FOTA WEB Account Settings

□

Contents

Settings

You can find **FOTA Web Settings** at the top-right of the page, there you are able to change web page language, generate API tokens, change account password and set your own time zone. More details about the functions are explained below.

Language

In the settings tab window you can select your preferred language. Currently there are 6 available languages:

- English
- Lithuanian
- Russian
- Spanish
- Portuguese
- France

API tokens

You can generate Token ID in the API Tokens window by clicking **Add token**, set a Token name and then click generate. This will generate FOTA Web API Token with which you can use it to integrate FOTA Web functionalities on your existing software system.

Full FOTA API documentation can be found **HERE**.

Change password

If your current password is too difficult to remember or not secure enough and you want to change it, you can freely change your password by entering your current password and then the password

you want it to be changed to.

If you do not remember your current password, in FOTA WEB initial window you can click forgot password. It will generate a link for resetting your password and send it to your email address.

Time zone

Time zone functionality lets you freely change how page will display time in different time zones. Changing it will change time information on when device was **Seen at**, **Created at** or **Updated at**.

Two-factor authentication

NOTE: We highly recommend using this feature as it will help you to protect your account from intruders

To improve user security and protect against unauthorized intrusions, Two-Factor Authentication (2FA) functionality was added to FOTA WEB.

This feature allows you to add Microsoft Authenticator or Google Authenticator or Email authorization in addition to your existing password.

If 2FA is enabled, the user will not only have to enter the correct email and password, but also a unique code generated by the chosen authentication service or code received via email is needed in order to successfully log in.

Enable 2FA

To enable 2FA, select "Settings" -> "Security" and click "Enable" button in the "Two-factor authentication" field.

After that, the user will have choose authentication method.

How to enable 2FA

Authentication via app

Select Authentication via app method

After choosing authentication via app method press "Next " button

Continue with Authentication app method

After that, the user will see a window where links to authorization methods will be provided, by clicking on which the user can get detailed instructions on how to work with them.

enter 2FA code

After pressing the button "Continue" the user should scan the displayed QR code with the help of authentication application on phone and enter the code provided by the authorization service.

NOTE: If you are unable to scan the QR code using the authenticator application, click on "Click here to manually type the code instead" to enter the code manually.

After clicking on the "Verify" button, if the code is correct, 2FA will be activated. If the entered code is incorrect, 2FA won't be activated and you will see an error on your screen.

In addition, the user will receive an email from FOTA stating that two factor authentication has been successfully enabled.

2FA account verification

On the next login into your account, in addition to the standard login and password you will be asked to enter a 6-digit code generated by the authenticator application you activated in previous steps.

Authentication via Email

Select Authentication via email method

After choosing authentication via app method press "Next " button

Send Authentication code via email

Enter verification code from the email

Before clicking the "Next" button, the user should verify that their email address is correct. Then, need to click the "Send code" button to receive a verification code via email.

Enter the verification code you received into the verification field.

After clicking on the "Verify" button, if the code is correct, 2FA will be activated. If the entered code is incorrect, 2FA won't be activated and you will see an error on your screen.

In addition, the user will receive an email from FOTA stating that two factor authentication has been successfully enabled.

On the next login into your account, in addition to the standard login and password you will be asked to enter a 6-digit code received via email.

Disable 2FA

To disable the 2FA function, just go to Settings" -> "Security settings" and click "Disable" in the "Two-factor authentication" field. The user will see a warning about disabling 2FA and after confirming the selection, two-factor authentication will be disabled. The user will also receive an email informing them that 2FA has been disabled.

NOTE: in case of password change, 2FA will be automatically disabled

Users - Previous page

Next page - **API**