UCA Universidad de Cádiz
Vicerrectorado de Digitalización e Infraestructuras
Área de Sistemas de Información
Edificio CITI
Avd, Rep, Saharaui s/n 11510 Puerto Real
Cádiz
Tel. 956 016400
http://asi.uca.es
area.sistinfo@uca.es

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.

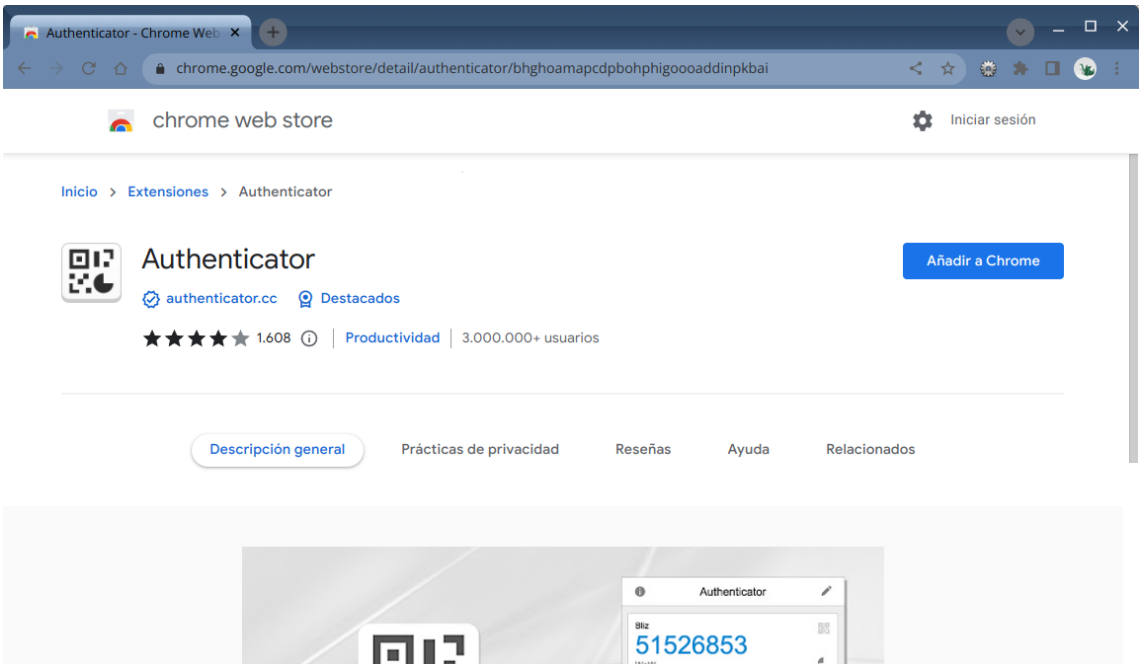
Los pasos para su activación son los siguientes:

1.- Instalar complemento de Google Chrome

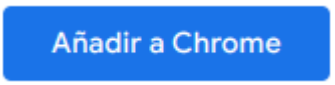
El primer paso será instalar un complemento de Google Chrome que permitirá generar el código de verificación del doble factor de autenticación.

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

https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai



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

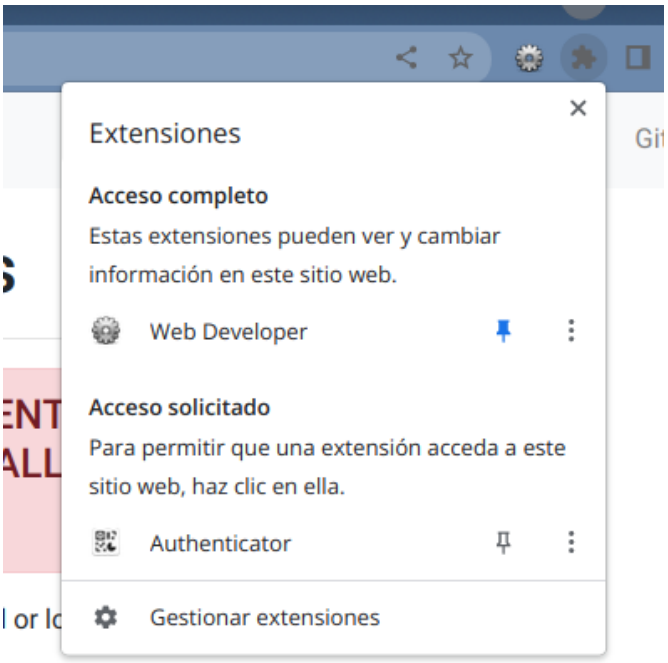
Una vez autenticado ya quedará activado el doble factor de autenticación:

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.

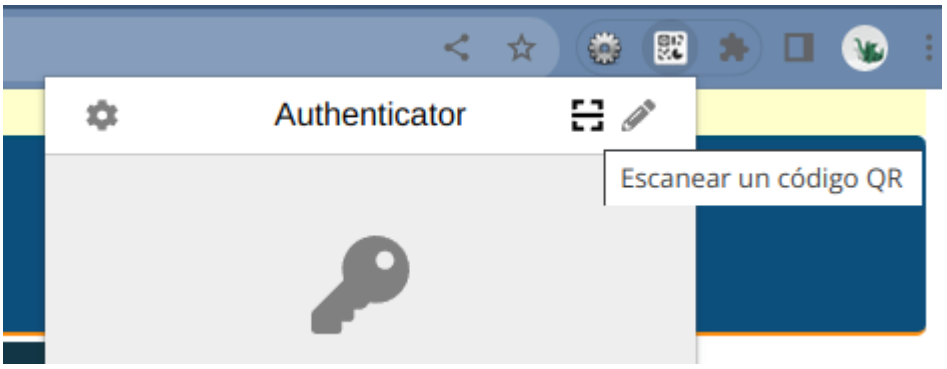
En la columna de la derecha tiene acceso a distintas aplicaciones que permiten generar el código necesario para el doble factor de autenticación basado en el código QR que puede ver en la página.

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:

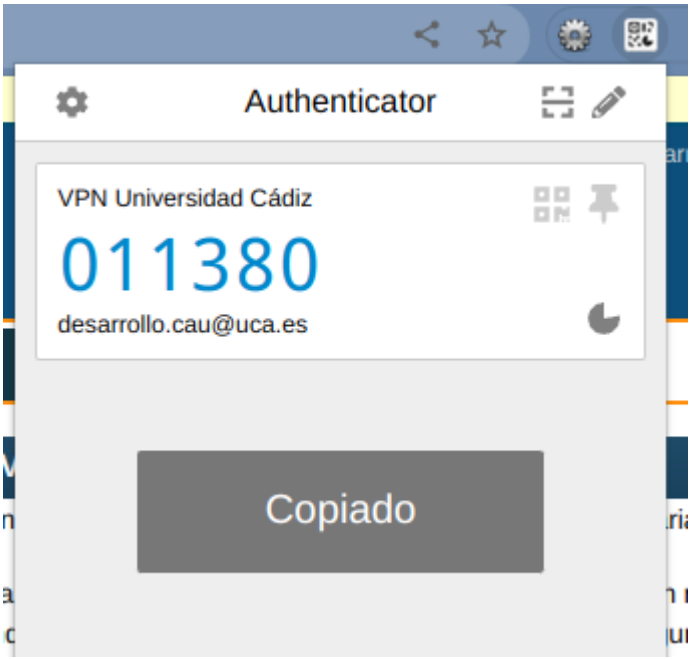


Se debe lanzar la extensión y pulsar el botón de "Escanear un código QR" y capturar el código que aparece en la página de configuración.



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

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.

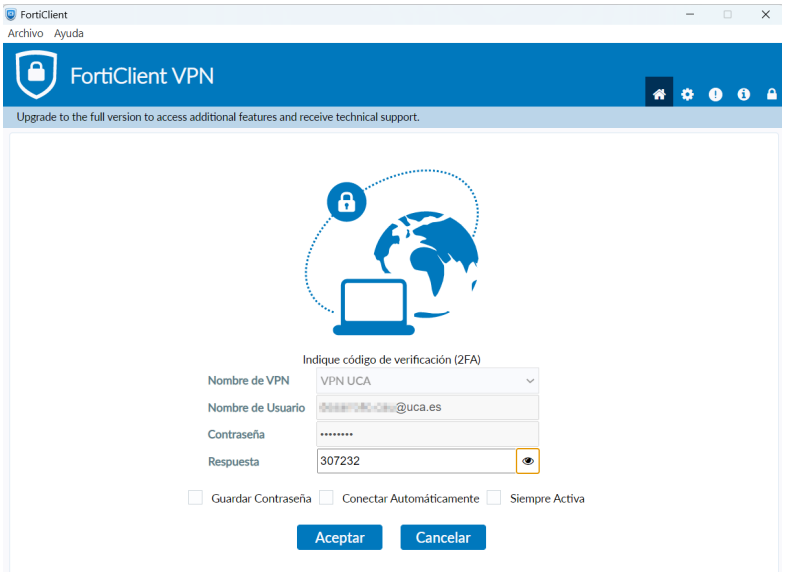


El código de verificación cambiará cada minuto y será el que debemos indicar cuando sea solicitado por el programa cliente de VPN.

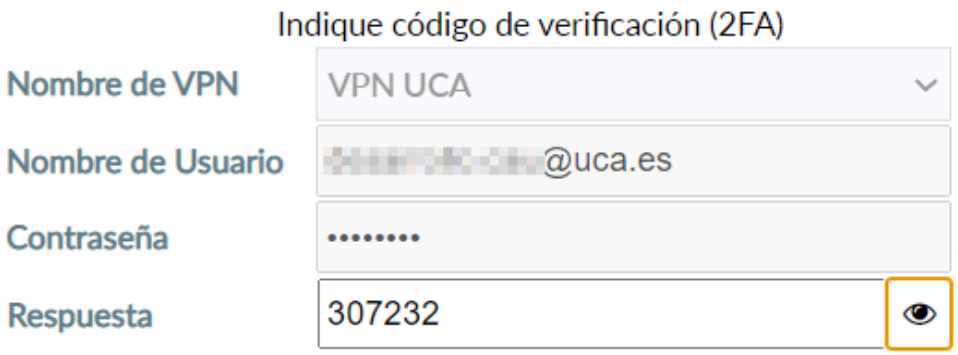
4.- Conexión a VPN con FortiClient

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)**":



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



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.