



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.



1st 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.

Enter your username and password and click Log In to authenticate.

Please sign in

Username

Password

Log In

2nd Step:

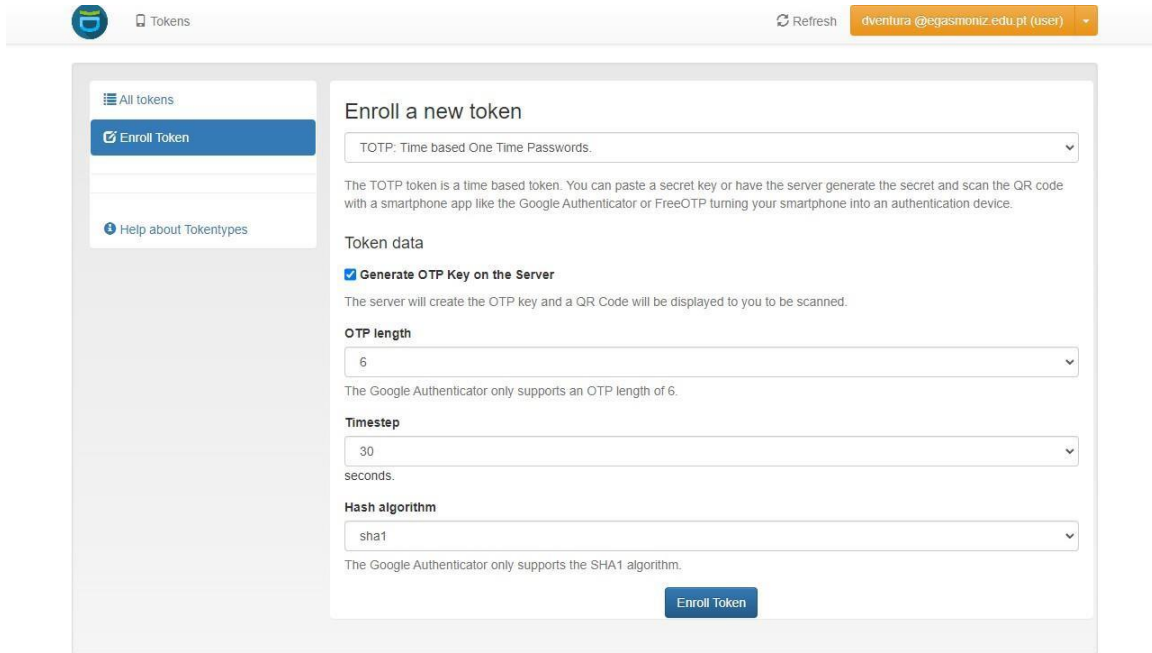
Please select "Enroll Token" on the left menu.

total tokens: 1

serial	type	active	description	failcounter	rollout state
TOTP0042C543	totp	active		0	

3rd Step:

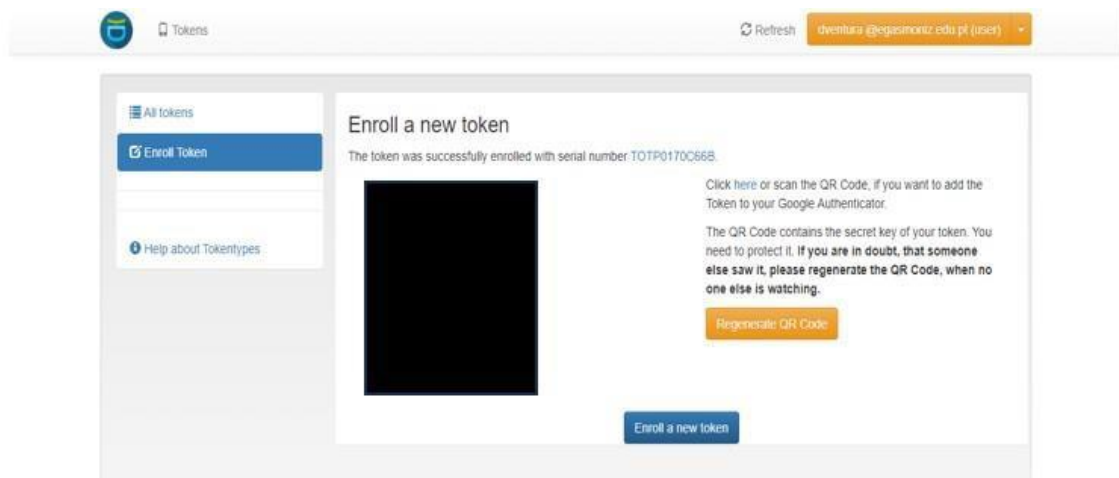
Click on the "Enroll Token" button on the bottom of the page.



The screenshot shows the 'Enroll a new token' page. The top navigation bar includes a 'Tokens' menu, a 'Refresh' button, and a user profile 'dventura @egasmoniz.edu.pt (user)'. The main content area is titled 'Enroll a new token' and features a dropdown menu set to 'TOTP: Time based One Time Passwords'. Below this, there is explanatory text: 'The TOTP token is a time based token. You can paste a secret key or have the server generate the secret and scan the QR code with a smartphone app like the Google Authenticator or FreeOTP turning your smartphone into an authentication device.' The 'Token data' section includes a checked checkbox for 'Generate OTP Key on the Server' with the note 'The server will create the OTP key and a QR Code will be displayed to you to be scanned.' Configuration options include 'OTP length' set to 6 (with a note 'The Google Authenticator only supports an OTP length of 6.'), 'Timestep' set to 30 seconds, and 'Hash algorithm' set to sha1 (with a note 'The Google Authenticator only supports the SHA1 algorithm.'). An 'Enroll Token' button is located at the bottom right of the form.

4th Step:

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



The screenshot shows the 'Enroll a new token' page after successful enrollment. The top navigation bar is the same as in the previous step. The main content area displays a message: 'The token was successfully enrolled with serial number TOTP0170C668.' Below this message is a large black square representing the QR code. To the right of the QR code, there is text: 'Click here or scan the QR Code, if you want to add the Token to your Google Authenticator.' and 'The QR Code contains the secret key of your token. You need to protect it. If you are in doubt, that someone else saw it, please regenerate the QR Code, when no one else is watching.' An orange 'Regenerate QR Code' button is positioned below this text. At the bottom of the main content area, there is a blue 'Enroll a new token' button.

5th Step:

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

