Leonardo Identity Provider
Multi Factor Authentication – User Manual

Date: February 2024

Document type: External user manual

Indice

INTRODUCTION

In the process of identifying and authenticating users to access critical and confidential services, data and information, the use of "username and password" credentials alone cannot be considered sufficient to guarantee the protection of users' data and identities.
For this reason, Leonardo has introduced a multi-factor authentication process that provides more secure access and protection of user identities.
This authentication procedure, with high security features, is called MFA, from the acronym Multi-Factor Authentication.

The MFA authentication enabled by Leonardo for the services offered to its stakeholders involves "2-factor" authentication:

1st authentication factor: User-Name and Password

2nd authentication factor: a "method" of identity confirmation chosen initially by the user and manageable during the course of use of the service by the user himself (self-service management).

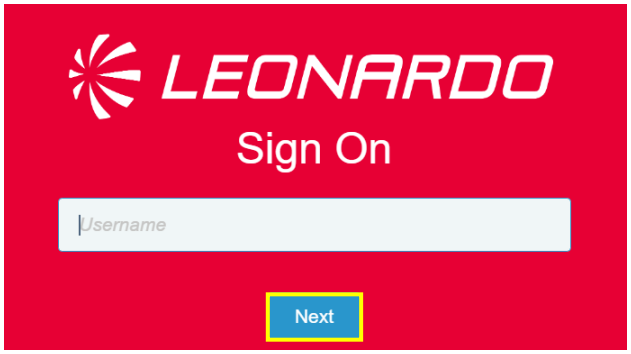
The methods made available by Leonardo for the 2nd authentication factor are:

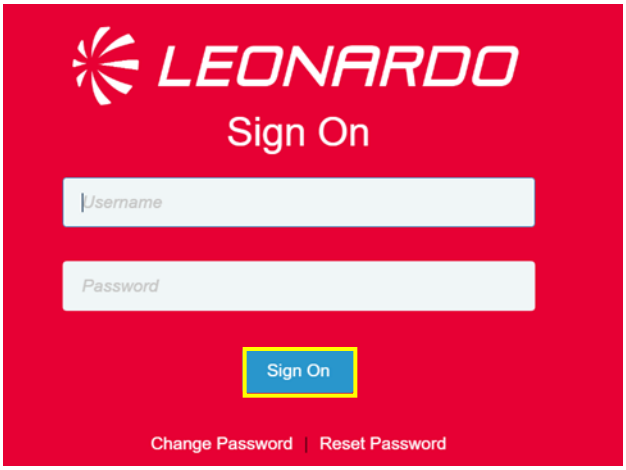
- Mobile App Method: Using application on smartphone via Push-Notification, when the mobile device is connected to Internet network, or passcode, when the mobile device is offline
- SMS Method: For receiving a single-use code (OTP)
- Voice Call method: for voice reception of a disposable code (OTP)
- Token Device Method: for generating a disposable code (OTP) via physical device.

The following will describe the procedures for choosing the method for the 2nd authentication factor, registering the device used for the chosen method, managing method and device, and the procedure for the proper use of Multi-Factor MFA authentication.

1 USER CREDENTIALS ENTRY

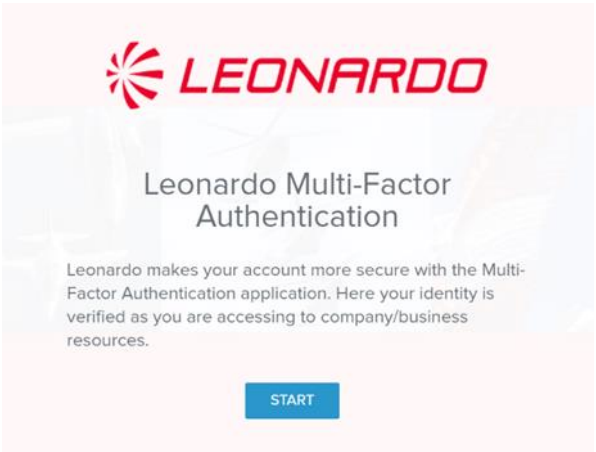
When accessing a Leonardo service protected by MFA (Multi-Factor Authentication) you are asked, as the 1st authentication factor, to enter your credentials (username and password) that you already have.
At this stage you are presented with the screens below in which you must enter your credentials and proceed with the **[Sign On]** button.





Next, the user may be in one of the following scenarios:

- **NO MFA method has been set up**: the user will be prompted to proceed with configuring at least one of the Multi-Factor Authentication methods made available by Leonardo. Click on **GetStarted"**:



  Follow the steps described in Chapter 2 **"Method Selection and Device Pairing"** for choosing and configuring at least one MFA method.

- **At least one MFA method <u>has already been configured</u>**: follow the steps described in Chapter 3 **"Use of Multi-Factor Authentication (MFA)"** to properly complete the authentication step according to the MFA method chosen.

2 METHOD CHOICE AND DEVICE PAIRING

After the first authentication step is completed, the user will see a screen where he/she can choose the MFA method from those made available by Leonardo. The screen is as follows and a brief description of the different authentication methods is given:

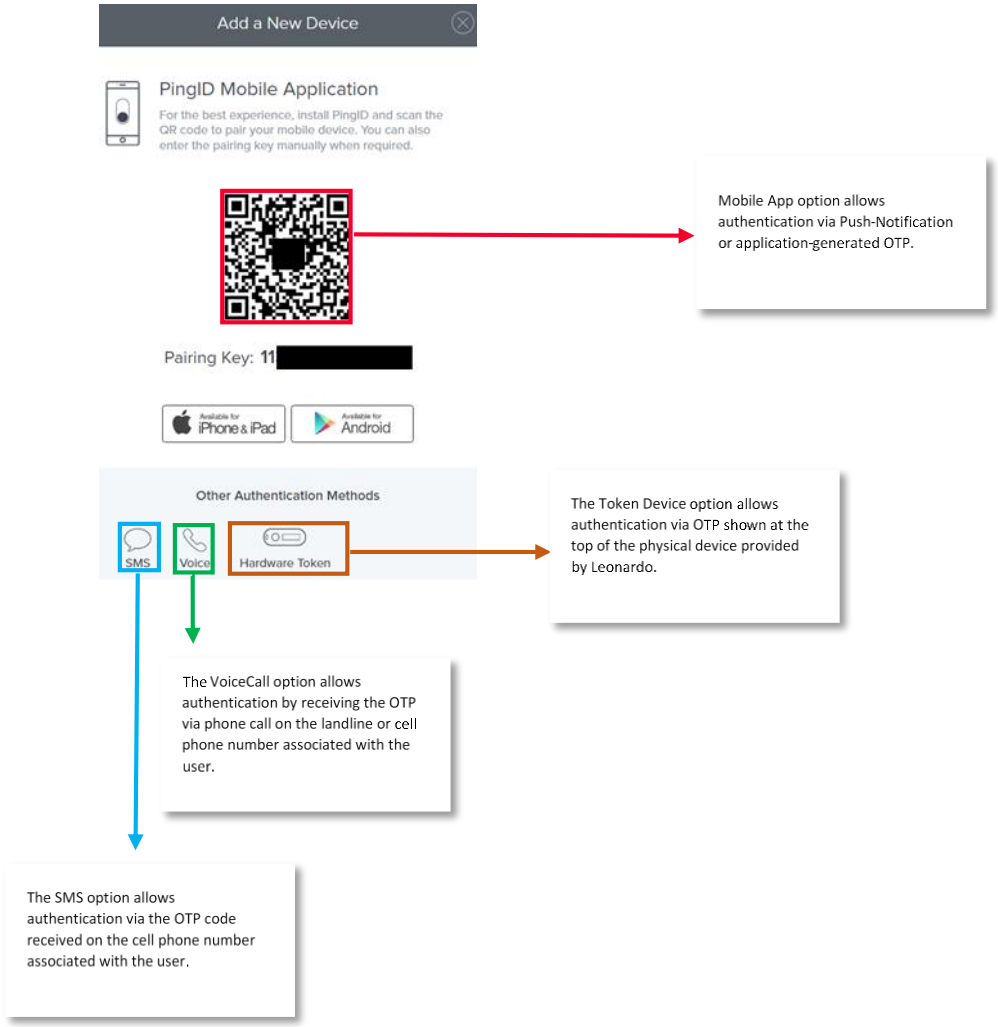


Figure 1 - MFA methods screen

Note how the above screen may vary depending on the contact information associated with the user. Please refer to section 2.1 "MFA mode configuration prerequisites" for further details.

2.1 Prerequisites configuration mode of MFA

The **prerequisites** for proper selection of different modes of MFA are given below:

- **Mobile App "Ping ID"**
  - **Internet-connected cellular device:** The device on which the application will be installed must be connected to an Internet network and have a biometric factor (e.g., face or fingerprint recognition) in order to complete the authentication.
  - **Offline device:** The OTP code authentication method is possible if the device is not connected to an Internet network or if the user chooses to use it by disabling the notifications, when the device is connected to an Internet network, from the settings of the application installed on the cellular device.
- "**SMS**": The user must have provided, when registering contact information, their cell phone number on which to receive the OTP code via SMS. Note how, if no mobile number has been provided, the "SMS" icon in Figure 1 - "MFA Methods Screen" will not be visible and available for selection. Contact your Leonardo contact person for more information on how to request number entry.
- "**Voice Call**": The user must have provided, when registering contact information, the landline number or cell phone number on which to receive the call. Note how, if no number has been provided, the "Voice call" icon in Figure 1 - "MFA methods screen" will not be visible and available for selection. Contact your Leonardo contact person for more information on how to request number entry.

The following sections will describe the steps to be followed for proper configuration of the MFA.

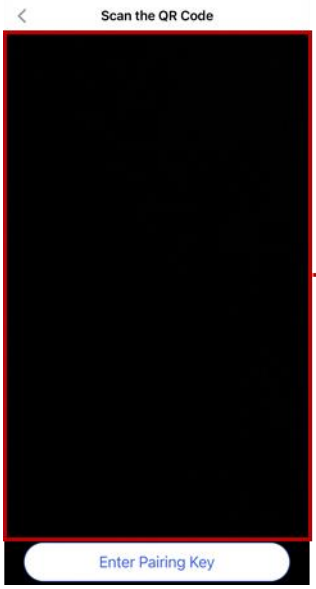
Note that the user has the option of entering two different numbers for the SMS option and the Voice Call option. In case the user wants it to be the same for both options he/she will have to specify it when registering the contact information.

2.2 MFA configuration via Mobile App “PingID” (Push-Notification or OTP)

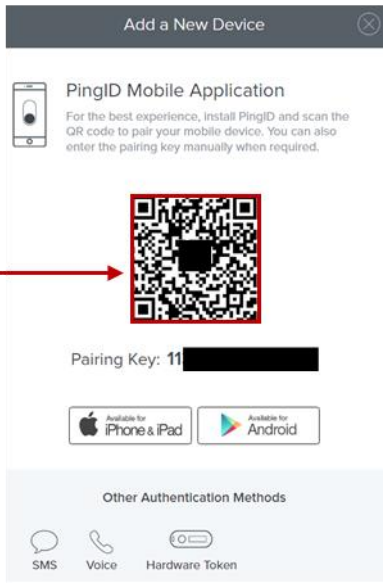
To configure the MFA via Mobile App, it is necessary to install the "PingID" application on the user's cell phone or tablet.

After completing the first authentication phase with the steps described in Chapter 1 *"Entering User Credentials"*, the user can choose to either frame the QRcode (**a.**) or, alternatively, enter the pairing key (**b.**) to proceed with device pairing:

a. To complete the association, the user must use the Mobile App "PingID" on the mobile device by scanning the QRcode on the web screen. Below are the screens that the user will see simultaneously on the mobile device (Mobile App "PingID") and on the browser (web) where the MFA configuration phase is taking place.

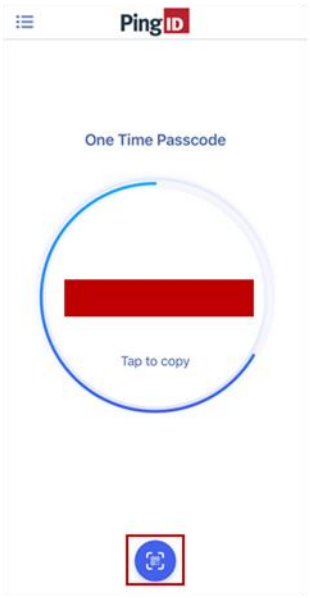


Initial screen "PingID" on mobile device



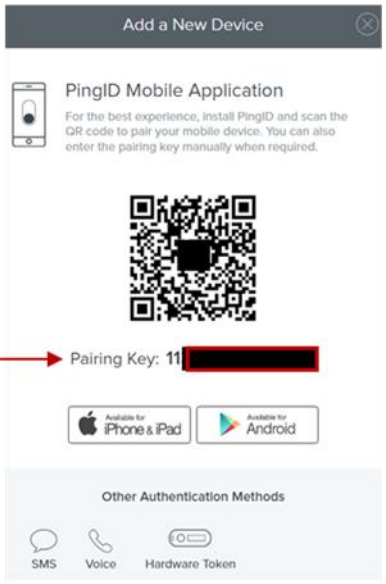
Web screen for device association

b. Alternatively, the user can complete the device pairing by entering the pairing key found on the web screen. The following are the screens that the user will simultaneously see on the mobile device (Mobile App "PingID") and the browser (web) where the MFA configuration phase is in progress.



One Time Passcode and Pairing key screeen

"PingID" screen by pairing key



Web screen to read pairing key

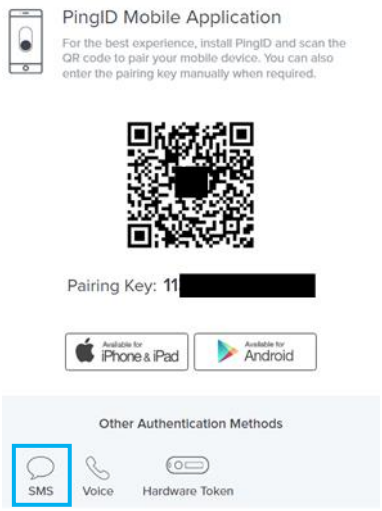
At the end of the process, the user will receive confirmation of the successful association on the mobile device.

The process of configuring the MFA via Mobile App "PingID" is finished.

Please refer to Section 3.1 - *"Authentication via Mobile App"* for details on the steps to be followed to authenticate with this mode.

2.3 MFA configuration via SMS

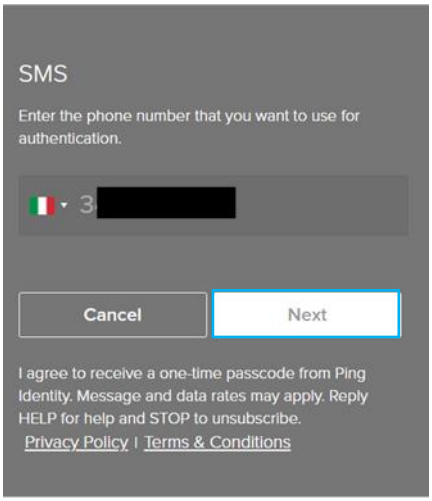
After completing the first authentication step as described in Chapter 1 "Entering User Credentials," the user should select the "SMS" option in the "Other Authentication Methods" section.



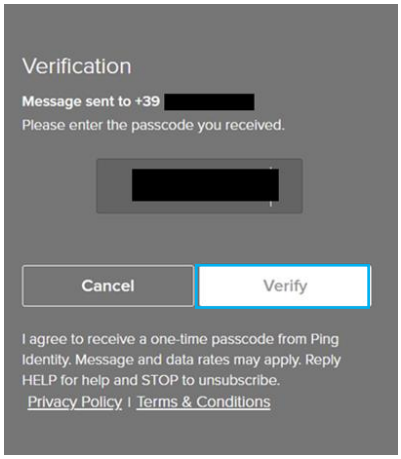
Next, a screen will appear asking you to confirm the cell phone number associated with the user on which to receive the SMS containing the OTP code to authenticate.

Click on "Next."

If the number does not match, you should contact your Leonardo contact person/referent to request a change.



Once the cell phone number is confirmed, the user will need to enter the OTP code received via SMS into the appropriate field and will need to click on "Verify."

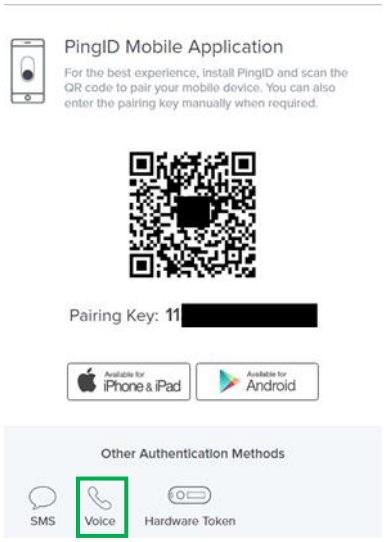


The process of configuring the MFA via SMS is finished.

Please refer to section 3.2- *"Authentication via SMS (OTP)"* for details on the steps to be followed to authenticate with this mode.

2.4 MFA configuration via Voice Call

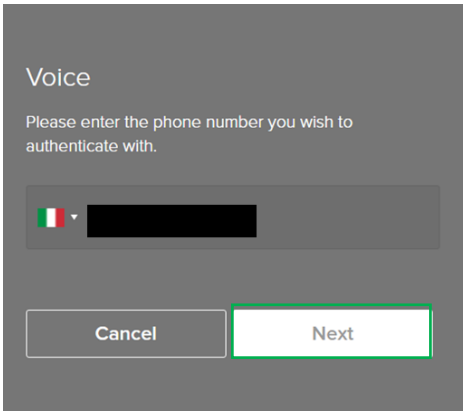
After completing the first authentication step as described in Chapter 1 "Entering User Credentials," the user should select the "Voice" option in the "Other Authentication Methods" section.



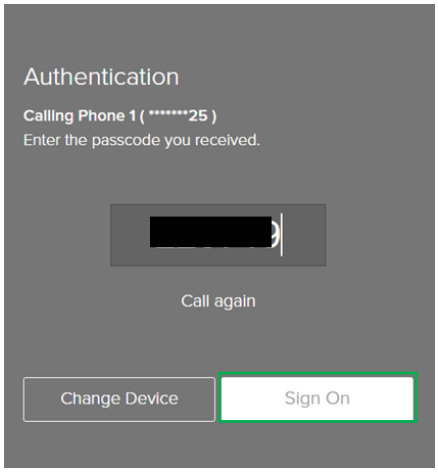
Next, a screen will appear displaying the cell phone number or landline number associated with the user on which to receive the call with which the OTP code to authenticate will be provided by voice.

Click on "Next."

If the number does not match, you should contact your Leonardo contact person/referent to request a change.



After confirming the mobile or landline number, the user should enter the OTP code received via phone call in the appropriate field and should click on "Verify."



The process of configuring the MFA via SMS is finished.

Please refer to Section 3.3 - *"Authentication via VoiceCall (OTP)"* for details on the steps to be followed to authenticate with this mode.

3 USE OF MULTI-FACTOR AUTHENTICATION (MFA)

The following sections will describe the steps to be able to authenticate using the previously configured authentication method. If different authentication methods have been configured, the user will be prompted at each login to choose which one to use.

3.1 Authentication via Mobile App

The user will be able to authenticate via Mobile app under the following conditions:

- If the mobile device is **connected to the Internet**, via Push Notification or OTP code,
- If the mobile device is **offline**, via OTP code.

3.1.1 Authentication via cellular device connected to the Internet network

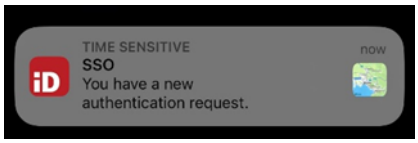
If the device has an active Internet connection, the user has the option to authenticate via mobile app via Push Notification or, alternatively, through the use of an OTP code generated by the app itself.

The user has logged in with credentials as described in Chapter 1:

- **Push Notification**

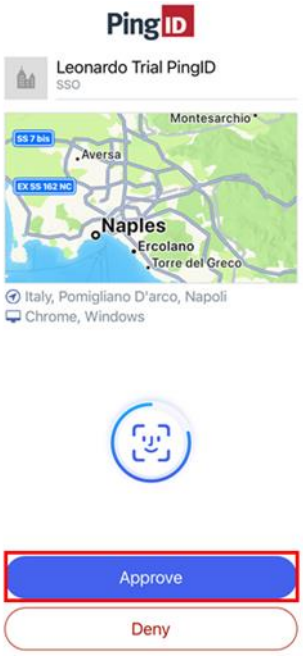
  In case the mobile device is connected to the Internet, the user can take advantage of authentication via Push-Notification by clicking on the notification to approve the authentication request.

Web screen waiting for approval of authentication request



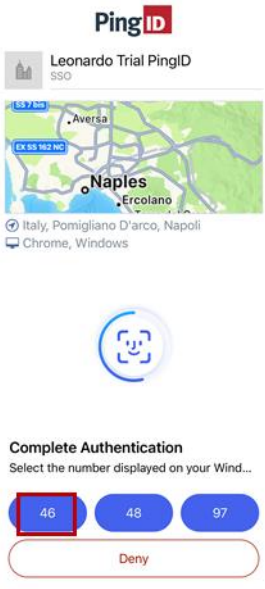
Notification on cellular device for authentication request

The user **must then open the PingID application**, click "Approve," and complete the verification with the biometric factor of the cellular device to authenticate correctly.



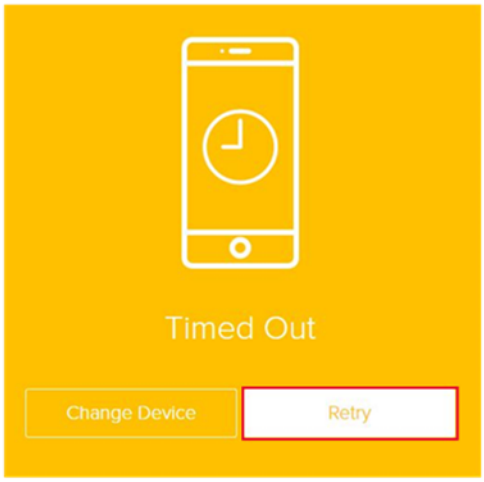
Following biometric factor authentication, further verification will be required.

The user will need to select, from the PingID application on the cellular device, the digit on the pc screen as depicted in the screenshots below.

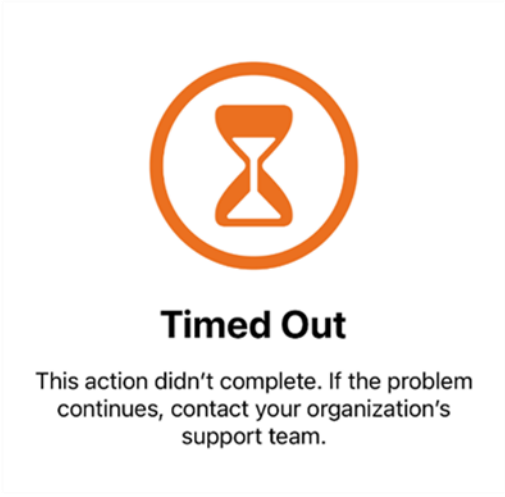


Note that the screens showed above are just an example

When the user opens the Mobile App but does not click the number showed on the web screen within 40 seconds of the authentication request, the session will be expired as depicted in the screenshots below.



Timed Out Web screen



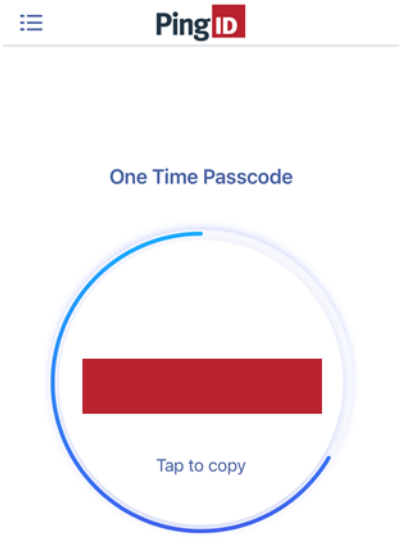
Timed Out «Ping ID» App screen

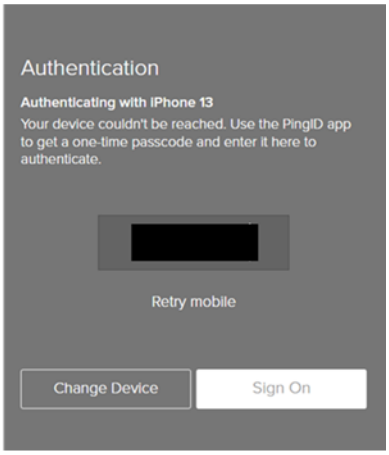
The user can then retry authentication by clicking on "Retry" and following the steps described above.

The authentication process via Push Notification via Mobile App "PingID" is finished and the following screen will be displayed.

Authenticated

If the user **does not** open the application to approve the authentication request within **25 seconds**, the user will be asked to enter the in-app generated OTP code as shown below:





Note that each OTP passcode expires after 30 seconds

Finally, the window confirming successful authentication will appear.

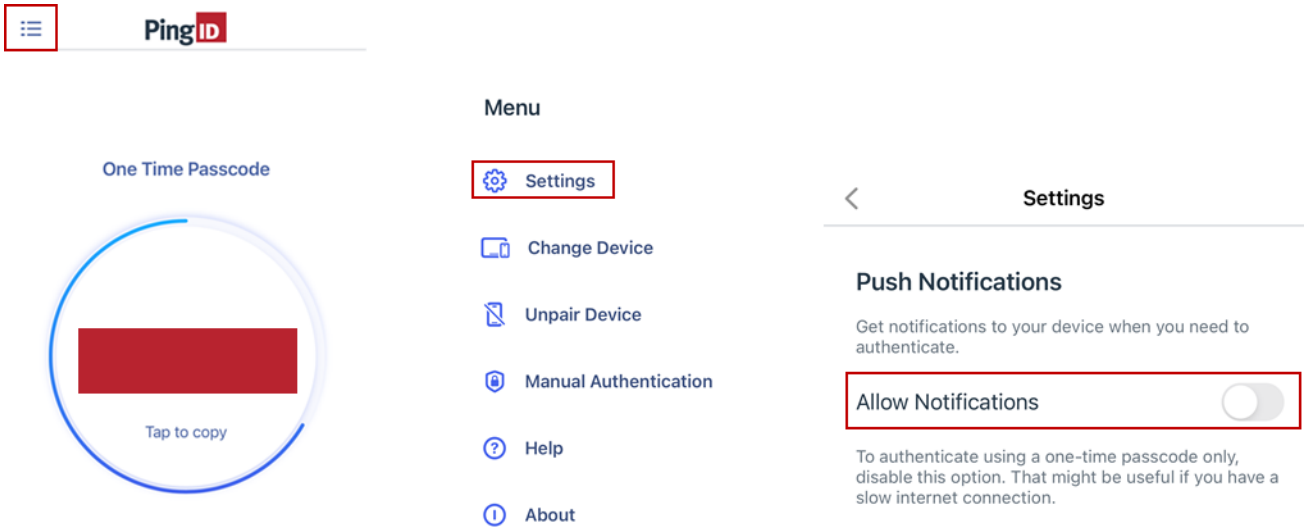
- **OTP passcode**

  In case the user wants to authenticate by OTP code, he/she will first have to make a change to the application settings by following the steps described and displayed below in the order given:

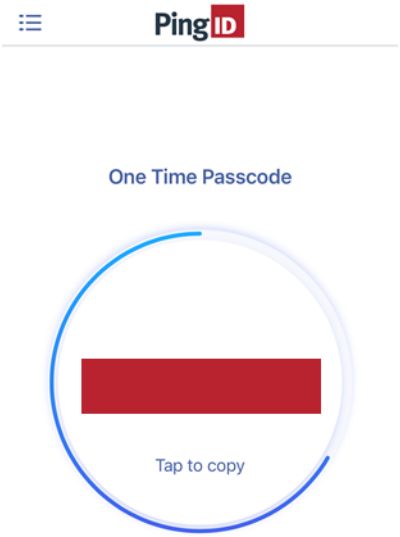
  1) Select the "gear" in the upper right corner to access the PingID application settings;

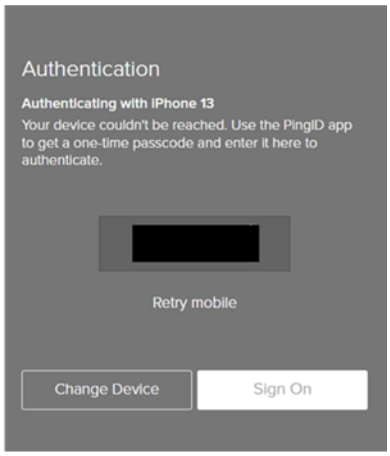
  2) Click on "Settings."

  3) Disable notifications.



Once the configuration is complete and as long as the above option remains disabled, the user will be able to authenticate via OTP passcode as shown below:





After logging in with credentials as described in Chapter 1, the user will need to enter the disposable passcode displayed in the application and click on "Sign On."

Note that each OTP passcode expires after 30 seconds

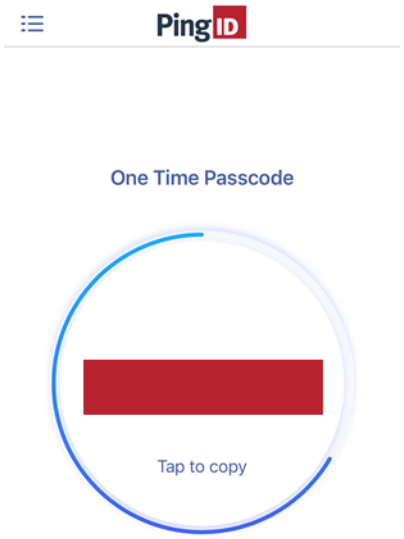
3.1.2 Authentication via cellular device offline

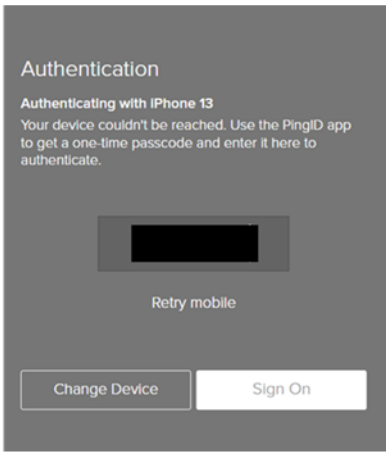
If the device turns out to be offline, the user still has the option to authenticate via Mobile app.

In this case, authentication **only and exclusively** through the use of an **OTP code** generated by the app itself as described below:

After logging in with credentials as described in Chapter 1, the user must click on "Sign On."

After **25 seconds** the authentication window will expire and the user will need to enter the disposable passcode and click on "Sign on" as it is shown below.





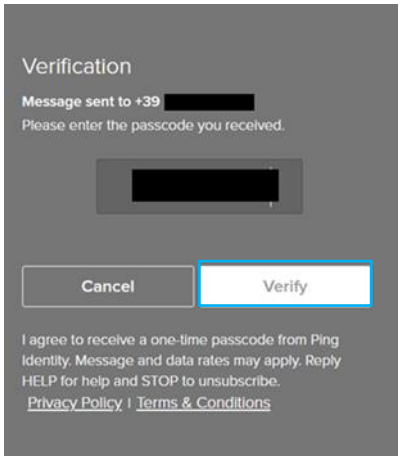
In case the first OTP passcode does not work, click on "New passcode"

Finally, the window confirming successful authentication will appear.

The authentication process via OTP via Mobile App "PingID" is finished.

3.2 Authentication via SMS (OTP)

After logging in with the credentials as described in Chapter 1, the user will receive via SMS the OTP to beentered in the appropriate field. The user will need to click on "Verify" to complete the authentication.

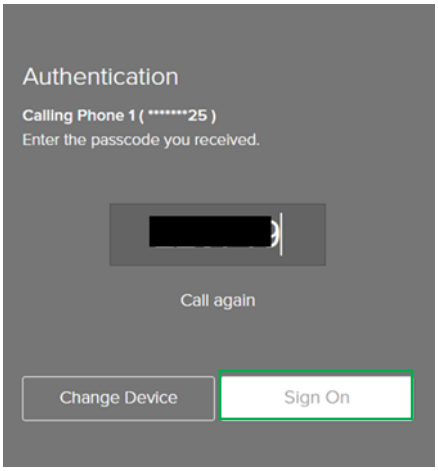


The authentication process by OTP via SMS is finished.

3.3 Authentication via VoiceCall (OTP)

After logging in with the credentials as described in Chapter 1, the user will receive a call on the configured number in which the user will be told the code to enter in the appropriate field.

The user will have to click on "Verify" to complete the authentication.



The authentication process using OTP via Voice Call is finished.

4 ADDITION, REPLACEMENT OR REMOVAL OF AUTHENTICATION METHODS FOR MFA

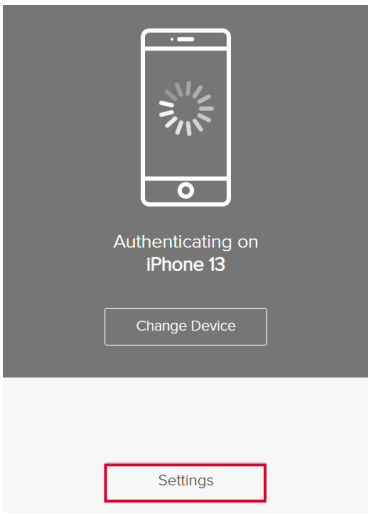
The user will have the ability to independently change the previously configured authentication methods.

Specifically, he will be able to:

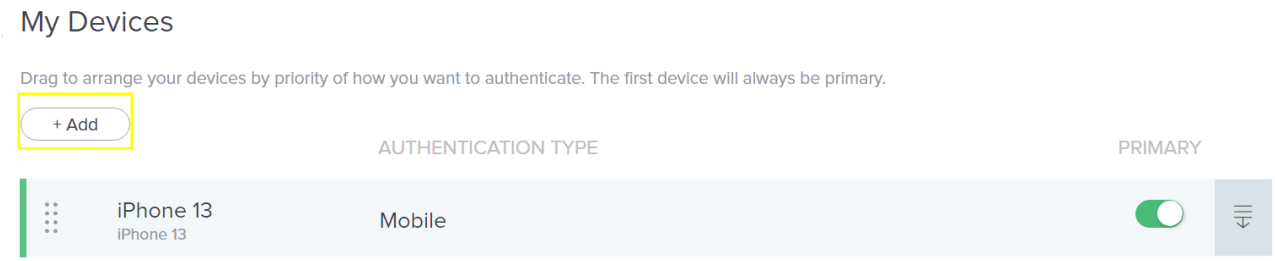
- Add a new authentication method
- Replace an authentication method
- Delete an authentication method

4.1 Configuration of a second authentication method

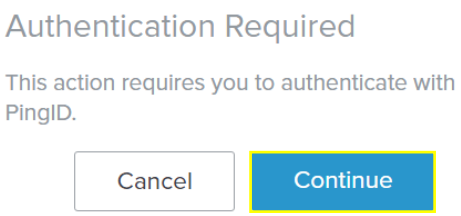
After logging in with credentials as described in Chapter 1, the user will not need to complete the authentication process via MFA but will need to click on "Settings" in order to add the second authentication method.



In the "My Devices" section, the user should click on "Add."



In order to proceed with the addition, you are required to authenticate via the previously configured authentication method. Click on "Continue" to proceed.

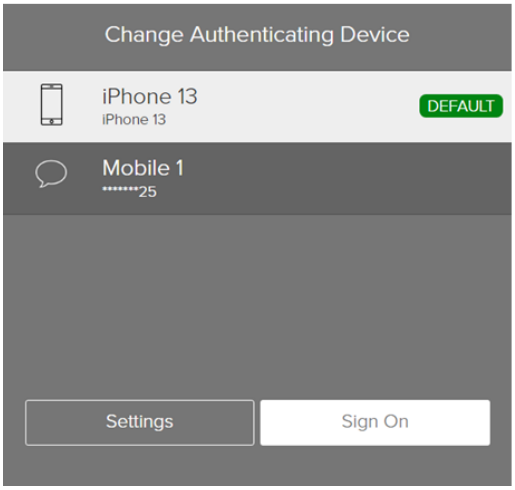


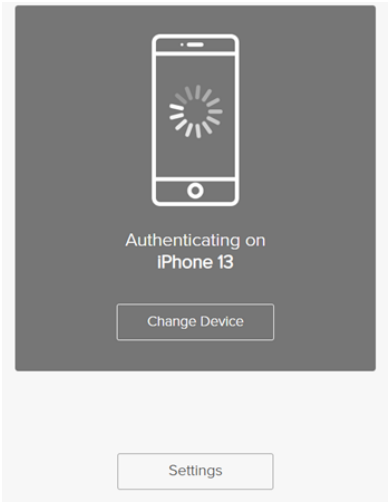
Once the authentication process is complete, please refer to Chapter 2 - "Choosing the Method and Device Pairing" for the steps to follow to configure the second chosen authentication method.

Next, the user can verify in the "My Devices" section that the addition of the second device was successful.

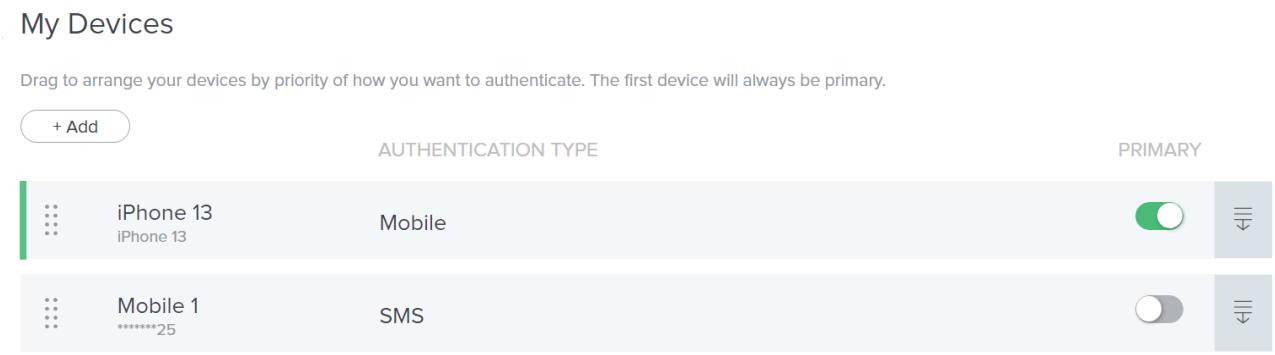
4.2 Removal or replacement of an authentication device

After logging in with credentials as described in Chapter 1, the user will not need to complete the authentication process via MFA but will need to click on "Settings" in order to add the second authentication method.



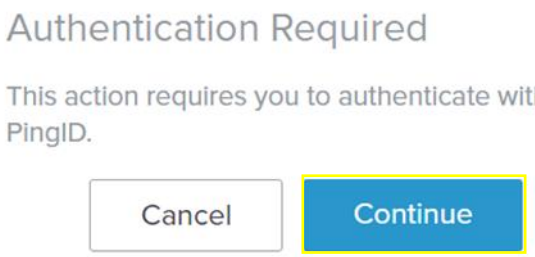


Next, in the "My Devices" section, the user can choose which authentication method to delete by clicking on the highlighted arrow.



The user is asked to authenticate via one of the previously configured authentication methods.

Click on "Continue" to proceed.



Next, the user can click on the highlighted arrow associated with the authentication method they want to delete and click on the trash can icon to proceed.