Index

1. Connection to the portal ................................................................. 3
2. MFA (Multifactor Authentication) Configuration ............................. 4
   a. Multifactor authentication through PingId mobile application.......................... 5
   b. Multifactor authentication via email ........................................................................ 8
   c. Multifactor authentication via SMS or Call ................................................................. 10
3. Change or recover the password ..................................................... 12
   a. Change my password ................................................................................................. 12
   b. I have forgotten my password ................................................................................... 13
4. Most common problems ..................................................................... 17
   a. How to change MFA authentication device / mechanism ........................................ 17
      i. I still have my old device ......................................................................................... 17
      ii. I do not have the old device (loss, theft, break, etc.) .............................................. 19
   b. I have forgotten the mobile phone that I have enrolled in PingId .......................... 22
   c. I have no signal coverage and I do not receive the PingID notification in the app ... 24
   d. My camera is broken or I cannot scan QRs ............................................................. 25
1. **Connection to the portal**

Once the portal is loaded, the authentication window will be displayed, where you must enter the credentials and select "Sign On".

Then, **if the credentials are valid**, one of the following things will happen:

1. User can access the web portal, in this case the user can proceed as usual.
2. PINGID welcome window appears. **This message usually only appears once**, and you must follow the steps described in section 2 "MFA (Multifactor Authentication) Configuration".
3. A validation of the authentication multifactor is requested via mobile application, email, SMS or call, … as established in step 2.

For security reasons, once you have finished using the application, you must log out.

*If you have any access problem that you cannot solve with this manual, please contact the person responsible for your user at Repsol.*
2. MFA (Multifactor Authentication) Configuration

If the credentials are correct, and only during the first access, the multifactor app welcome window will appear, where the user must select “Start”.

Subsequently, the following window will appear, where the user must choose the second authentication factor of their choice:
a) through the PingID application of the mobile device or
b) some of the methods that appear in “Other Authentication Methods” or “Otros métodos de autenticación” such as SMS, Voice or Email.

The steps to configure the multifactor authentication with PingID based on the authentication method chosen by the user are detailed below.

**a. Multifactor authentication through PingId mobile application**

If the mobile application is chosen as the second factor authentication method, the following steps must be followed.

1. Go to the Apple App Store or the Google Play Store, download and install the PingID app, accepting all authorization messages. (Android devices will require a version 7 or higher).
2. A QR code will be shown on the computer screen where you are trying to log in.
3. Use the PingID app downloaded on the mobile device to scan the QR code. It is possible that PingID asks for permissions to access the location, if this happens, accept them:

a. You can also enter these numbers manually, instead of using the QR code.
4. At this point, you will have configured multifactor authentication with the mobile application. The multifactor usually consists of swiping the red ball that appears on the mobile device screen, as shown below, but it is also possible to use biometric authentication if the device allows it and is configured.

5. The browser will report that the process has finished, and a similar message will be shown on the screen of your mobile device.
b. Multifactor authentication via email

If the option "Email" is chosen in "Other Authentication Methods" to add the corporate email as the second authentication factor, the following steps must be followed.

1. Check the email address that appears on this form and select "Next".
2. A verification code will be requested and received after a few seconds (it should not take more than a minute) at the email you have entered previously. Then you must choose the option "Verify".

![Verification Code Image]

3. In the following image you can see an example of an email that contains the verification code.

![Email Example]

4. If the code is correct, the authentication will be successful, and the portal will be accessible. You will also receive an email confirming that the email has been added as a second authentication factor.

**New authentication device added**

The following device was successfully added and can be used to authenticate with PingID at Repsol Prep.
c. Multifactor authentication via SMS or Call

If the option "SMS" or "Voice" is chosen in "Other Authentication Methods" in order to add the telephone number as a second authentication factor, the following steps must be followed (both methods are configured in the same way):

1. Choose in "Other Authentication Methods" or "Otros métodos de autenticación" the option "SMS", "Voice" or "Voz" to include the telephone number as the second authentication factor.

! Important: THIS WILL BE THE PHONE WHERE YOU WILL RECEIVE AN SMS OR CALL IN THE FUTURE. CHOOSE A NUMBER YOU USE REGULARLY AND A NON-SHARED DEVICE.
2. Select the country of your phone number and enter it.

2. You will receive, at the number provided, an SMS or a call with a written or dictated access code, respectively. On the next screen enter this access code and click on “Verify” or “Verificar”.

3. Finally, it will be indicated on the screen of the device that it has been successfully enrolled and you will receive an email indicating that the second factor mechanism has been configured correctly.
3. Change or recover the password

a. Change my password

To change the password follow these steps:

1. Click on the link “Change my password”.

2. Write all the requested data and click on “Submit”, if all the data are correct, your password will be changed (image 2).
ATTENTION: Your new password must comply with the following policies:

Your password must contain at least 10 characters, cannot use the last 24 passwords, and must meet at least 3 of the following 4 conditions:

- Have an uppercase letter (A-Z)
- Have a lowercase letter (a-z)
- Have a number (0-9)
- Have a special character (~! @ # $ % ^ & _ - + = ' | ' ( ) ; " ' < > , . ? / )

You can only change the password once every 24 hours.

b. I have forgotten my password

If you have forgotten your password, you can create a new one by clicking on "Forgot Password?" or "He olvidado mi contraseña" and follow the steps detailed below.
1. Write your username or email in the username field and click on “Send Request”.

2. Next, you will receive an email with the verification code that you will have to enter.
3. Enter the verification code on the screen that will show.

4. Finally, you will have to enter your new password and confirm it.
5. Once the password has been changed and if it meets the complexity requirements, you will receive an email indicating that the change has been successful.

Hello
Your password has been reset. You can now use your new password to sign on.

If you didn't make this request, please contact your administrator.
Best Regards,
Your PingFederate Team
4. **Most common problems**

   a. **How to change MFA authentication device / mechanism**

      i. **I still have my old device**

   In the event that it is required to change the device where you have the PingID application and you still have access to the old device, *(otherwise and if you do not have the device go to I do not have the old device (loss, theft, break, etc.) section)* the procedure is as follows:

   1. Log in with your usual credentials. At that moment this screen will be displayed, where you will have to click on "Settings" or "Configuración"
2. Next, the following screen will be displayed, where you will have to select the option “+ Add” or “+ Añadir” to add a new MFA authentication device.

3. After clicking the button, authentication will be requested on the main device. Once authenticated, the option of adding a new authentication device will be offered, the process of which is detailed in the section “Connection to the portal”.

Finally, the new added device should appear.
ii. I do not have the old device (loss, theft, break, etc.)

If the device used for multifactor authentication has been lost, stolen or broken, you will have to delete the old device and add a new authentication one. To do this, the following steps have to be followed:

1. Log in with your usual credentials. At that moment this screen will appear, where you will have to click on “Settings" or “Configuración"
2. Once in the configuration screen, the first thing to do is delete the old device. To do this, you will have to click on the drop-down that appears on the right and click on the delete icon.

3. Next, the user will be asked to authenticate. However, as the main device is not available, the procedure described in the section
4. **I have forgotten the mobile phone that I have enrolled in PINGID** need to be followed to complete the authentication. Once authenticated, the drop-down will open, and you will have to click on the delete icon (it is possible that if it takes too long, the user will be requested to authenticate again).

5. Once the device is erased, there should be none among “My Devices”.

6. Next, a new device will have to be added, for this, the option “+ Add” must be selected.
7. Once authenticated, the option to add a new authentication device will be offered, the process of which is detailed in the section "Connection to the portal"

8. After adding the new device, phone number or email, it will appear among “My Devices” and can now be used to authenticate in the portal.
b. I have forgotten the mobile phone that I have enrolled in PINGID

If you have forgotten the device used for multifactor authentication you can access your account by clicking on "Forgot your device" and follow the steps detailed below.

1. Select the email account with which to recover your account and click "Next".
2. Next, you will receive a verification code in said email.

**New Authentication Request from One-Time Passcode**

Enter this one-time passcode (OTP) to authenticate with PingID.

652673

3. Finally, you must enter this code on the screen that is shown below and click on “Sign On”
c. I have no signal coverage and I do not receive the PingID notification in the app

Even if you do not have signal, if you use the PingID app on your smartphone, you can authenticate yourself. To do this, when you have to validate yourself with the PingID app, click on the "Use code" option.

Next, you will be asked to enter the authentication code:
On your smartphone, open the PingID app, you will see a code that you can enter on the previous screen.

If the passcode does not work for you, try pressing the green "New Passcode" button on your smartphone and try again.

**d. My camera is broken or I cannot scan QRs**

PingID allows you to enter the code manually without having to scan the QR, as explained in the step: "You can also enter these numbers manually, instead of using the QR code."