



1. First of all, setup a recovery account with a different email that you have access to. In your desktop, go to <https://idm.ucm.es> identify yourself and make sure there is an alternative email (email alternativo) set in the section user data (Datos de usuario). When you have the data ready, save changes with “Salvar los cambios”. **Remember to check the NIF/NIE field. You will be asked exactly the content of that field in case of account recovery.**

Datos de usuario

Cambiar contraseña

Segundo factor de autenticación

Buzones vinculados

Solicitudes

Renovar

**Administrar**

Administrar Externos

Gestión de Autorizaciones

**Servicios**

Buzón para.TI@UCM

**Acceso**

Inicio

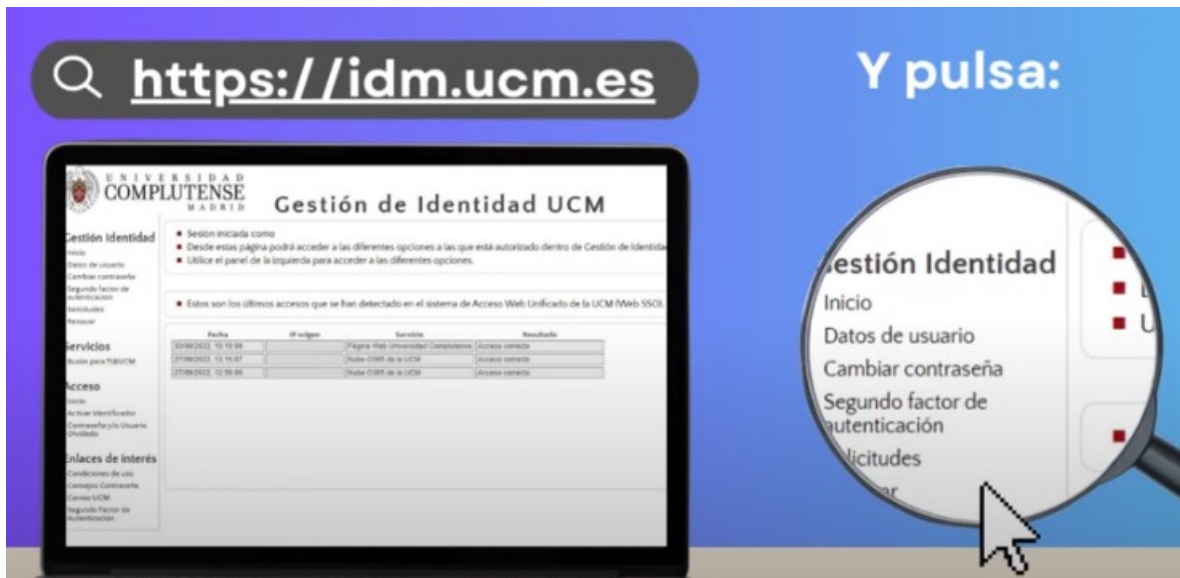
Activar Identificador

Contraseña y/o Usuario Olvidado

Atributo	Val
Nombre	
Primer Apellido	
Segundo Apellido	
Fecha expiración de la cuenta	
Fecha caducidad de la contraseña	
NIF/NIE...	
European Student Identifier (ESI)	
Email alternativo	
Teléfono móvil	

Deshacer los cambios Salvar los cambios

2. Choose one or two of the following options
  1. If you want to use your mobile, install in your mobile either the FreeOTP Authenticator or the Google Authenticator app
  2. If you choose to use your desktop, install in your chrome browser the authenticator extension (<https://chromewebstore.google.com/detail/authenticator/bhghoamapcdpbohphigooaddinpkbai> )
  3. Or the FreeOTP
3. In your desktop, go to <https://idm.ucm.es> and click on “segundo factor de autenticación” (second factor of authentication)



3. In the second factor of authentication page, click on “mostrar QR” (show QR)



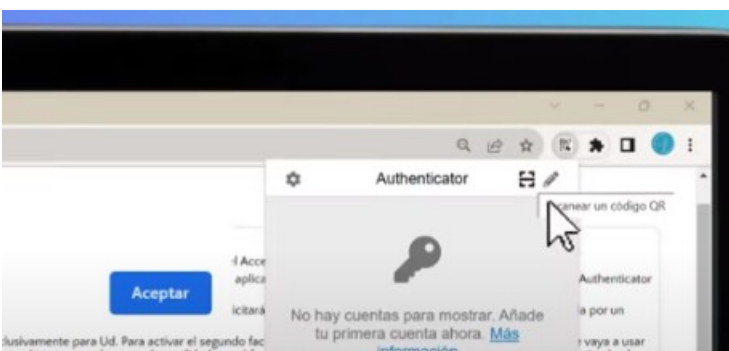


4. if you want to set up the mobile app, go to the authentication app, if it was the google authenticator app, you will see a “scan QR” option. Choose it and proceed to scan the QR from the previous step in the desktop browser



4.1 . Once done, the mobile will start showing numbers associated to this @ucm account. Then go to your desktop computer where the QR was. The browser will ask for a number with “introduzca la clave generada”. Quickly input the number the mobile is showing. It will last 30 seconds.

5. if you want to setup the desktop to provide the authentication numbers, go to your chrome browser where you installed the authentication extension. Click on the QR icon on the bar



Click on the [-] icon to start the scanning of the QR shown in the **step 3**

5.1 the chrome extension now should show numbers. Copy the number generated by the extension and paste it in the browser field “introduzca la clave generada en su movil”. Afterwards, the extension and your account will be setup.



6. Everytime you are asked for the “segundo factor de autenticación” (see third field), you have to type the number generated either by the installed mobile app or the chrome extension in your desktop. If you choose “confiar en este equipo” (trust this device), you will not be asked for a while this number when using this device.

### Acceso Web Unificado a la UCM (Web SSO)

Identificarse correctamente en esta página le habilitará la entrada en la mayoría de las aplicaciones y en los servicios en la nube @UCM.

**SI NO HAS CAMBIADO TU CONTRASEÑA EN LOS ÚLTIMOS 6 MESES, NI ACTIVADO EL DOBLE FACTOR DE AUTENTICACIÓN, TE RECOMENDAMOS QUE LO HAGAS AHORA: CAMBIA TU CONTRASEÑA Y ACTIVA 2FA**



Dirección de correo UCM

Contraseña

Si tiene activado el Segundo Factor de Autenticación introduzca la clave numérica generada con su dispositivo

Confiar en este equipo.

Iniciar sesión

[¿Olvidó la contraseña?](#)  
[Más información](#)

7. If something goes wrong, and you loose access to your account, you can reset. To do this, go to <https://idm.ucm.es/clave> and request an activation code to be sent. You need to choose the second option, that you don't have a recovery code (Si no dispone de un código de recuperación). You need to choose the document type. It should be either passport (pasaporte), numero identificación extranjero (foreigner identification number - NIE), or Numero identificación fiscal (fiscal identification number - NIF), most probably, but if they don't work, try the others. This is the value you need to remember from step 1. Select the appropriate one and select the code to be sent to your alternative account (again the one from step 1).

Accede con un Código de Recuperación

Si NO dispone de un Código de Recuperación

Tipo doc. de identidad

Número doc. de identidad

En función de los datos de que dispongamos le enviaremos un nuevo código a:

su dirección alternativa de correo electrónico

Enviar



8. Once received the code, you will have to go the same page and input it. Again, the identification data (the passport, NIE, NIF, or the most adequate in your situation), and the recovery code.

**● Accede con un Código de Recuperación**

Tipo doc. de identidad ⓘ

Número doc. de identidad ⓘ

Código de Recuperación ⓘ

**● Si NO dispone de un Código de Recuperación**

9. Once finished, you can gain temporarily access to your account and retry the second factor of authentication. There is an option to disable it in case you find too many problems. Desactivation may cut you from the services that require second factor of authentication. Eventually, all services in UCM will require this second factor.

**Segundo factor de autenticación**  
Buzones vinculados  
Solicitudes  
Renovar

### Administrar

Administrar Externos  
Gestión de Autorizaciones

### Servicios

Buzón para.TI@UCM

- Si activa el servicio, cuando el servicio de SSO le solicite a un corto período de tiempo.
- La aplicación móvil necesita cargar una clave inicial que se vaya a usar el código QR que se muestra más abajo con si manualmente en la aplicación, para lo que dispone del bo
- Para desactivar el segundo factor de autenticación use el l

Ya ha activado el segundo factor de autenticación.

Si desea desactivarlo, pulse el siguiente botón:

El siguiente código QR contiene su clave privada para el segu