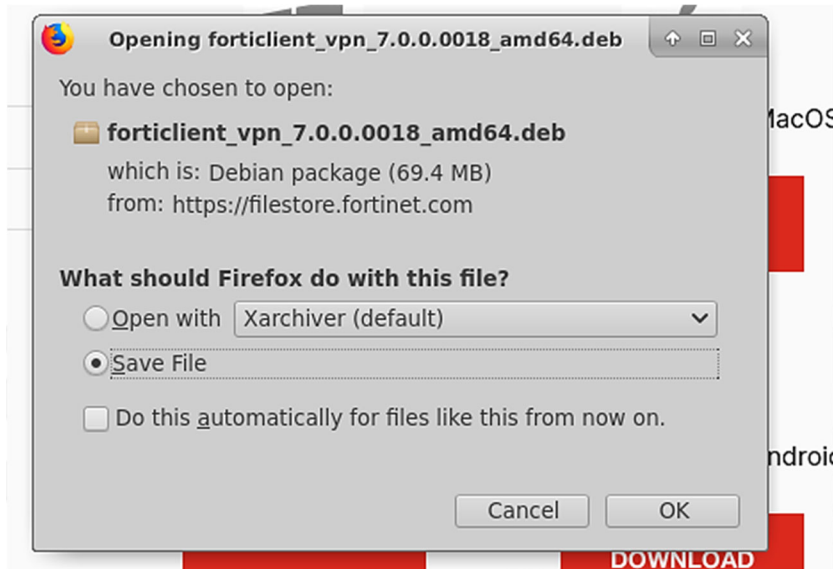
Lo cual nos abre la interfaz gráfica de instalación de paquetes, donde solo tenemos que darle a instalar para continuar.



Instalación con un GUI “ligero” como XFCE4

Si nuestra máquina *Linux* tiene un GUI ligero es posible que ciertas opciones de instalación gráfica de paquetes no estén disponibles, por lo que tenemos que hacer una instalación más bien manual. Antes de empezar, hay que destacar que se han detectado casos en los que el cliente, aunque se instale correctamente y haga todo el proceso de conexión hasta el final, **no llega a establecer la VPN en un**

Linux con XFCE4, por lo que se recomienda el uso de Gnome o similar para evitar posibles problemas. En cualquier caso, al descargar el fichero tenemos este dialogo, donde no se nos ofrece la instalación, sino la apertura del fichero del paquete descargado (que es un archivo comprimido con una estructura interna especial) o su descarga. En nuestro caso solo nos es útil la segunda:



Los GUIs ligeros no instalan algunos paquetes para disminuir su uso de recursos y en este caso nos falta uno que el cliente de Fortigate VPN necesita, libappindicator1. Por ello, debemos proceder a su instalación con `sudo apt install libappindicator1`. Vemos que en este caso nos da un error de dependencias que podemos reparar simplemente con `sudo apt -fix-broken install`, con lo que se volverá a instalar la librería necesaria.

```

ssiuser@vagrant:~/Downloads$ sudo apt install libappindicator1
Reading package lists... Done
Building dependency tree
Reading state information... Done
You might want to run 'apt --fix-broken install' to correct these.
The following packages have unmet dependencies:
 libappindicator1 : Depends: libdbusmenu-gtk4 (>= 0.4.2) but it is not going to be installed
                   Depends: libindicator7 (>= 0.4.90) but it is not going to be installed
E: Unmet dependencies. Try 'apt --fix-broken install' with no packages (or specify a solution
).
ssiuser@vagrant:~/Downloads$ sudo apt --fix-broken install
Reading package lists... Done
Building dependency tree
Reading state information... Done
Correcting dependencies... Done
The following packages were automatically installed and are no longer required:
 linux-image-4.15.0-58-generic linux-modules-4.15.0-58-generic
 linux-modules-extra-4.15.0-58-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
 libappindicator1 libdbusmenu-gtk4 libindicator7
Suggested packages:
 indicator-application
The following NEW packages will be installed:
 libappindicator1 libdbusmenu-gtk4 libindicator7
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
1 not fully installed or removed.
Need to get 67.8 kB of archives.
After this operation, 275 kB of additional disk space will be used.
Do you want to continue? [Y/n] █

```

Hecho esto, ya podemos instalar el paquete con `sudo dpkg -i <fichero descargado de la web de fortigate>`

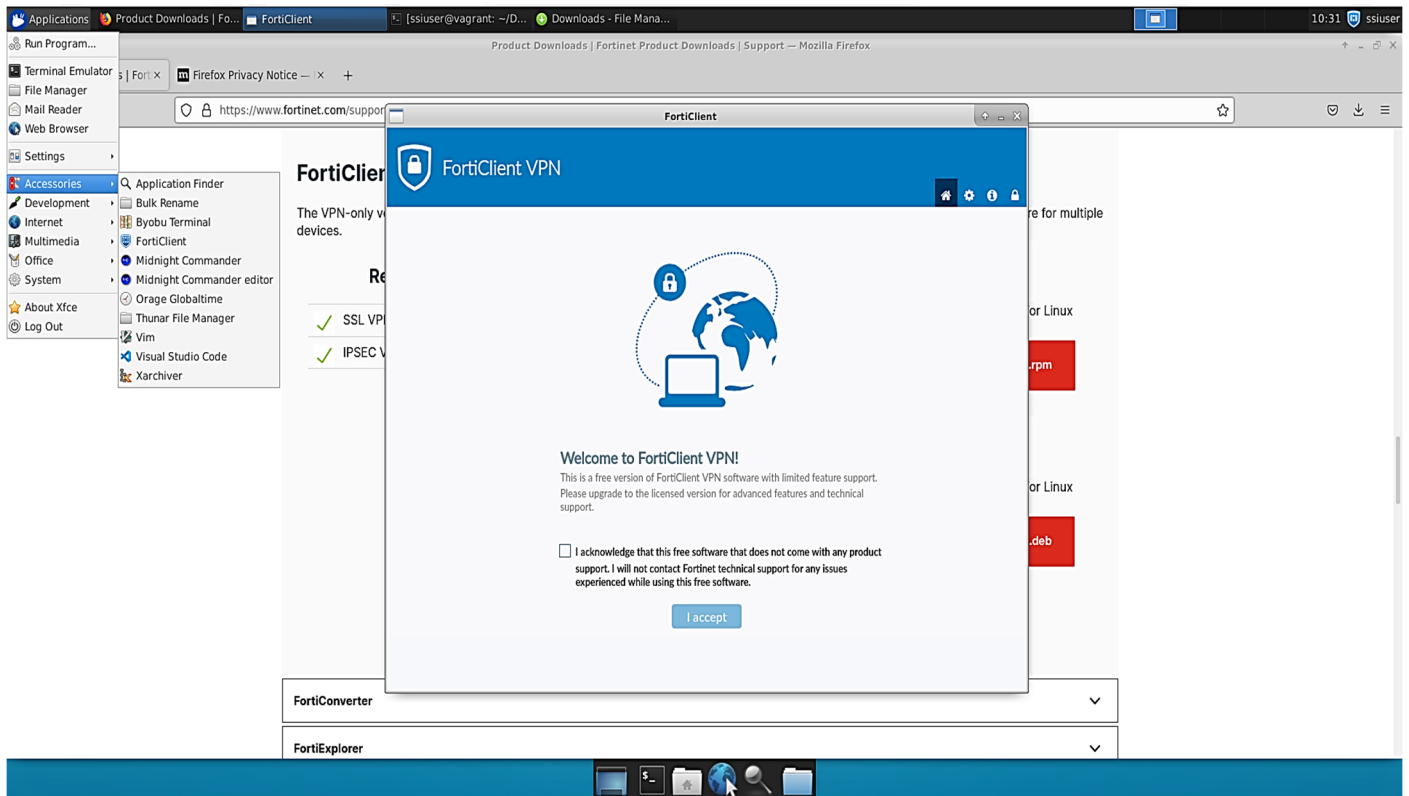
```
ssiuser@vagrant:~/Downloads$ ls -la
total 71028
drwxr-xr-x  2 ssiuser ssiuser   4096 Mar 23 10:26 .
drwxr-xr-x 16 ssiuser ssiuser   4096 Mar 23 10:26 ..
-rw-rw-r--  1 ssiuser ssiuser 72721126 Mar 23 10:26 forticlient_vpn_7.0.0.0018_amd64.deb
ssiuser@vagrant:~/Downloads$ sudo dpkg -i forticlient_vpn_7.0.0.0018_amd64.deb
```

Si todo es correcto, tendríamos que ver esta pantalla y ya podemos proceder a la configuración inicial.

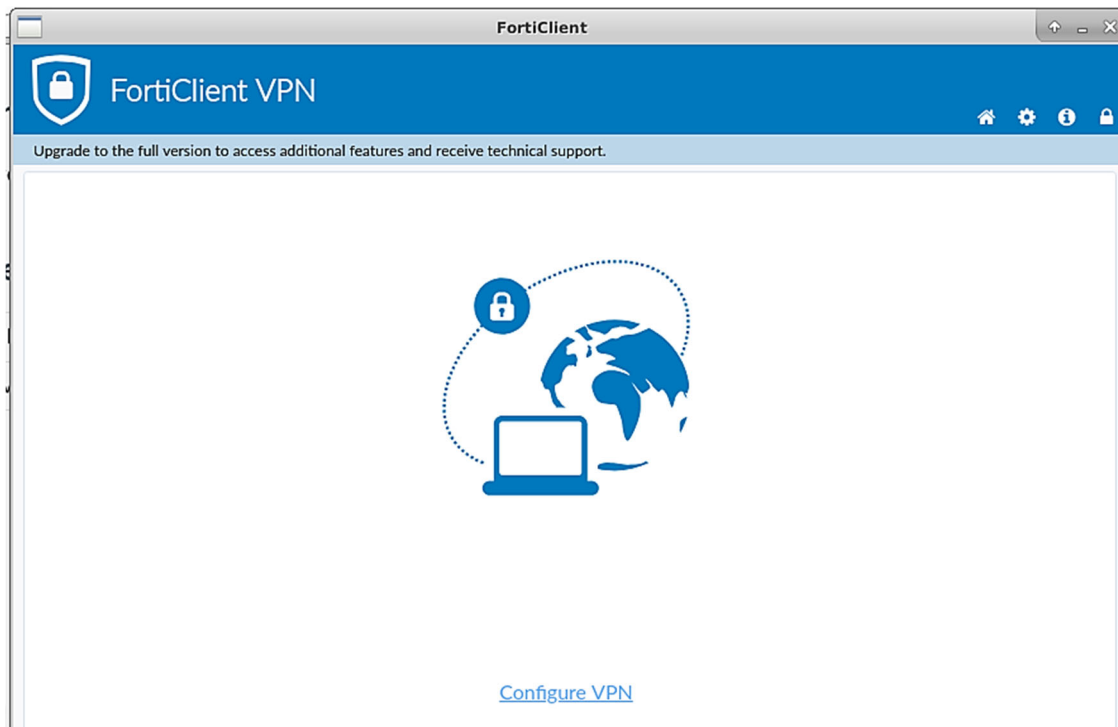
```
ssiuser@vagrant:~/Downloads$ sudo dpkg -i forticlient_vpn_7.0.0.0018_amd64.deb
(Reading database ... 132711 files and directories currently installed.)
Preparing to unpack forticlient_vpn_7.0.0.0018_amd64.deb ...
Unpacking forticlient (7.0.0.0018) over (7.0.0.0018) ...
Setting up forticlient (7.0.0.0018) ...
gtk-update-icon-cache: Cache file created successfully.
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for desktop-file-utils (0.23-1ubuntu3.18.04.2) ...
Processing triggers for mime-support (3.60ubuntu1) ...
ssiuser@vagrant:~/Downloads$
```

Configuración inicial

Una vez instalado el cliente de *Fortigate VPN*, podemos acceder a él mediante el menú de programas del sistema operativo (*Accesorios* en la imagen) o bien mediante un icono que nos aparecerá en la barra de menú superior del mismo. En cualquier caso se abrirá la pantalla de bienvenida donde tendremos que **aceptar el acuerdo de licencia** para usar el programa.



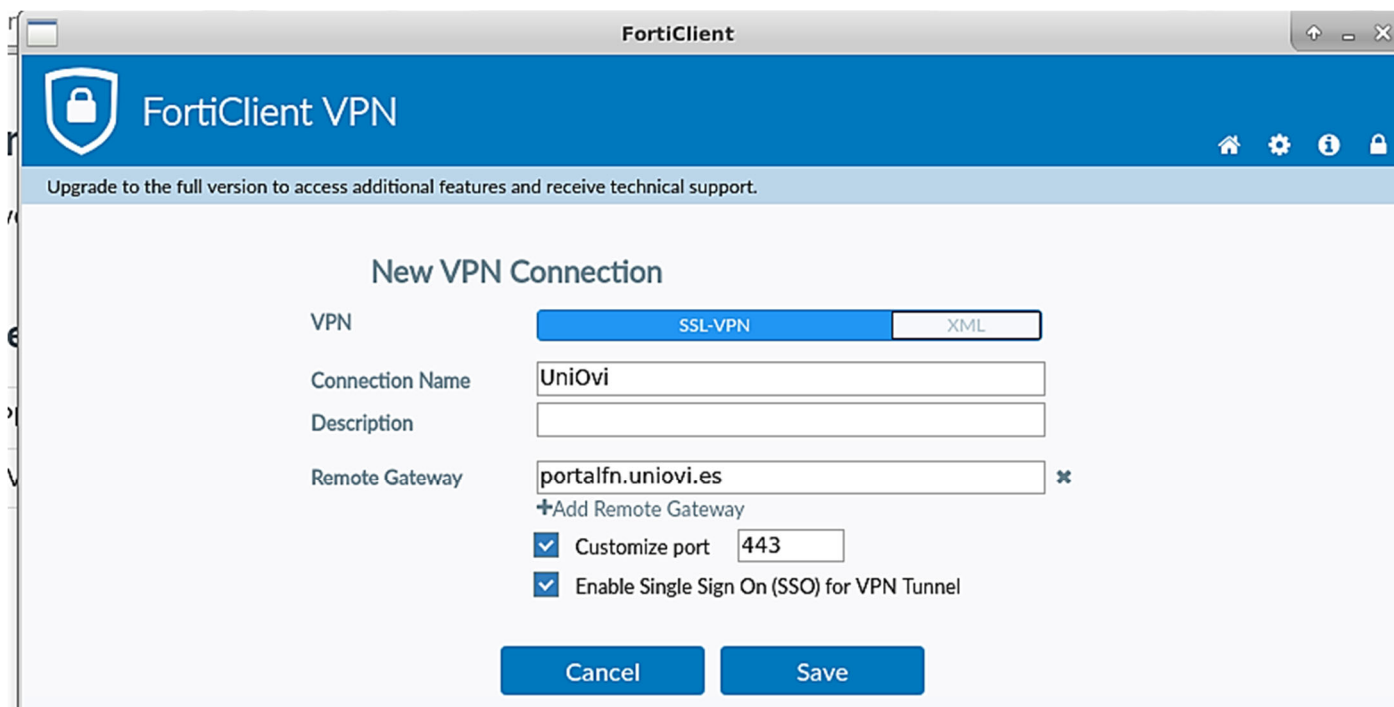
Hecho esto, ya estamos en disposición de configurar nuestra conexión de VPN con la opción *“Configure VPN”* del programa.



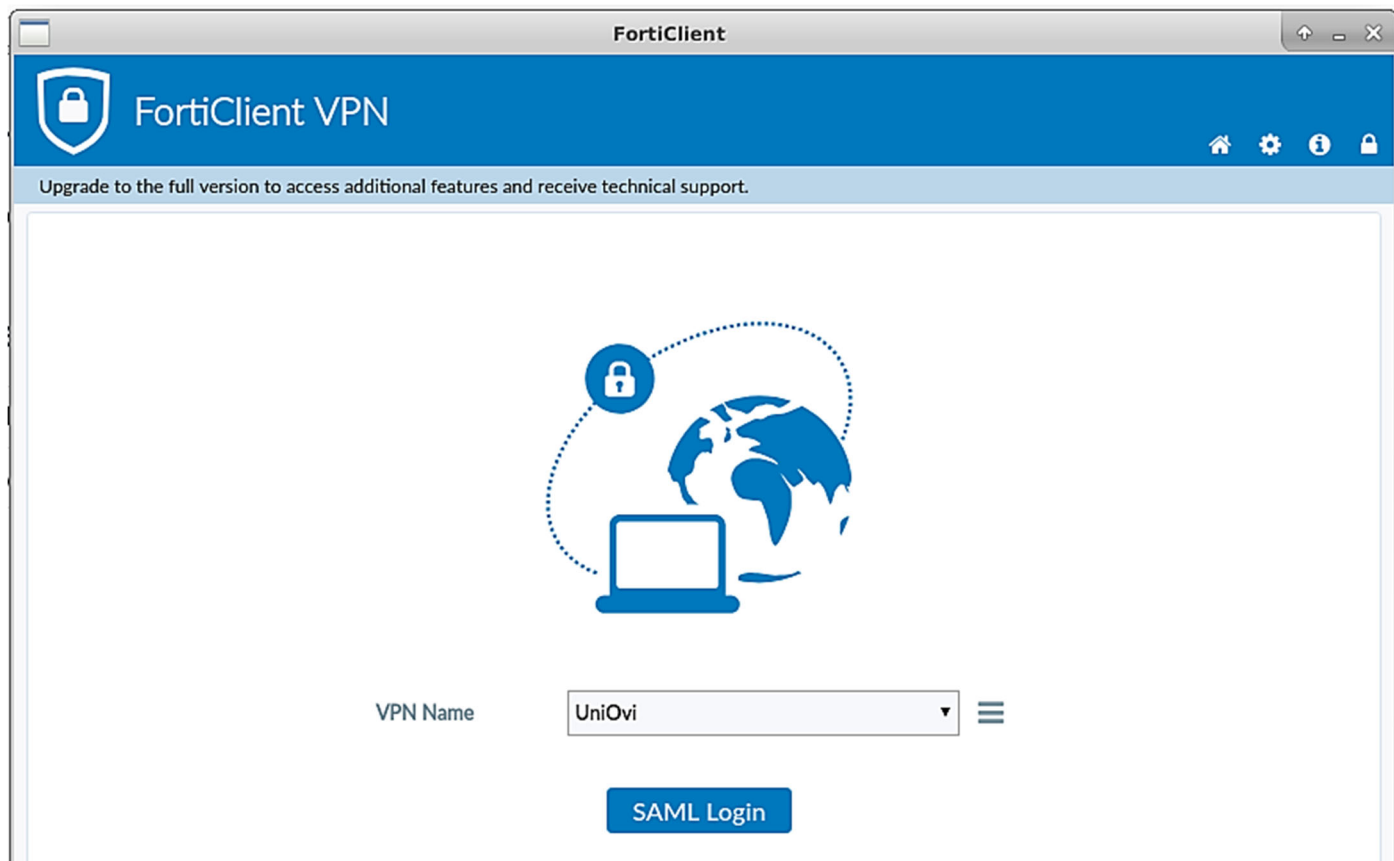
Los parámetros para una conexión a nuestra universidad son principalmente dos. El nombre de la conexión puede ser el que queramos:

- Remote Gateway: **portalfn.uniovi.es**
- Activar “Enable Single Sign On (SSO) for VPN Tunnel”

Hecho esto, salvamos la configuración y ya podemos usar una conexión con ese nombre en adelante.

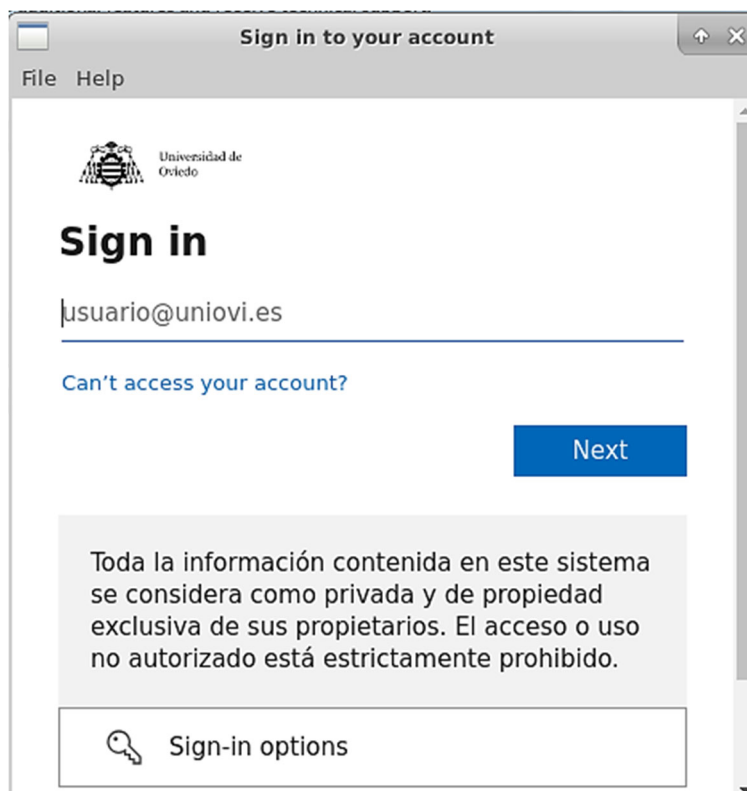


Ahora ya podemos iniciar la conexión pulsando en el botón “SAML Login”. Si nos hemos equivocado al configurar la conexión o queremos cambiar algo, podemos pulsar en el botón de las tres rayas horizontales para volver a la pantalla anterior.

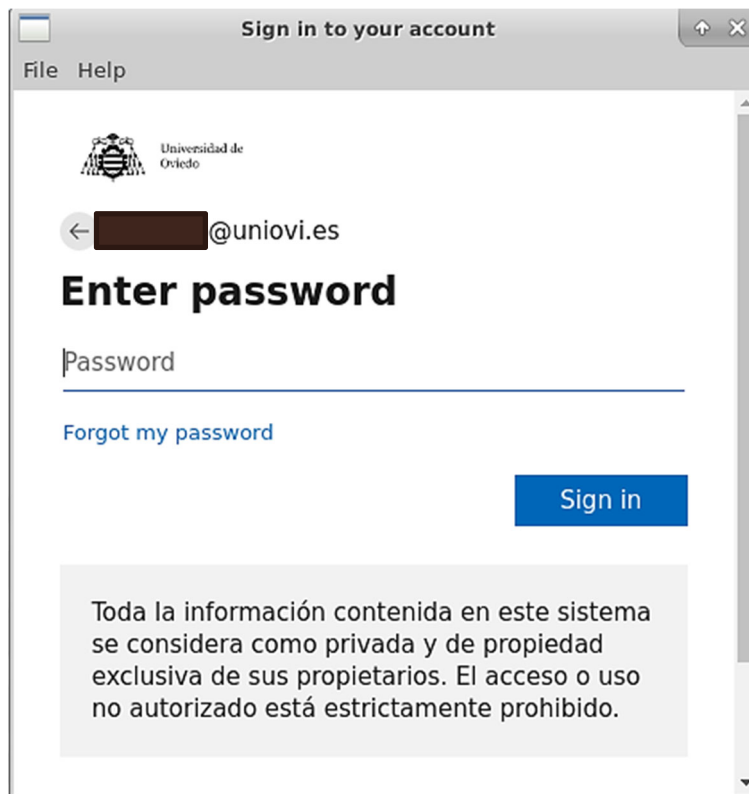


Conexión

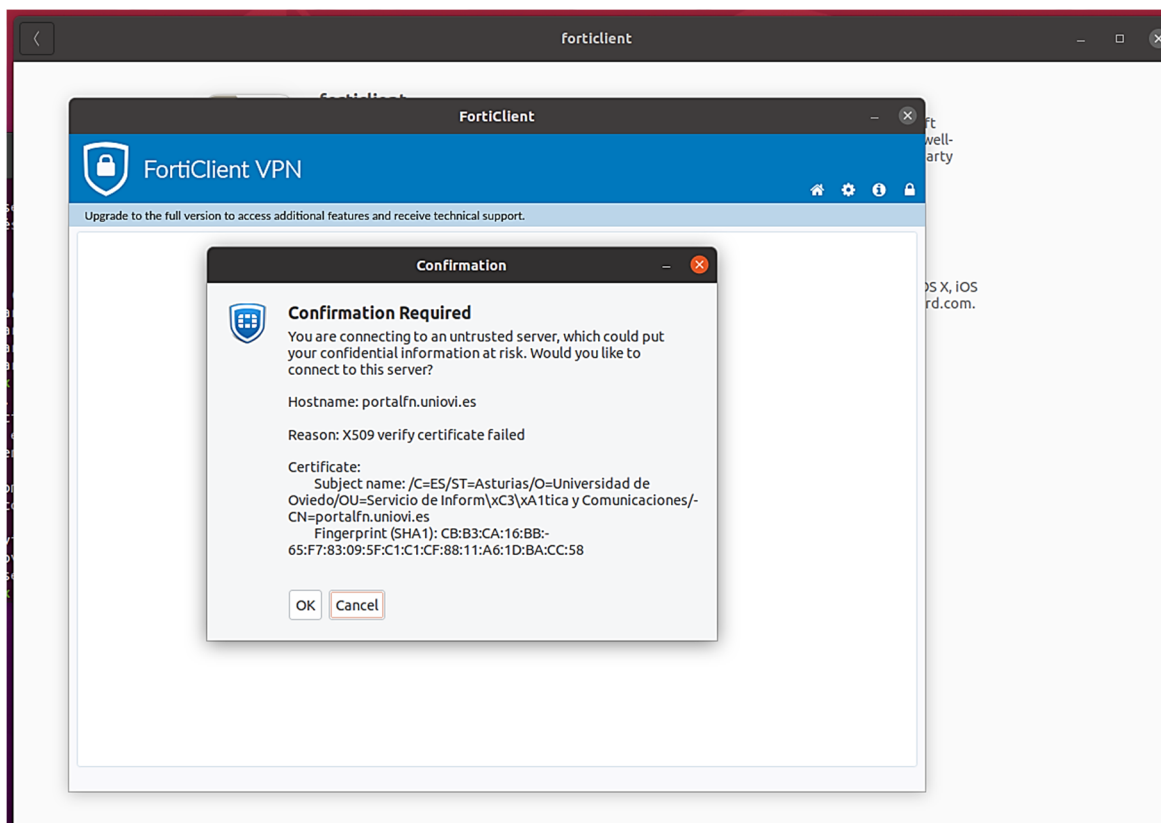
Una vez iniciemos la conexión, se nos preguntará en primer lugar por nuestro identificador de la Universidad de Oviedo (incluyendo el @uniovi.es).



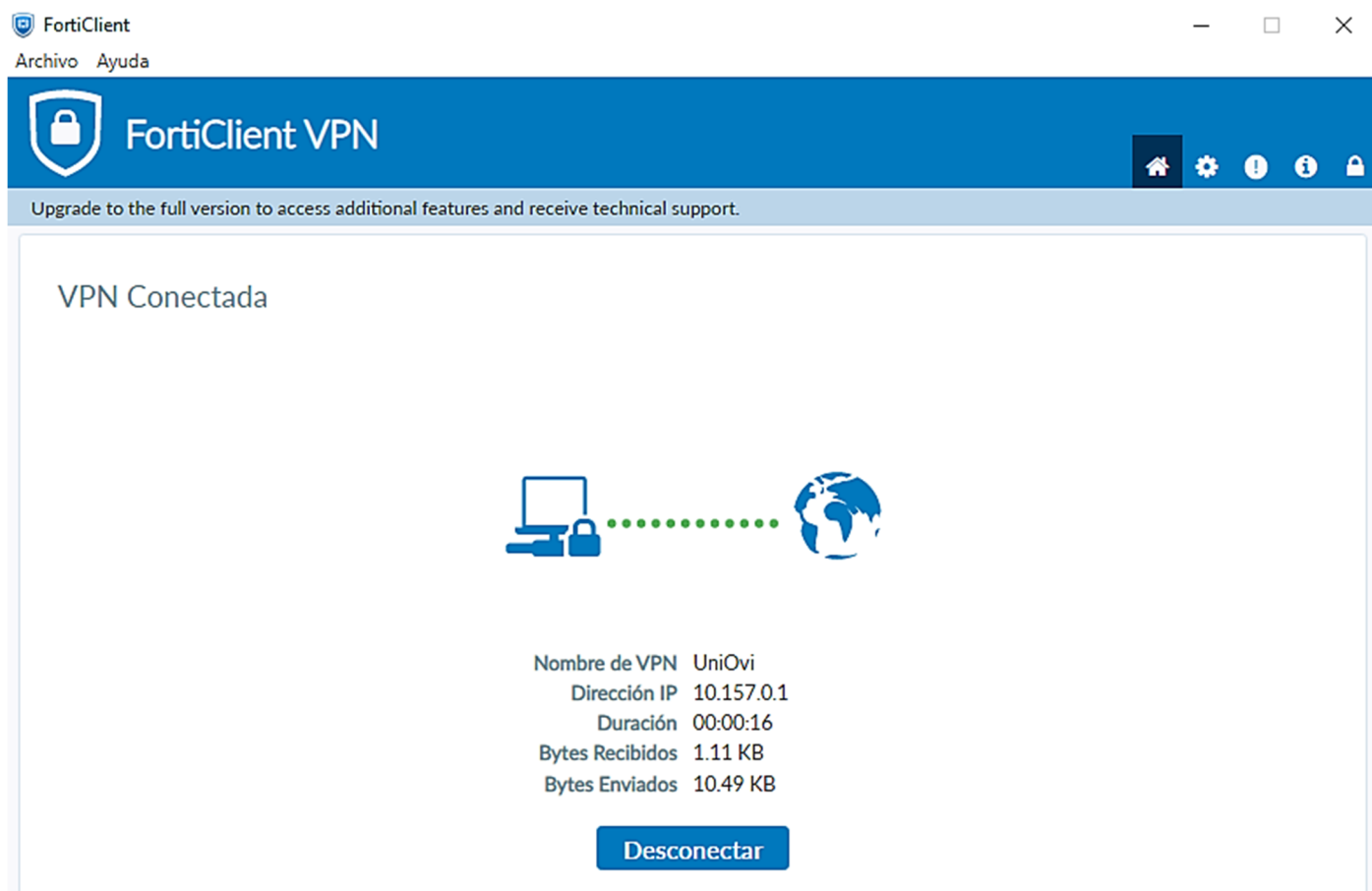
Ahora debemos introducir nuestra password de la Intranet para continuar



Si la clave es correcta, ahora nos pedirá que introduzcamos el código del sistema 2FA que hayamos introducido (tradicionalmente el que nos llega por SMS al móvil) para poder continuar. Si es correcto, veremos este dialogo de confirmación al que debemos darle OK para conectar (NOTA: este dialogo no parece que se muestre en sistemas Windows).



Si todo es correcto, deberíamos ver esta pantalla de información que nos muestra nuestra IP dentro de la VPN, el tiempo que llevamos conectados y el tráfico de datos enviados y recibidos a / desde la red de Uniovi. Pulsando en “Desconectar” interrumpiremos nuestra conexión VPN.



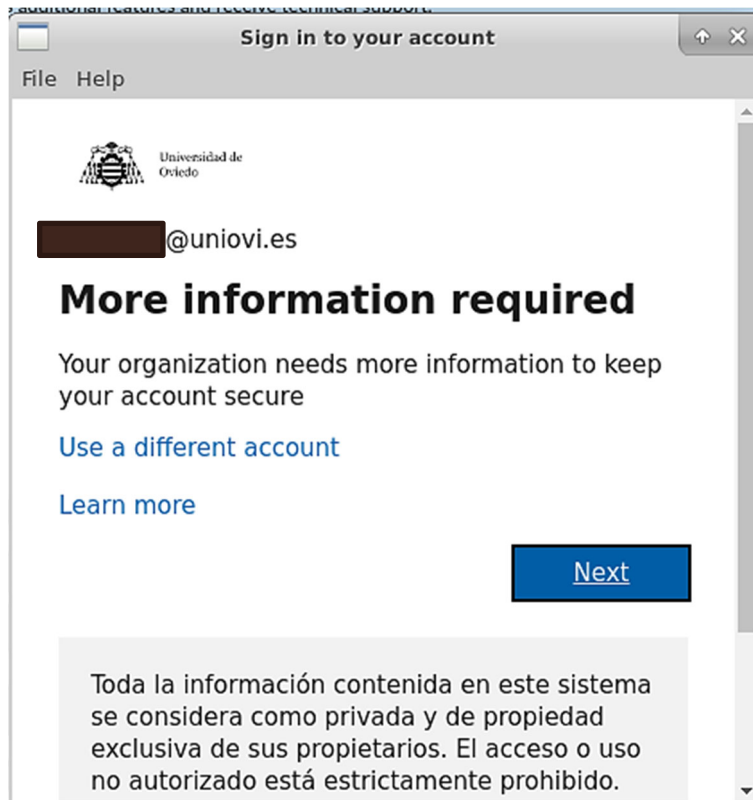
A modo de curiosidad, en línea de comandos podemos ver cómo mientras la VPN está activa tenemos un nuevo interfaz de red virtual creado, a través del cual se envían los datos a la red de la Universidad.

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
vpn: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1400
inet 10.157.0.1 netmask 255.255.255.255 destination 10.157.0.1
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500
(UNSPEC)
RX packets 13 bytes 1896 (1.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 14 bytes 1141 (1.1 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

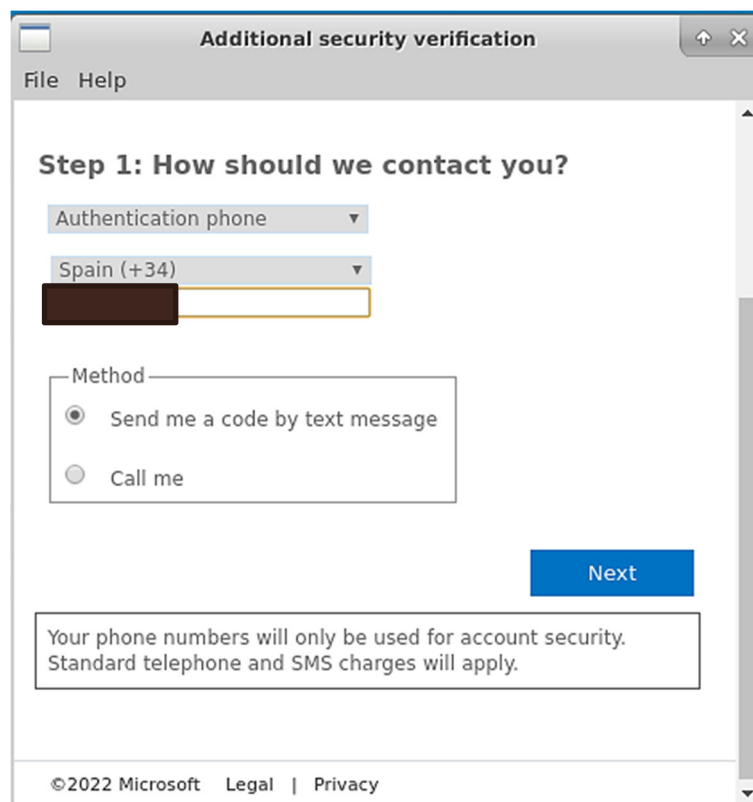
Posibles errores

¿Qué pasa si no he activado aún el 2FA?

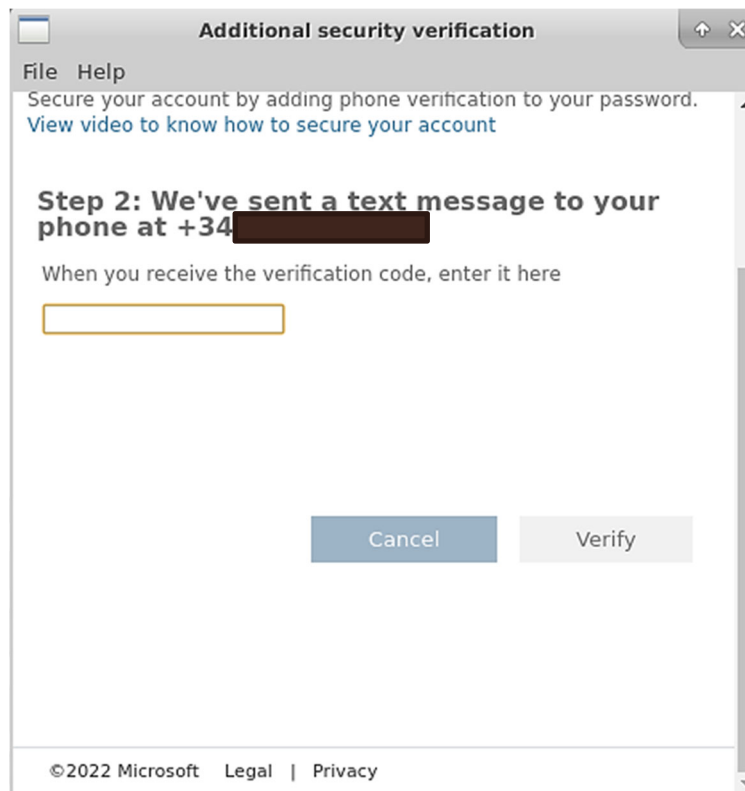
Para usar la VPN es necesario tener el 2FA activo, ya que ahora es obligatorio para toda la Universidad. Si aún no lo hubiéramos hecho por cualquier motivo, al introducir correctamente la clave de nuestro usuario se nos notificaría esto, que es lo que nos permite establecer el método 2FA que usaremos en adelante.



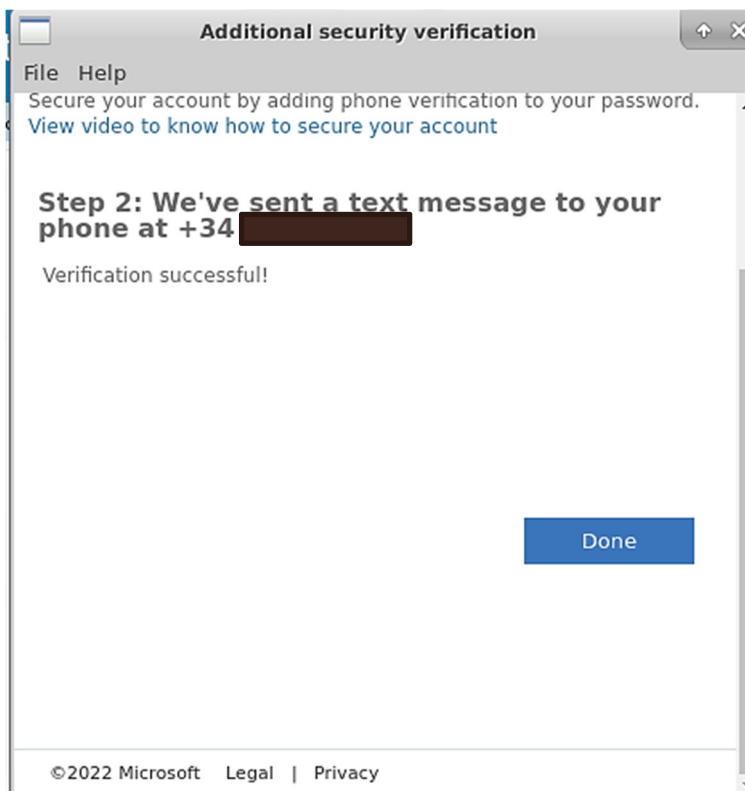
En la pantalla siguiente podemos dar un nº de teléfono donde se nos enviará un SMS o una llamada para verificar nuestra identidad.



Si elegimos enviar un mensaje de texto, ahora deberíamos recibir uno en el teléfono indicado e introducirlo en la siguiente pantalla

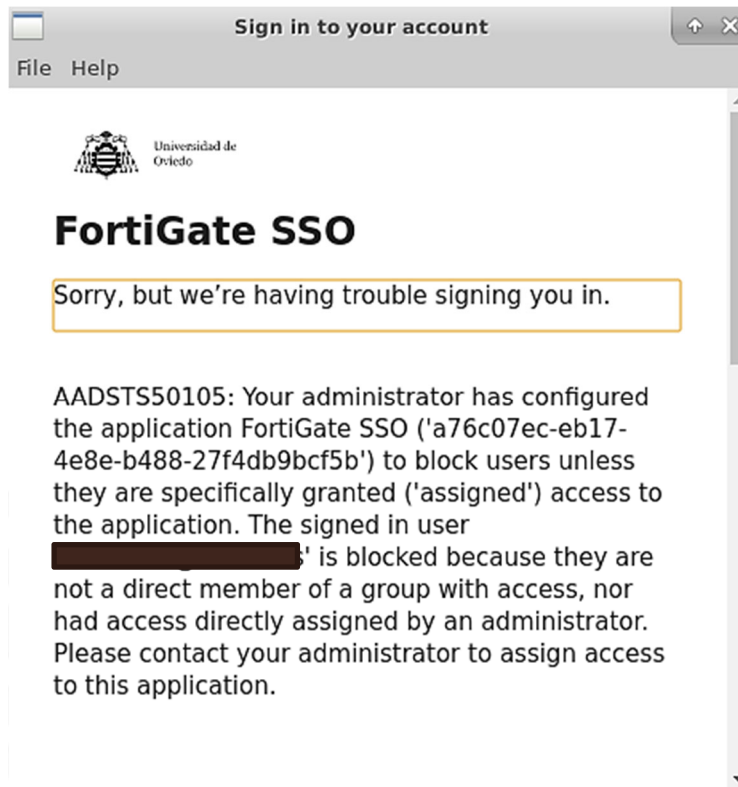


Si lo introducimos correctamente habremos configurado satisfactoriamente el 2FA para este servicio y todos los de Uniovi que lo requieran en adelante.

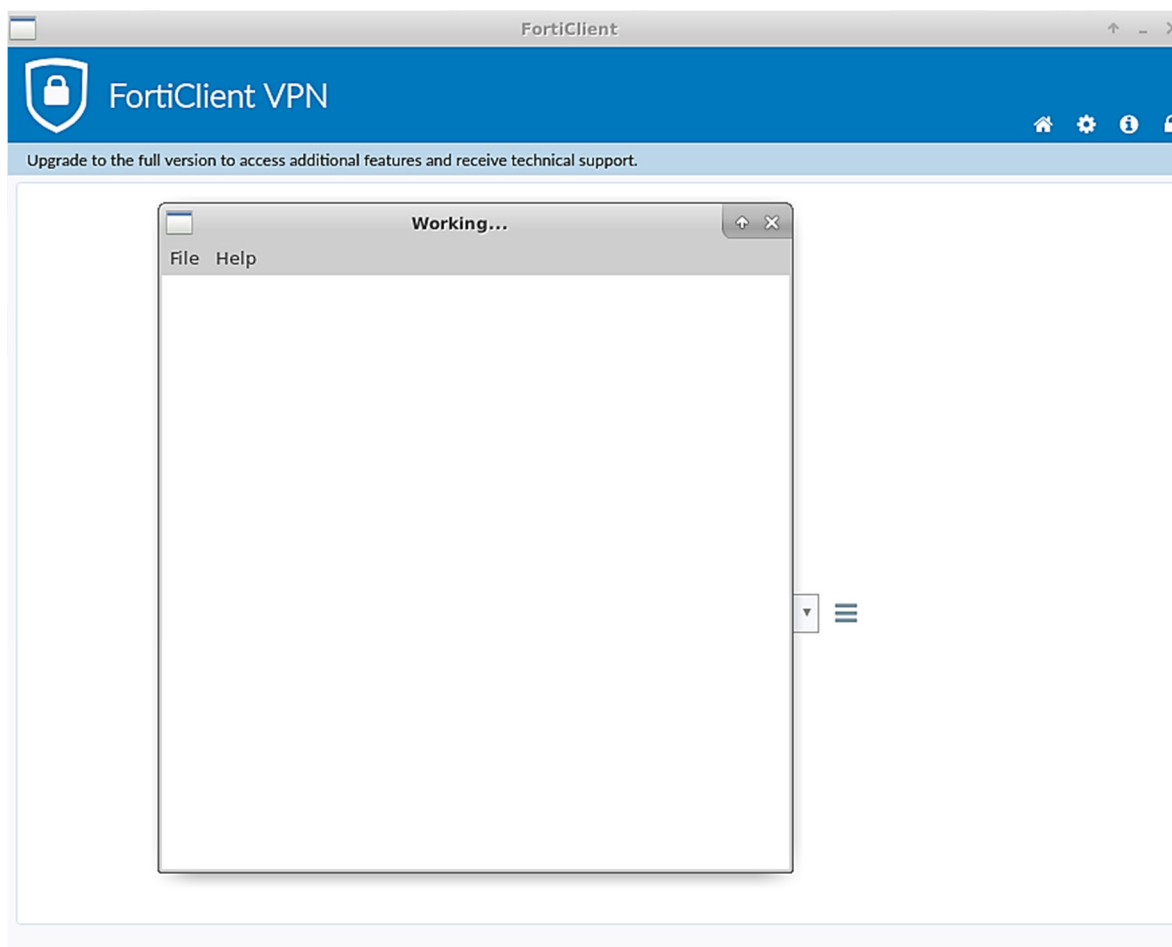


Otros errores

El servicio VPN no está disponible para personas que ya no tienen ninguna vinculación con la Universidad de Oviedo (antiguos empleados o estudiantes, por ejemplo), y en ese caso se muestra el siguiente error. Si consideras que es un error, debes hablar con el Causi para que lo puedan arreglar.



En determinados sistemas operativos, una vez que se ha introducido la clave y el 2FA correctamente el cliente se queda parado en esta pantalla y nunca termina de avanzar.



En estos casos, se cierra la ventana "Working" y se intenta otra vez desde la ventana de conexión y ya se puede establecer la conexión.