

# Simple example

## Signal sous Tails sans smartphone

### Objectifs

Le but de ce tuto est de posséder un compte Signal qui n'est pas lié à un Smartphone. Il sera ainsi possible d'utiliser Signal uniquement depuis Tails. Pour ce faire, nous allons utiliser trois logiciels différents :

1. signal-cli (comme «Command Line Interface» ), qui permet, comme son nom l'indique, d'utiliser signal en ligne de commande
2. «Signal Desktop», une interface graphique pour Signal sur ordinateur. Cette interface est très similaire à celle pour smartphones à quelques exceptions près : il n'est pas possible de créer un nouveau compte, ni de démarrer une nouvelle conversation en utilisant tor et il peut être compliqué de récupérer les fichiers joints sous Tails (d'où l'usage de signal-cli)
3. «Nouvelle Conversation Signal», un logiciel très basique qui permet de démarrer une nouvelle conversation

### Avertissements

1. Signal demande que les comptes soient régulièrement consultés. Il y a une suspicion de risque de fermeture de compte.
  2. Les appels audio et vidéo ne fonctionnent pas avec cette méthode (et à priori pas avec Tor)
  3. La sécurité de Tails sera abaissée étant donné que le code de signal-cli et Signal Desktop n'est pas vérifié avec la même rigueur que le reste du code de Tails et Debian. Néanmoins, c'est du code open-source, lu et vérifié par de nombreuses personnes compétentes à travers le monde.
  4. Il n'y a pas de mises à jour des logiciels. C'est à vous de vérifier quand des nouvelles versions sont disponibles et de les installer. Utiliser des logiciels non mis à jour implique le risque que des attaquants exploitent des failles de sécurités connues et corrigées dans les versions ultérieures.
- Merci aux blogs bisco.org et ctrl.alt.coop pour les tutos, à ??? dont ce tuto est très fortement inspiré, et à AsamK pour signal-cli

### Ressources

À compléter :

\* le wiki de signal-cli : <https://github.com/AsamK/signal-cli/wiki>

### Ce qui est nécessaire

- \* Une connaissance minimale de l'usage du terminal (ce tutoriel essaie d'expliquer chaque manipulation)
- \* Un numéro de téléphone jetable (nommé +336XXXXXXX dans ce tuto, en cas de numéro en 07, le numéro à 10 chiffres)

1. Utiliser un boîtier téléphonique jetable. Par exemple, un téléphone à touche que l'on trouve en grande quantité dans les magasins de téléphonie.
2. Réaliser l'opération ailleurs que chez soi. Attention : l'activation d'une nouvelle carte SIM peut poser problème.
3. Bien évidemment une carte SIM ; LycaMobile ou SymaMobile se trouvent dans de nombreux tabacs et elles sont jetables.

### Configuration de la persistance

1. Ouvrir Tails en déverrouillant la persistance

2. lancer l'application « Configurer le volume persistant »
3. Cocher les options : "dotfiles" et "logiciels supplémentaires"

## Installation de Signal

Pour l'instant, l'installation peut se faire de deux manières :

1. Manuellement comme décrit ci-dessous
2. Avec le script d'installation en cours de développement. Méthode décrite au point suivant.

Nous travaillons à un paquet Debian qui automatisera le processus et devrait à terme gérer les mises à jour.

### Installation manuelle de Signal

1. Démarrer sous Tails, déverrouiller la persistance, définir un mot de passe d'administration
2. Télécharger le dossier qui contient de la doc et facilite l'installation depuis cette adresse : [https://tails.boum.org/doc/howto-install/fr/using\\_persistent\\_volume/](https://tails.boum.org/doc/howto-install/fr/using_persistent_volume/) et l'extraire
3. Installer Signal Desktop :
  - a. Ouvrir un terminal et taper les lignes de commandes suivantes (pour chaque encadré, taper la commande)
  - i. Télécharger la clé PGP de Signal :

```
wget -O- https://updates.signal.org/desktop/apt/keys.asc | gpg --dearmor > signal-desktop-keyring.gpg
```

- ii. Ajouter la clé PGP de Signal au gestionnaire de paquet APT :

```
cat signal-desktop-keyring.gpg | sudo tee -a /usr/share/keyrings/signal-desktop-keyring.gpg > /dev/null
```

- iii. Ajouter le dépôt de paquet de Signal à APT :

```
echo 'deb [arch=amd64 signed-by=/usr/share/keyrings/signal-desktop-keyring.gpg] tor+https://updates.signal.org/desktop/apt /' | sudo tee -a /etc/apt/sources.list.d/signal-desktop.list
```

- iv. Mettre à jour la liste des paquets :

```
sudo apt update
```

- v. Télécharger le paquet Signal Desktop :

```
apt download signal-desktop
```

- vi. Créer le dossier dans le quel décompresser Signal Desktop :

```
mkdir -pv /live/persistence/TailsData_unlocked/dotfiles/Applications/signal-desktop
```

- vii. Décompresser Signal Desktop :

```
dpkg-deb -xv $(ls signal-desktop*.deb) "$DOTFILES/Applications/signal-desktop"
```

- viii. Aller dans le dossier signal/ précédemment téléchargé, puis dans le dossier install et copier le fichier signal.desktop.in

- ix. Effectuer le raccourci clavier ctrl+l et taper le chemin du dossier suivant : **\*/live/persistence/TailsData\_unlocked/dotfiles/.local/share/applications/**

- x. Finalement les deux dernière ligne de commande :

```
mkdir -vp /live/persistence/TailsData_unlocked/dotfiles/.local/share/applications/
```

- xi. et la dernière qui permet de copier le lanceur de Signal Desktop afin de l'avoir à chaque redémarrage :

```
cp /live/persistence/TailsData_unlocked/dotfiles/Applications/signal-desktop/usr/share/applications/sig
```

4. Installer `signal-cli` :

a) Ouvrir l'explorateur de fichier, raccourci clavier `ctrl+l` et taper la ligne suivante : `*/live/persi`

### Installation avec le script fournis

1. Démarrer sous Tails, déverrouiller la persistance, définir un mot de passe d'administration
2. Télécharger le dossier qui contient de la doc et facilite l'installation depuis cette adresse : et le décompresser (clique-droit et choisir **extraire ici...**). Par la suite nous appellerons ce dossier **signal/**
3. Naviguer dans le dossier **signal/** puis **install/** Depuis là, clique-droit et choisir Ouvrir dans un terminal...
4. Dans le terminal, taper la ligne suivante :

```
./install.sh
```

5. Renter le mot de passe administrateur quand demandé, si tout c'est bien passé Signal Desktop et signal-cli sont installés. Il ne reste plus qu'à redémarrer l'ordinateur.

## Configurer un nouveau compte Signal

### 1. Résoudre un Captcha

Sous Tails, toutes les connexion Internet utilisent Tor. En conséquence, le serveur de Signal demande de valider l'enregistrement avec un (captcha)[<https://github.com/AsamK/signal-cli/wiki/Registration-with-captcha>].

1. ouvrir avec le Navigateur Tor: (la page pour captcha de Signal)[<https://signalcaptchas.org/challenge/generate.html>] ou (une cette adresse si la précédente ne fonctionne pas)[<https://signalcaptchas.org/registration/generate.html>] (au choix).
2. Dans le navigateur, ouvrir une console (clic droit sur la page, **inspecter**, puis **console** dans le bandeau des outils développeur).
3. Résoudre le captcha, C'est long !!!
4. Dans la console, copier la longue suite de caractère qui s'affiche après **signalcaptcha://**

### 2. Enregistrer le compte

Comme exemple, nous allons utiliser le numéro de téléphone **06xxxxxxxx**

Dans un terminal :

```
signal-cli -a +336xxxxxxx register -captcha CAPTCHA
```

### 3. Une fois le code reçu sur son boîtier téléphonique

Taper dans un terminal :

```
signal-cli -a +336xxxxxxx verify CODE
```

où CODE est le code reçu sur son téléphone jetable

### 4. Ajouter un code pin au compte Signal

Ceci évitera qu'une fois le numéro jetable réattribué après quelques mois, quelqu'un écrase votre compte Signal !

Dans un terminal :

```
signal-cli -a +336xxxxxxx setPin VOTRECODEPINAUCHOIX
```

Noter votre code PIN dans la persistance ou ayez une bonne mémoire!

### 5. Optionnel:

se donner un nom de profil sur Signal (pour les autres modifs du profil, CF: <https://github.com/AsamK/signal-cli/blob/master/man/signal-cli.1.adoc#updateprofile>) Dans un terminal : `signal-cli -a +336xxxxxxx updateProfile -name VOTRENOM`

### 6. À faire absolument!!

Il faut sauvegarder la configuration de **signal-cli** et ainsi le compte Signal nouvellement créé dans la persistance.

Ouvrir un terminal et taper sur une seule ligne :

```
cp -rv ~/.local/share/signal-cli/* cp /live/persistence/TailsData_unlocked/dotfiles/.local/share/signal-cli
```

## Relier Signal Desktop à un compte existant

Nous allons voir comment dire à Signal de lier **Signal Desktop** à un compte existant. En effet, **Signal Desktop** ne peut pas fonctionner en tant que tel. Un compte Signal doit déjà avoir été créé, comme par exemple à l'étape d'avant.

### Le compte principal est lié à un smartphone

Cette méthode ne garanti pas la même confidentialité que avec celle qui utilise un signal-cli et un téléphone jetable. Nous la mettons quand même : 1. Ouvrir Signal Desktop : Applications → Autres → Signal 2. Suivre les instruction au bas du QRCode

### Le compte principal est lié à Tails avec signal-cli

C'est la méthode dans la continuité de ce tuto. Pour cette étape, il est nécessaire de configure un mot de passe administrateur au démarrage de Tails. 1. Dans un terminal, taper :

```
sudo apt update && sudo apt install zbar-tools
```

2. Ouvrir **Signal Desktop** : Applications → Autres → Signal

3. Effectuer une capture d'écran en sélectionnant uniquement la zone du QRCode : Applications → Utilitaires → Capture d'écran Puis «Sélection».
4. Enregistrer la capture dans le dossier Images et la renommer «qrcode.png»
5. Ouvrir «Fichiers» aller dans le dossier Images, clique-droit → ouvrir dans un terminal
6. Dans le terminal, taper :

zbar-tools qrcode.png 7. Copier la ligne qui commence par «sgnl: · ..». Pour copier : sélectionner le texte, puis clique-droit → copier. 8. Taper dans le terminal la ligne suivante :

```
signal-cli -a +336XXXXXXX addDevice --uri "COLLER ENTRE LES GUILLEMETS DOUBLE LA LIGNE COPIÉE PRECEDEMAN"
```

Avec le curseur à la position désirée, Clique-droit → coller 9. Enregistrer dans la persistance la configuration de Signal Desktop. Taper dans un terminal la ligne suivante :

```
cp -rv ~/.config/Signal/* /live/persistence/TailsData_unlocked/dotfiles/.config/Signal
```

## Utilisation

Presque tout peut se faire depuis **Signal Desktop**. Pour le lancer :

Applications → Autres → Signal

Pour commencer une nouvelle conversations, lancer le logiciel «Nouvelle Conversation Signal». Cela va commencer une nouvelle conversation avec le numéro entré. La personne recevra le message «salut». À partir de ce moment là, il sera possible de continuer la conversation depuis Signal Desktop. Ne pas oublier de paramétrer les messages éphémères.

## Mises à jour

Il n'y a pas encore de mise à jour automatique. Les explications suivront bientôt sur comment faire manuellement. Un jour il devrait y avoir des mises à jour automatiques ???