



Configuración de FortiClient para acceso remoto

Versión 1.0 junio 2026

Contenido

Qué es FortiClient y para que se usa en la Universidad.....	1
A tener en cuenta antes de poder usar la VPN.....	2
Descarga e instalación	2
Activación EMS.....	5
FortiClient en equipos de escritorio (Windows, Linux y macOS).....	8
Forticlient en IOS.....	9
Forticlient en Android	13
Gestión de la conexión VPN	17
Preguntas frecuentes.....	17
¿Necesito ser administrador de mi equipo para instalar el cliente?	17
Desinstalar el cliente.....	17
¿Puedo instalar el cliente en un ordenador compartido?	17
¿Por qué esta mi conexión a la telemetría no alcanzable y qué hacer?	17
No me ha llegado el túnel de acceso remoto	18
¿Qué hago si me aparece que el acceso VPN está disponible sin licencia hasta una fecha?	18
¿Qué hago si el cliente me dice que estoy conectado a un túnel, pero no puedo hacer escritorio remoto a mi equipo?	19
Cambiar de conexión WIFI Unican a otra red	19

Qué es FortiClient y para que se usa en la Universidad

FortiClient es la aplicación oficial de seguridad y acceso remoto utilizada por la Universidad de Cantabria. Su función principal es crear un canal de comunicación seguro y completamente cifrado (llamado VPN) entre tu ordenador y la red interna del campus.

En la UC, este programa actúa como la herramienta unificada para cualquier tipo de teletrabajo o movilidad. Es decir, tanto si necesitas conectarte desde tu casa, durante un viaje o desde un portátil externo, FortiClient te permitirá acceder a tus herramientas habituales (como tu equipo de la oficina,.) de forma tan segura como si estuvieras

físicamente en el campus, garantizando que la información confidencial viaje totalmente protegida frente a amenazas de Internet.

A tener en cuenta antes de poder usar la VPN

Para poder conectarse a la VPN de la UC debemos comprobar:

A- Estamos dados de alta en la VPN.

Si no sabe si está dado de alta o quiere solicitarlo contacte con nosotros.

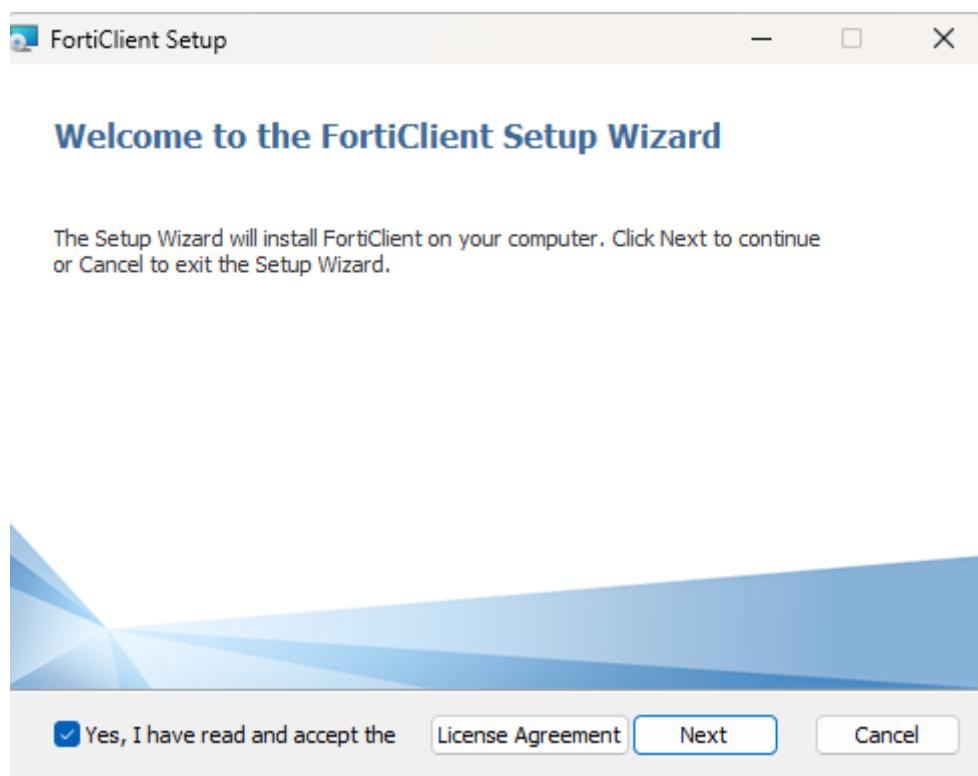
B-Debe tener registrado al menos un método de validación MFA.

Para ello siga [los manuales y tutoriales de nuestra página](#).

Descarga e instalación

Descargue el instalador que necesite según su sistema operativo desde la web del servicio de informática

Ejecuto el instalador descargado



FortiClient Setup

Choose Setup Type

Choose the setup type that best suits your needs

- ☒ **Zero Trust Telemetry**
Fabric Telemetry
- ☒ **Secure Remote Access**
SSL and IPsec VPN
- ☒ **Vulnerability Scan**
Host vulnerability scanning and remediation
- ☐ **Advanced Persistent Threat (APT) Components**
FortiSandbox detection and cloud scan
- ☐ **ZTNA**
Zero Trust Network Access

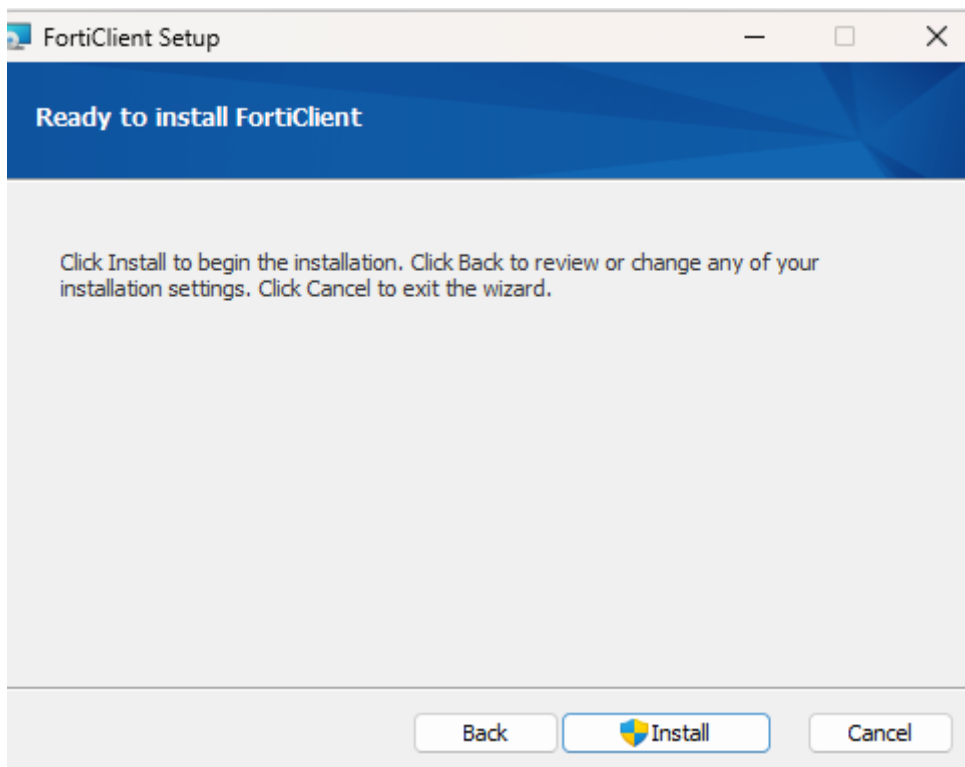
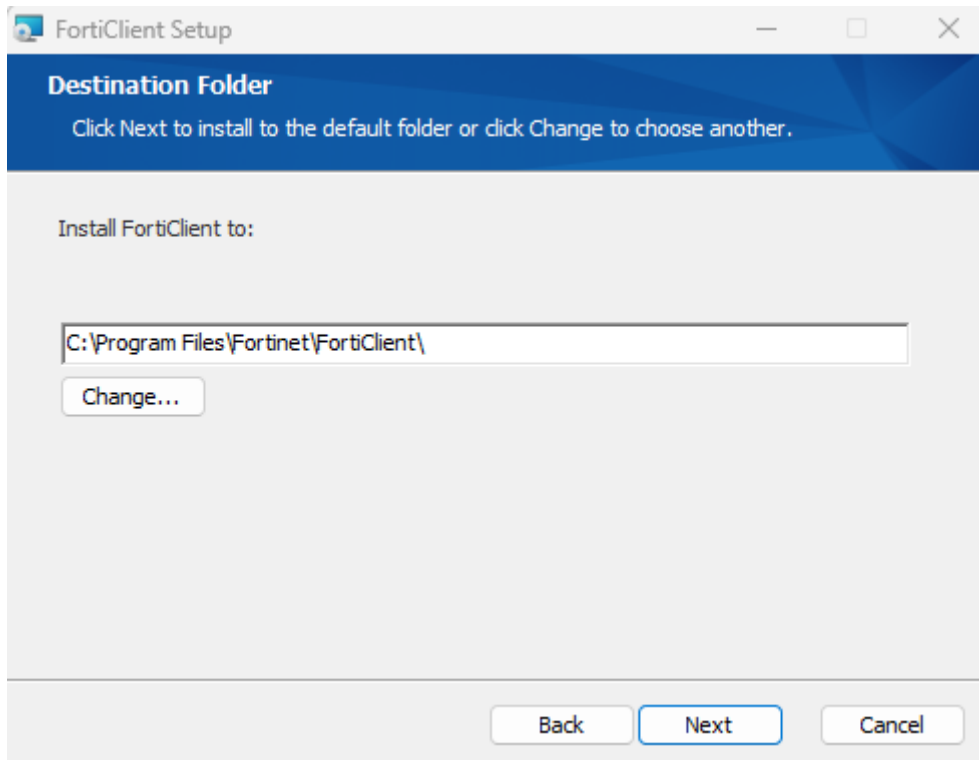
Back Next Cancel

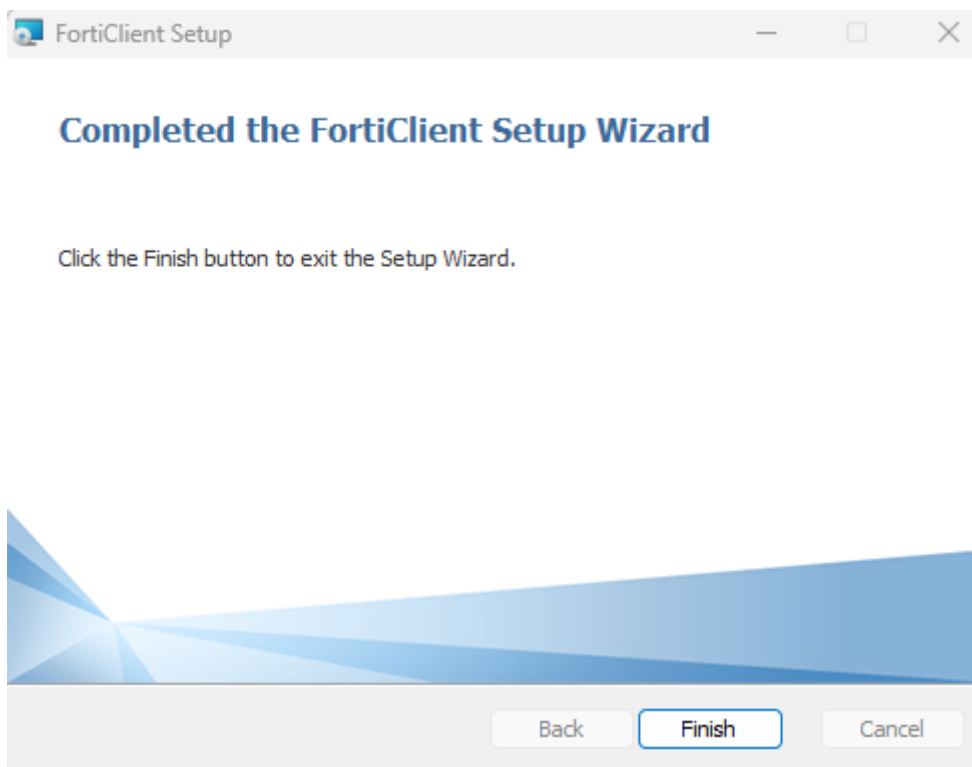
FortiClient Setup

Additional Security Features

- ☐ **AntiVirus**
Real-Time and On-Demand AntiVirus scanning
- ☐ **Web Filtering**
Web Filtering
- ☐ **Single Sign-On Mobility Agent**
Single Sign-On Mobility Agent
- ☐ **Anti-Ransomware**
Anti-Ransomware
- ☐ **Application Firewall**
Application Firewall
- ☐ **PAM**
Privilege Access Management
- ☐ **Data Protection**
Integration with FortiData

Back Next Cancel



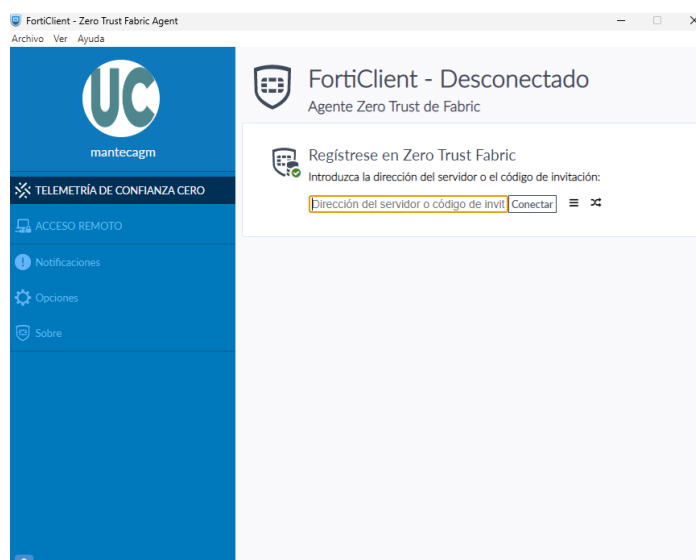


Nota para macOS: Debido a las políticas de seguridad de Apple, tras la instalación, es posible que el sistema le solicite otorgar **permisos de acceso a la red** o **notificaciones**. Asegúrese de seleccionar 'Permitir' en todas las ventanas emergentes del sistema operativo durante la primera conexión para que el túnel VPN pueda establecerse correctamente.

Activación EMS

Para automatizar la configuración y asegurar que su equipo cumpla con las políticas de seguridad de la universidad, utilice el sistema de gestión centralizado (EMS):

1. **Introducción del código:** En la aplicación FortiClient, busque el apartado de Telemetría de confianza cero "**Código de invitación**" (o "EMS Invitation").



2. **Activación:** Introduzca el siguiente código:

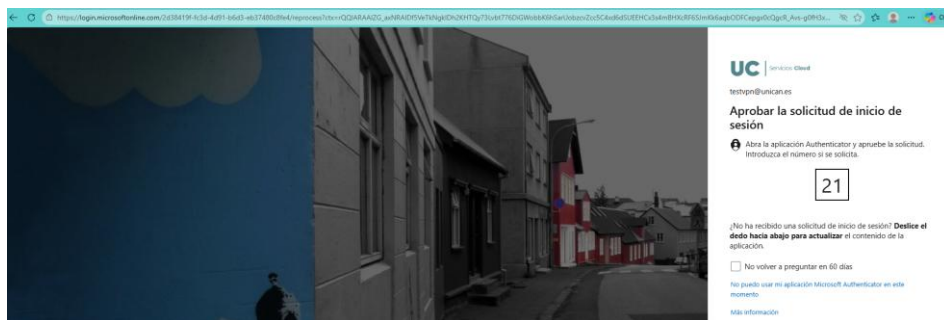
_VjE6Zmd0ZW1zLnVuaWNhbi5lczo4MDEzOmRlZmF1bHQ6NzM0M2ZmYTctMmE2MS00NTFkLTkzYTktMGFhNTI0NWM4M2Fm

3. Una vez introducido, pulse "**Conectar**". El código quedará guardado en su perfil de FortiClient. De esta forma, si la sesión se desconecta, no tendrá que volver a configurar nada; únicamente deberá pulsar el botón "**Conectar**" en la interfaz principal.

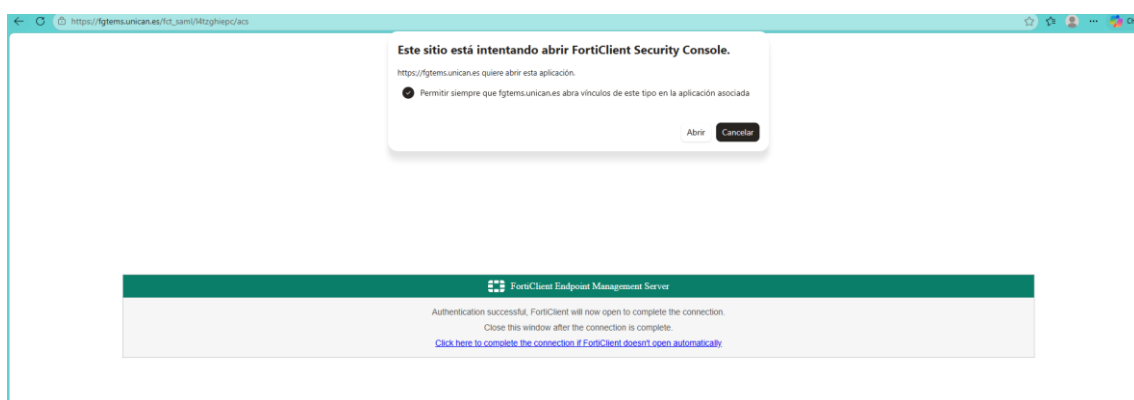
Cuando pinche en conectar le pedirá sus credenciales de dominio. Recuerde que debe poner usuario@unican.es o usuario@gestion.unican.es.

Como en el resto de servicios de la universidad se le pedirá el MFA.

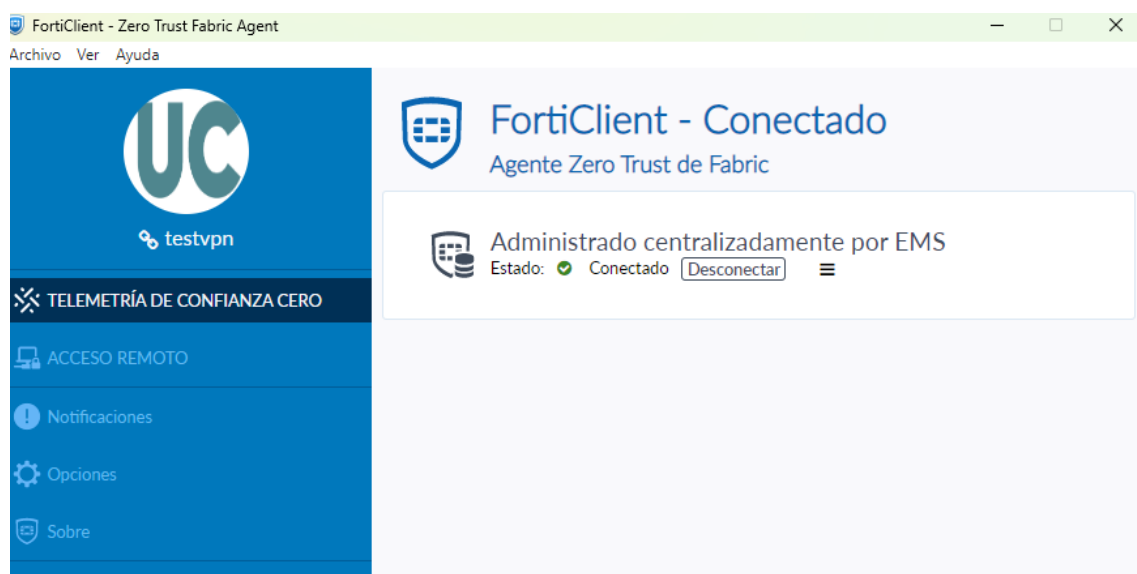




Una vez completada la validación, **aparecerá** la siguiente pantalla, donde deberá hacer clic en '**Permitir**'. Este mensaje solo se **mostrará** la primera vez o en caso de que la sesión de validación de su equipo haya caducado.



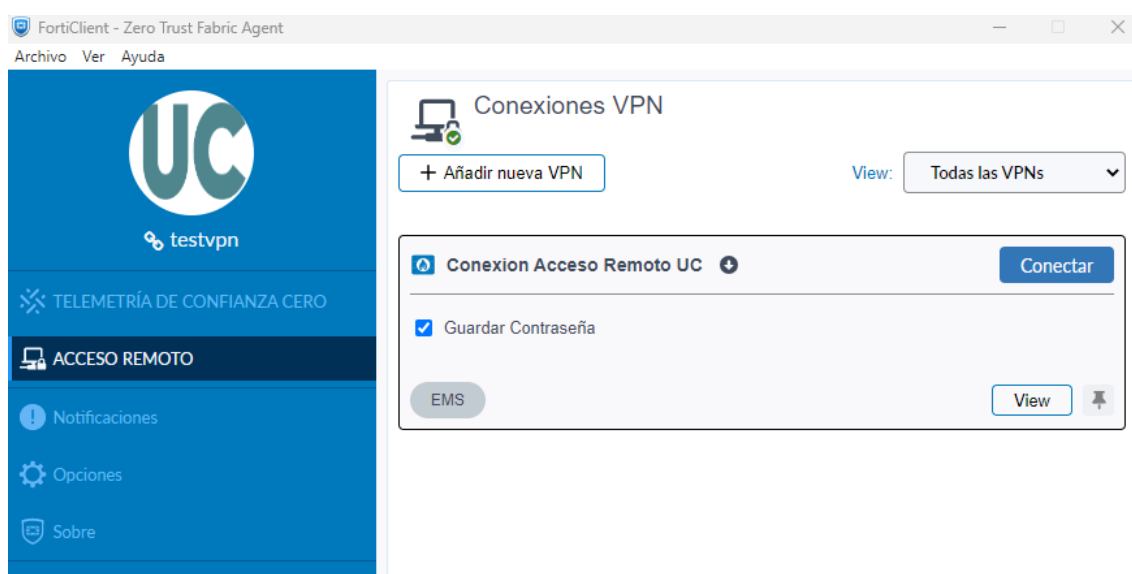
Si todo el proceso ha sido exitoso, le aparecerá en la pantalla que está conectado al EMS.



Nota para Linux y macOS: "Para crear el túnel seguro, FortiClient requiere modificar la tabla de rutas de su equipo. Es posible que el sistema le solicite introducir su **contraseña de usuario local** (la misma que usa para iniciar sesión en su ordenador) durante el proceso de activación o al conectar por primera vez.

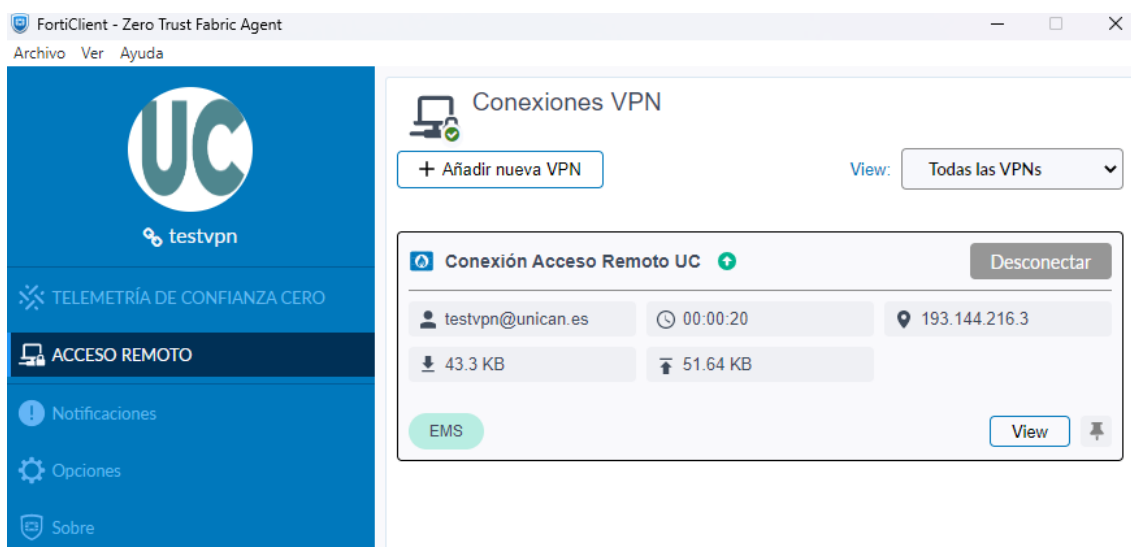
FortiClient en equipos de escritorio (Windows, Linux y macOS)

En el menú '**Acceso Remoto**' aparecerá la conexión VPN configurada para establecer el túnel seguro con la universidad. **Tenga en cuenta que el perfil de conexión es enviado por el EMS, por lo que la primera vez puede tardar unos segundos en mostrarse.**



Para establecer el túnel y acceder a los recursos de la universidad de forma segura, inicie la conexión desde este apartado. Durante este proceso, el sistema le solicitará sus credenciales institucionales y la validación del **MFA** (autenticación en dos pasos).

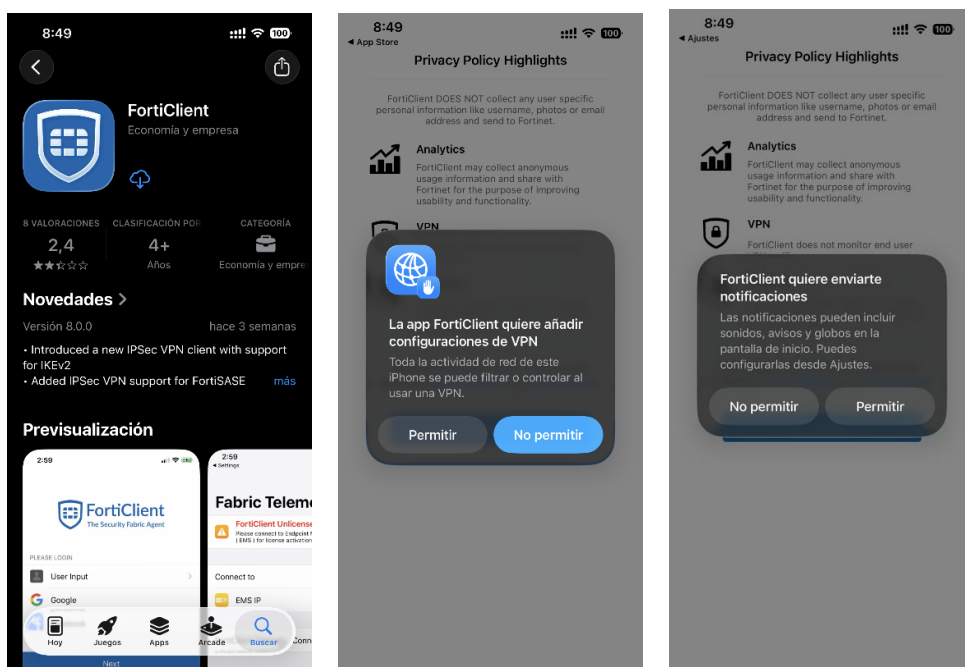
- **Nota:** Puede marcar la opción “**Guardar contraseña**” para evitar introducir sus credenciales en cada sesión.



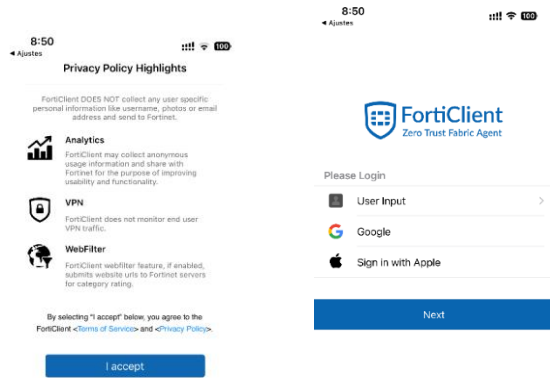
Cuando haya terminado de trabajar, pulse el botón '**Desconectar**' en el apartado de la VPN. **No es necesario desconectar el EMS**; el EMS debe permanecer activo en segundo plano para asegurar que su equipo mantenga las políticas de seguridad y configuración de la universidad actualizadas.

Forticlient en IOS

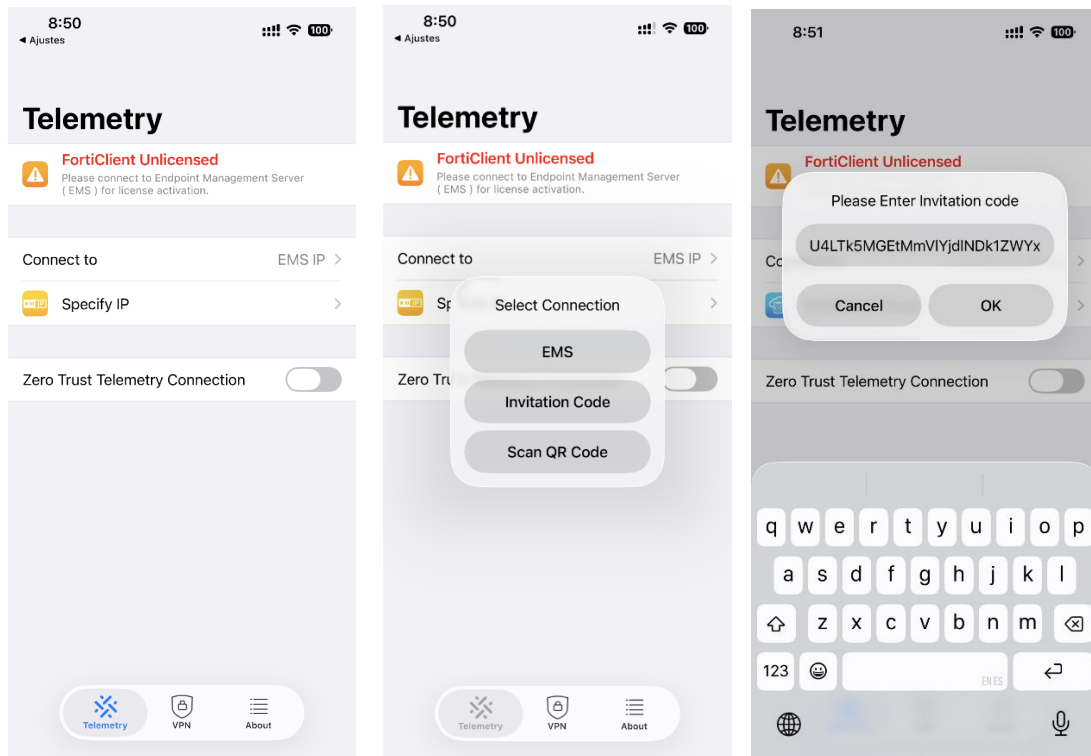
En primer lugar, instalamos el cliente Forticlient desde el App Store. Nos pedirá permiso para crear conexiones VPN y para enviar notificaciones. Debemos permitirlo.



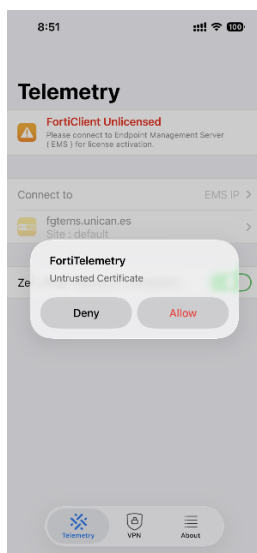
A continuación, aceptamos las condiciones de uso. En la siguiente pantalla podemos pulsar Next, **sin hacer login en ese momento**.



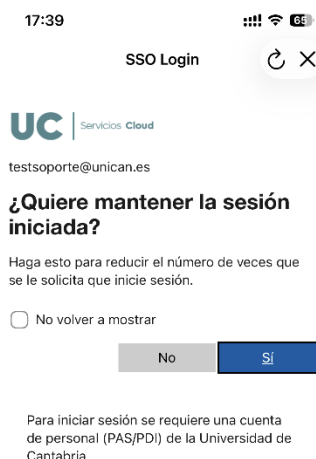
En Telemetry, pulsamos en “Connect to” y seleccionamos “Invitation Code”.



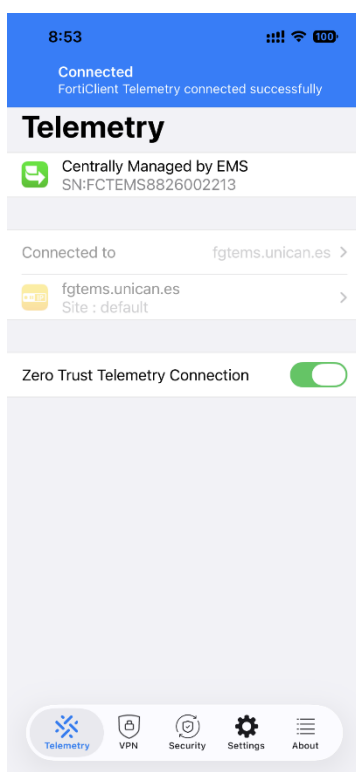
Al conectarse nos dará un aviso del certificado y pulsamos aceptar (Allow)



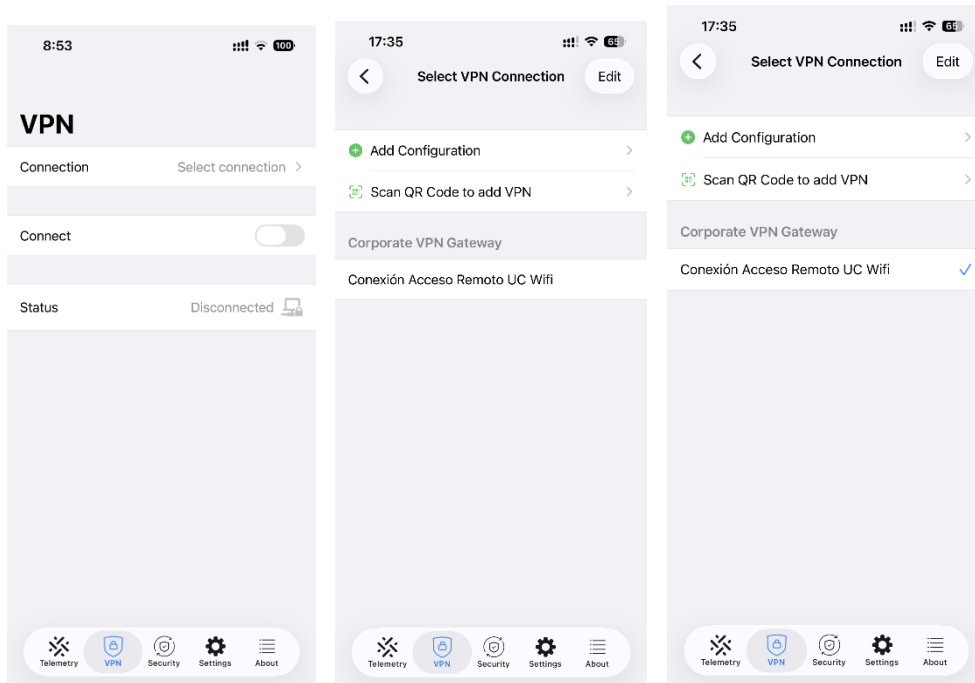
Se nos pedirá validarnos con nuestra cuenta de la UC (formato usuario@uncian.es o usuario@gestion.unican.es).



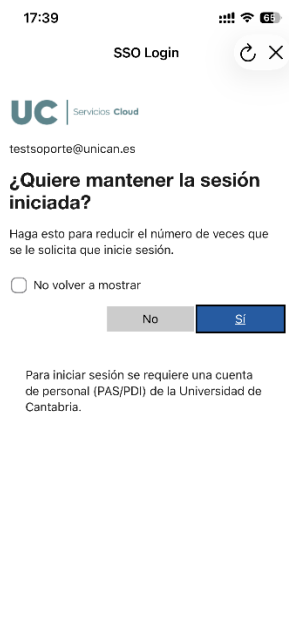
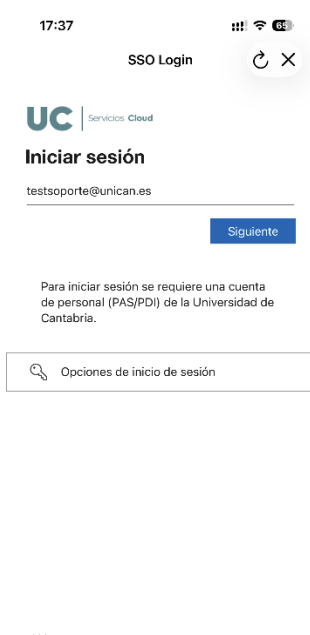
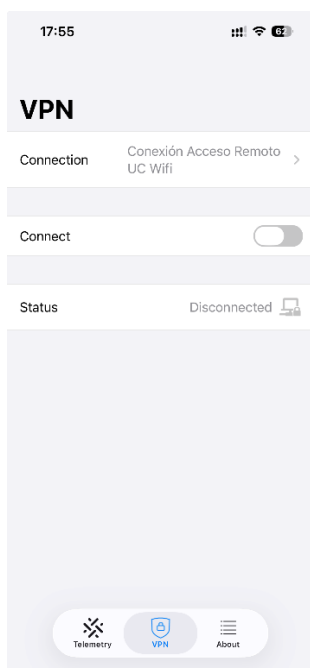
Al conectarnos recibimos los parámetros necesarios. **Esta conexión de telemetría, en principio, solo es necesaria hacerla una vez para activar y configurar la aplicación, pero si por algún motivo se desconecta necesitará volver a conectarse.**



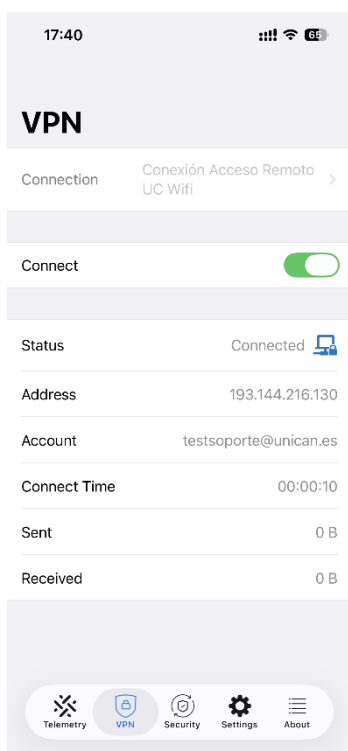
Pasamos a la pestaña VPN, seleccionamos la conexión que nos ha creado. Pulse en “Connection” y selecciónela. Tenga en cuenta que recibiremos una configuración VPN distinta en función del lugar (Wifi UNICAN o fuera de la UC) desde el que nos estemos conectando.



Pulsando “Connect” nos saldrá la ventana de validación, incluido el MFA



Una vez validados estaremos conectados a la VPN:

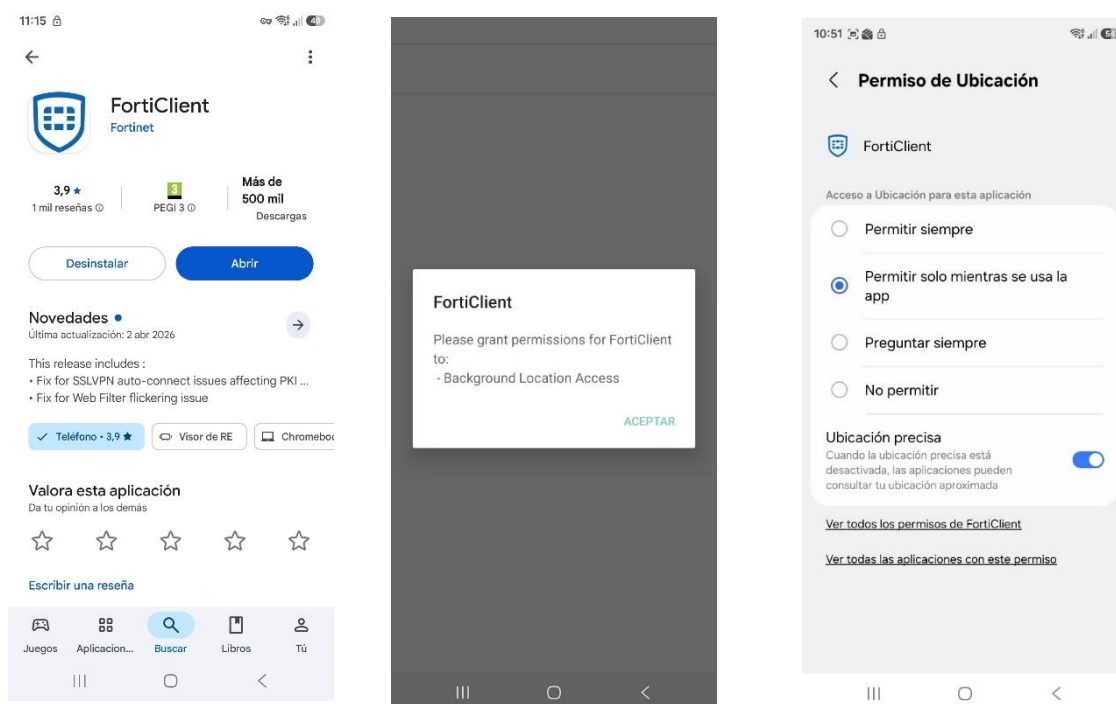


Forticlient en Android

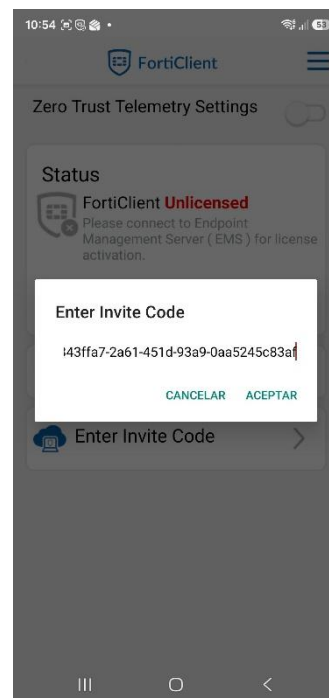
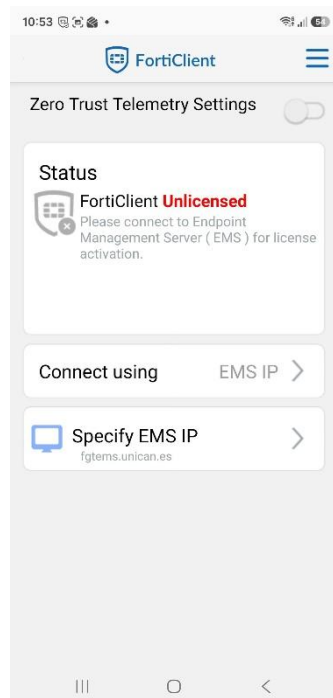
Para instalar el cliente en Android, acceda a la **Play Store** y descargue la aplicación **FortiClient VPN** (que se muestra en la imagen).

Durante la configuración inicial, la aplicación le solicitará varios permisos necesarios; es importante que los acepte para asegurar su correcto funcionamiento.

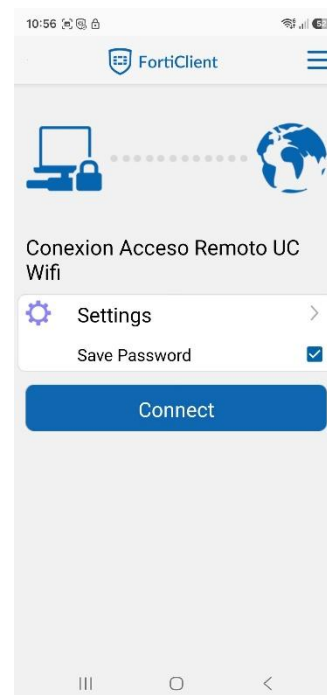
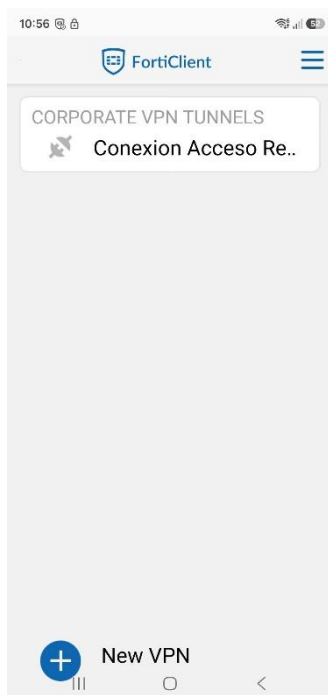
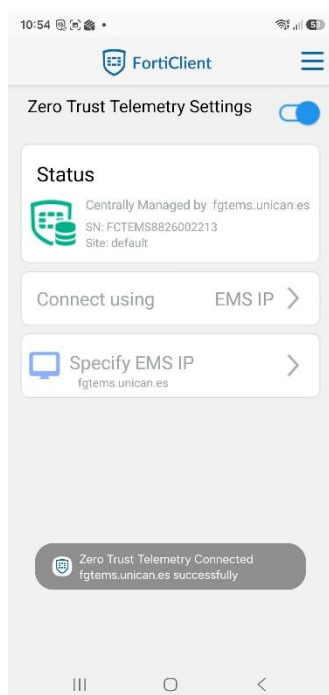
Nota sobre el permiso de ubicación: FortiClient requiere acceso a la ubicación para detectar correctamente la red Wi-Fi a la que está conectado, información técnica necesaria para establecer los túneles IPsec. Se recomienda seleccionar '**Permitir solo mientras se usa la app**'; esta opción garantiza su privacidad sin afectar la operatividad de la VPN



Una vez que tenemos el cliente instalado y tiene todos los permisos necesarios, continuamos conectándonos al EMS para obtener los perfiles de conexión a la VPN. Para ello seleccionamos en “Connect using” invitation code y añadimos el código de invitación tal y como se ve en las imágenes.

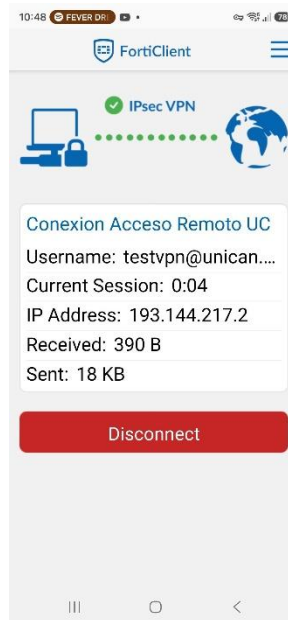
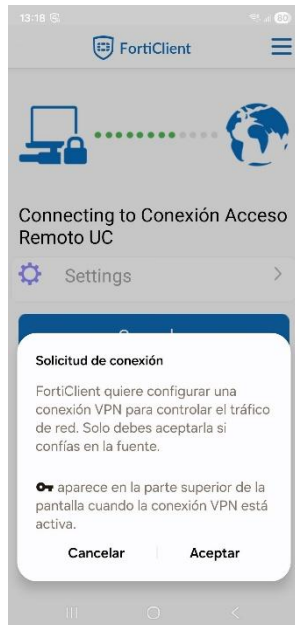


Si se ha conectado correctamente a la telemetría, el indicador de estado aparecerá en color verde y se mostrará un mensaje de confirmación. Una vez establecido el enlace, dirijase al menú **'VPN'**; allí aparecerá su conexión de acceso remoto. Haga clic sobre ella para iniciar el túnel. Recuerde que, si no desea introducir sus credenciales en cada sesión, puede marcar la opción **'Save password'**



Durante el primer intento de conexión, aparecerá el mensaje mostrado en la imagen; deberá aceptarlo para poder establecer el túnel.

Si la conexión se ha realizado correctamente, se visualizará toda la información de la sesión, tal como se muestra a continuación.



Gestión de la conexión VPN

Es importante destacar que el acceso a la red corporativa a través de la VPN requiere una **gestión manual** por parte del usuario. Esto significa que usted debe conectar y desconectar el túnel VPN de forma proactiva cada vez que inicie o finalice su actividad.

¿Por qué es necesario este proceso manual?

- **Seguridad:** Garantiza que el acceso a los recursos internos de la empresa solo esté abierto cuando usted lo necesite.
- **Control de recursos:** Evita el consumo innecesario de ancho de banda y recursos de red cuando no está trabajando activamente con aplicaciones corporativas.

Por lo tanto, al finalizar su jornada o cuando no requiera acceder a recursos internos, recuerde **desconectarse manualmente** del túnel VPN para asegurar la integridad de su acceso.

Preguntas frecuentes

¿Necesito ser administrador de mi equipo para instalar el cliente?

Sí, es necesario contar con **privilegios de administrador** en su equipo para poder instalar el cliente FortiClient y gestionar los perfiles de acceso.

Desinstalar el cliente

Para poder desinstalar el cliente en tu equipo, es necesario desvincularlo de la Telemetría de Confianza Cero (EMS) para liberar la gestión centralizada.

¿Puedo instalar el cliente en un ordenador compartido?

Sí, es técnicamente posible, pero **no es recomendable** a menos que el equipo cuente con perfiles de usuario de sistema operativo independientes. Si utiliza un perfil compartido, se recomienda encarecidamente desinstalar el cliente al finalizar su trabajo para evitar que otros usuarios accedan a los recursos corporativos o utilicen sus credenciales guardadas.

¿Por qué esta mi conexión a la telemetría no alcanzable y qué hacer?

Si experimenta una caída en la conexión o un error de sincronización con el servidor de telemetría, es posible que el estado de la conexión aparezca como '**No alcanzable**'. En este caso, debe hacer clic en 'Desconectar' y, a continuación, volver a conectar para restablecer el enlace con el servicio.



FortiClient - Conectado

Zero Trust Fabric Agent



Administrado centralizadamente por EMS

Estado:  No alcanzable Desconectar 

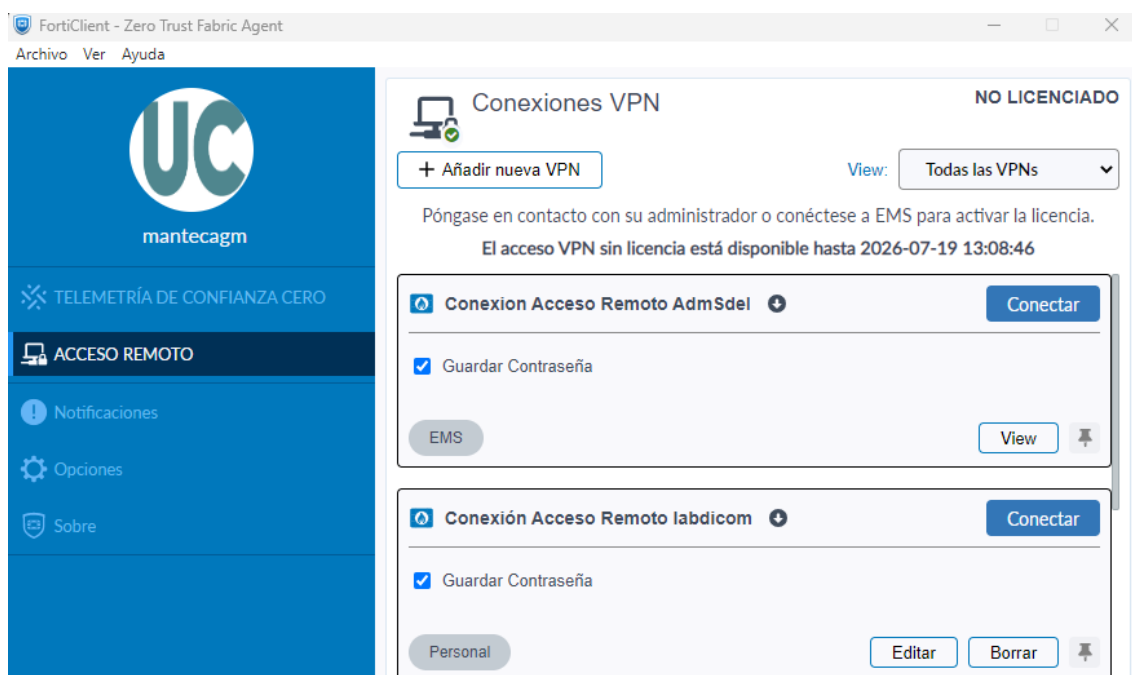
No me ha llegado el túnel de acceso remoto

Si no aparece ninguna conexión de acceso remoto en la pestaña correspondiente, espere unos minutos, ya que si es la primera vez que se conecta a la telemetría, es posible que el sistema tarde un poco en sincronizar y mostrar la configuración. Si trascurrido este tiempo la conexión sigue sin aparecer, póngase en contacto con el soporte técnico de la universidad.

¿Qué hago si me aparece que el acceso VPN está disponible sin licencia hasta una fecha?

Si su equipo pierde la conexión con la telemetría, el cliente mostrará un aviso indicando que el acceso está disponible en modo 'sin licencia' durante un mes, contado desde la última conexión exitosa al servidor. Transcurrido este periodo, no podrá utilizar el cliente para establecer conexiones de acceso remoto.

Para restablecer la licencia y recuperar la operatividad, únicamente debe conectarse de nuevo a la telemetría corporativa.



¿Qué hago si el cliente me dice que estoy conectado a un túnel, pero no puedo hacer escritorio remoto a mi equipo?

Si, a pesar de aparecer conectado, observa que no tiene acceso a los recursos de red, es posible que la **sesión haya quedado bloqueada**. En este caso, desconecte y vuelva a conectarse para refrescar la conexión.

Cambiar de conexión WIFI Unican a otra red

Si necesita cambiar su red de conexión (por ejemplo, pasar de la red **Wi-Fi UNICAN** a otra red, o viceversa), le recomendamos **desconectarse y volver a conectar la telemetría**. Este proceso permite que el sistema actualice correctamente su perfil de acceso remoto y asegure la estabilidad de la conexión al cambiar de entorno de red.

Si está conectado a la wifi unican le aparecerá la conexión “Acceso remoto UC Wifi”



testvpn

TELEMETRÍA DE CONFIANZA CERO

ACCESO REMOTO

Notificaciones

Opciones

Sobre



Conexiones VPN

+ Añadir nueva VPN

View: Todas las VPNs

Conexion Acceso Remoto UC Wifi

Conectar

☒ Guardar Contraseña

EMS View

Y si estamos conectados a otra red.



testvpn

TELEMETRÍA DE CONFIANZA CERO

ACCESO REMOTO

Notificaciones

Opciones

Sobre



Conexiones VPN

+ Añadir nueva VPN

View: Todas las VPNs

Conexion Acceso Remoto UC

Conectar

☒ Guardar Contraseña

EMS View