Setting up Two-Factor Authentication (2FA) in HelpDesk

[Main Page](#) > [General Information](#) > **Setting up Two-Factor Authentication (2FA) in HelpDesk**

Introduction

Two-factor authentication (2FA) is a security process that requires users to provide two different authentication factors to verify their identity. These factors typically fall into three categories: something you know (like a password), something you have (like a smartphone or token), and something you are (like a fingerprint or iris scan). By requiring two different types of authentications, 2FA significantly enhances security compared to using only a password.

The reason why 2FA was introduced in Helpdesk, is to enhance security by adding an extra layer of protection against unauthorized access to sensitive data that may be shared, thereby mitigating the risk of data breaches and ensuring compliance with industry regulations.

Setting the 2FA

Things you'll need:

1.Your smartphone

2.Authenticator app (available on **Google Play Store** or **Apple App Store**)

Download APP For Android OS:

Download APP For Apple iOS:

Microsoft Authenticator

Google Authenticator

Steps:

1. Download and Install the Authenticator App (Microsoft Authenticator, Google Authenticator or similar)

1.1. Open the app store on your smartphone (Google Play Store for Android or Apple App Store for iPhone).

1.2. Search for e.g. "Google Authenticator" and install the app.

1.3. Depending on the app chosen, you may need to create or sign in with your Google or Microsoft account.

2. Sign in to Helpdesk account

2.1. Open the web browser and go to Helpdesk URL: https://helpdesk.teltonika-iot-group.com

2.2. Log in to your account using your username and password.

3. Enable 2FA and proceed with the setup

3.1. After a successful login attempt, you will be presented with a pop-up window in the middle of the screen. This window will contain a large QR code and instructions to set up 2FA using an authentication app. Leave this window open.

4. Sync Helpdesk with Authenticator app

4.1. Launch the Authenticator app on your smartphone.

4.2. Press "Add" and choose "Scan QR Code": Use your phone's camera to scan the QR code displayed in the 2FA setup window on your computer screen. If desired, secret key can be entered manually by hand, we recommend to scan it with camera.

5. Verify and Complete Setup

5.1. After scanning the QR code or entering the secret key, a new account will be added to your Authenticator app.

5.2. The app will generate a unique 6-digit code that changes every minute.

5.3. Enter code displayed in your Authenticator app to Helpdesk window.

Once you enter the correct code, the 2FA setup will be complete. From now on, with every new log in to Helpdesk, you will be asked to enter code displayed in your Authenticator app.