

The Lisbon School of Architecture Informatics Center (CIFA) has implemented a **Two Factor Authentication Method 2FA** for all users' safety.

This authentication method, used to protect online users' accounts, is a measure that adds a security layer further than the traditional username/password combination.

Please install the authenticator "**Google Authenticator**" on your smartphone.



### 1<sup>st</sup> Step:

Visit the following web link: <https://mfa.fa.ulisboa.pt>

Log in with your student's credentials (student number + password) to proceed to next step.

The screenshot shows the login interface. At the top right is a "Login" button. Below it is a light blue box with the instruction: "Enter your username and password and click Log In to authenticate." In the center, there is a large blue circular logo with a white 'U' and a yellow bar. Below the logo, the text "Please sign in" is displayed. Underneath, there are two input fields: "Username" and "Password". At the bottom center is a blue "Log In" button.

### 2<sup>nd</sup> Step:

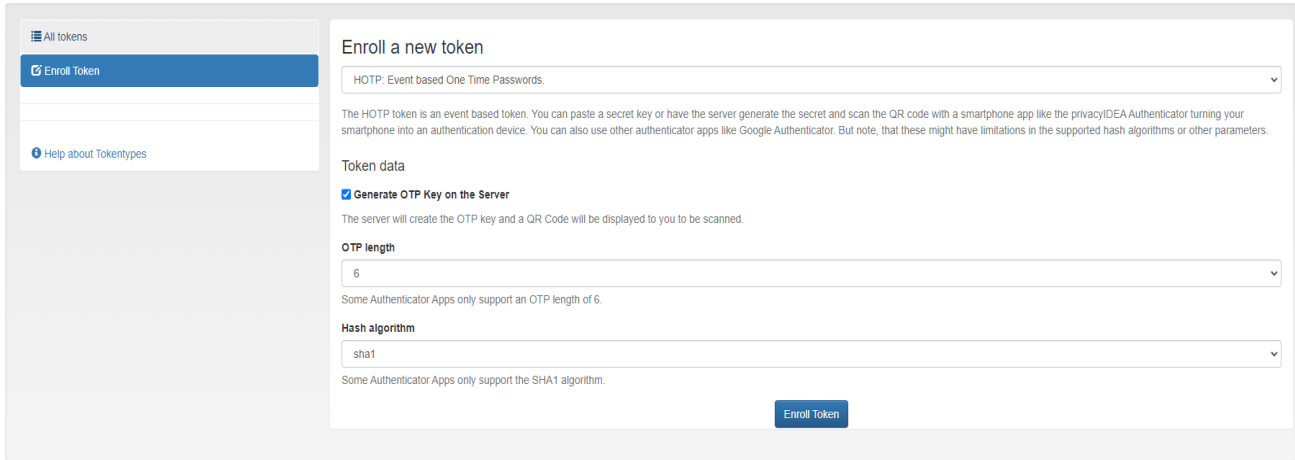
Please select "Enroll Token" on the left menu.

The screenshot shows the "Tokens" management page. At the top left is a blue circular logo with a white 'U'. To its right is a "Tokens" menu item. At the top right is a "Refresh" button and a user profile dropdown showing "dventura @egasmoniz.edu.pt (user)". On the left side, there is a sidebar menu with "All tokens" selected and "Enroll Token" as an option. The main content area shows "total tokens: 1" and a table with the following data:

serial	type	active	description	failcounter	rollout state
TOTP0042C543	totp	active		0	

### 3<sup>rd</sup> Step:

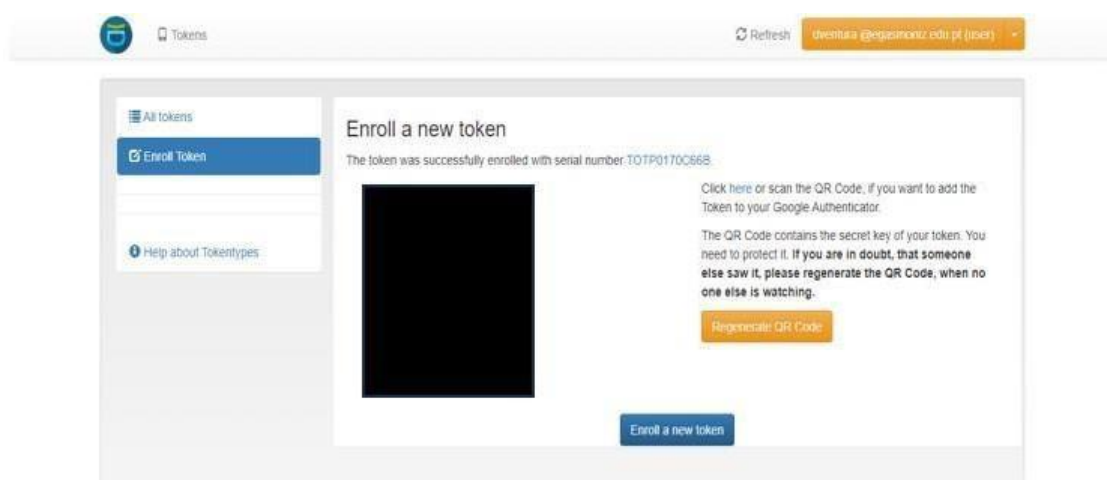
Click on the “Enroll Token” button on the bottom of the page.



The screenshot shows a web interface for enrolling a new token. On the left, there is a sidebar with 'All tokens' and 'Enroll Token' (highlighted in blue), and a link for 'Help about Tokentypes'. The main content area is titled 'Enroll a new token' and contains a dropdown menu set to 'HOTP: Event based One Time Passwords'. Below this, there is explanatory text about HOTP tokens. Under 'Token data', the checkbox 'Generate OTP Key on the Server' is checked, with a note that the server will create the OTP key and a QR code. There are two more dropdown menus: 'OTP length' set to '6' and 'Hash algorithm' set to 'sha1', both with explanatory text below them. An 'Enroll Token' button is located at the bottom right of the form.

### 4<sup>th</sup> Step:

A QR code will be generated (in the same place where you find the black square in the example image below).



This screenshot shows the 'Enroll a new token' page after a successful enrollment. The page title is 'Enroll a new token' and it displays a success message: 'The token was successfully enrolled with serial number: TOTP0170C668'. A large black square is present where the QR code would have been. To the right of the black square, there is text instructing the user to click a link or scan the QR code to add the token to their Google Authenticator. Below this text is a 'Regenerate QR Code' button. At the bottom of the main content area, there is an 'Enroll a new token' button. The top of the page shows a navigation bar with a 'Tokens' link and a user profile for 'dvesitka @egasmoniz.edu.pt (user)'.

### 5<sup>th</sup> Step:

Please use the Google Authenticator app installed on your smartphone. Check the images below.

