goAML Web

2FA

Two Factor Authentication

(goAMLWeb version 4.8.x)

Content

1. Introduction 2
2. Google Authenticator application 3
3. Logging in to goAMLweb 4
   3.1. Email One Time Password 4
   3.2. Google Authenticator 5
      3.2.1. Installation 5
      3.2.2. Logging in 6
      3.2.3. New or lost phone and disabling the Authenticator 6
4. Forgot Password 7

1. Introduction

Two-Factor Authentication (**2FA**) is a method to protect your user account from unauthorized access. The principle is that to log in you need to **know** something and to **have** something.

What you need to know in GoAML Web is your **username and password.** For what you need to have there are two options; either your **mobile phone** (with Google Authenticator application) or **access to your email**.

1. **Email** as second factor works so, that with every login the system sends you a One Time Password which is valid for 5 minutes. The benefit is that it doesn't require any special arrangements from you. The disadvantage is that the email may take a couple of minutes to be delivered, which doesn't really produce a good user experience.

2. **Google Authenticator** is a free app to be installed in your mobile phone (Android or IOS). It calculates you a personal authentication code, which changes every 30 seconds. The benefit is that the login happens instantly. On the other hand this requires the app to be installed and reading a new QR code every time you change your password. You can anyway always use the One Time Password sent to your email as described above.

   For the best user experience we recommend the use of Google Authenticator.

2. Google Authenticator application

Google Authenticator can be found from the Androidin and IOS App Stores. The use of the app is safe, because it doesn't store or handle any information about the user or organization. It is not communicating anywhere either. It is just a calculator which works locally in the phone. You can install it equally safe either to your personal phone or to your work phone as long as it is only in your personal use.

During your first login (and when you change your password) goAMLweb shows you a QR code, which contains your personal 16-character identification code. You will read it to your phone memory with the Google Authenticator app.

After that the Authenticator app will use your personal identification code and the current date and time to calculate a 6-digit authentication code, which you need to log in and which will change every 30 seconds. goAMLweb server knows both your personal identification code and the current date and time and calculates which code your Authenticator app is showing right now.

When you have inserted the code to the login window goAMLweb compares it to the code it has calculated himself. If they are the same the system knows that the code you entered is calculated from your identification code with your phone and lets you in.

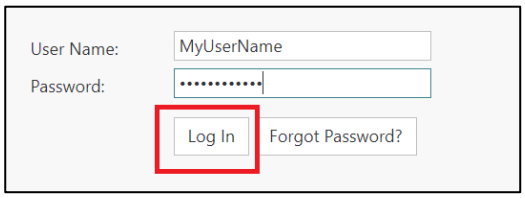
NOTICE! Every timer when goAMLweb shows you a QR code you need to read it into your phone's app! The code will be displayed **only once** and at the same time the old code, which you may have in your phone, stops working (even if it is still displayed).

If you miss reading the QR code, your phone breaks or gets lost or the code (or the whole app) disappears from your phone, you can still log in with the email One Time Password. Then change your goAMLweb password and with the next login the system will give you a new QR code.

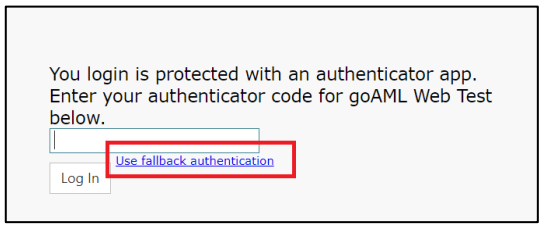
3. Logging in to goAMLweb

3.1. Email One Time Password

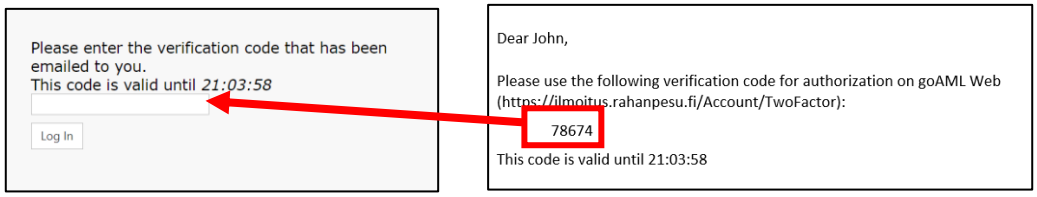
Enter your username and password on the login page and click “login.”



On next page goAMLweb will ask you to enter Google Authenticator code (see chapter 3.2). If you cannot (or don’t want) to use it, click the ”**Use fallback authentication**” link.



You will get a code by email. It is valid only for a couple of minutes and it may take a moment to be delivered. If the time window for login expires, restart the login process from the beginning.



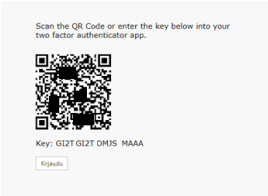
3.2. Google Authenticator

3.2.1. Installation

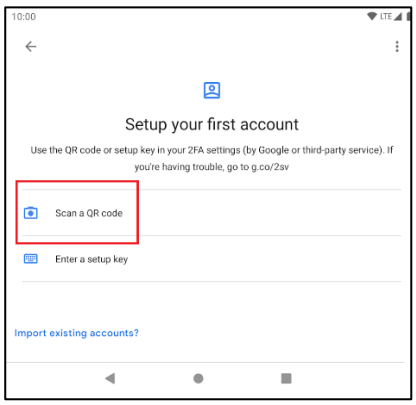
Install the app from the App Store. You will find it with name ”Google Authenticator”, manufactured by ”Google LLC”. You can recognize it also from the app icon.

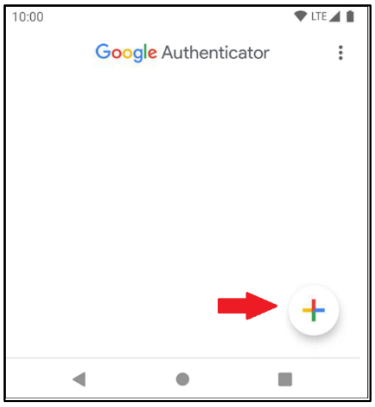


When you log in to goAMLweb with you username and password for the first time after 2FA has been taken into use (or you have changed your password), goAMLweb will show you a QR-code.

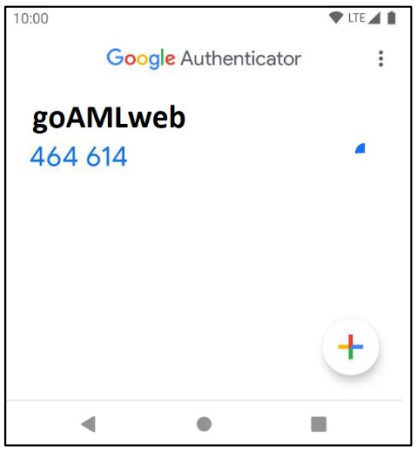


Start the app in your phone and choose ”Scan a QR code” or click the + in the right bottom corner and read the QR code with your phone camera.



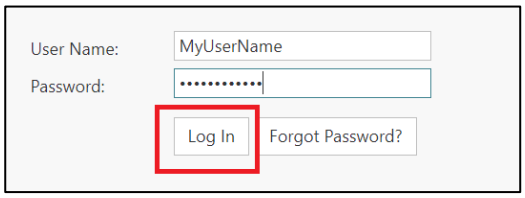


goAMLweb appears on the front page of the app together with the changing authentication code.

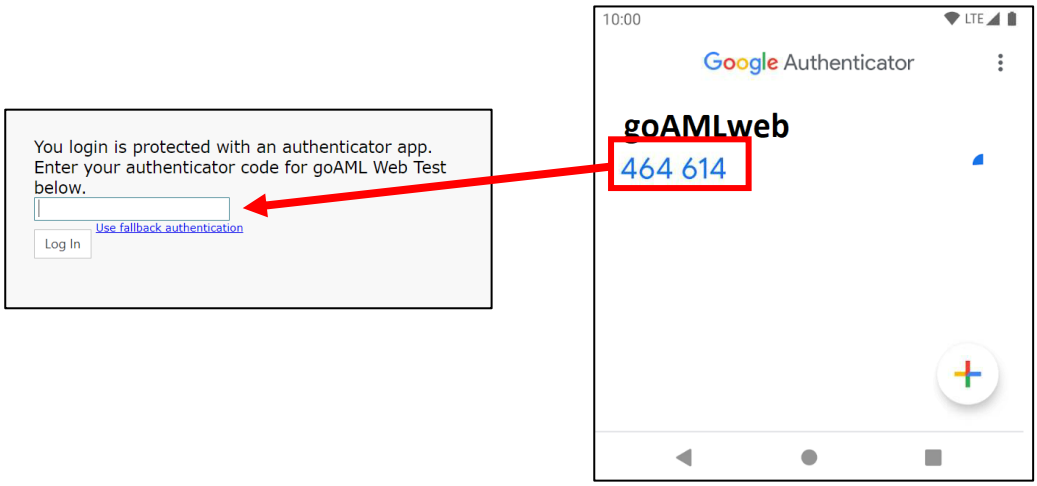


3.2.2. Logging in

Enter your username and password and click “login.”



goAMLweb asks for Google Authenticator code. Find the code from the app, enter it and click “log in.”



Ready. You have logged in.

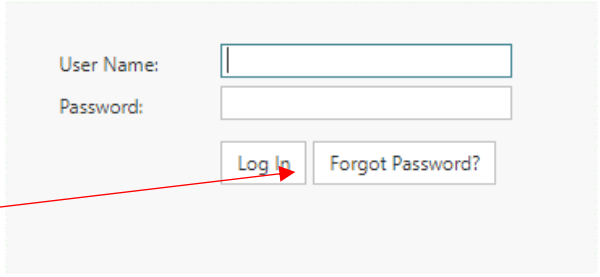
If the Authenticator code is for some reason not available (or does not work), click the “use fallback authentication” and continue as described in chapter 3.1 “Email One Time Password”.

3.2.3. New or lost phone and disabling the Authenticator

If you lose your phone, buy a new one or want to stop using Authenticator for another reason, change your goAMLweb password. The system will disable your old Authenticator code and the codes which the phone still displays are not valid anymore. At the next login the system will give you a new QR code. You can read it to your new device or dismiss it and use the Email One Time Password instead.

4. Forgot Password

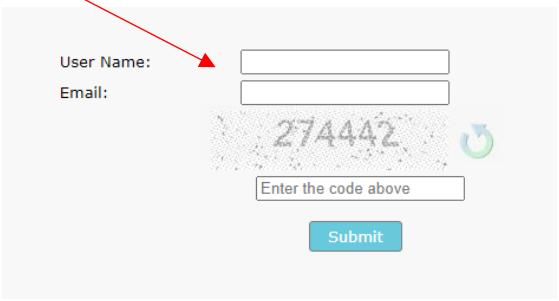
In order to retrieve a forgotten password:



1) Press ”LOGIN”
2) Click the "Forgot Password?" - button on the login screen
3) Fill in the User Name, Email address, CAPTCHA-code and choose *Submit*".

   NOTE! If the CAPTCHA- character are not clear enough, tap  -button, which gives a new series of numbers.

4) Open the Email and tap the link in the message.
5) A page will open in the browser, where you must enter your User Name, Email address and a new password.
6) Login in to the goAMLweb using your new password.



NOTE! If the user cannot recall their username or email associated with their account, they must contact the FIU Finland (Email: goaml.krp@poliisi.fi, phone: 0295 486 833).