

Uso del doble factor de autenticación en VPN con extensión Authenticator de Google Chrome

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 extensión del navegador chrome se generará un código numérico que permitirá verificar que es usted realmente quién está accediendo al servicio VPN.

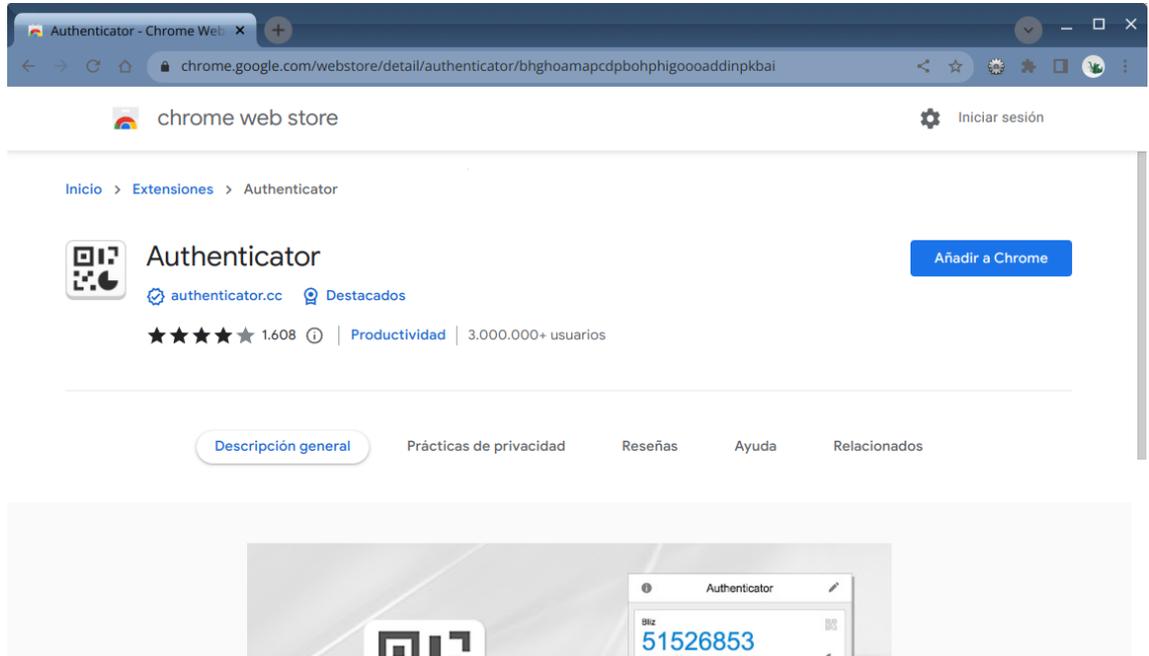
Los pasos para su activación son los siguientes:

1.- Instalar complemento de Google Chrome

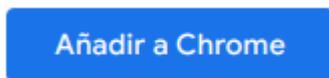
El primer paso será instalar un complemento de Google Chrome que permitirá generar el código de verificación del doble factor de autenticación.

Desde un navegador chrome (tanto en Windows, MacOSX como en linux) hay que conectar con la dirección:

<https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigooaddinpkbai>



Y pulsar el botón:



Con esto ya estará instalado el complemento de Chrome

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:

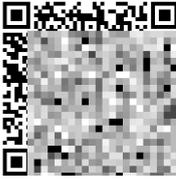
Universidad de Cádiz Inicio Guías de uso Salir

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](#)
- * [Authenticator](#)

Entorno Linux:

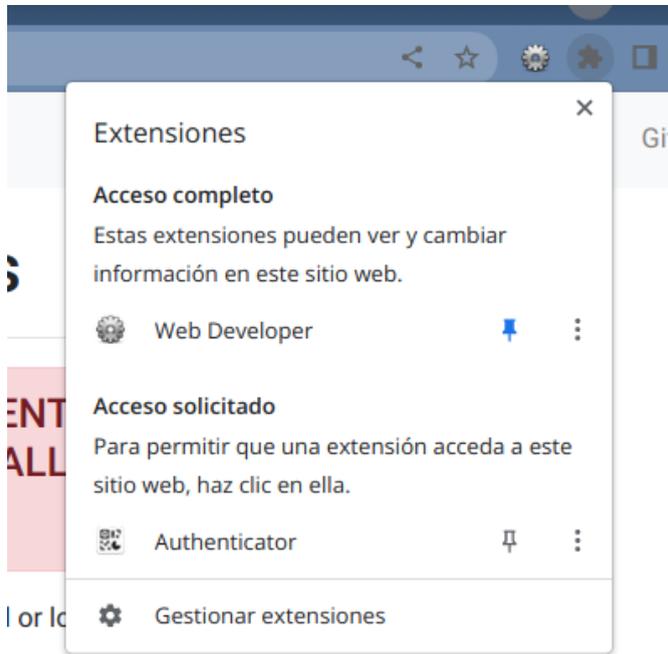
- * [OATH Toolkit](#)

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.

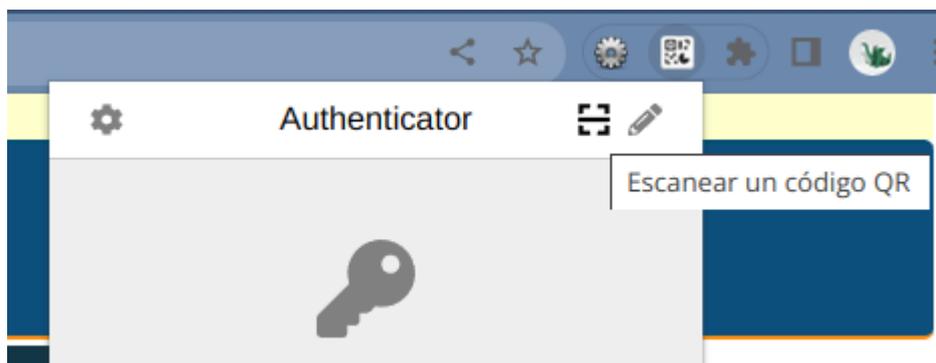
En la columna de la derecha tiene acceso a distintas aplicaciones que permiten generar el código necesario para el doble factor de autenticación basado en el código QR que puede ver en la página.

3.- Configurar extensión de Chrome con su clave de configuración

La extensión de chrome que hemos instalado en un paso anterior es accesible desde el botón de extensiones:



Se debe lanzar la extensión y pulsar el botón de “Escanear un código QR”  y capturar el código que aparece en la página de configuración.



Al pulsar el botón nos aparecerá un cursor que permite seleccionar el espacio de la pantalla en el que aparece el código QR:

Código QR:



En todos los casos solo es necesario añadir un nuevo código o bien indicando a mano la clave de

* [Guía de uso del doble factor Authenticator](#)

* [Guía de uso del doble factor navegador Chrome](#)

Aplicación Móvil:
Puede usar alguna de las siguientes

* [FreeOTP+ \(2FA Authenticator\)](#)

* [Google Authenticator Android](#)

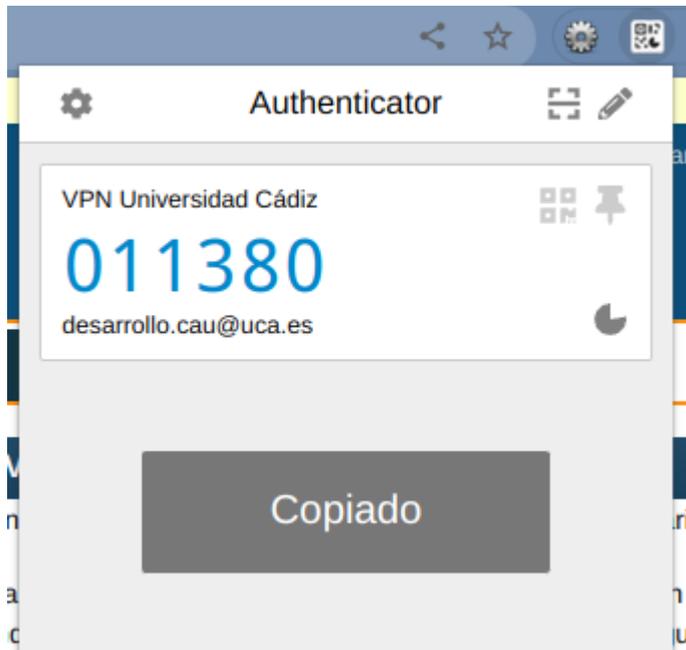
* [Microsoft Authenticator Android](#)

* [2FAS Authenticator Android](#)

* [FreeOTP Authenticator \(iOS\)](#)

El modo de usar el doble factor de autenticación es el

Una vez importado el código QR al ejecutar la extensión le generará un nuevo código de verificación, pulsando sobre el código lo copiará de forma automática.

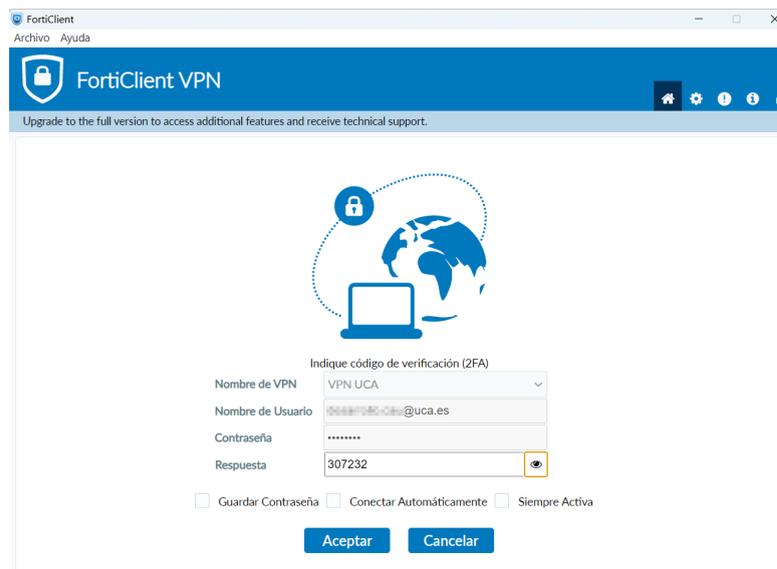


El código de verificación cambiará cada minuto y será el que debemos indicar cuando sea solicitado por el programa cliente de VPN.

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)”:



The screenshot shows the FortiClient VPN application window. The title bar reads 'FortiClient' and 'Archivo Ayuda'. The main window has a blue header with the FortiClient VPN logo and a notification bar that says 'Upgrade to the full version to access additional features and receive technical support.' The main content area features a central graphic of a globe with a lock icon and a laptop. Below this, the text 'Indique código de verificación (2FA)' is displayed. The login form includes the following fields: 'Nombre de VPN' (VPN UCA), 'Nombre de Usuario' (XXXXXXXXXX@uca.es), 'Contraseña' (masked with asterisks), and 'Respuesta' (307232). At the bottom, there are three checkboxes: 'Guardar Contraseña', 'Conectar Automáticamente', and 'Siempre Activa'. Two buttons, 'Aceptar' and 'Cancelar', are located at the bottom of the form.

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	██████████@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.