INSTRUCCIONES PARA LA ACTIVACIÓN DEL 2FA EN ACCESOS VPN A LA UMA

Actualmente tienes concedido permiso de acceso a tu ordenador en la UMA a través de un túnel VPN con *FortiClient* desde tu ordenador de casa.

Esta utilidad es de alto riesgo respecto a la seguridad de nuestros sistemas, por lo que vamos a incrementar las medidas preventivas mediante un mecanismo de refuerzo conocido como doble factor de autenticación (2FA) y que posiblemente ya te resulte familiar por estar extendido su uso en aplicaciones bancarias, de pagos y otros.

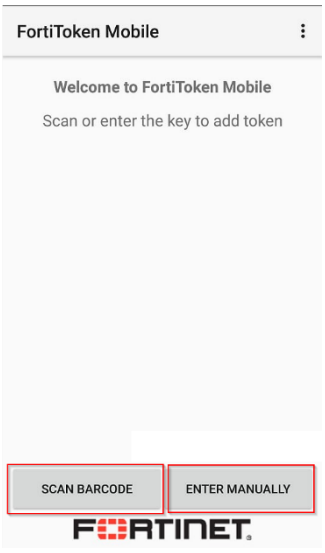
Básicamente, se trata de que cuando conectes al túnel a través de la aplicación *FortiClient*, se enviará un mensaje a tu teléfono móvil para que autorices la conexión.

Para ello te vamos a enviar por correo electrónico una clave que será personal y única para cada persona autorizada. La clave la recibirás tanto en formato numérico como en formato QR y deberás instalarla en tu móvil una única vez en la forma que te vamos a describir ahora.

1. DESCARGA E INSTALA LA APLICACIÓN "FORTITOKEN MOBILE" EN TU MÓVIL

"*Fortitoken Mobile*" la puedes obtener en el "*Play Store*" o en "*App Store*" de tu móvil. Una vez la hayas instalado, espera a recibir un correo electrónico que te enviaremos que contendrá una clave y un código QR para que puedas continuar.

2. CARGA TU CLAVE EN LA APLICACIÓN "FORTITOKEN MOBILE"



Una vez recibas el correo, arranca la aplicación ***Fortitoken Mobile*** en tu dispositivo móvil.

Verás que al pie de pantalla hay dos opciones: "**SCAN BARCODE**" o "**ENTER MANUALLY**". Para cargar tu clave puedes elegir aquella que prefieras.

La primera opción (SCAN BARCODE) es para introducir tu clave mediante un escaneo del QR que te habremos enviado en el email. Solamente tienes que pulsar esta opción y leer el QR.

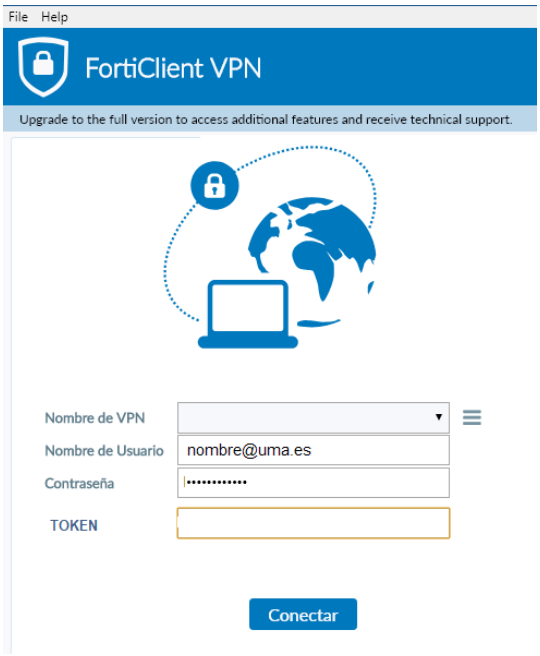
La segunda opción (ENTER MANUALLY) es para introducir tu clave de forma manual. En este caso te pedirá la clave numérica que has recibido en el correo, que deberás teclear en el campo "**Key:**".

Con esto ya tendremos activado el 2FA.

MUY IMPORTANTE!!: La clave y QR que te enviaremos por email, tienen una caducidad de 24 horas. Eso significa que la activación en el dispositivo móvil que acabamos de describirte, deberás hacerla antes de que concluya ese plazo. De no hacerlo así perderás la posibilidad de conectar al túnel SSL y tendrás que solicitar nuevas claves.

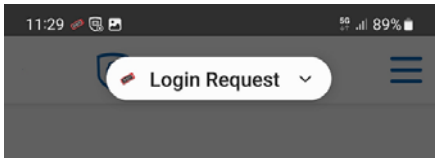
3. CONECTAR AL TÚNEL

A partir de ahora, cuando hagas “login” para acceder al túnel, además del nombre de usuario y contraseña, se te pedirá una autorización (TOKEN) que la conseguirás desde tu móvil.

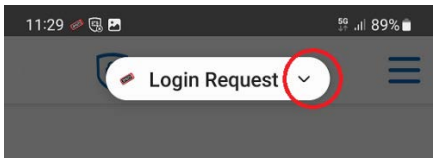


Esta autorización se puede dar de dos formas: aceptando desde el móvil el intento de conexión (es la más rápida y cómoda) o generando un código para introducirlo en el campo TOKEN.

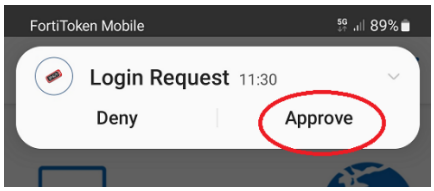
a. **ACEPTAR LA CONEXIÓN**: Cuando llegas a la pantalla anterior de petición del TOKEN, verás que en la parte superior de la pantalla del móvil aparece este mensaje:



Abre el desplegable:

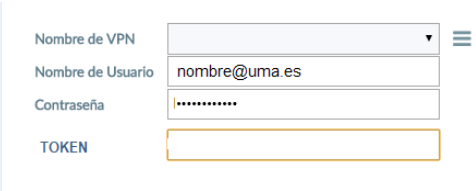


Y entonces aprueba la conexión:

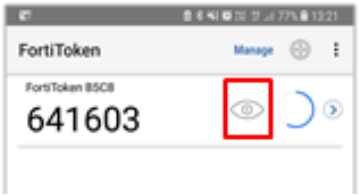


A partir de ahí ya tienes abierto el túnel SSL y puedes continuar como lo hacías antes.

b. GENERAR UN CÓDIGO: No obstante, puedes obtener la autorización por otra vía. Cuando te está pidiendo el TOKEN:



En vez de aceptar desde el móvil como hemos visto antes, pulsa para abrir la aplicación *FortiToken* en el móvil y obtén un código numérico (para poderlo ver tienes que pulsar sobre el ojo, como se muestra en la siguiente imagen):



Verás que va cambiando el número cada minuto, así que ese es el tiempo del que dispones para introducirlo en el campo TOKEN y poder continuar.