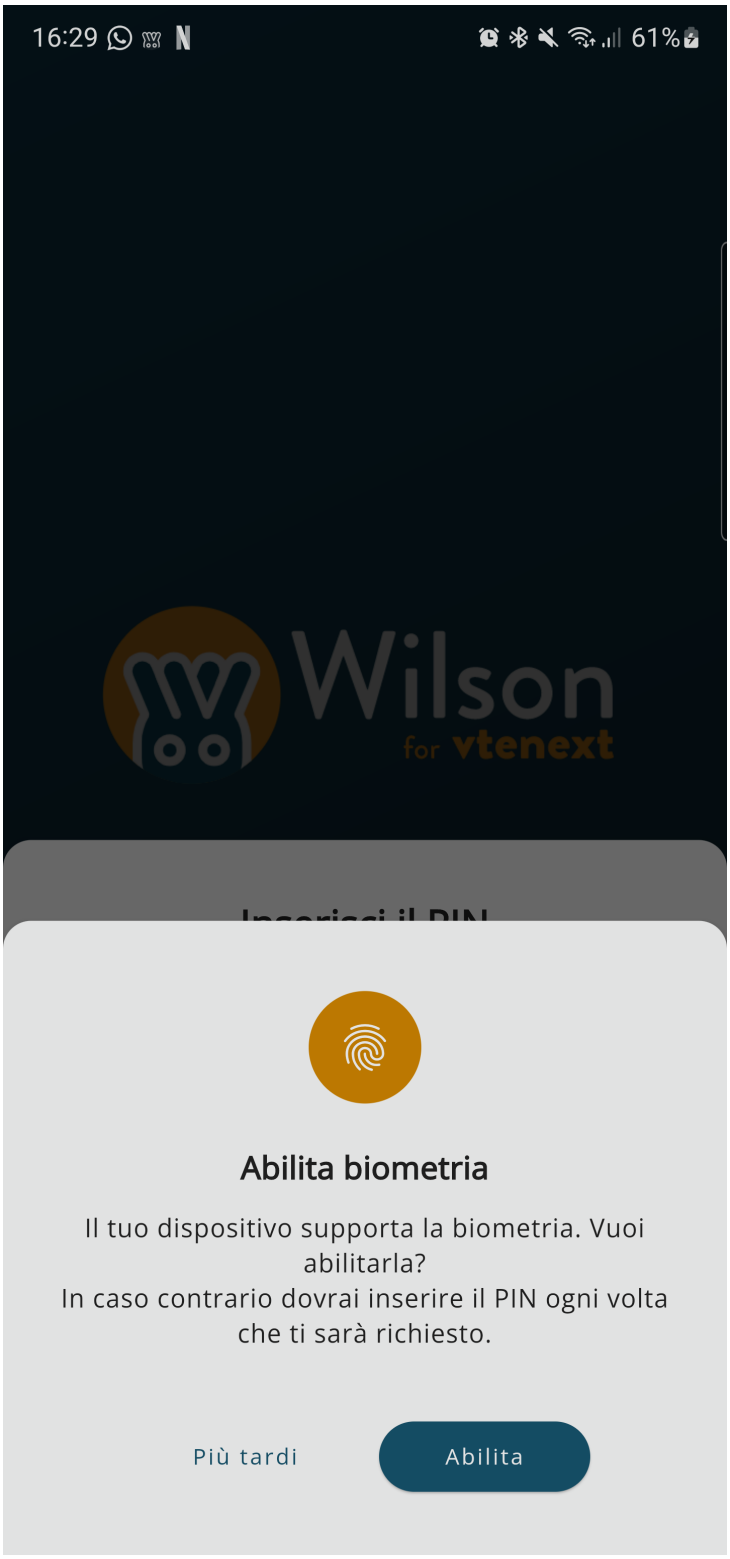
5.4 Two-factors Authentication

With the Wilson app, you can enable two-factor authentication by first configuring it in the user settings, as explained in Chapter **2.7.2 Two-Factor Authentication (2FA)**.

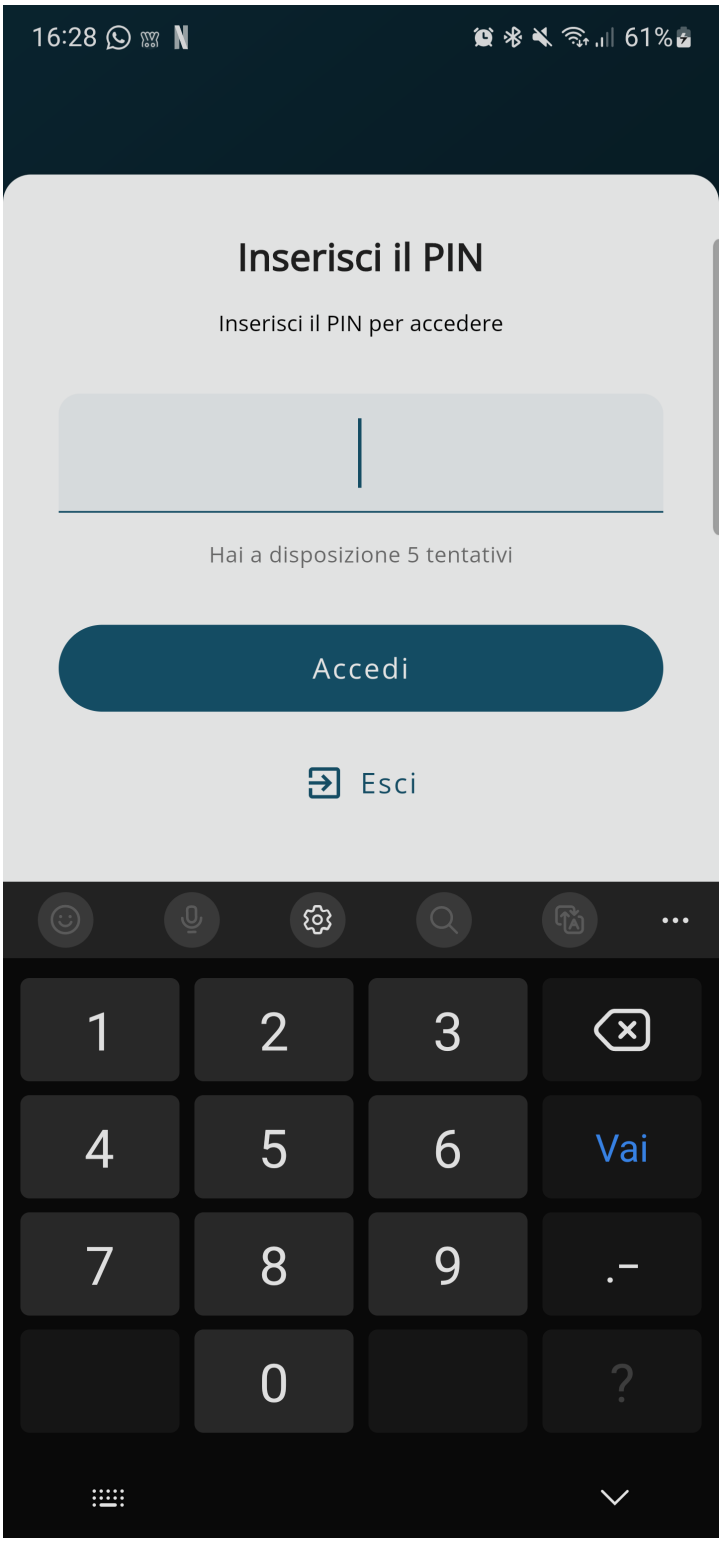
Two-factor authentication can be done in two ways:

- via device code sent by email (a 6-digit number to be entered when prompted)
- through biometric fingerprint or face registered on your mobile device

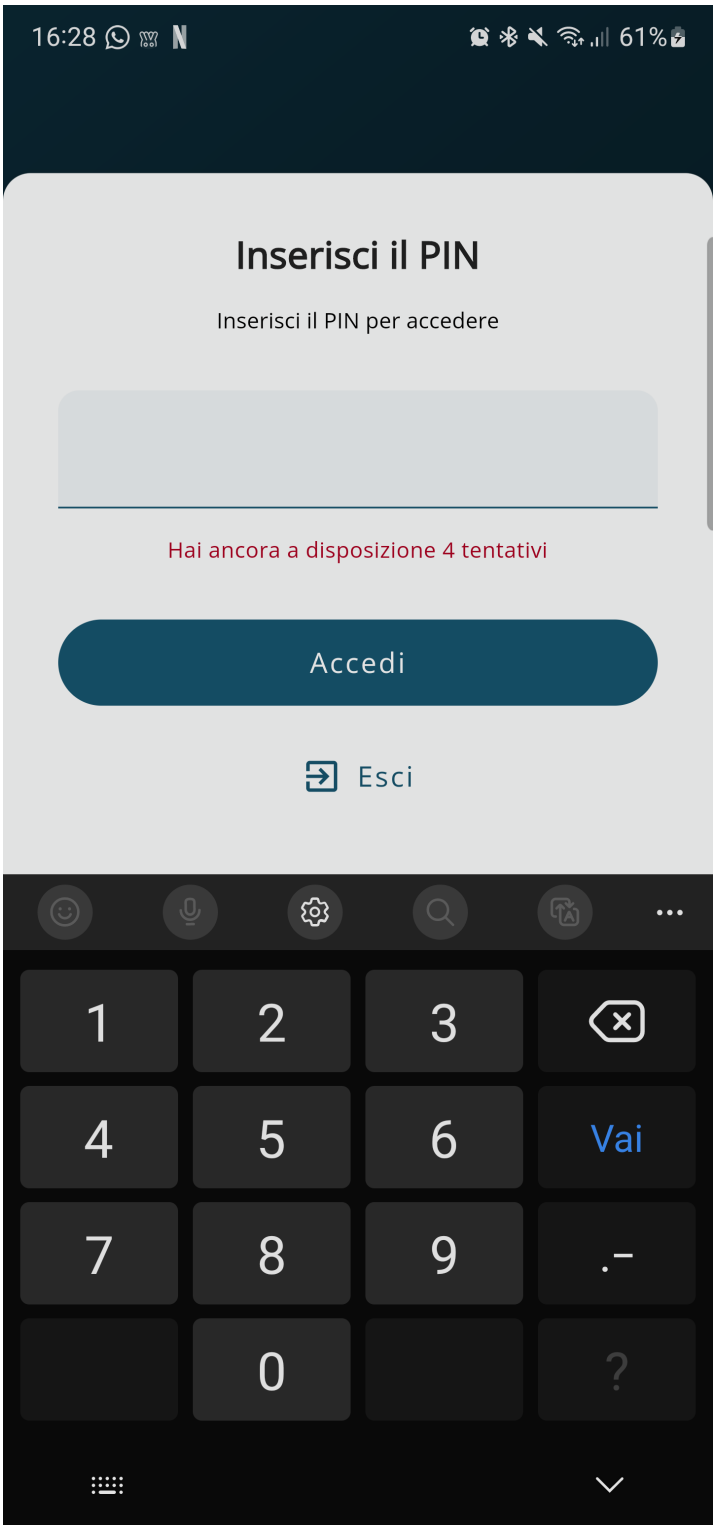
With active two-factor authentication (2FA), when accessing the Wilson app, an action will be required from the user



As a first step, upon login, you will be asked whether to enable biometrics to avoid entering the 6-digit device code that is sent to the user's email address every time.



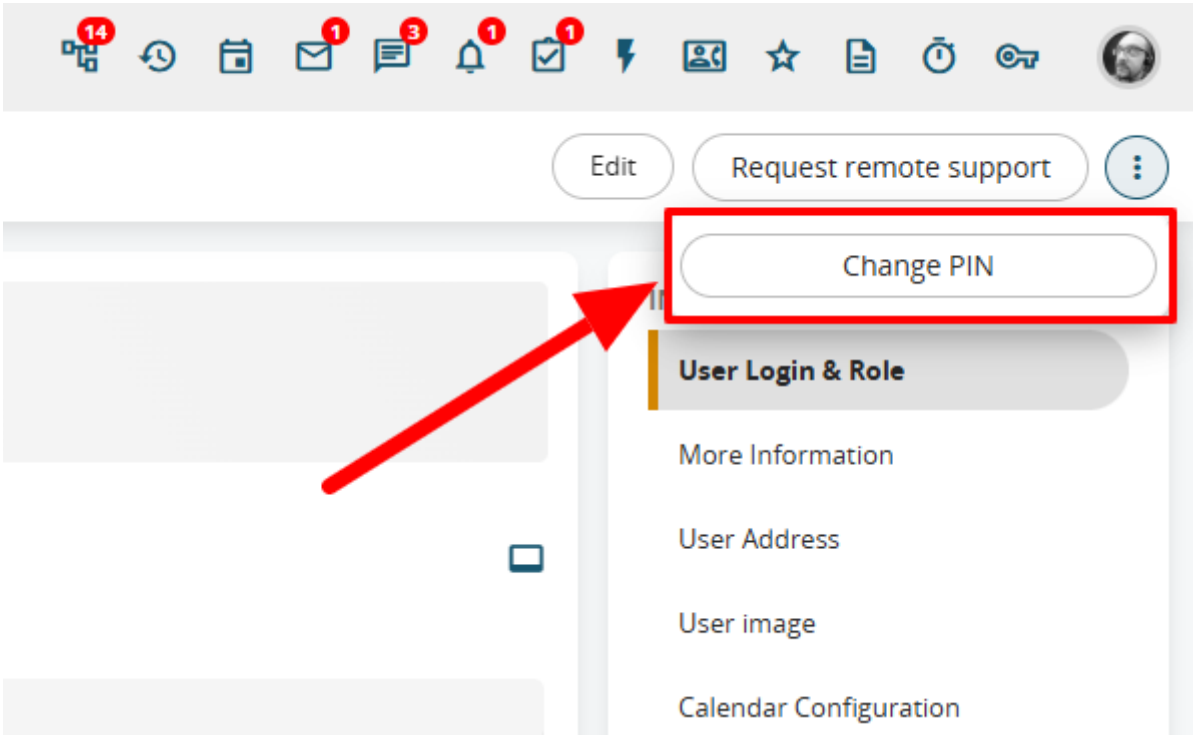
*If you have chosen to **access the Wilson app with two-factor authentication** from user settings and fingerprint access has not been activated, this is the screen that will appear. In this screen, you need to enter the code that you chose during the activation of the function (ranging from 4 to 8 digits).*



*If fingerprint access has been activated from the app settings, this is the screen that appears. Click on **Biometric Access**, and the following screen will appear:*

You will then be prompted to place your fingerprint on the sensor of your mobile device to complete the login.

If you wish to reset the **PIN** for accessing the **Wilson App**, simply log in from the web interface, go to your **User Preferences**, click the **MORE** button at the top right, and then use the **CHANGE PIN** button, as shown in the figure.



Revision #3
Created 2023-08-24 09:26:44 UTC
Updated 2026-03-25 14:36:14 UTC by Admin