Google Authenticator

Google Authenticator is a multifactor app for mobile devices. It generates timed codes used during the 2-step verification process. To use Google Authenticator, install the Google Authenticator application on your mobile device.

Installing Google Authenticator

If you would like to use Google Authenticator, please first ensure you're using the latest LastPass browser extensions and mobile clients everywhere. You will also need a supported mobile device, to run the Google Authenticator application.

Next, install the Google Authenticator application on your mobile device. Google officially supports Android, iOS (iPhone, iPod Touch, or iPad), and BlackBerry devices. You can follow the instructions here to install Google Authenticator onto these devices.

For other devices:

If you would like to run Google Authenticator on an Android device that doesn't have access to Google Play Store, you can install from here.

If you would like to run Google Authenticator on your Windows Phone, Jamie Garside has developed Authenticator.

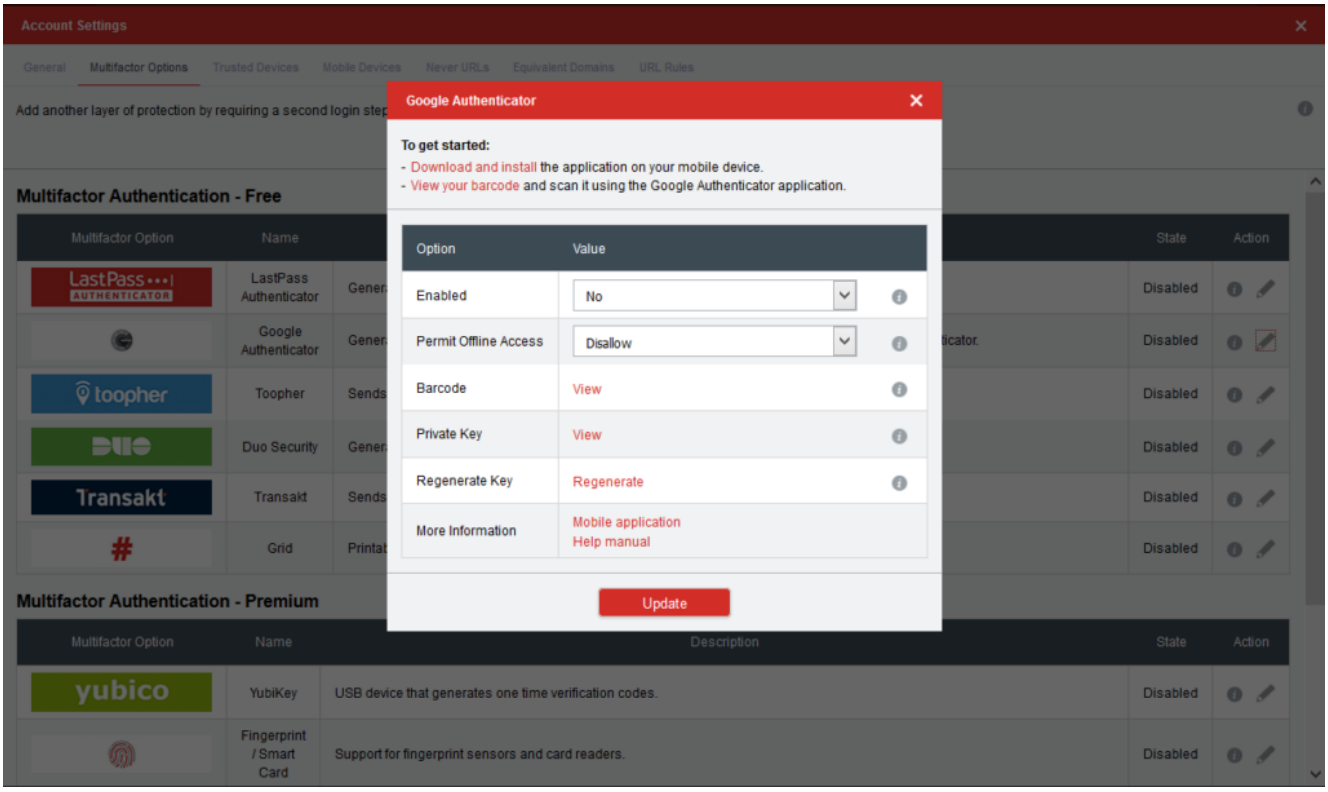
If you would like to run Google Authenticator on your webOS device, Greg Stoll has developed GAuth.

If you would like to run Google Authenticator on your Symbian device, or any device that supports Java ME, Rafael Beck has developed lwuitgauthj2me. Alternatively, Rodrigo A. Diaz Leven has developed gauthj2me.

Setting up Google Authenticator

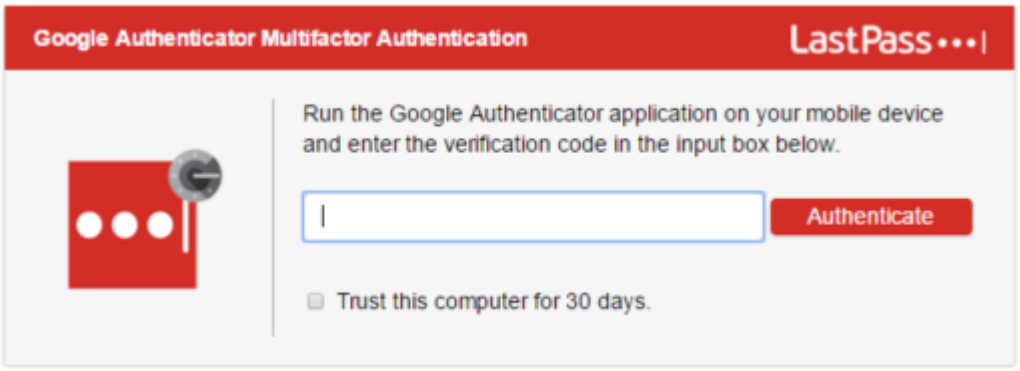
Once you have the Google Authenticator application running on your mobile device, go to https://lastpass.com/?ac=1&opengoogleauth=1. Follow the instructions there to finish setting up Google Authenticator.

You will be prompted to use a Bar Code scanning app (Androids, iPhones and supported devices with cameras) to scan your unique bar code or you can manually enter the Google Authentication Key found on that setup page.



After your LastPass account is registered within the Google

Authenticator app, the next time you login to LastPass on an untrusted device, you will receive the Google Authentication dialog:



Go to your Google Authenticator App and input the current authentication code you see in the app into this dialog. If the code expires before you have a chance to authenticate, simply use the next code that appears in the app.

Logging in Offline when Google Authenticator is Enabled

As with our other multifactor authentication options, you can choose whether to allow LastPass to store an encrypted vault locally so you can log in without an internet connection. If you enable offline access, you will be able to login without using your Google Authenticator code in case of a connectivity issue.

With some internet configurations (typically wireless connections and waking from sleep), LastPass may log in offline first before establishing connectivity to your online vault and prompting for your authenticator code. This may cause LastPass to AutoFill any login credentials you have saved in LastPass for the current page you are on.

If you wish to disable offline access, you may do so in your Account Settings.

Administrating Google Authenticator in Enterprise

You can require Google Authenticator for your users via the 'Require use of Google Authenticator' policy. This policy can be enabled for your Enterprise account by accessing your Enterprise console and clicking the 'Setup' tab > 'Add Policy' button > Select 'Require use of Google Authenticator' from the dropdown menu: