Graphene-Os

> [!toc] Table of Contents

Recommended Apps

Install Accrescend

Download the `Accrescend` App Store from the default `App Store`, that comes preinstalled with GrapheneOS From `Accrescend` install `App Verifier` and `Inter Profile Sharing`, if you plan to share files between different Android Profiles.

Install Signal

- Download the Signal APK from Signals own website: https://signal.org/android/apk/. After downloading the APK, verify it via the `App Verifier` You can do so by selecting the downloaded APK in your `Downloads` folder and `share` the APK with the `App Verifier`. This will display **SUCCESS** at the top. On the bottom it can say **UNKNOWN**, that's ok. If the top also says **UNKNOWN**, than something went wrong and downloaded a wrong APK!
- Go back to the `Download` folder and click on the signal APK to start the installation.
- In case the warning `For your security, your phone currently isn't allowed to install unknown apps from this sources.` pops up, this is correct. You have to give you `Files` App the permission to install Applications. Click `Settings` and toggle `Allow from this source`

> [!warning] Warning {static}
>
> For security reasons, eg. preventing yourself from unintentionally installing some malicious APK you downloaded from the internet, **remove this permission after successfully installing signal**, by turning it off again under: `Settings`, `Apps`, `Files`, `Install unknown apps`

Only for very high threat levels:

If you are at home, in your personal WiFi and you want to active you signal anonymously, wait with the activation of your account until you installed Orbot from F-Droid. Just follow the guide below.

Install F-Droid

- As with signal, get the APK **from their official website**: https://f-droid.org

Your Browser `Vanadium` might show you a warning, that `This file might be harmful`. This is also a good warning, since usually one shouldn't download random APK's from the web, but instead from an app store, like F-Droid. Since we don't have an app store yet, from which we can install the apps we like, we need to do this once: `Download anyway`

- Share the downloaded APK with the `App Verifier` and confirm the **"SUCCESS"** at the top of `App Verifier`
- Go back to the `Download` folder and click on the signal APK to start the installation.
- In case the warning `For your security, your phone currently isn't allowed to install unknown apps from this sources.` pops up, this is correct. You have to give you `Files` App the permission to install Applications. Click `Settings` and toggle `Allow from this source`

> [!warning] Warning {static}
>
> For security reasons, eg. preventing yourself from unintentionally installing some malicious APK you downloaded from the internet, **remove this permission after successfully installing f-droid**, by turning it off again under: `Settings`, `Apps`, `Files`, `Install unknown apps`

Install Orbot and Tor Browser from F-Droid

`Orbot` will direct all your phones internet traffic through Tor.

First, you have to copy the guardian projects repository link from their website. The link on the very top of the webpage should work.

- add the repository of the guardian project to your F-Droid by following these instructions
- go back to the main page of your F-Droid App and pull down on the screen, to refresh the page. Now the newly added repositories should be included
- search for `Orbot` from the "Guardian Project" and install it
- search for `Tor Browser` from the "Guardian Project" and install it

>

> [!technical] For high threat level
>
> If you are at home in your personal WiFi and you would like to register your signal account anonymously, first activate Orbot, then start the registration.
>
> The reason for that lies in the potential metadata. The only information signal store on it's users are the timestamp of the registration of the account and the timestamp from when the account was logged in the last time.
>
> Theoretically, if you one day will have do plausible deny to be the owner of this signal account and your network was tapped, while you created the account, one could "prove" that you connected to the signal servers just at that moment, when this account was created.
>
> But this is, to be quit honest, a very theoretical threat scenario.

Recommended Settings

> [!tip] Tip {static}
>
> To see, why we recommended the following settings on GrapheneOS, go to our GrapheneOS recommendations

Device Unlock

In the settings app, go to: `Security and Privacy` > `Device unlock`. Here you find settings for:

- Screen lock: set your strong password here
- Fingerprint unlock and it's strong 2FA feature
  - also see the PIN scrambling feature
- `Duress Password`
- `PIN scrambling`:
  - if you don't use the fingerprint unlocking with it's 2FA Pin: `Device unlock > Cog-Wheel icon` to the right of Screen lock `> Scramble PIN input layout`
  - if you're already using the 2FA method, than you have to go to: `Device unlock > fingerprint unlock >` input your password `> second factor PIN` > toggle `Scramble PIN input layout`

If you're interested why this is in two different locations, see:

https://discuss.grapheneos.org/d/18661-where-is-pin-scramble-feature/11

Exploit Protection

In the settings app, go to: `Security and Privacy` > `Exploit protection`. Here you find settings for:

- `auto reboot`
- `USB-C Port` *Tip:* `Charging only`
- `Turn off WiFi & Bluetooth automatically`

More Security & Privacy

In the settings app, go to: `Security and Privacy` > `More security & privacy`. Here you find settings for:

- Allow Sensors permission to apps by default. *Tip: turn this off*

Apps

In the settings under `Apps` > `Special app access`:

- `Install unknown apps`

Version #3
Erstellt: 2026-02-15 16:15:58 UTC von ESC-IT Migration Bot
Zuletzt aktualisiert: 2026-05-24 10:23:57 UTC von ESC-IT Migration Bot