

Mobile UniOTP Usage Guide

Mobile UniOTP First launch and Settings

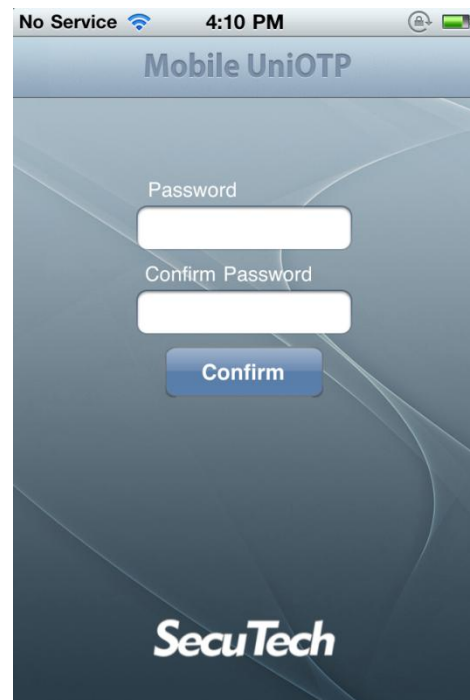
This is the screen you will see the first time you use Mobile UniOTP.

At this step, you must step the password to access the application.

Fill in the fields [Password] and [Confirm password] and click the [Confirm] button.

The next time you will launch the application, this password will be requested.

If you forgot the password, please delete and reinstall the application on your device. In this case, you will need to synchronize your One Time Password application with the server once again.



Once you have finished setting up your password, you will be redirected automatically to the main screen.

From the main screen, please click [Synchronize] at the bottom of the screen to access to the synchronization interface.



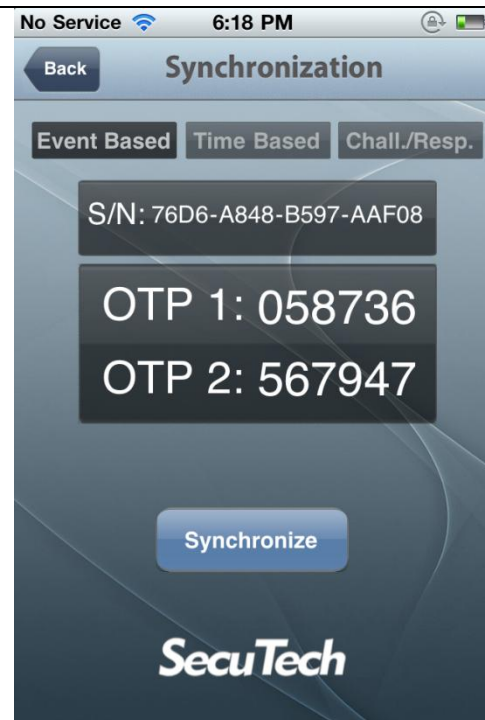
Please choose the type of One Time Password you want to use from the synchronization interface. You can choose among [Event-Based] [Time-Based] and [Challenge/Response].

Depending on the type of OTP chosen, information needed for synchronization is different. Please communicate to your administrator the information displayed on the screen.

As Mobile UniOTP won't connect to the network to send information. You should tell your administrator this information directly or through mail/phone.

If you decide to use Mobile UniOTP with OTP MGS, you will need to have a **token file**. Please send your synchronization information to support@esecutech.com to get the token file corresponding to your device. We will give you an answer within 24 hours.

If you decide to use UniOTP API (included in UniOTP SDK), you can use directly this information.



Once information communicated to your administrator, click the [Synchronize] button to apply changes.

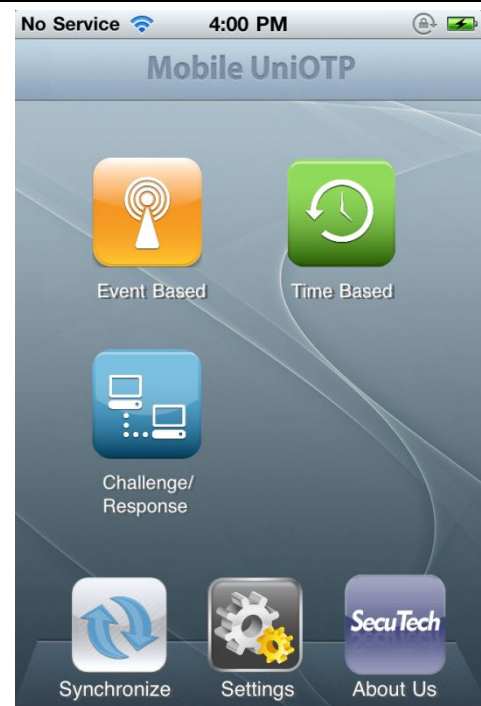
If you go back to the main screen without clicking the button, synchronization information will not be changed and you will not be able to use the One Time Password. Make sure to push the [Synchronize] button before going back to the main screen.

A message will be displayed if the synchronization succeeded.

Every time you open the Synchronization interface, new synchronization information is generated, but it is only saved if you click the [Synchronize] button.



Once back to the main screen, choose the icon corresponding to your type of OTP in order to access to the OTP generation interface.

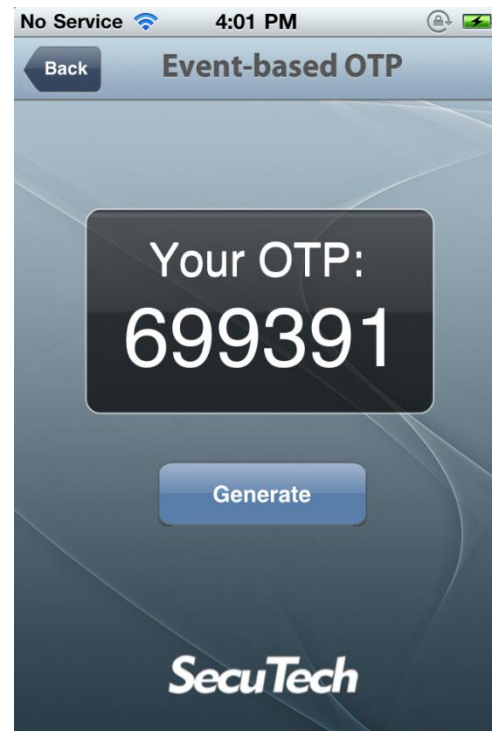


Event-Based

Every time you access the Event-Based OTP generation interface, a new password will be automatically generated.

If you are already on this screen, you can push the [Generate] button in order to generate a new password.

⚠: If you switch back and forth between the main screen and this screen, or if you push the button too many times, the OTP may get desynchronized and need to be synchronized again.



Time-Based OTP

A new password is generated automatically every 60 seconds. Even if you go back to the main screen and come back to this interface, if 60 seconds have not passed, the password won't change.

There is no way for the user to urge the generation of a new password.

⚠: If the device time get desynchronized from the server time more than it is allowed, the device may get desynchronized. Make sure to not change the time of your device after you have synchronized it with the server.

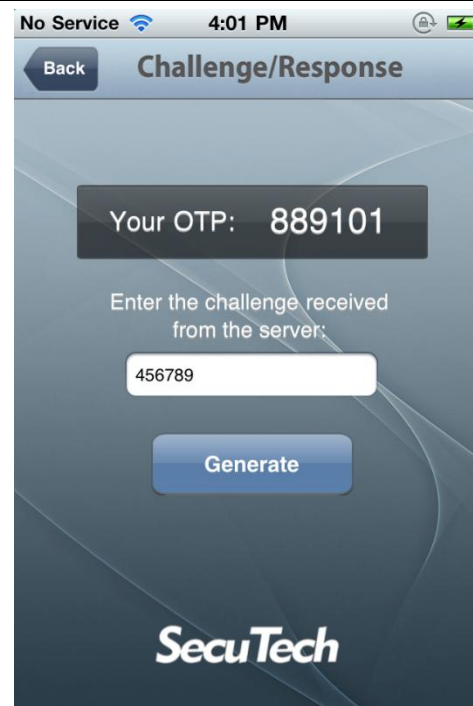


Challenge/Response

In order to generate a OTP, you must first input the challenge code received from the server.

Example of Use:

After the user logged in the website, the server will display a challenge code to the user and asks to input the corresponding OTP for this code. The user inputs the challenge code on this interface to calculate the correct OTP. In this way, we can even strengthen the authentication process security.



Other settings

From the [Settings] screen, you can perform operations listed below.

- Change password to access the application
- Show the S/N (Serial Number)
- Show the device time



