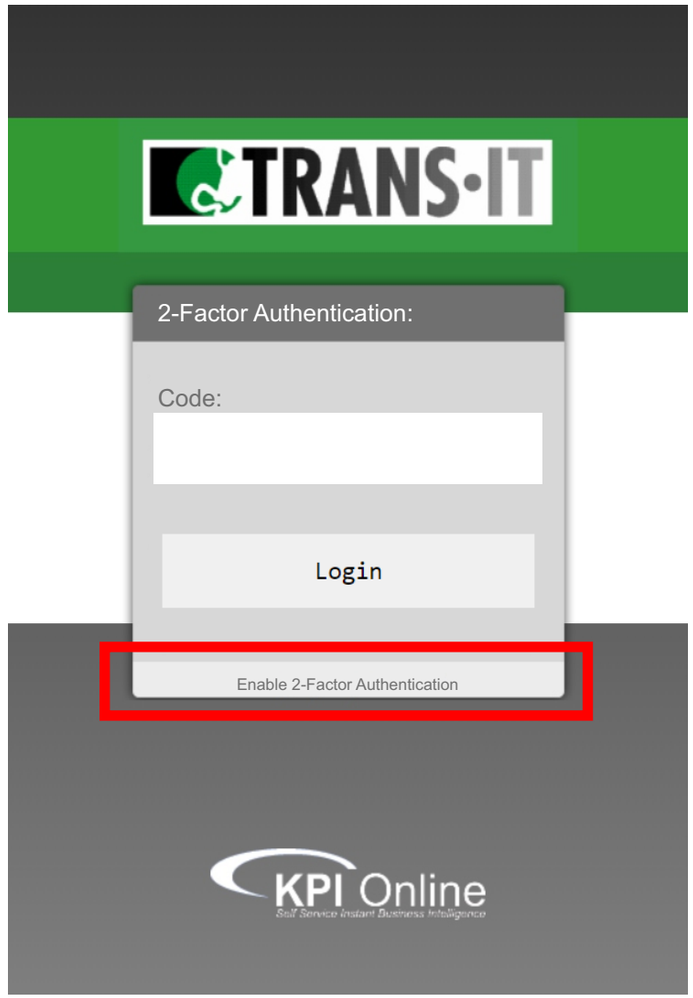
2-Factor Authentication with Google Authenticator Setup

If the 2-Factor Authentication will be enforced for all your users without notice.

Step 1:
Once the 2-Factor Authentication is enabled, when you log into your account, after entering your user name and password, instead of accessing your default dashboard, you will be redirected to a second login screen that will request the Google Authenticator code.

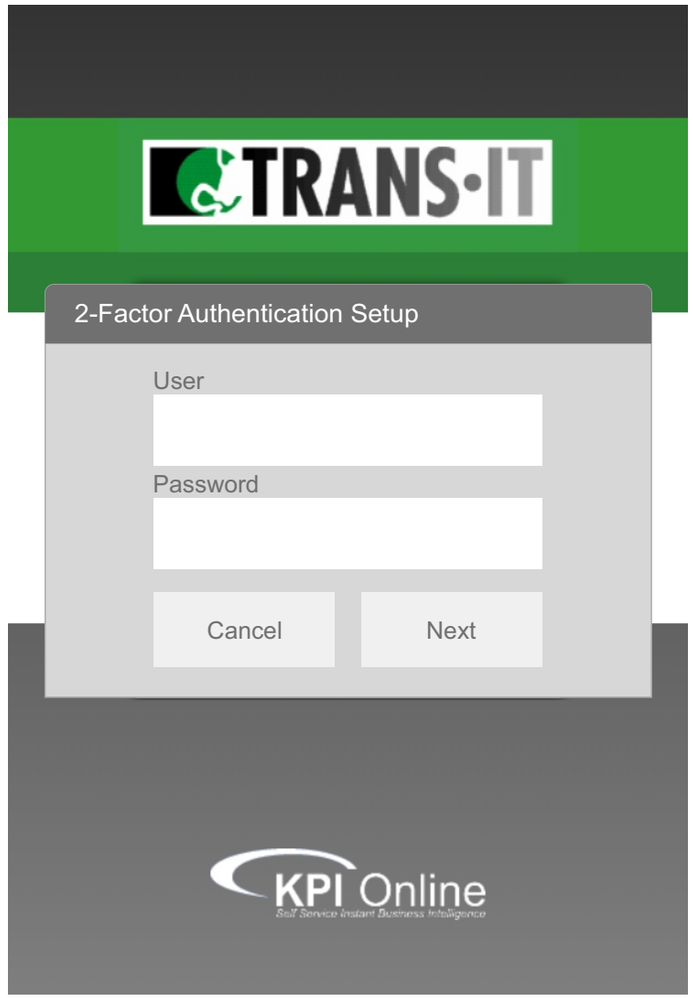
Click in the link labeled “Enable 2-Factor Authentication”, located below the “Login” button to start the setup of this feature.



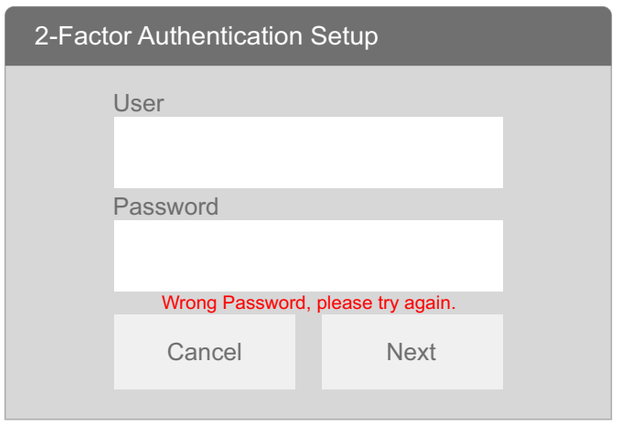
2-Factor Authentication with Google Authenticator Setup

If the 2-Factor Authentication will be enforced for all your users without notice.

Step 2:
Clicking in the link “Enable 2-Factor Authentication” will open a popup requesting you to log in again, do it and click “Next”.



Error Message:

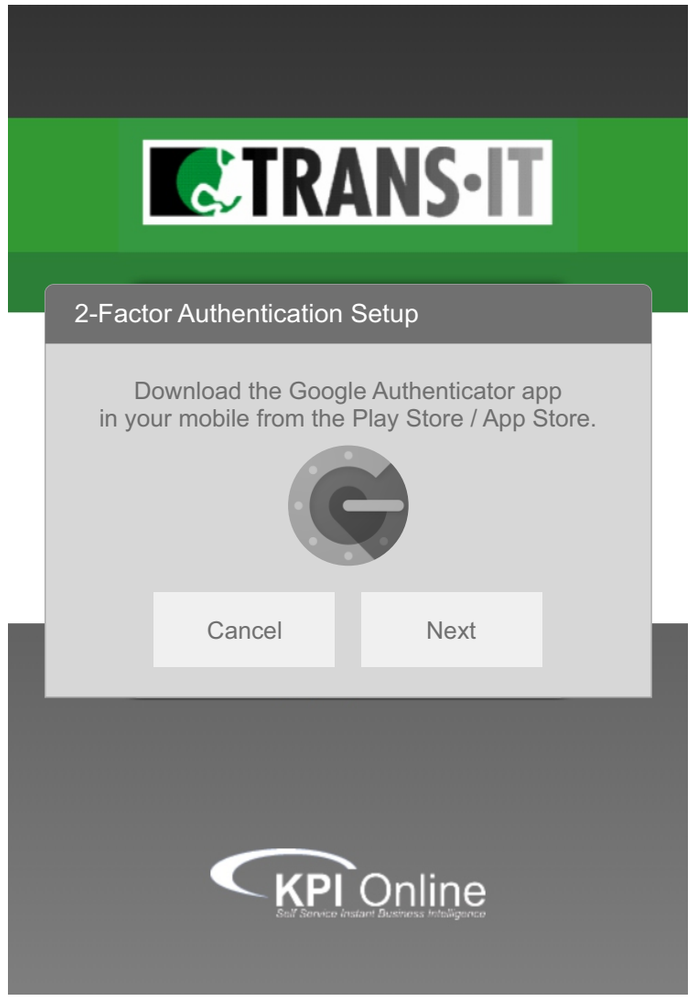


2-Factor Authentication with Google Authenticator Setup

If the 2-Factor Authentication will be enforced for all your users without notice.

Step 3:
Once your credentials are provided, Artus will promt the user to download the Google Authenticator app from the App Store / Play Store.

Click “Next”.



2-Factor Authentication with Google Authenticator Setup

If the 2-Factor Authentication will be enforced for all your users without notice.

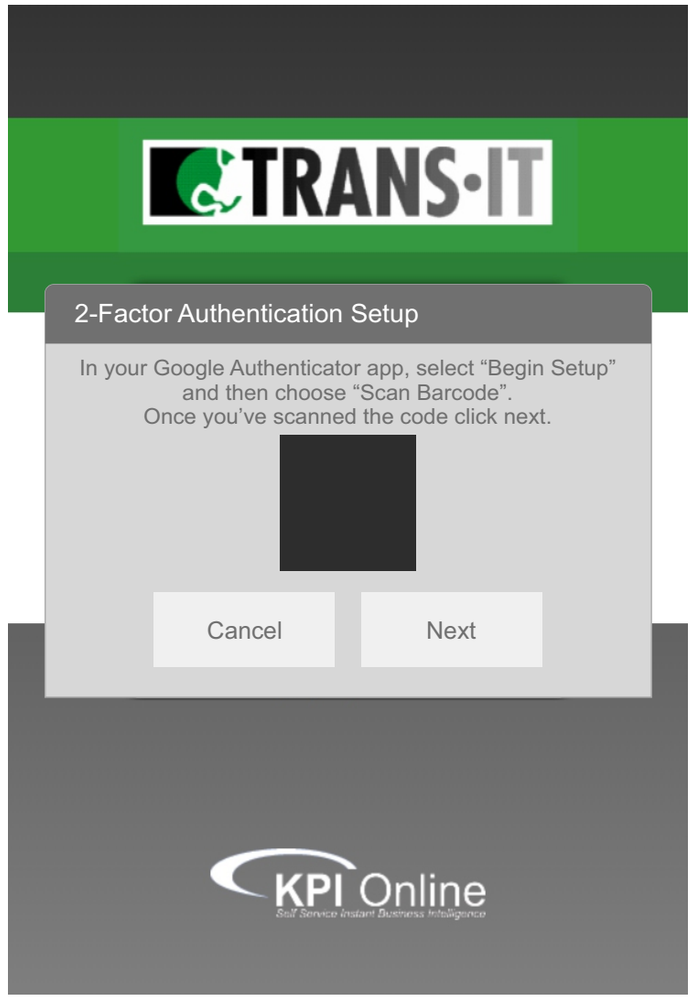
Step 4:
A QR Code will be generated.

Now, go to your device, open your Google Authenticator app, select “Begin Setup” and then choose “Scan Barcode” to enable the camera.

Go back to the 2-Factor Authentication wizard and scan the code using your device’s camera through your Google Authenticator app.

Once you’ve scanned the code, your Google Authenticator app will start generating codes.

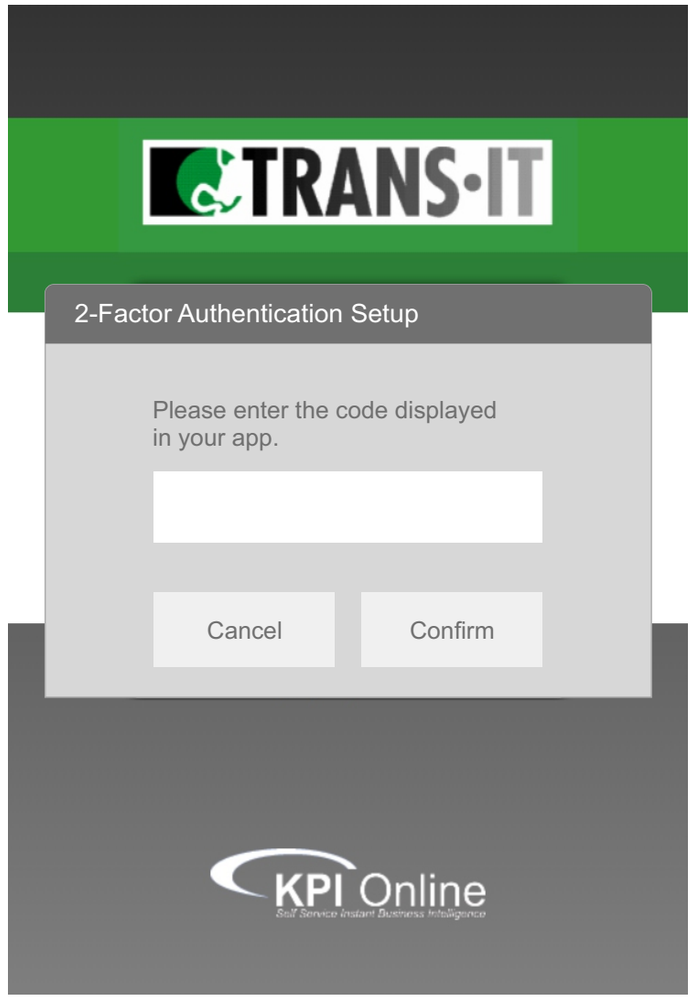
If this is the case, click “Next” in the 2-Factor Authentication wizard.



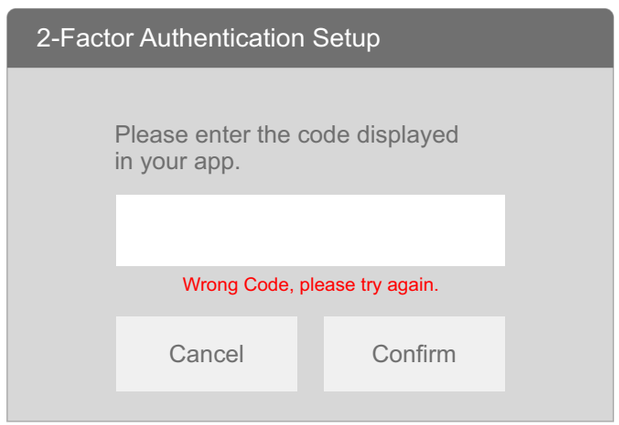
2-Factor Authentication with Google Authenticator Setup

If the 2-Factor Authentication will be enforced for all your users without notice.

Step 5:
To complete the setup, enter the code displayed in your Google Authenticator app and click “Confirm”.



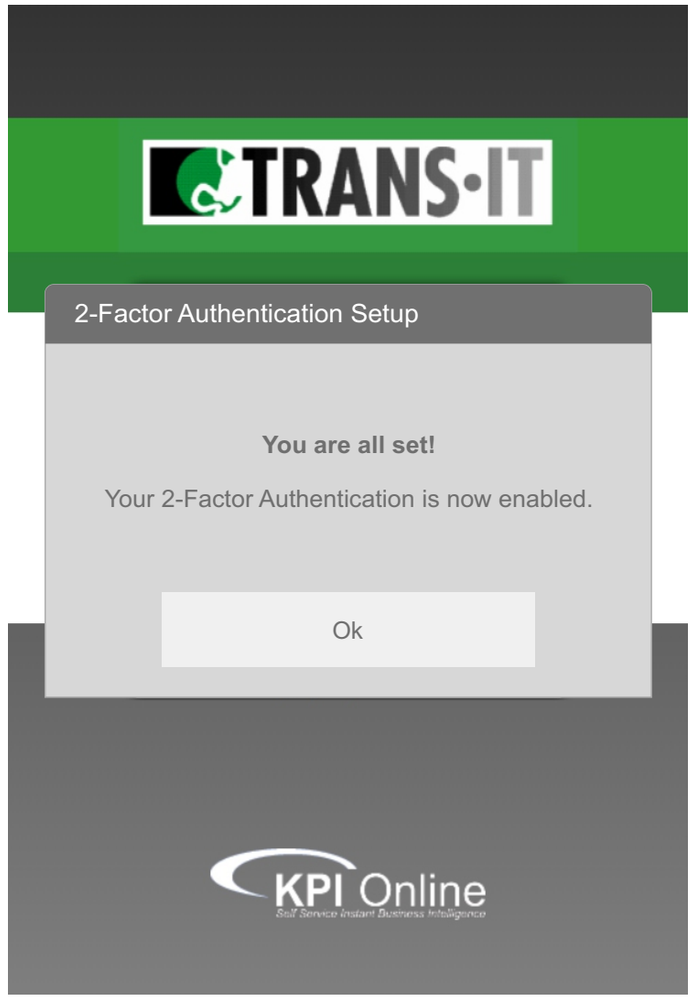
Error Message:



2-Factor Authentication with Google Authenticator Setup

If the 2-Factor Authentication will be enforced for all your users without notice.

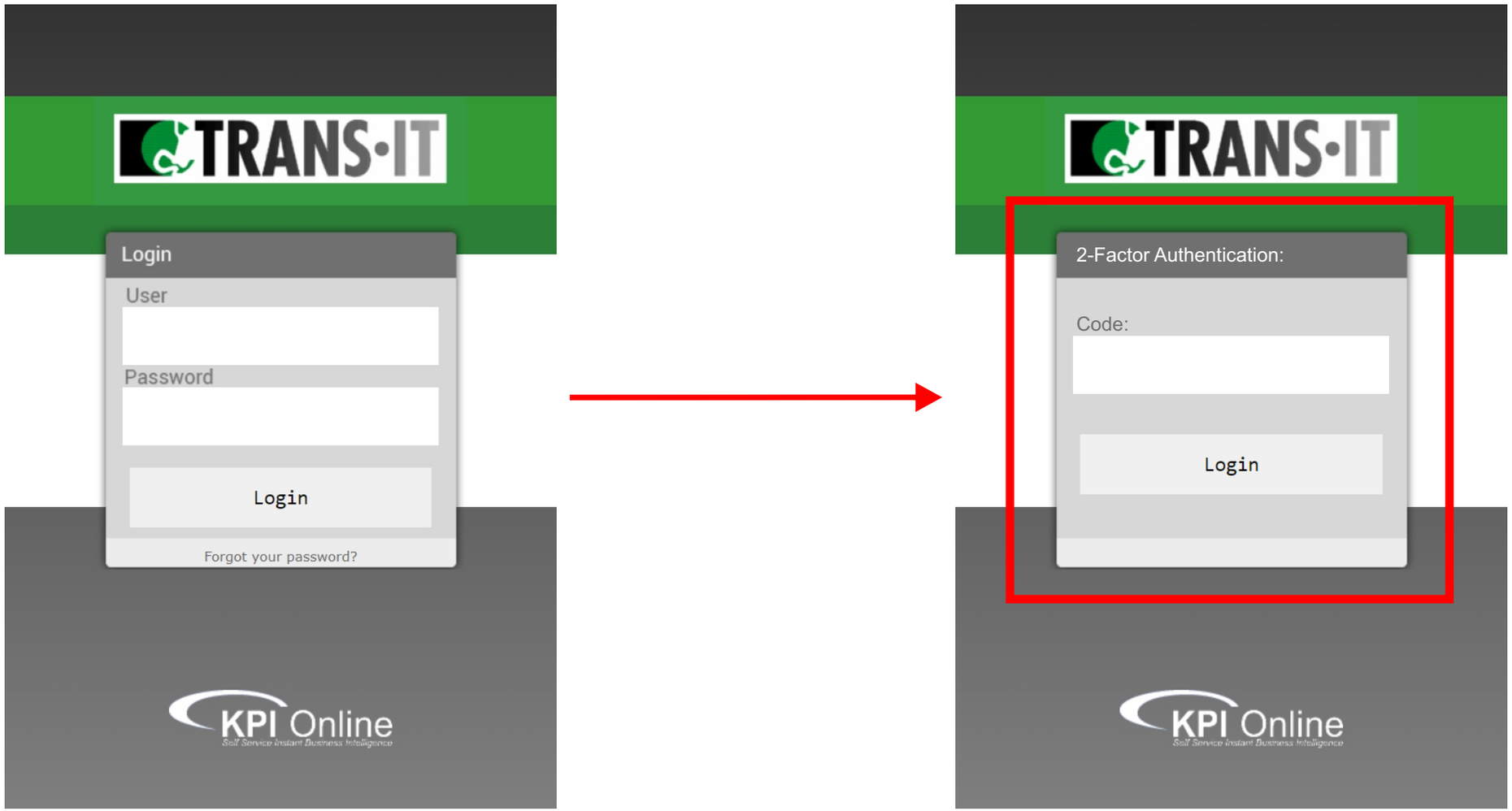
Step 6:
Finally a confirmation message will appear. Click “Ok” and now you will have your 2-Factor Authentication enabled.



2-Factor Authentication with Google Authenticator Setup

If the 2-Factor Authentication will be enforced for all your users without notice.

After clicking “Ok” you will be redirected to your Login screen, and now you will be able to access using Google Authenticator codes.



2-Factor Authentication with Google Authenticator Setup

If the 2-Factor Authentication will be enforced for all your users without notice.

Note:
Notice that once a the 2-Factor Authentication is enabled, the link “Enable 2-Factor Authentication” will be removed.

If a user needs to change its device, this would be solved manually by us, returning that specific user to a state as if he hadn’t activated the 2-Factor Authentication.

In the near future if those requests happen to be a lot, we could develop a dedicated site for the client administrator to attend those requests himself.