2-factor authentication for Customer Portal

Contents

As a part of making login more secure, we have implemented 2-factor authentication for all customers. This is using a time based code (a code that changes every 30 seconds) in addition to the username+password combination. Those are the two factors.

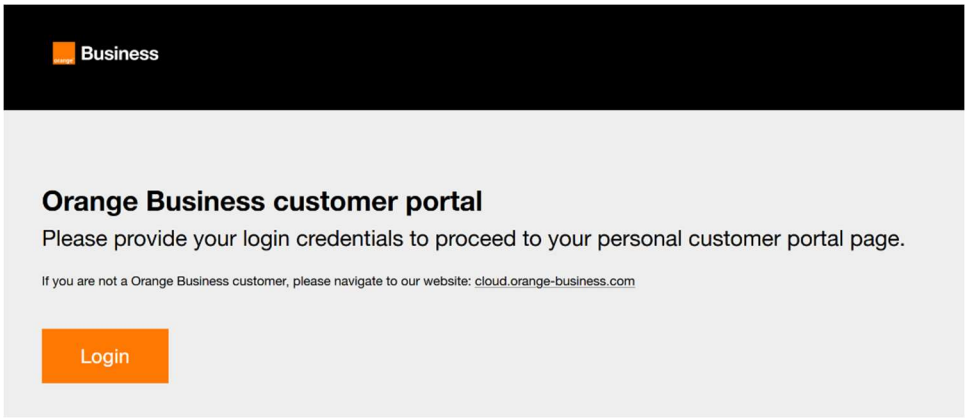
For this to work you need a mobile app which will generate the code for you. A number of free apps can be used, such as “Google authenticator” and “Microsoft authenticator”, “Authy” and a number of others, as the authentication is based on an open standard called “TOTP”.

The first time you login, you’ll be asked to setup the 2FA. This is only the first time. After that you will need to provide the code from the app when logging in.

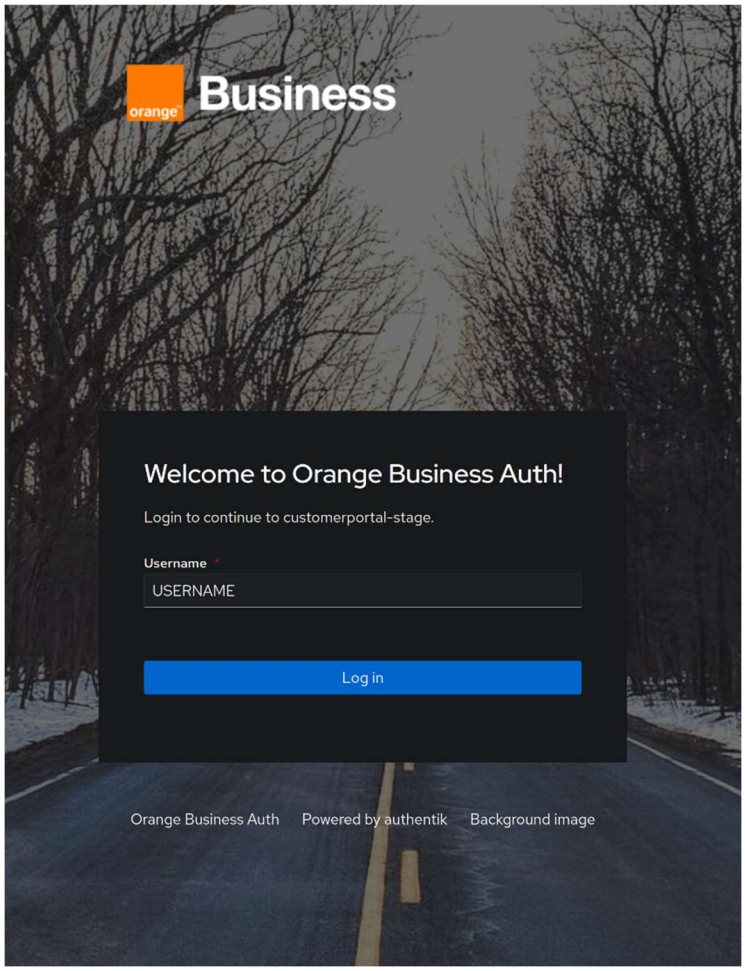
Customer portal first login steps

When you first open the customer portal page, you will be presented with the following page

Press the “Login” button.

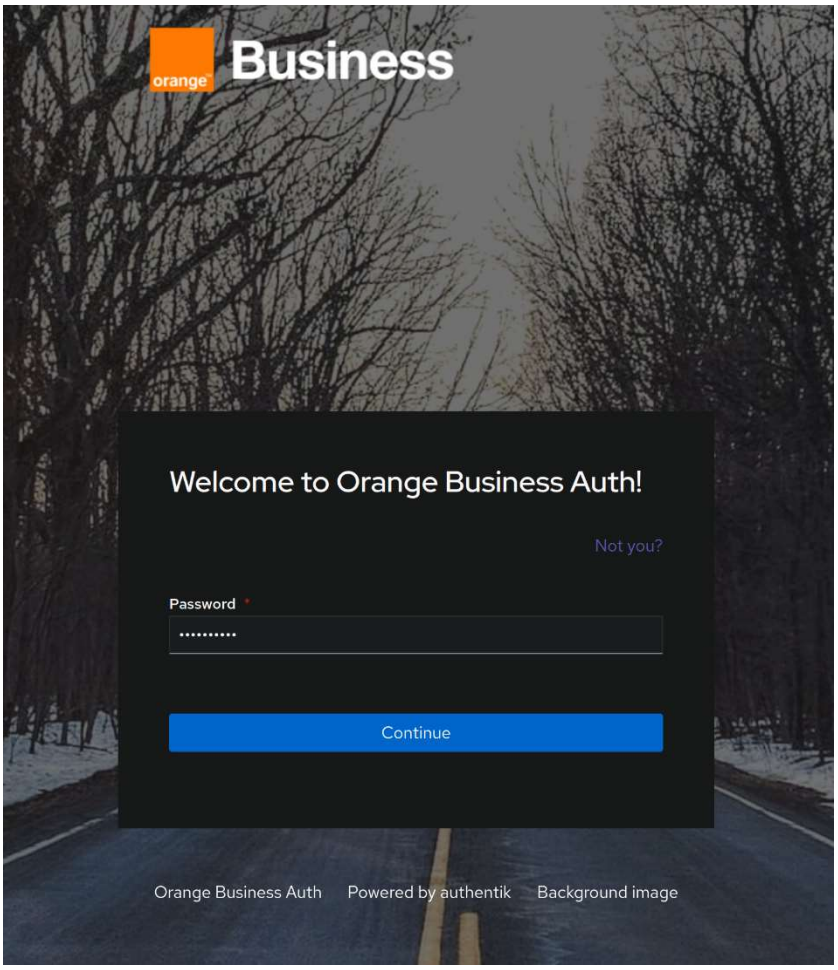


You will be redirected to the following page. Here, you are prompted to enter your username. “USERNAME” is just an example for demonstrational purposes



Enter your username and press “Log in”.

Next you’re presented with the password prompt page



Enter your user password and press “Continue”

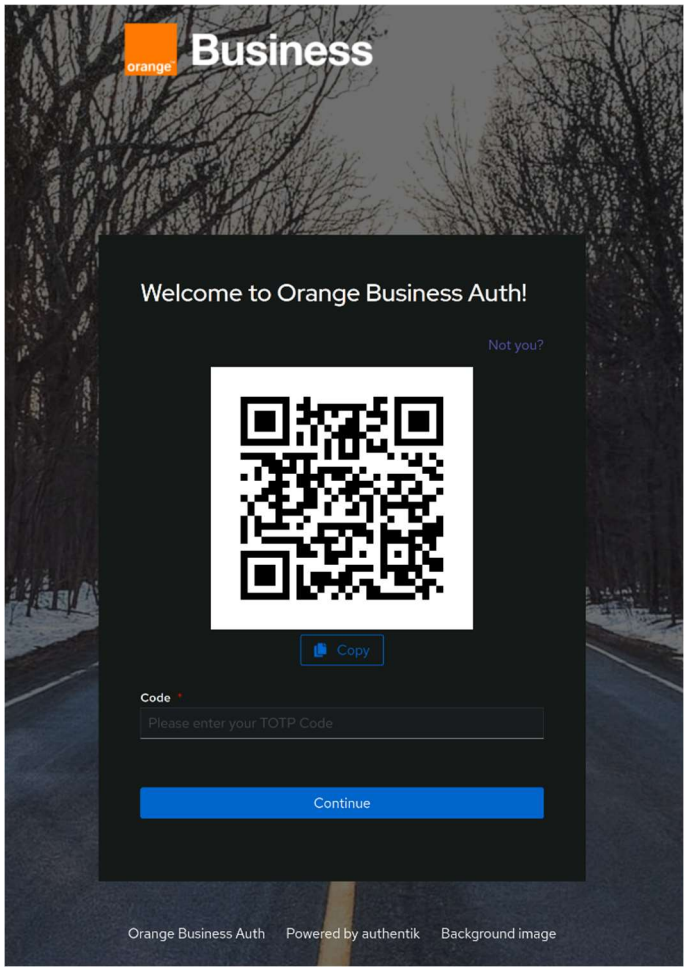
If this is your first login on our new 2FA service, you will be presented with a QR code, with a copy button below and further below, an entry prompt for your “TOTP code”. To explain simply, a TOTP code is a security code generated by a separate service or application, which has been tied to your login on this authentication service using the process you’re currently in.

Most commonly, TOTP authenticators can be certain apps on one’s phone, though there are other such authenticators one can use as well.

You’ll most likely be using your phone. Common TOTP authenticators are “Google authenticator” and “Microsoft authenticator” (Creative names, I know). We can recommend Google authenticator, as it is quick and easy to use. They can be found on both the App Store and Google play store.

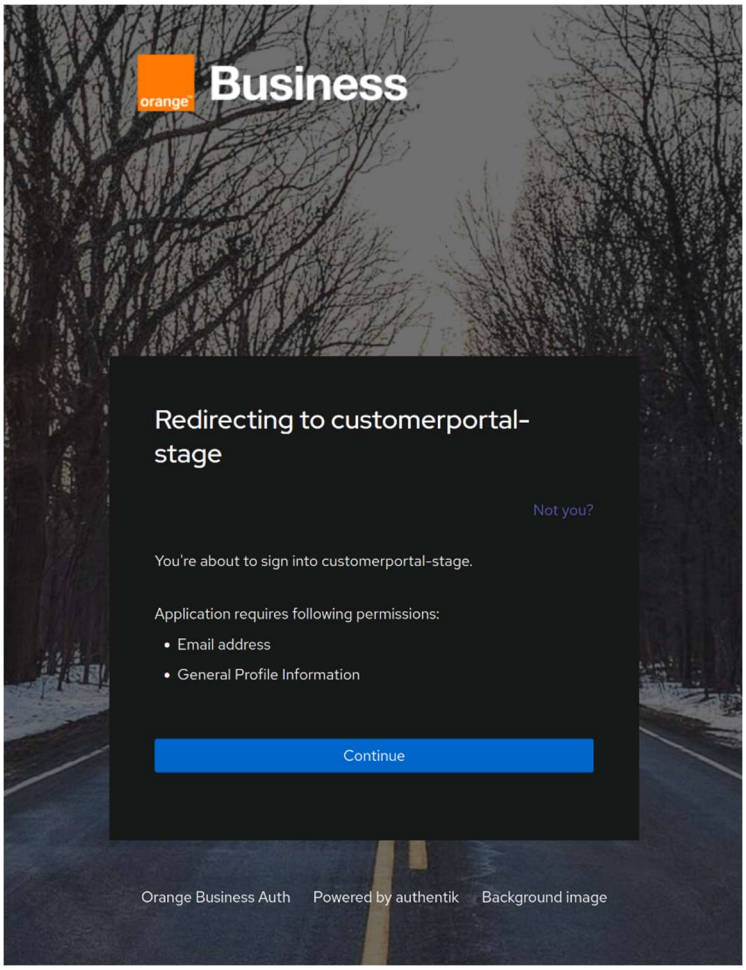
Once you have one, open your TOTP authenticator and look for an “add new service” functionality. For example, some “+” button. On Google authenticator the +-button expands to a choice set. Choose “Scan a QR code”. Now point your phone camera at the QR code enough for the entire graphic to be within the scanning border of the app. Very quickly this should add an entry to your TOTP authenticator named “Orange Business: [username]”, where “username” is your username, and you’ll see a 6-digit code and

some lifetime indicator. This lifetime is just the time when the TOTP code is regenerated. Whenever you log in, you will be using the then current TOTP code.



Enter the TOTP code you've been given, and press "Continue".

You should now be on a redirection page.



Press “Continue”

Now, your 2FA authentication for the customer portal has been set up and you should be able to log in using the TOTP authentication code as multifactor authentication whenever you wish to log in to the customer portal.

If you encounter any problems with the process, please contact our customer support

Customer Portal subsequent logins

After the initial setup, every time you login you will be asked for username and password, and also a code.

This code is the code you will get from the authenticator app you used. It will change every 30 seconds.

A note about log out

The 2-factor authentication is using Orange Business Single Sign-on system. Logging out from customer portal does not log out from the whole single-sign on system. This is similar to logging into a webpage using “Google” or “Facebook”. Logging out of that webpage doesn’t log you out of Google or Facebook.

I.e. when logging back in, you won’t need to specify your google/facebook password again.

Customer Portal works the same way. Even if logged out of customer portal, you can click Login and get logged in without “logging in”, because you are logged in the Orange Business’ Single Sign on.

You will be automatically logged out from the whole single-sign on after 12 hours.