INTCOMEX
CLOUD

Default Security Settings

REVISIÓN ENERO 2023

DEFAULT SECURITY VALUES IN MICROSOFT ENTERPRISE ID (SECURITY DEFAULTS)

Important: If the Tenant was created on October 22, 2019, or later, the default security values are already enabled in the Tenant.

Default security values make it easier to protect your organization against identity-related attacks, requiring all users registered in the tenant to use MFA and disabling legacy protocols.

Microsoft ensures that these previously configured default security values are available to ALL users. More than 99.9% of these common identity-related attacks are stopped through multifactor authentication and blocking of legacy authentication.

IMPLEMENTATION CONSIDERATIONS

User Preparation

It is essential to notify users about upcoming changes, registration requirements, and actions they need to take. Direct users to https://myprofile.microsoft.com to register, where they should select the 'Security info' link on that page.

IMPLEMENTATION CONSIDERATIONS

Blocking Legacy Authentication Protocols

To provide users with easy access to cloud applications, a variety of authentication protocols, including legacy authentication, are supported. Legacy authentication refers to an authentication request made by:

- Clients not using modern authentication (e.g., Office 2010 client).
- Any client using old email protocols such as IMAP, SMTP, or POP3.

After enabling default security values in the tenant, all authentication requests made with an old protocol will be blocked. The default security values block basic authentication for Exchange Active Sync. Validate that this will not impact your infrastructure.

HOW TO ENABLE SECURITY DEFAULTS:

1. Log in to the Microsoft Admin Center at https://admin.microsoft.com/ with at least the Security Administrator or Global Administrator role.

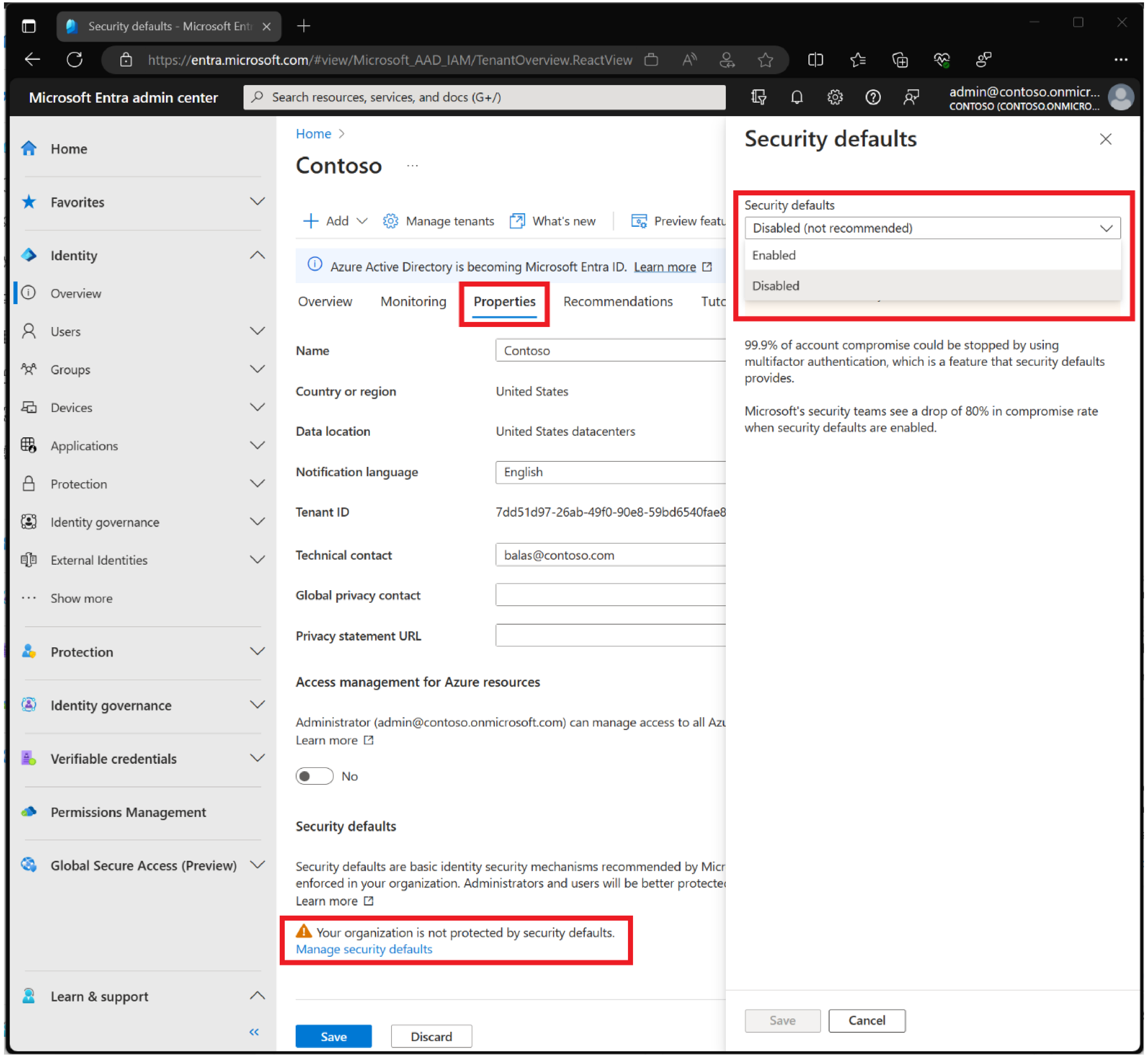
2. Go to Overview > Properties.

3. Select Manage Security Defaults.

4. Set Security Defaults to Enabled.

5. Select Save.

INTCOMEX CLOUD



Azure Active Directory is becoming Microsoft Entra ID. Learn more

Name	Contoso
Country or region	United States
Data location	United States datacenters
Notification language	English
Tenant ID	7dd51d97-26ab-49f0-90e8-59bd6540fae8
Technical contact	balas@contoso.com
Global privacy contact	
Privacy statement URL	

Access management for Azure resources

Administrator (admin@contoso.onmicrosoft.com) can manage access to all Azu
Learn more

No

Security defaults

Security defaults are basic identity security mechanisms recommended by Micr
enforced in your organization. Administrators and users will be better protecte
Learn more

⚠ Your organization is not protected by security defaults.
Manage security defaults

Security defaults

Security defaults: Disabled (not recommended)

- Enabled
- Disabled

99.9% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.

Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.

Configuring Security Information

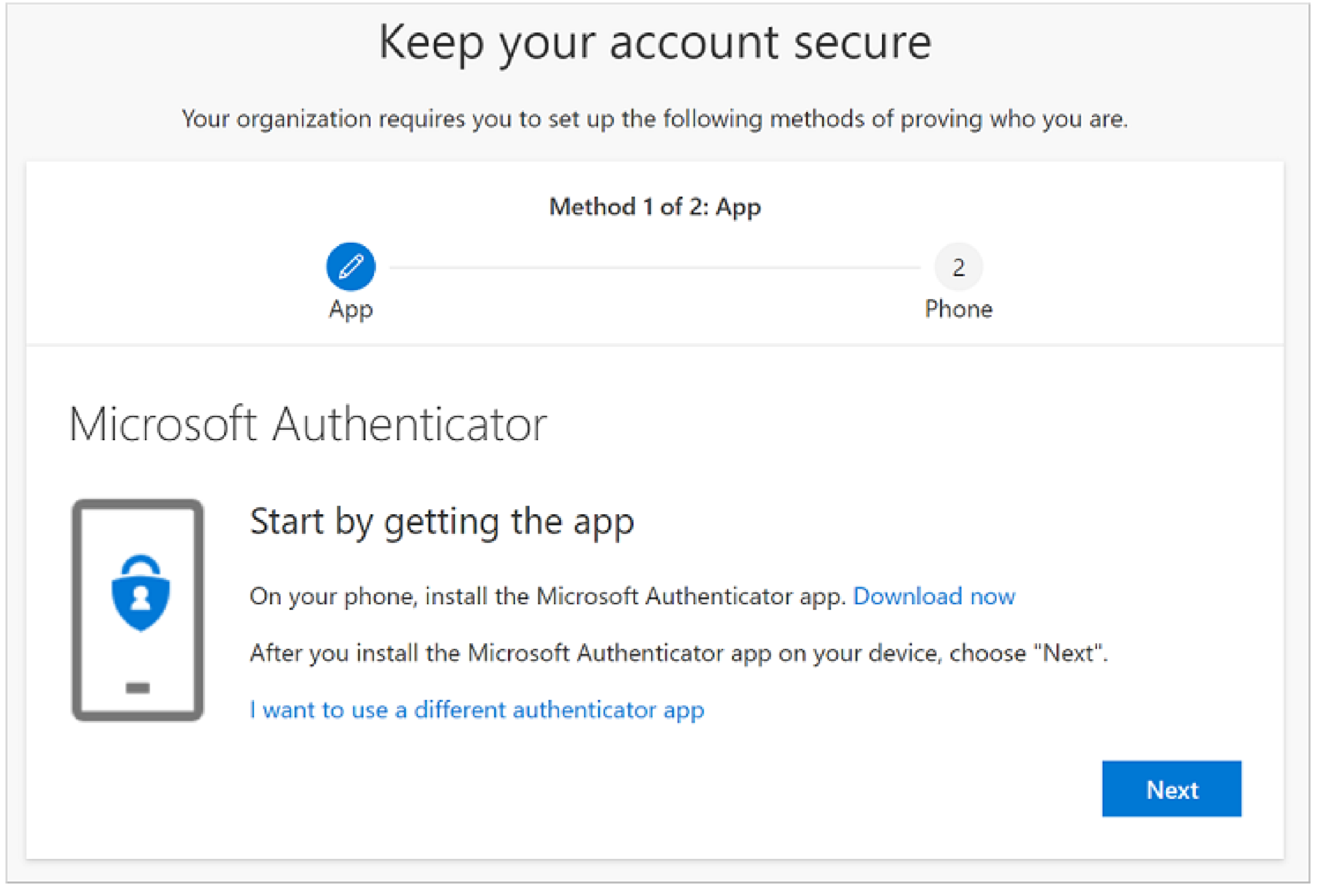
Follow these steps to configure the security information for your work or school account from the message.

Important: This is just an example process. Depending on your organization's requirements, the administrator may have set up different verification methods that you'll need to configure during this process. For this example, two methods are required: the Microsoft Authenticator app and a mobile phone number for verification calls or text messages.

1. After selecting Next, a wizard appears titled "To keep your account secure," which displays the first method required for configuration by the administrator and the organization. For this example, it is the Microsoft Authenticator app.

Notes:

- If you want to use an authenticator app other than the Microsoft Authenticator app, select "I want to use a different authentication app."
- If your organization allows you to choose another method besides the authenticator app, you can select "I want to set up a different method.



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 1 of 2: App

Microsoft Authenticator

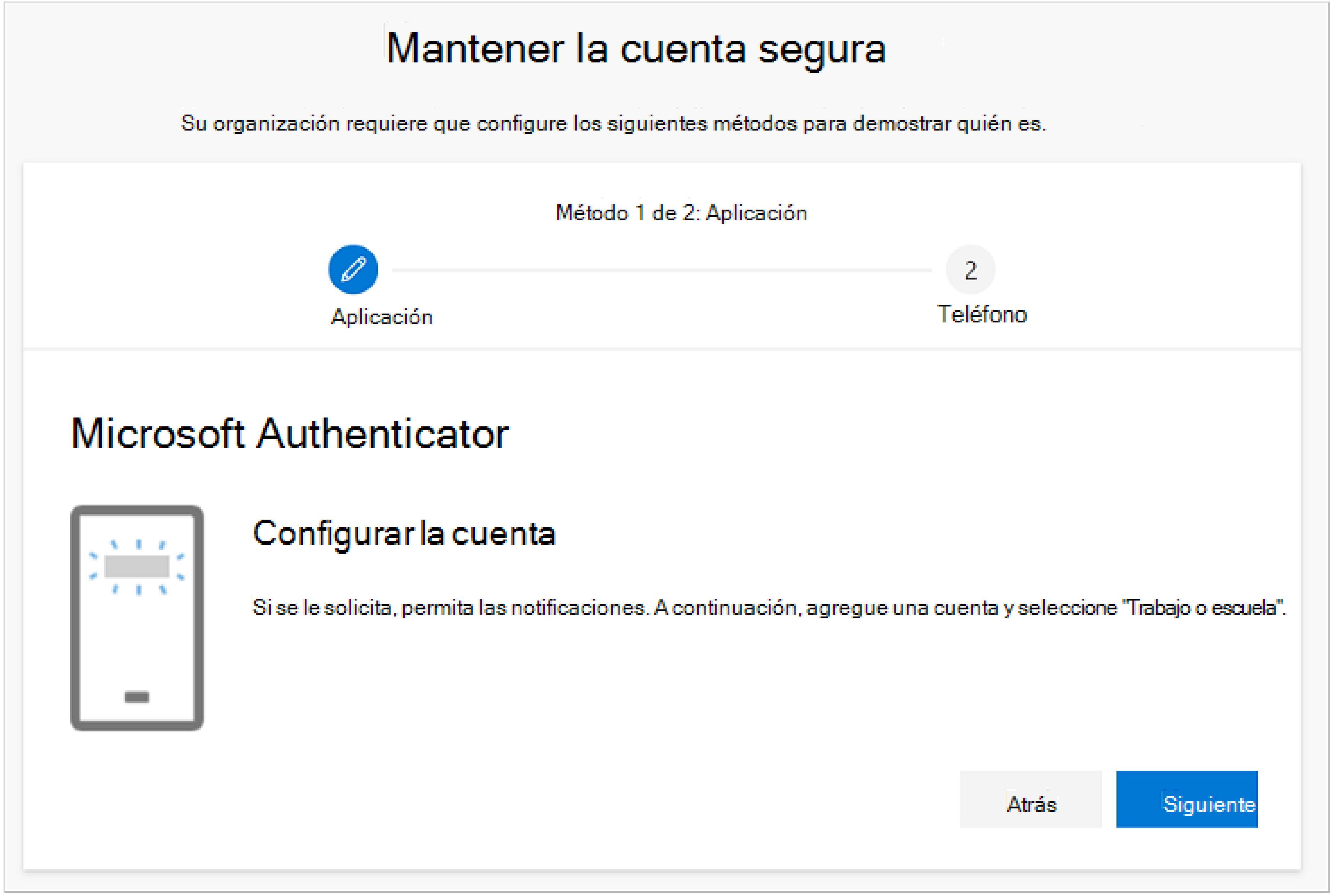
Start by getting the app

On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

2. Select **"Download now"** to download and install the Microsoft Authenticator on your mobile device, and then select "Next."



Mantener la cuenta segura

Su organización requiere que configure los siguientes métodos para demostrar quién es.

Método 1 de 2: Aplicación

Microsoft Authenticator

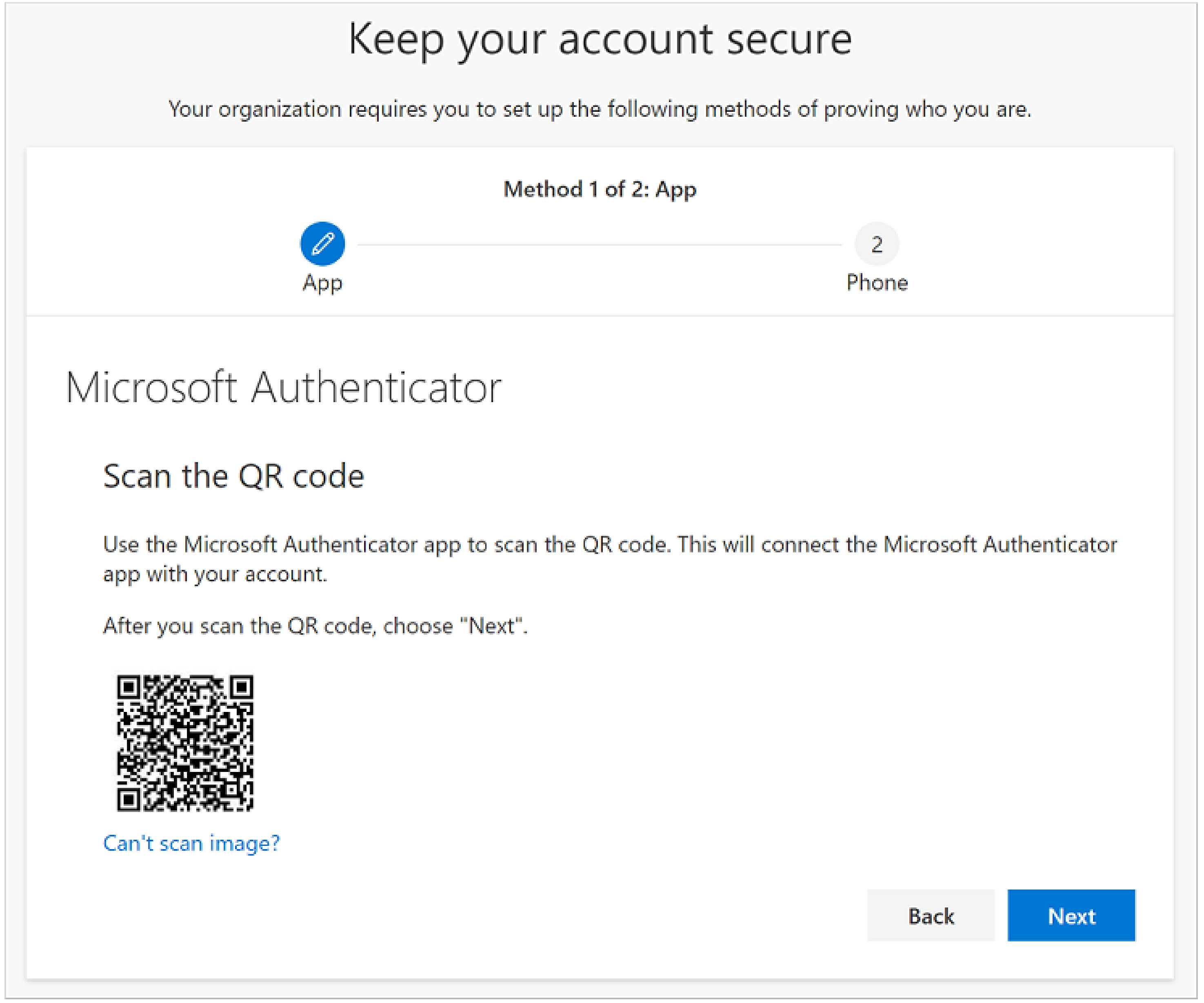
Configurar la cuenta

Si se le solicita, permita las notificaciones. A continuación, agregue una cuenta y seleccione "Trabajo o escuela".

3. **Stay on the "Set up your account"** page while you set up the Microsoft Authenticator app on your mobile device.
4**. Open the Microsoft Authenticator** app, select to allow notifications (if prompted), select "Add account" from the Customize and control icon in the top right corner, then select "Work or school account.

Note: The first time you set up the Microsoft Authenticator app, you may receive a message asking if you want to allow the app to access your camera (iOS) or allow the app to take pictures and record video (Android). You must select "Allow" for the authenticator app to access the camera to take a photo of the QR code in the next step. If you don't allow the camera, you can still set up the authenticator app, but you'll need to add the code information manually. For information on how to manually add an account to the app, see "Manually add an account to the app.

5. Return to the "Set up your account" page on your computer, then select "Next." The "Scan the QR code" page will appear.



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 1 of 2: App

Microsoft Authenticator

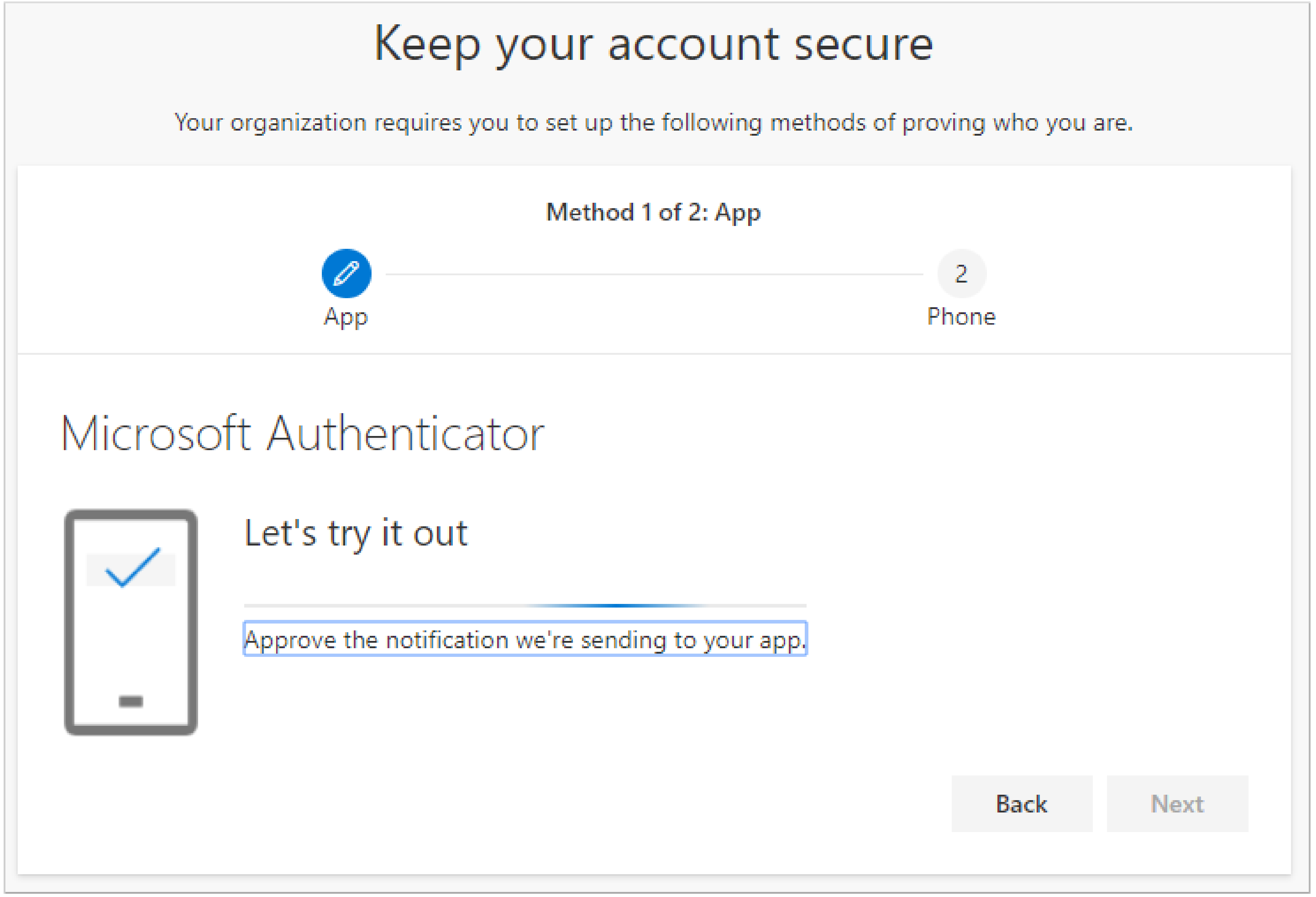
Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".

6. Scan the provided code with the QR code reader in the Microsoft Authenticator app, which appeared on your mobile device after creating your work or school account in step 5. If the QR code reader cannot read the code, you can select the option "Can't scan the QR image" and manually enter the code and URL into the Microsoft Authenticator app. For more information on manually adding a code, see "Manually add an account to the app.“

7. Select "Next" on the "Scan the QR code" page on your computer. A notification is sent to the Microsoft Authenticator app on your mobile device to verify your account.



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

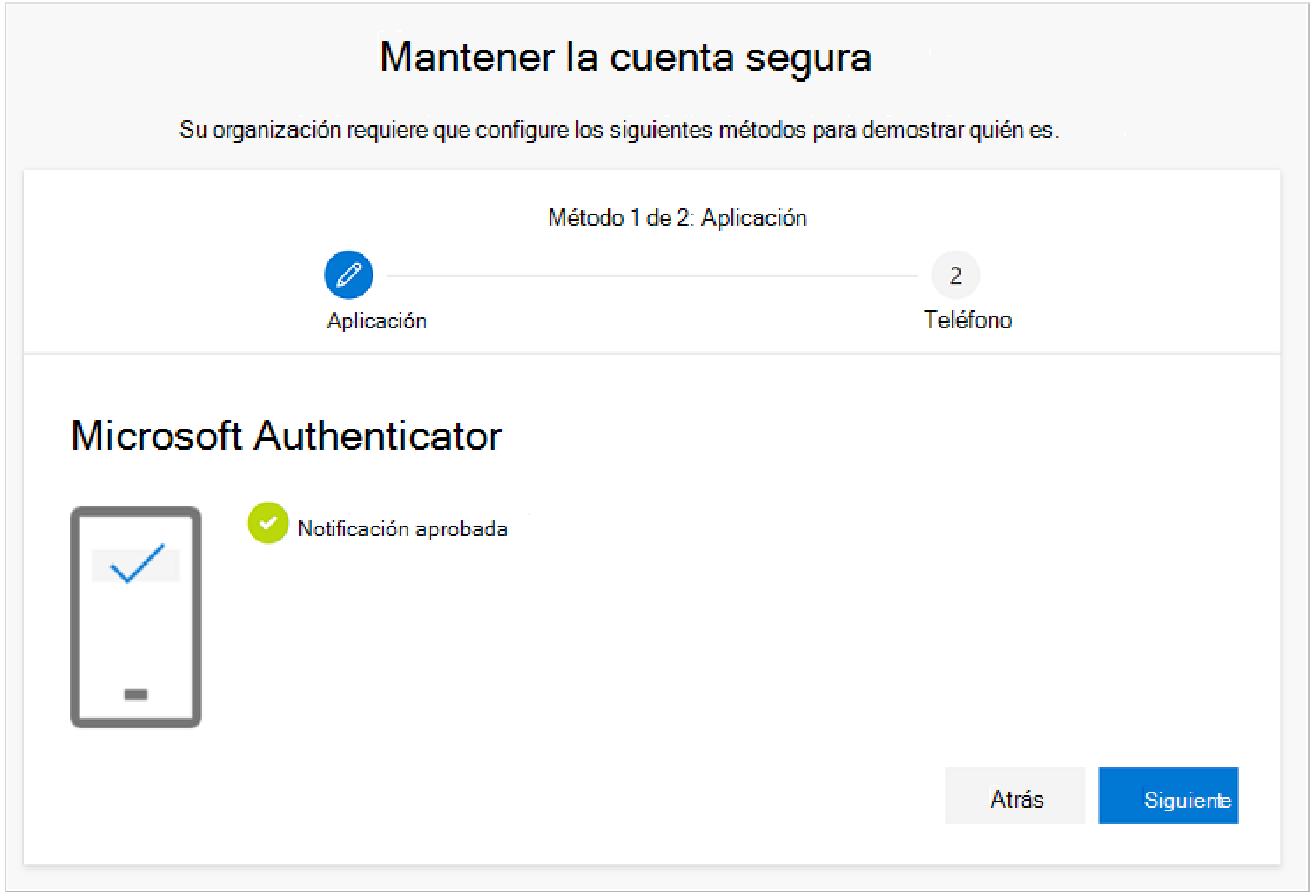
Method 1 of 2: App

Microsoft Authenticator

Let's try it out

Approve the notification we're sending to your app.

8. Approve the notification in the Microsoft Authenticator app, then select "Next." The security information is updated to use the Microsoft Authenticator app by default to verify your identity when using two-step verification or password reset.



Mantener la cuenta segura

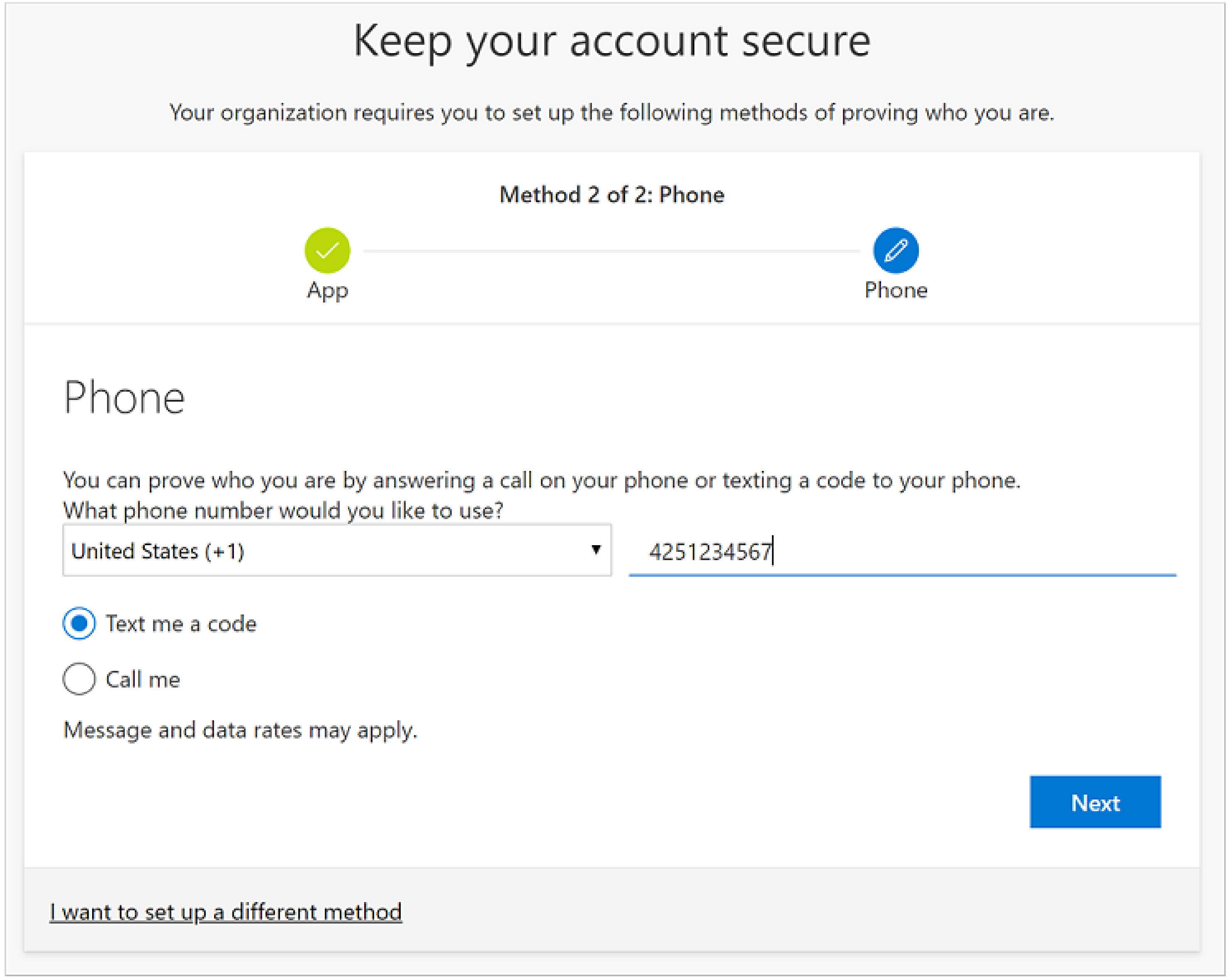
Su organización requiere que configure los siguientes métodos para demostrar quién es.

Método 1 de 2: Aplicación

Microsoft Authenticator

✓ Notificación aprobada

9. In the "Phone setup" section, choose whether you want to receive a text message or a phone call, then select "Next." In this example, we are using text messages, so you should use a phone number for a device that can accept text messages. A text message is sent to your phone number. If you prefer to receive a phone call, the process is similar.



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 2: Phone

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

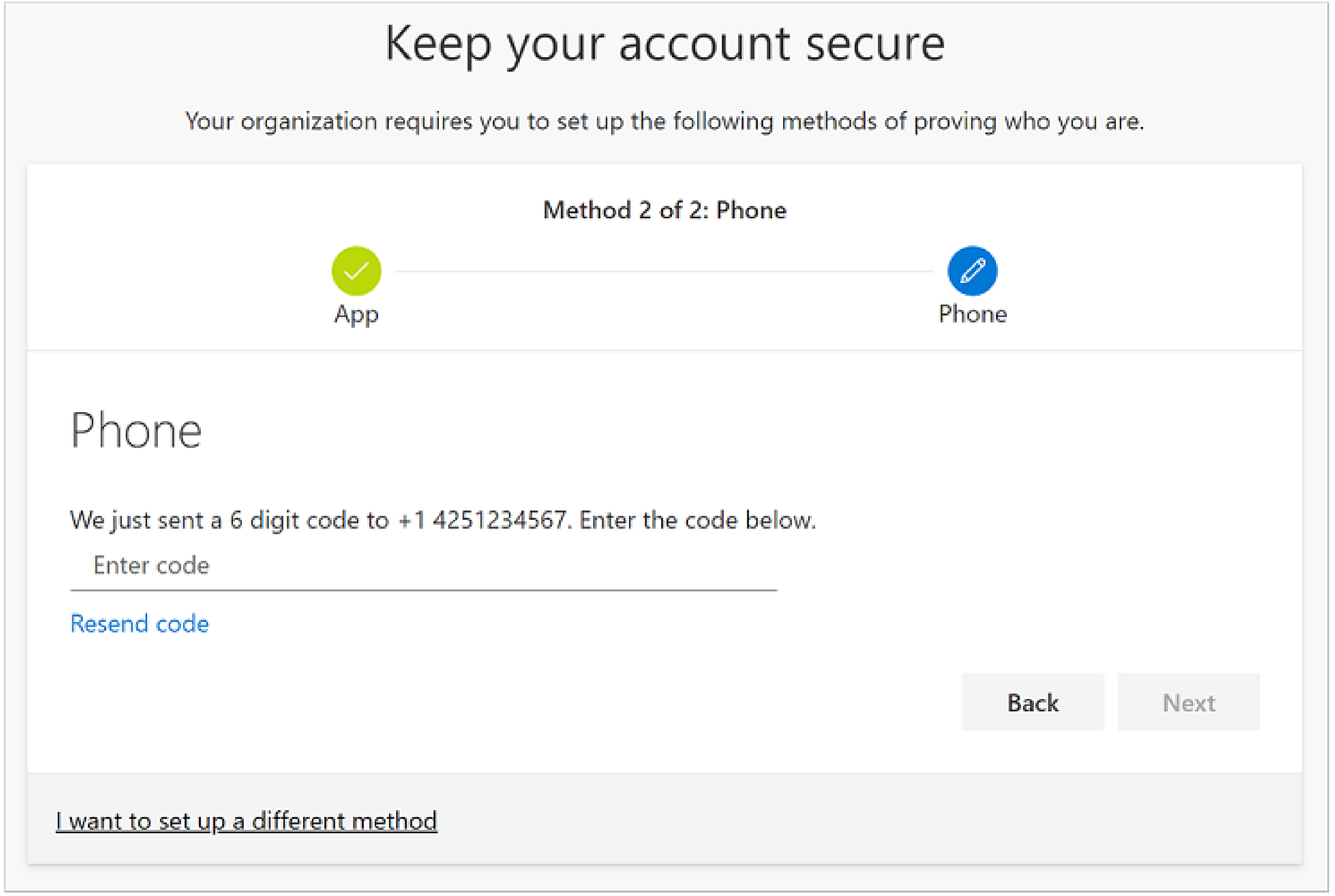
United States (+1) ▾ 4251234567

● Text me a code

○ Call me

Message and data rates may apply.

10. Enter the code provided by the text message sent to your mobile device, then select "Next."



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

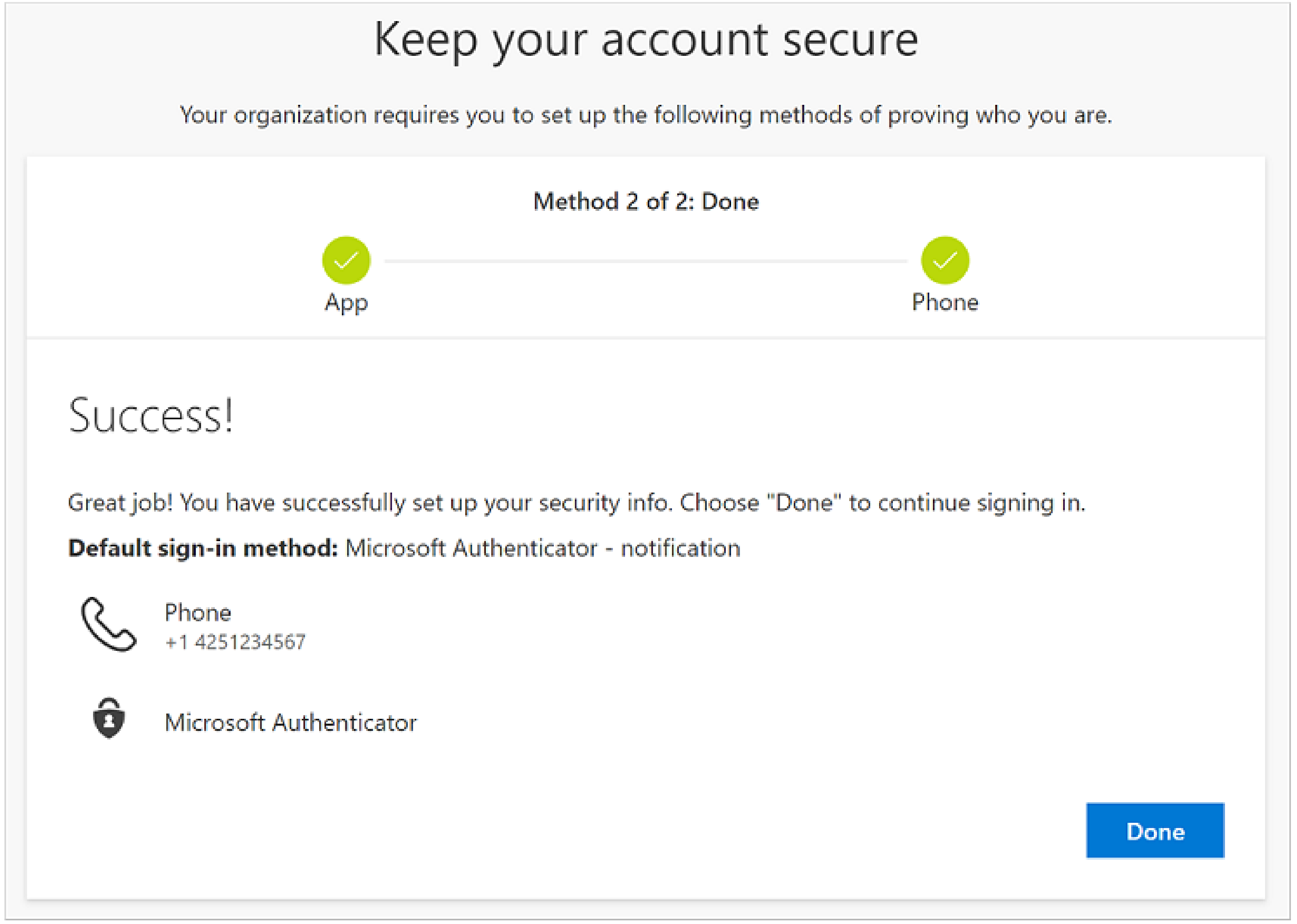
Method 2 of 2: Phone

Phone

We just sent a 6 digit code to +1 4251234567. Enter the code below.

11. Review the success notification, then select "Done."

12. Review the Success page to verify that you have successfully set up the Microsoft Authenticator app and a phone method (either a text message or a phone call) for security information, then select "Done."



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 2: Done

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method: Microsoft Authenticator - notification

Phone
+1 4251234567

Microsoft Authenticator

WELCOME TO A NEW ERA

INTCOMEX
CLOUD