

Uso del doble factor de autenticación en VPN con Google Authenticator

Para mejorar la seguridad de su cuenta de usuario de acceso al servicio VPN de la UCA con el software FortiClient se ha habilitado el uso del doble factor de autenticación.

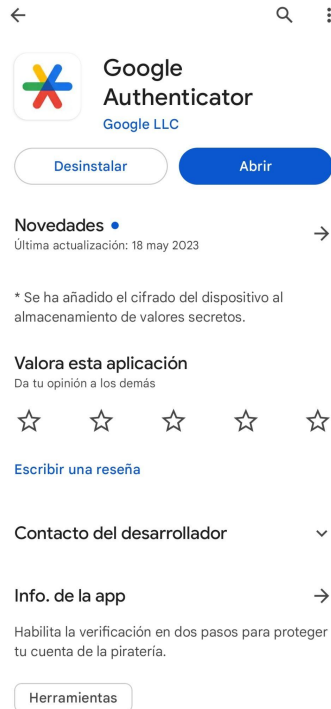
El doble factor de autenticación (2FA) es una medida de seguridad que requiere dos o más métodos de verificación para acceder a un servicio. Proporciona una capa adicional de seguridad al reducir la probabilidad de acceso no autorizado, protege contra contraseñas débiles y le permite tener una mayor tranquilidad de que su información personal está más protegida. El doble factor de autenticación es una herramienta efectiva para mejorar la seguridad en los accesos desde redes externas a la UCA y para, en el caso de VPN, evitar que personas no autorizadas y externas a la organización puedan tener acceso a recursos y servicios destinados a los usuarios de la universidad.

En este caso, con una aplicación móvil se generará un código numérico que permitirá verificar que es usted realmente quién está accediendo al servicio VPN.

Los pasos para su activación son los siguientes:

1.- Instalar la aplicación Google Authenticator en su dispositivo móvil:

El primer paso será instalar la aplicación desde el Google Play Store:
<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>



O bien desde el App Store de Apple:

<https://apps.apple.com/es/app/google-authenticator/id388497605>

2.- Activar el doble factor de autenticación para VPN y generar un nuevo código de configuración

Para activar el doble factor de autenticación debe acceder a la siguiente dirección y autenticarse con su usuario de la UCA:

<https://cau.uca.es/vpn-2fa>

Una vez autenticado ya quedará activado el doble factor de autenticación:

Universidad de Cádiz


Guías de uso Salir

Doble factor de autenticación VPN

Ha activado el doble factor de autenticación para su acceso VPN.

Clave de configuración: **DPBXHKG6RSZRCWUN2IP4K25YCLYQKVPI**

Código QR:



El modo de usar el doble factor de autenticación es el siguiente:

Debe indicar el código generado por la aplicación (normalmente 6 números) en el campo de "Respuesta" que pide la aplicación FortiClient con la pregunta: "Indique código de verificación (2FA)" después de verificar que su cuenta de usuario y contraseña es correcta.

Generar un nuevo código de verificación

Para poder generar la clave necesaria para el acceso a VPN tiene varias opciones:

En todos los casos solo es necesario instalar la aplicación y añadir un nuevo código o bien escaneando el código QR o indicando a mano la clave de configuración.

- * Guía de uso del doble factor en FortiClient con Google Authenticator
- * Guía de uso del doble factor en FortiClient con extensión navegador Chrome

Aplicación Móvil:
Puede usar alguna de las siguientes aplicaciones:

- * FreeOTP+ (2FA Authenticator) (Android)
- * Google Authenticator Android - iPhone/iPad
- * Microsoft Authenticator Android - iPhone/iPad
- * 2FAS Authenticator Android - iPhone/iPad
- * FreeOTP Authenticator (iPhone/iPad)

Complemento de Google Chrome:

- * Authenticator

Aplicación de escritorio:

Entorno Windows:

- * 2fast
- * OTP Manager

Entorno Mac OSX:

- * Step Two

Entorno Linux:

- * OATH Toolkit

En la página puede ver a la izquierda la clave de configuración que se le ha asociado y el código QR que debe usar para vincularlo con la aplicación de validación del doble factor de autenticación.

En la columna de la derecha tiene acceso a distintas aplicaciones que permiten generar el código necesario para el doble factor de autenticación basado en el código QR que puede ver en la página.

3.- Configurar la aplicación Google Authenticator con su clave de configuración

Una vez instalada la aplicación, la ejecutamos y si es la primera vez nos pedirá que se escanee un código QR o introduzca la clave de configuración.



Configura tu primera cuenta

Utiliza el código QR o la llave de configuración en los ajustes de la verificación en dos pasos de Google o de un servicio de terceros. Si tienes dificultades, visita g.co/2sv



Escanear un código QR

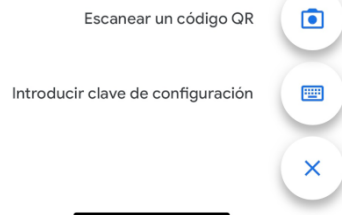


Introducir clave de configuración

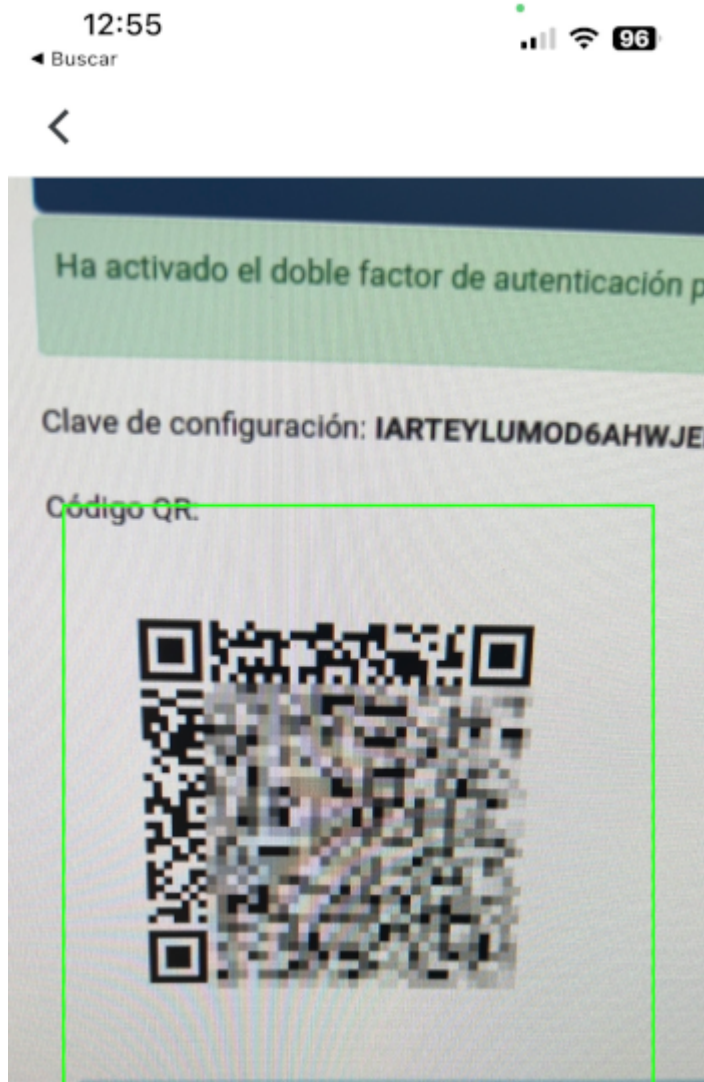


Si no es la primera vez que se puede usar el botón de **escanear un código QR**

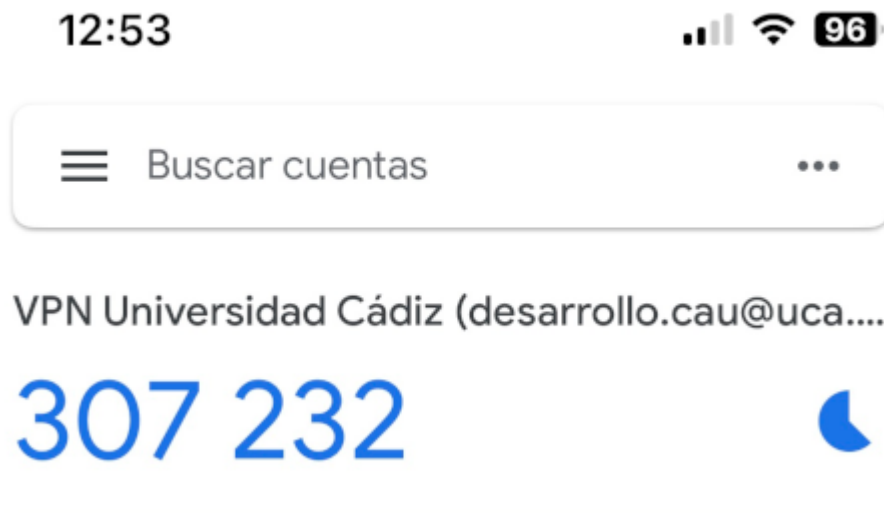
y seleccionar la opción de



Se debe escanear el código QR que aparece en la página de activación:



Y ya estará activada la aplicación para generar el código de verificación del doble factor de autenticación para el acceso VPN:



El código de verificación cambiará cada minuto y será el que debemos indicar cuando sea solicitado por el programa cliente de VPN.

4.- Conexión a VPN con FortiClient

Una vez activado el doble factor de autenticación, cada vez que se conecte a VPN con la aplicación VPN le solicitará el código de verificación para evitar que alguien pueda suplantar su cuenta de usuario.

Cuando se conecte a VPN de la UCA mediante la aplicación FortiClient debe indicar como siempre su cuenta de usuario y clave de acceso como siempre y si tiene activado el doble factor de autenticación aparecerá una nueva pantalla en la que le pedirá “**Indique código de verificación (2FA)**”:



En este momento debe indicar el código generado por la aplicación en este momento.

Indique código de verificación (2FA)

Nombre de VPN	VPN UCA
Nombre de Usuario	XXXXXXXXXX@uca.es
Contraseña
Respuesta	307232

El código generado por Authenticator es en este caso **307232**.

Una vez validado el código quedará conectado su equipo a la red VPN de la UCA.