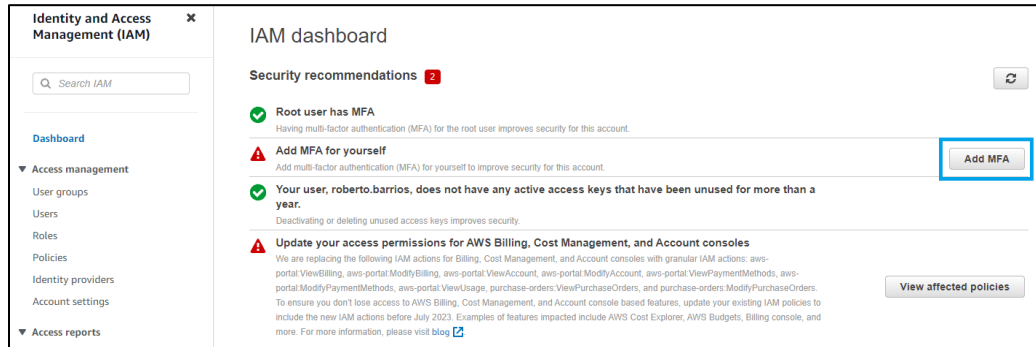
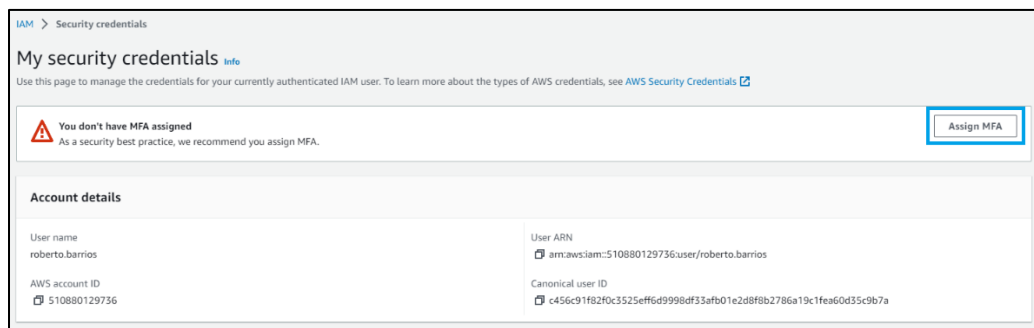


Manual de activación de MFA

1. Nos dirigimos al servicio de IAM y seleccionamos la opción resaltada en azul:



2. Posteriormente, seleccionamos la opción *Assign MFA*:



3. En esta sección, debemos configurar un nombre para identificar el dispositivo de MFA y elegir la primera opción como herramienta de autenticación (*Authenticator app*). Posterior a ello, damos click en *next*:

The screenshot shows the 'Select MFA device' configuration screen. The 'Specify MFA device name' section has a text input field with 'testMFA' entered. Below this is the 'Select MFA device' section, which has three radio button options: 'Authenticator app' (selected), 'Security Key', and 'Hardware TOTP token'. The 'Authenticator app' option is described as 'Authenticate using a code generated by an app installed on your mobile device or computer.'

4. Para el siguiente paso:
- a. descargaremos una aplicación de MFA dentro de nuestro móvil. La siguiente lista muestra las diferentes opciones tanto para dispositivos Android como iOS:

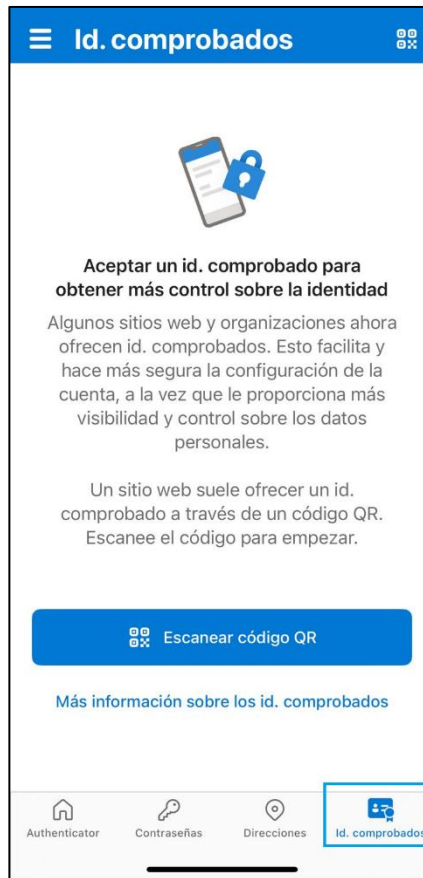
Android	Twilio Authy Authenticator , Duo Mobile , LastPass Authenticator , Microsoft Authenticator , Google Authenticator , Symantec VIP
iOS	Twilio Authy Authenticator , Duo Mobile , LastPass Authenticator , Microsoft Authenticator , Google Authenticator , Symantec VIP



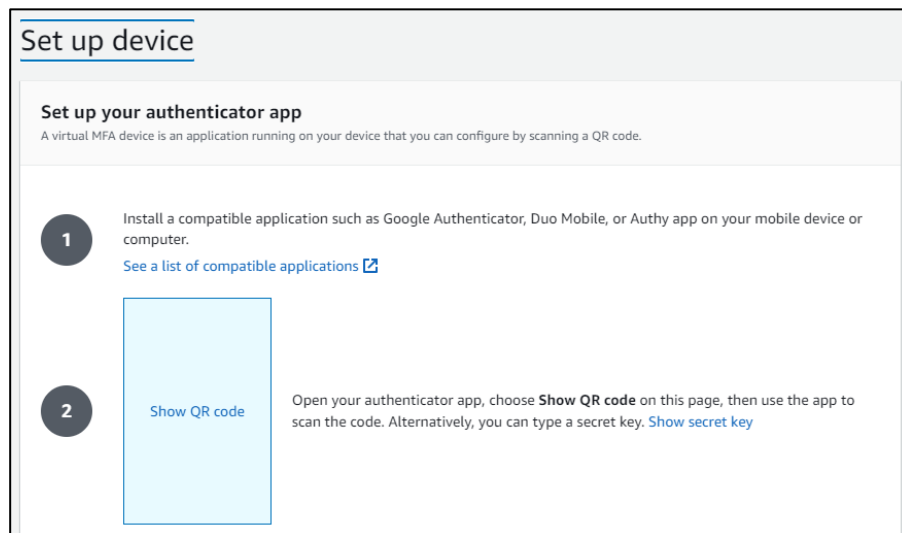
- b. Realizaremos el proceso de activación de MFA a través de la aplicación de Microsoft Authenticator. Podrás obtenerla a través de los siguientes códigos QR:



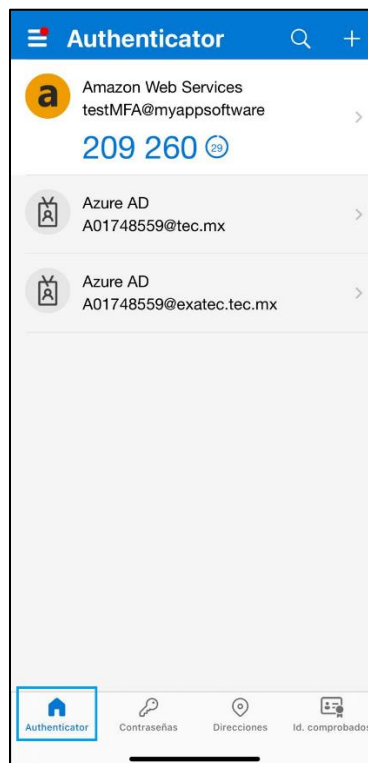
- c. Una vez descargada nuestra aplicación, nos dirigimos a ella y seleccionamos la opción *Id. comprobados* en el menú inferior.



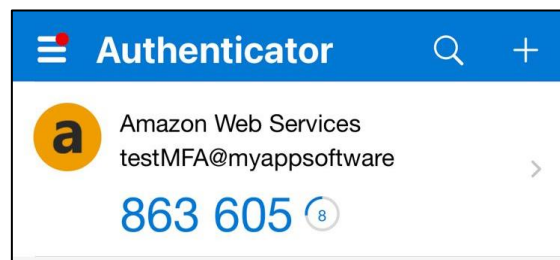
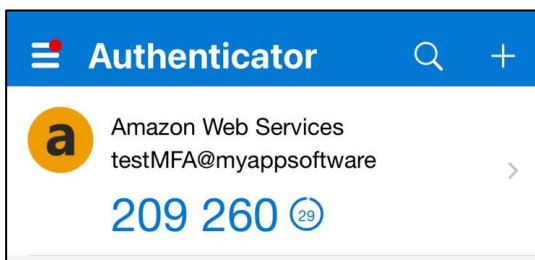
- d. Regresamos a la pestaña de configuración de MFA y seleccionamos *Show QR code*. Posterior a ello, dentro de nuestra app damos click en el recuadro azul *Escanear Código QR*.



- e. Una vez escaneado el código QR, damos click en *Continuar* y nos dirigimos a la sección *Authenticator* seleccionándolo en el menú inferior:



- f. Continuamos el proceso colocando dos códigos consecutivos de la sección *Amazon Web Services* dentro del paso 3 y damos click en el recuadro amarillo *Add MFA*:



Set up device


Set up your authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)

2



Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key.
[Show secret key](#)

3

Fill in two consecutive codes from your MFA device.

MFA code 1

MFA code 2

Cancel

Previous

Add MFA

- g. Finalmente, se nos confirmará la activación del servicio de MFA a través de nuestra aplicación de Microsoft Authenticator:

MFA device assigned

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the [AWS CLI](#) with that user.

IAM > Security credentials

My security credentials [info](#)

Use this page to manage the credentials for your currently authenticated IAM user. To learn more about the types of AWS credentials, see [AWS Security Credentials](#)

Ahora, cada que iniciemos sesión, se nos solicitará ingresar un código de autenticación:



Autenticación multifactor

Escriba un código de MFA para completar el inicio de sesión.

Código de MFA:

Enviar

[Cancelar](#)

Español

[Términos de uso](#) [Política de privacidad](#) © 1996-2023, Amazon Web Services, Inc. o sus empresas afiliadas.