Configuración de MFA si no tenemos un teléfono móvil

Versión 1.1 diciembre 2025

Contenido

Qué es el MFA

La Autenticación Multifactor (**M**ulti**F**actor **A**uthentication, **MFA**) es una forma de seguridad que requiere que los usuarios proporcionen más de una forma de autenticación para verificar su identidad al iniciar sesión en un sistema o servicio. Es decir, **no es suficiente con saberse una contraseña, sino que es necesario más cosas.**

Casi todos los servicios en línea (bancos, redes sociales, compras, ..etc.) han agregado una forma de MFA para que sus cuentas sean más seguras, ya que usar únicamente una contraseña es arriesgado. Es posible que escuche, o ya use, lo que se denomina "Verificación en dos pasos" o "Autenticación multifactor",” Confirmación con la aplicación del banco”, ...etc., pero todos ellos funcionan con el mismo principio, es decir además de nuestra contraseña se nos pide verificar nuestra identidad con un segundo factor, normalmente mediante el móvil.

Una de las ventajas de MFA es que ayuda a proteger a la institución contra vulnerabilidades causadas por la pérdida o el robo de credenciales, que suelen ser la puerta de entrada de ciberataques más graves.

El MFA en la UC

El uso de MFA desde fuera de la red institucional además de ser una medida necesaria para proteger nuestra institución, y que ya han adoptado la mayoría de universidades, es una obligación legal de acuerdo al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Si ya tiene configurado el MFA porque usa la VPN, no es necesario reconfigurarlo. No obstante, compruebe que tiene más de un método configurado para así evitar posibles problemas en el futuro.

Desde agosto de 2023 el uso de MFA es obligatorio para la utilización de la VPN de la UC. A partir del 21 de octubre de 2025, y para los empleados, esta obligación se extendió al Correo Electrónico, Teams, OneDrive UNICAN y en general a todos los servicios en la nube de la institución **siempre y cuando se utilicen fuera de la Red UNICAN.**

Posteriormente su uso se extenderá a otras aplicaciones y servicios, así como al estudiantado.

Si es empleado, ya tiene configurada una aplicación, por ejemplo, el correo electrónico, en un ordenador o móvil, a partir del 21 de octubre de 2025, si se encuentra fuera de la UC, la aplicación le pedirá hacer la verificación MFA.

Tenga en cuenta que algunas aplicaciones pueden que no lo hagan correctamente y sea necesario reconfigurarlas desde el principio.
Si tiene problemas con la aplicación de correo de su móvil le recomendados usar Outlook Mobile. Más información en
https://sdei.unican.es/Paginas/servicios/correo/correopdipas.aspx

A diferencia de la VPN, el uso de MFA no será necesario en cada consulta al correo electrónico, por ejemplo. **Podremos decir que nos lo pida cada 60 días si es que estamos en un dispositivo de confianza.** Si estamos configurando una aplicación (como el Correo o Teams) la petición de MFA solo se realizará cada 60 días. Es decir, con un cliente de correo configurado, por ejemplo, en el móvil, nos pedirá el segundo factor una vez cada dos meses, pero debemos estar listos para usarlo.

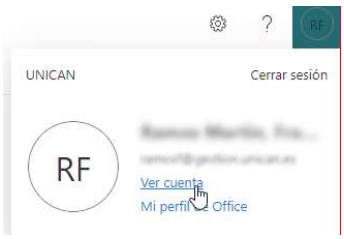
Configurar métodos para el MFA sin tener un teléfono móvil

Para poder usar MFA es necesario primero dar de alta diferentes mecanismos para tener ese segundo factor de autenticación.

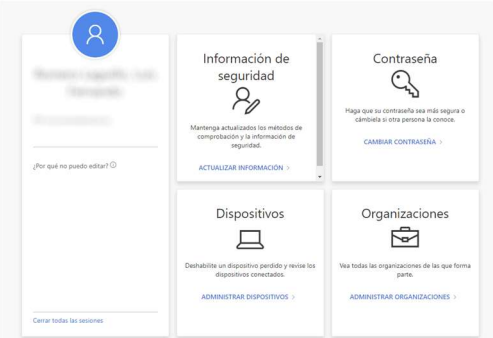
Para ello Iniciamos sesión en la gestión de nuestra cuenta en la nube (formato *usuario*@gestion.unican.es o *usuario*@unican.es) en:

https://myaccount.microsoft.com/

o si ya estamos validados, por ejemplo, en el correo web, pulsamos sobre nuestro icono y elegimos la opción ‘Ver cuenta’.



Elegimos la opción de Actualizar información en ‘Información de seguridad’:



A la pantalla de configuración de MFA también se puede llegar directamente desde https://aka.ms/mfasetup

La forma más natural y cómoda de tener un segundo factor de autenticación en mediante una app en el móvil o/y SMS/llamada al móvil. **Para ello consulte el manual correspondiente en https://sdei.unican.es/mfa**

Este manual pretende cubrir a aquellas personas que quieren seguir usando los servicios protegidos por MFA de forma remota pero no tienen un teléfono móvil, o no quieren usarlo.

Desde el Servicio de Informática ofrecemos este manual como referencia, pero la elección de este tipo de herramientas es una decisión personal contraria a las recomendaciones técnicas de la institución y como tal, el usuario asume la responsabilidad de su uso, configuración y la solución de problemas. Recuerde que el MFA solo se aplicará a determinados servicios cuando se acceda a ellos desde fuera de la UC.

Las opciones aquí mostradas son ejemplos.

Opción A. Registro de la extensión de navegador Authenticator Extension

Authenticator Extension es una extensión de navegador disponible para los navegadores más habituales (Edge, Chrome y Firefox), que permite obtener códigos de un solo uso para autenticación MFA.
Esta extensión **deberemos instalarla en un ordenador que esté siempre bajo nuestro total control, que se encuentre fuera de la UC.** Existen otras extensiones en el mercado cuyo funcionamiento es similar.

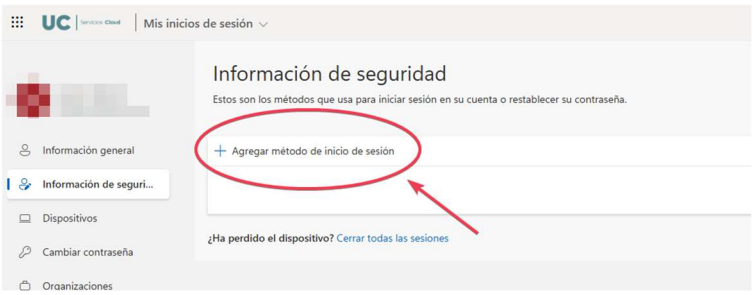
Para ello vamos a https://authenticator.cc/ e instalamos la extensión para el navegador que queramos.

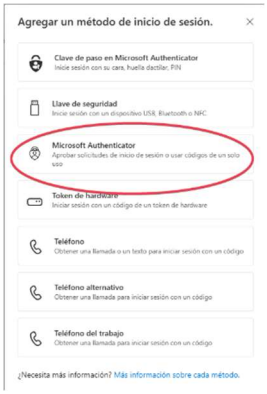
Se recomienda fijar la extensión instalada para facilitar su uso. Por ejemplo, en Chrome bastara con clickear sobre (Extensiones) y fijar la extensión dándole a (Fijar).

En otros navegadores el mecanismo para fijar una extensión es similar.

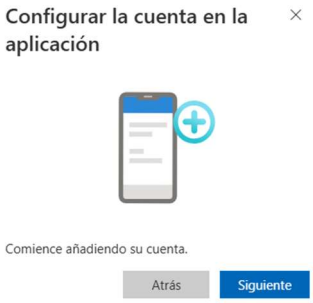
Para registrar Authenticator Extension como método MFA podemos acceder directamente desde https://aka.ms/mfasetup desde el navegador donde hemos configurado la extensión.

Agregamos un método de tipo “Microsoft Authenticator”:



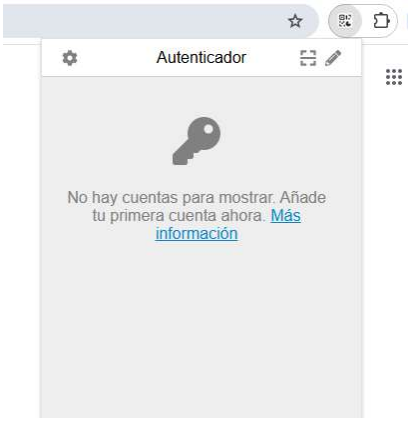


Seleccionamos **“Configurar una aplicación de autenticación diferente”.**



Se le mostrará el código QR:

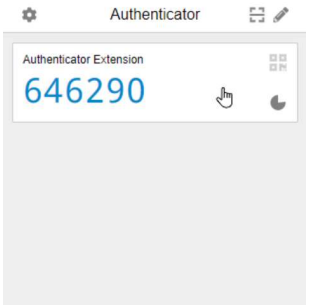
Ahora haga click en el icono de Authenticator Extension en la barra de extensiones.



Seleccione la opción para escanear código QR.

Arrastre el curso hasta cubrir completamente el código QR que se muestra en pantalla, e el portal de Microsoft.

La cuenta se registrará y generará un código de un solo uso que se actualizará cada 30 segundos.

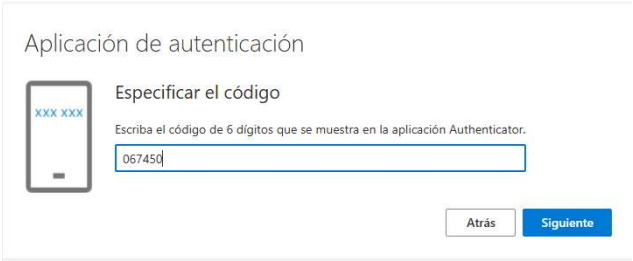


Como alternativa, también podemos agregar la cuenta manualmente. Para ello seleccionamos:

Debemos introducir el nombre de la cuenta y la clave secreta proporcionada en el portal de Microsoft durante el proceso de registro. Para ello indique en la pantalla del QR “No puedo escanear el QR” y se le mostrará una clave secreta para introducir en Authenticator:

Ya sea por el QR o de forma manual, una vez agregada la cuenta a Authenticator Extension debemos pulsar siguiente en el portal de registro de Microsoft.

Se nos pedirá introducir una clave de un solo uso (la clave de 6 dígitos que ahora vemos en Authenticator Extension) para confirmar todo el proceso.



Si todo ha ido bien debería salir el siguiente mensaje

A partir de este momento, cuando inicie sesión, tras introducir usuario y contraseña, se solicitará el segundo factor, que, por defecto, será un código de seis dígitos de un solo uso en la Authenticator Extension.

Se recomienda agregar más de un método para MFA. En este caso deberá tener configurado Authenticator Extension (u otra alternativa) en varios ordenadores bajo los que tenga el control

Opción B. Registro de la aplicación WinAuth

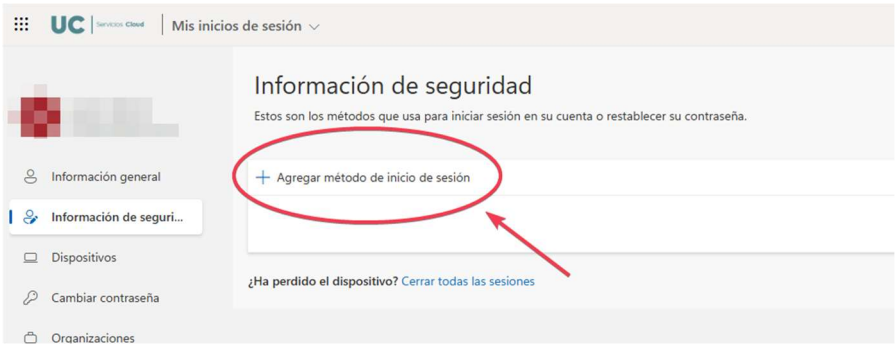
Existen otro tipo de aplicaciones que no son extensiones del navegador sino aplicaciones Windows normales. Un ejemplo es WinAuth.

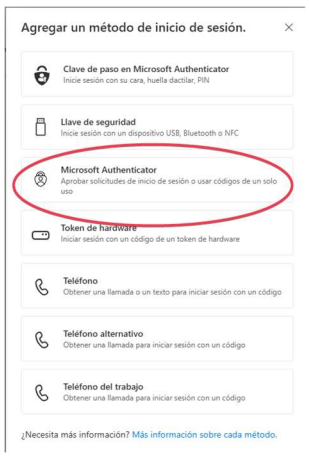
Este programa **deberemos instalarlo en un ordenador que esté siempre bajo nuestro total control, que se encuentre fuera de la UC.** Existen otras aplicaciones en el mercado cuyo funcionamiento es similar.

WinAuth se puede instalar desde https://winauth.github.io/winauth/

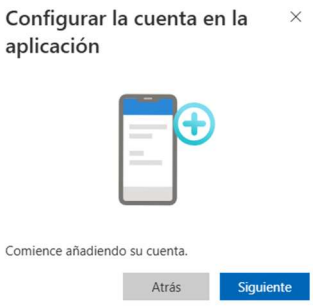
En la primera ejecución se recomienda establecer una contraseña maestra para proteger nuestros códigos de un solo uso.
Para configurarlo WinAut como método MFA podemos acceder directamente desde https://aka.ms/mfasetup desde el navegador.

Agregamos un método de tipo “Microsoft Authenticator”:

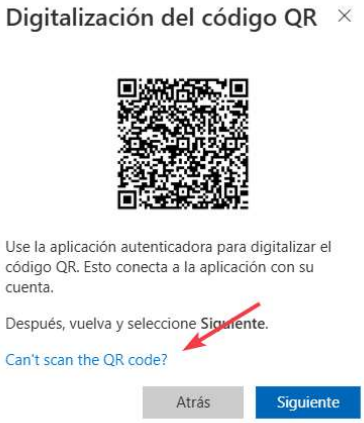




Seleccionamos **“Configurar una aplicación de autenticación diferente”.**

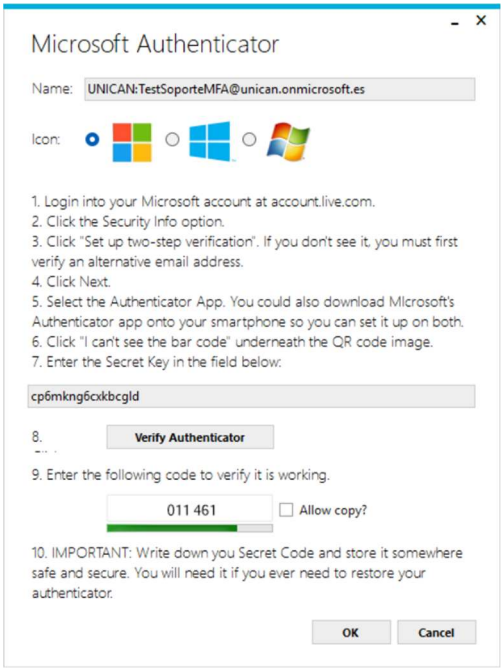


Se le mostrará el código QR. Seleccione “No puedo escanear el código QR”.

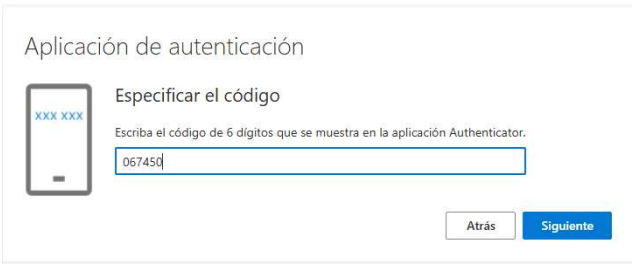


Se nos mostrará la clave secreta:

En la aplicación WihAuth seleccionado “Add” y de tipo “Microsoft”. Copiamos la clave secreta que vemos en el portal de Microsoft.



Una vez agregada la cuenta a WitnAuth debemos pulsar siguiente en el portal de registro de Microsoft para verificar el registro introduciendo el código de un solo uso que nos muestra WinAuth.



Si todo ha ido bien debería salir el siguiente mensaje:

A partir de este momento, cuando inicie sesión, tras introducir usuario y contraseña, se solicitará el segundo factor, que, por defecto, será un código de seis dígitos de un solo uso en la WinAuth.

Se recomienda agregar más de un método para MFA. En este caso deberá tener configurado WinAuth (u otra alternativa) en varios ordenadores bajo los que tenga el control

Opción C. Registro de llave de seguridad

Existe la posibilidad de adquirir una llave de seguridad, tipo FIDO2, siendo un fabricante popular Yubico https://support.yubico.com/hc/en-us/articles/360015669179-Using-YubiKeys-with-Microsoft-Entra-ID-MFA-OATH-TOTP

Tiene las instrucciones de configuración de llaves de seguridad con las cuentas de la UC en:

https://support.microsoft.com/es-es/account-billing/configurar-una-clave-de-paso-fido2-como-m%C3%A9todo-de-verificaci%C3%B3n-2911cacd-efa5-4593-ae22-e09ae14c6698

Las llaves de seguridad aportan una solución robusta, pero, además de adquirir un dispositivo, requiere tenerlas con nosotros siempre que sea necesaria una validación MFA. Además, al ser un dispositivo pequeño es fácil de perder u olvidar.

Probar MFA

Dado que desde la propia Red UNICAN no se pide normalmente el MFA, una vez que tenga registrados los mecanismos de MFA en su cuenta, puede probarlo usando la antigua página para generar reuniones en Teams. No es necesario crear una reunión, simplemente se trata de comprobar que al iniciar sesión te pide el MFA.

https://campusvirtual.unican.es/teams

Según los mecanismos que haya registrado y use, durante la validación con MFA necesitará, además de su contraseña, introducir un código de un solo uso de seis cifras que obtendrá por una aplicación de autenticación o bien haciendo uso de una llave de seguridad.

Pérdida de todos los mecanismos MFA

La pérdida de todos los mecanismos MFA nos impedirá acceder a los servicios que lo requieran, aunque sepamos nuestra contraseña. Por ejemplo, no podremos acceder al correo electrónico desde fuera de la Universidad, aunque sí desde nuestro puesto de trabajo. Es posible que, si hemos indicado que solo nos pida MFA cada 60 días, los accesos en dispositivos existentes sigan funcionando, pero al final dejarán de funcionar.

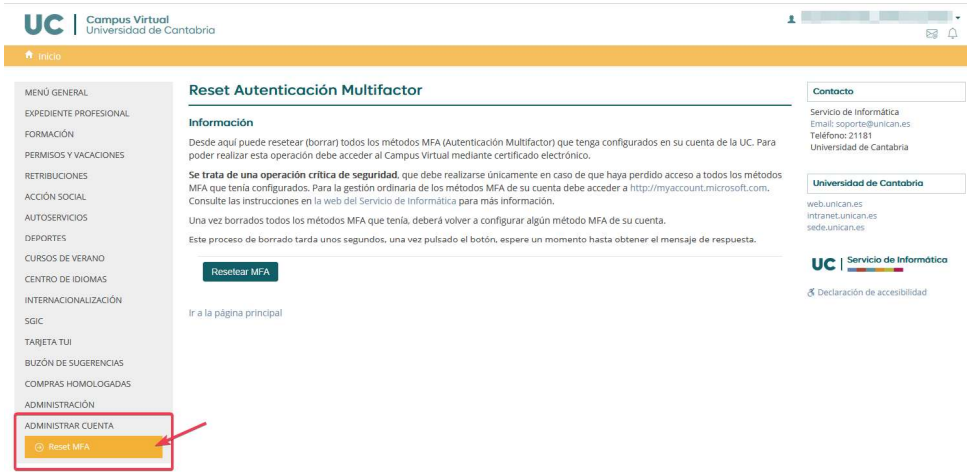
Si es empleado y en caso de que no dispongamos de un certificado electrónico personal (tipo FNMT o DNIe) deberemos contactar con soporte y personarnos en el Servicio de Informática con nuestra documentación (DNI, Tarjeta Universitaria o Pasaporte) para solicitar el borrado de mecanismos MFA. Este trámite solo se puede hacer personalmente previa cita.

Sin embargo, si disponemos de un certificado electrónico personal podemos hacer este proceso nosotros mismos desde el Campus Virtual.

Para borrar todos los mecanismos existentes deberemos acceder **con certificado electrónico personal (FNMT o DNIe)** al Campus Virtual de la UC (https://campusvirtual.unican.es) y seleccionar la opción de **Administrar Cuenta -> "Reset MFA".**

Se trata de una operación crítica de seguridad que no debe realizarse a la ligera. Solo debe realizarse si hemos perdido acceso a todos los métodos MFA que teníamos configurados, ya que **borra todos** los métodos.

Una vez borrados todos los métodos MFA podremos volver a hacer el registro de los mismos.



Para evitar este trastorno, que puede ocurrir en un momento inconveniente, se recomienda agregar más de un método para MFA.

Preguntas frecuentes

Puede consultar las preguntas más frecuentes en el Manual de Configuración de la Autenticación Multifactor (MFA) que encontrará en https://sdei.unican.es/mfa