

Two-factor Authentication (2FA)

Acerca de la autenticación de dos factores (2FA)

La autenticación de dos factores (2FA) es una capa adicional de seguridad que se utiliza al iniciar sesión en sitios web o aplicaciones. Con 2FA, tienes que iniciar sesión con tu nombre de usuario y contraseña y proporcionar otra forma de autenticación que solo tú conoces o a la que solo tú tienes acceso.

¡Alerta!

Es muy importante que descargue la aplicación Microsoft Authenticator, ya que le proporcionará 2 métodos de inicio de sesión: Microsoft Authenticator app y número de teléfono. Así, en caso de pérdida del móvil o cambio de número de teléfono, se podrá iniciar la sesión de Esade.

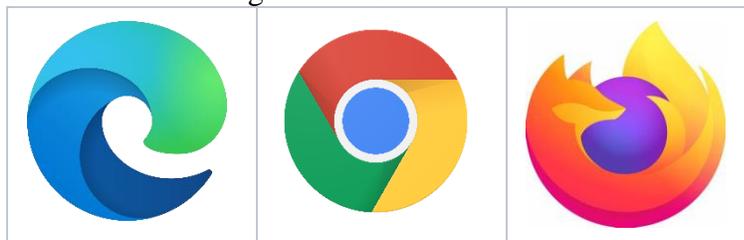
Aplicación 2FA para smartphone: Microsoft Authenticator

- **Configuración de Esade 2FA con Microsoft Authenticator en su teléfono**
Para acceder a la guía, pulse [aquí](#).
- **Inicie sesión con Microsoft Authenticator**
Para acceder a la guía, pulse [aquí](#).

Alternativa sin smartphone - Cliente 2FA en el navegador de su ordenador

- **Instale Authenticator: 2FA Client plugin en el navegador de su ordenador**

1. Seleccione su navegador e instale la extensión desde el botón azul.



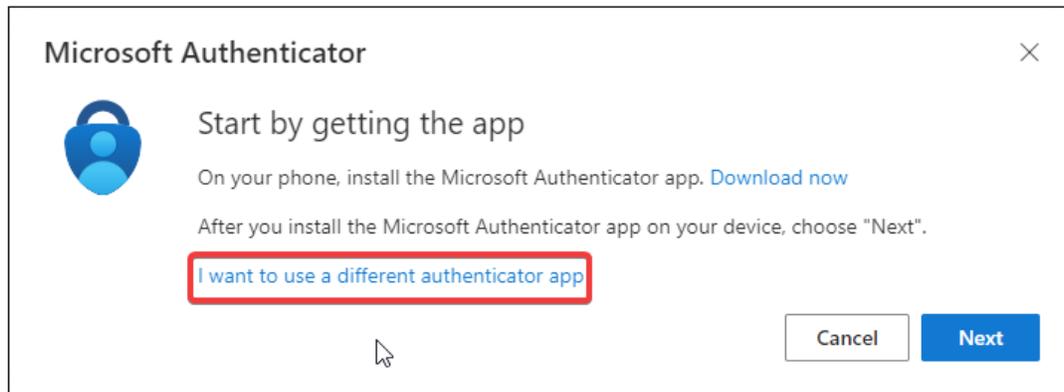
2. Haga clic para añadir la extensión en la ventana emergente que aparecerá.

- **Configure Esade 2FA in Authenticator: 2FA Client plugin**

Para añadir la autenticación de dos factores (2FA) a su cuenta de Esade, siga estos pasos:

1. Abra una ventana del navegador y vaya a este [enlace de Microsoft](#). Inicia sesión con tu ID y contraseña de Esade.
2. Seleccione añadir método de inicio de sesión y seleccione la aplicación de autenticación. A continuación, haz clic en el botón añadir.

3. Seleccione Quiero usar una aplicación de autenticación diferente.



4. Haga clic en el botón siguiente.
5. Aparecerá un código QR en la pantalla. Vaya a la parte superior derecha de la pantalla y seleccione Authenticator: 2FA Client.
6. Cuando se abra Authenticator, haga clic en Escanear código QR y marque dónde se encuentra el QR en la pantalla.
7. Aparecerá una ventana emergente diciendo que su cuenta esade ha sido añadida. Seleccione Aceptar.
8. En su pantalla seleccione el botón siguiente.
9. Abra el Authenticator: 2FA Client y copie el código de 6 dígitos que se mostrará. Seleccione el botón siguiente.
10. Ya está listo para utilizar Authenticator: 2FA Client. A partir de ahora, la próxima vez que inicie sesión en MyEsade/Outlook, se le pedirá que introduzca el código temporal de 6 dígitos generado por Authenticator: 2FA Client.

Qué puedo hacer si he cambiado mi número de móvil o no tengo acceso a él temporalmente? No puedo usar 2FA en MyEsade / Office365

En caso de no disponer temporalmente de un método alternativo.

Contacta con el CAU a través del [portal de Soporte Informático](#), por correo electrónico a cau@esade.edu, o por teléfono al 935 676 699 (ext. 5555), indicando que no tienes tu móvil **temporalmente**. El CAU generará un código de acceso temporal que dura 8 horas.

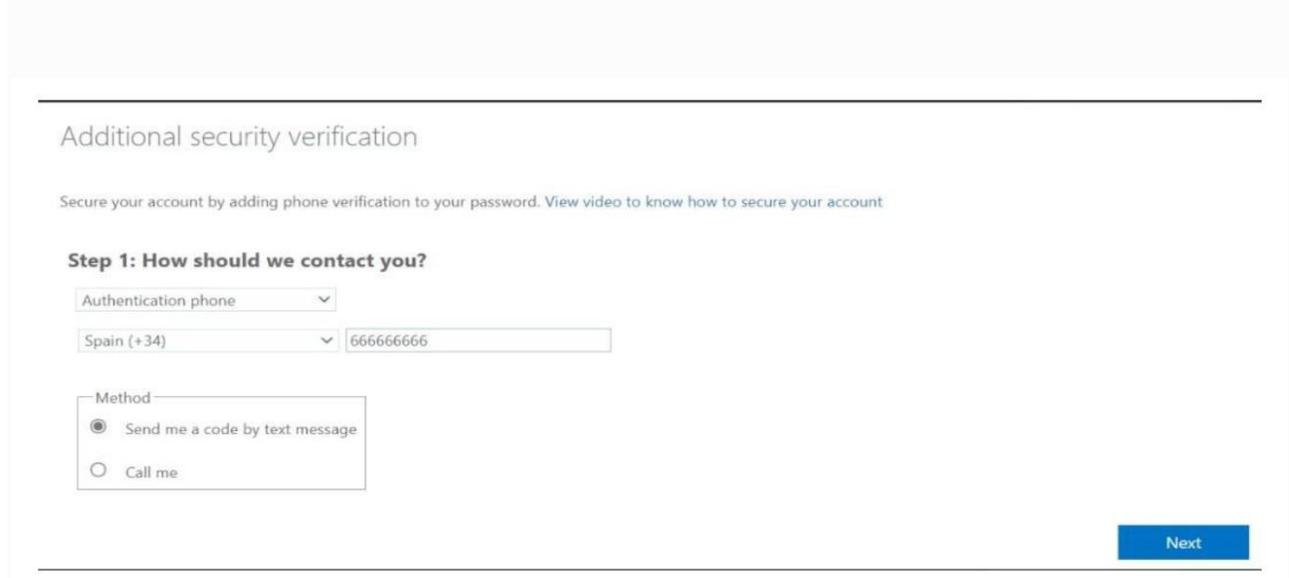
En caso de cambio o pérdida de su teléfono móvil.

Póngase en contacto con el CAU a través del [portal de Soporte Informático](#), por correo electrónico en cau@esade.edu, o por teléfono en el 935 676 699 (ext. 5555), indicando que ha cambiado de número de móvil o que ha perdido el teléfono. El CAU restablecerá el 2FA de la cuenta correspondiente para que pueda volver a configurarlo desde cero con un nuevo número.

No quiero descargar otra aplicación, ¿puedo configurar la 2FA sin la app Microsoft Authenticator?

Si, es posible configurarla solamente con el número de móvil, sin necesidad de descargar la aplicación Authenticator. Desde el TIC de Esade, recomendamos utilizar la *app* para tener una mejor experiencia de uso.

Si se configura solamente con el número de móvil, se recibe un SMS o una llamada (en vez de una notificación) cada vez que se intenta acceder a uno de los servicios de Microsoft.



The screenshot shows the 'Additional security verification' setup page. It includes a title, a subtitle, a step indicator, a dropdown for 'Authentication phone', a dropdown for 'Spain (+34)' and a text input for '666666666', a 'Method' section with radio buttons for 'Send me a code by text message' (selected) and 'Call me', and a blue 'Next' button.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Authentication phone

Spain (+34) 666666666

Method

Send me a code by text message

Call me

Next

Una vez configurada desde la página de Microsoft, aparece lo siguiente:

Additional security verification App Passwords

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
[View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default:

1

how would you like to respond?

Set up one or more of these options. [Learn more](#)

Authentication phone * Spain (+34) 2

Office phone (do not use a Lync phone) Select your country or region Extension

Alternate authentication phone Spain (+34)

Authenticator app or Token [Set up Authenticator app](#)

restore multi-factor authentication on previously trusted devices

[Restore](#)

[Save](#) 3 [cancel](#)