



# MANUEL DE CONNEXION SANS FIL LINUX



Ce document vous permettra de vous connecter au réseau sans fil VIA en quelques minutes<sup>1</sup>.

## 1 Installer votre carte réseau sans fil

Votre noyau doit disposer des modules suivants :

- les wireless extensions ;
- les algorithmes de cryptage ARC4 et Michael MIC ;
- le pilote de ta carte réseau<sup>2</sup>.

Tous ces modules sont normalement présents dans les noyaux fournis par les distributions récentes<sup>3</sup>.

Si votre carte réseau sans fil est bien détectée, la commande `ifconfig -a` doit faire apparaître deux cartes réseaux réelles : `eth0` et `eth1`, `wlan0` ou `wifi0`. Notez le nom de la seconde interface, qui correspond à votre carte sans fil.

## 2 Installer les outils de connexion sans fil

### 2.1 Wireless tools

Il s'agit d'un ensemble d'outils pour configurer les cartes wifi, scanner et se connecter aux réseaux environnants. Sous Ubuntu ou Debian, installez le paquet *wireless-tools*.

Vous pouvez maintenant scanner les réseaux qui vous entourent avec la commande `iwlist wlan0 scan`<sup>4</sup>. Si vous êtes à portée d'une borne VIA, vous devez voir apparaître notre réseau.

### 2.2 OpenSSL

Installez le paquet *openssl* et téléchargez le certificat SSL de notre serveur Radius, au <https://radius.via.ecp.fr/ssl/cacert.crt>. Placez ce certificat dans `/etc/ssl/certs/`.

### 2.3 NetworkManager

Si vous souhaitez utiliser une interface graphique, installez également le paquet *network-manager-gnome*, ou *network-manager-kde* selon le bureau que vous utilisez. Vérifiez ensuite que vous faites bien partie du groupe *netdev*.

### 2.4 WPA supplicant

Installez le paquet *wpa\_supplicant*. Récupérez ensuite le fichier de configuration [https://radius.via.ecp.fr/conf/wpa\\_supplicant.conf](https://radius.via.ecp.fr/conf/wpa_supplicant.conf) et placez-le dans `/etc/`. Éditez ce document, et mettez-y votre login et votre mot de passe VIA.

## 3 Configurer votre connexion

Vous avez le choix : en ligne de commande, ou avec l'interface graphique du NetworkManager.

<sup>1</sup>Information non contractuelle : le WPA sous Linux n'est pas encore tout à fait trivial...

<sup>2</sup>Pour les portables Centrino, il s'agit du pilote IPW2100 ou 2200, et ils nécessitent hélas l'installation d'un *firmware* propriétaire.

<sup>3</sup>Si ce n'est pas le cas, il te faudra recompiler un noyau à la main.

<sup>4</sup>Remplacez `wlan0` par le nom de votre interface sans fil.

## 3.1 En ligne de commande

### 3.1.1 Debian, Ubuntu

Avec Ubuntu ou Debian, vous pouvez éditer le fichier `/etc/network/interfaces`. Il doit contenir :

```
iface wlan0 inet dhcp
    wpa-driver wext
    wpa-conf /etc/wpa_supplicant.conf
```

Vous pouvez maintenant vous connecter au réseau sans fil VIA en lançant la commande :

**Debian** `su -c 'ifup wlan0'`

**Ubuntu** `sudo ifup wlan0`

### 3.1.2 Autres distributions

Vous pouvez vous reporter au manuel de votre distribution et à la documentation fournie, sans doute dans `/usr/share/doc/`. Il existe une commande générique, adaptée à toutes les distributions, pour se connecter à un réseau sans fil crypté par WPA :

```
wpa_supplicant -w -i wlan0 -D wext -c /etc/wpa_supplicant.conf
```

Il faut ensuite demander une adresse IP avec la commande : `dhclient wlan0`.

## 4 Avec une interface graphique

1. Assurez-vous d'abord que vous n'avez pas déjà configuré votre connexion sans fil par un autre moyen : le Network manager ne gère que les interfaces qu'on lui laisse. . .
2. Lancez le Network manager : s'il ne figure pas dans le menu de votre bureau, lancez-le par sa commande (`nm-applet` pour la version Gnome). Une icône apparaît dans la zone de notification de votre bureau.
3. Cliquez du bouton droit sur cette icône, et choisissez le réseau sans fil VIA.
4. Dans la fenêtre de configuration qui s'ouvre, choisissez :
  - Sécurité** WPA Entreprise ;
  - Méthode** PEAP ;
  - Type de clef** TKIP ;
  - Identité** <login SdE> ;
  - Mot de passe** ;
  - Certificat AC** `/etc/ssl/certs/cacert.crt`
5. Cliquez sur « Connexion au réseau », patientez, et vous obtenez normalement une connexion fonctionnelle au bout de quelques instants.