



O Centro de Informática da Faculdade de Arquitetura implementou, para a segurança de todos, o método de autenticação **2FA (TWO FACTOR AUTHENTICATION)**

Tal autenticação, é um **método de segurança** utilizado para proteger contas online, que adiciona mais uma camada de segurança, além da tradicional combinação de nome de utilizador e palavra-passe.

Instalar o autenticador "**Google Authenticator**" no smartphone.



1º passo:

Entrar no link: <https://mfa.fa.ulisboa.pt>

Aceda com as suas credenciais da FA para proceder ao próximo passo:

The screenshot shows a web browser window with a login form. At the top right, there is a 'Login' button. Below it, a blue box contains the instruction: 'Enter your username and password and click Log In to authenticate.' The main content area features the FA logo and the text 'Please sign in'. There are two input fields: 'Username' and 'Password', followed by a 'Log In' button.

2º Passo:

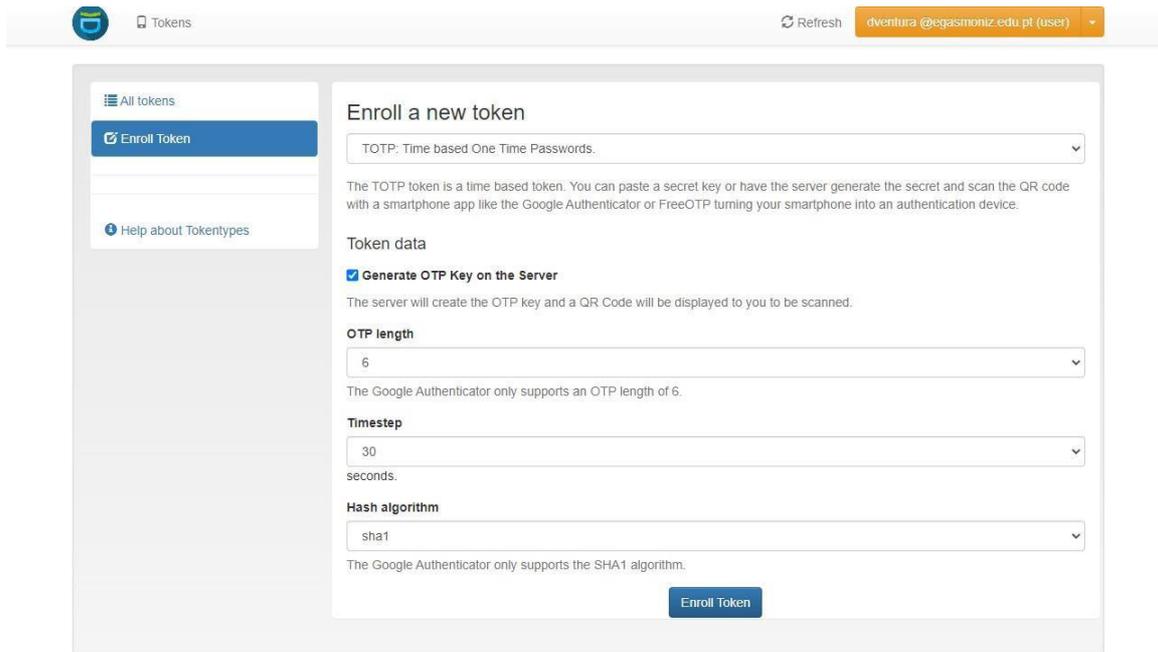
Na barra lateral esquerda terá de escolher a opção de "**Enroll Token**"

The screenshot shows the 'Tokens' management interface. The top navigation bar includes a 'Tokens' tab, a 'Refresh' button, and a user profile dropdown for 'dventura @egasmoniz.edu.pt (user)'. The main content area has a sidebar with 'All tokens' and 'Enroll Token' options. The main table displays a list of tokens with columns for serial, type, active status, description, failcounter, and rollout state. A table with one row is visible:

serial	type	active	description	failcounter	rollout state
TOTP0042C543	totp	active		0	

3º Passo:

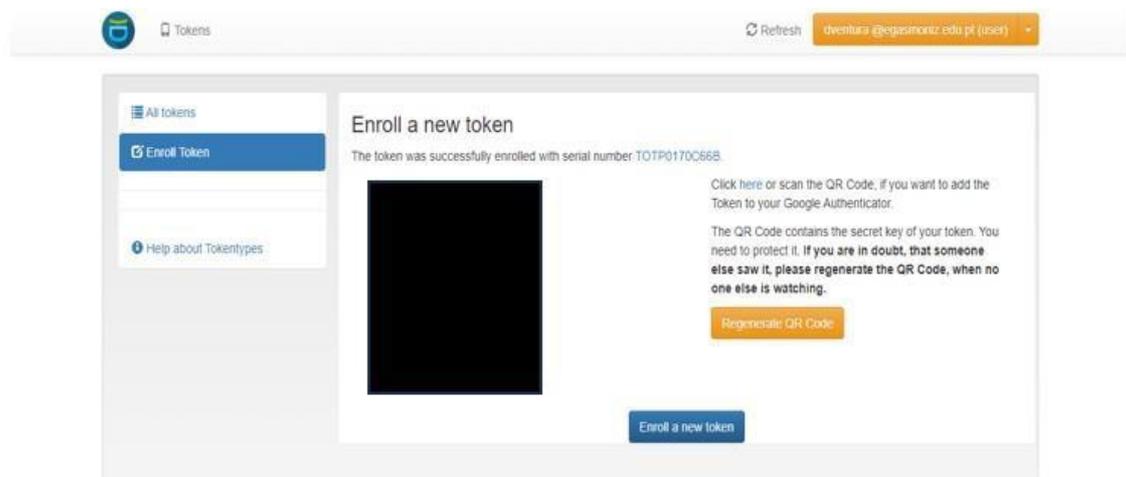
Clicar no botão “Enroll Token”.



The screenshot shows the 'Enroll a new token' page. On the left, there is a sidebar with 'All tokens', 'Enroll Token', and 'Help about Tokentypes'. The main content area is titled 'Enroll a new token' and contains 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.' Under 'Token data', the checkbox 'Generate OTP Key on the Server' is checked. Below that, the 'OTP length' is set to 6, with a note: 'The Google Authenticator only supports an OTP length of 6.' The 'Timestep' is set to 30 seconds. The 'Hash algorithm' is set to sha1, with a note: 'The Google Authenticator only supports the SHA1 algorithm.' At the bottom right of the form is an 'Enroll Token' button.

4º Passo:

Deverá aparecer uma janela com um código QR no espaço que está em preto na seguinte imagem



The screenshot shows the 'Enroll a new token' page after successful enrollment. The title is 'Enroll a new token'. A message states: 'The token was successfully enrolled with serial number TOTP0170C668.' Below this, there is a large black rectangular area where the QR code was displayed. To the right of the black area, there is text: 'Click here or scan the QR Code, if you want to add the Token to your Google Authenticator. 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.' Below this text is an orange 'Regenerate QR Code' button. At the bottom right of the main content area is a blue 'Enroll a new token' button.

5º Passo:
Instalar e configurar o Google Authenticator

