Configure WiFi encryption

OpenWrt supports WPA/WPA2 PSK ("WPA Personal"), 802.11i ("WPA Enterprise") and WEP encryption. The used encryption protocol is defined per network in the `wifi-iface` sections of the wireless configuration.

All encryption settings can also be changed via the LuCI (Network > Wifi).

Key generation

To generate a random password for your key you can use the `pwgen` program. `pwgen` is available for most Linux distributions and is also packaged for OpenWrt.

Example for `pwgen`:

```
$ pwgen --secure 13 1
54wdMvBKo9abu
```

This generates one password with a length of 13 letters/numbers.

WPA encryption

- ***Only WPA2 is secure**; 1st gen WPA is not*

Broadcom proprietary WiFi

For Broadcom wireless chips using the proprietary driver you have to install the nas package.

```
root@OpenWrt:~# opkg update
root@OpenWrt:~# opkg install nas
```

Atheros and generic mac80211 WiFi

For Atheros and mac80211 supported wireless chips, the *wpad*, *hostapd* or *wpa_supplicant* package is required. There are several WPA packages with different support [http://www.fixithere.net/bt-customer-services/how-to-change-bt-wi-fi-password/] options available.

The table below outlines the features supported by the packages and since which OpenWrt version they're available.

Package	AP support	Client support	WPA Enterprise	OpenWrt Version
wpad	yes	yes	yes	10.03+
wpad-mini **(recommended)**	yes	yes	no	10.03+
hostapd	yes	no	yes	7.06+
hostapd-mini	yes	no	no	8.09+
wpa-supplicant	no	yes	yes	7.06+
wpa-supplicant-mini	no	yes	no	8.09+

If not installed yet, choose the appropriate package for the desired configuration.

```
root@OpenWrt:~# opkg update
root@OpenWrt:~# opkg install wpad-mini
```

Configure WPA (PSK)

Configure WPA (PSK) encryption using UCI.

```
root@OpenWrt:~# uci set wireless.@wifi-iface[0].encryption=psk
root@OpenWrt:~# uci set wireless.@wifi-iface[0].key="your_password"
root@OpenWrt:~# uci commit wireless
root@OpenWrt:~# wifi
```

(!) The length must be between 8 and 63 characters. If the key length is 64 characters, it is treated as hex encoded.

Configure WPA2 (PSK)

Configure WPA2 (PSK) encryption using UCI.

```
root@OpenWrt:~# uci set wireless.@wifi-iface[0].encryption=psk2
root@OpenWrt:~# uci set wireless.@wifi-iface[0].key="your_password"
root@OpenWrt:~# uci commit wireless
root@OpenWrt:~# wifi
```

The length must be between 8 and 63 characters. If the key length is 64 characters, it is treated as hex encoded.

Configure WPA2 Enterprise (EAP-TLS with external RADIUS server)

The default `-mini` packages for Atheros hardware will not work with Enterprise mode. (See the table above.)

The example below defines WPA2 Enterprise encryption in AP mode with authentication against an external RADIUS server at 192.168.1.200, port 1812.

```
root@OpenWrt:~# uci set wireless.@wifi-iface[0].encryption=wpa2
root@OpenWrt:~# uci set wireless.@wifi-iface[0].key="shared_secret"
root@OpenWrt:~# uci set wireless.@wifi-iface[0].server=192.168.1.200
root@OpenWrt:~# uci set wireless.@wifi-iface[0].port=1812
root@OpenWrt:~# uci commit wireless
root@OpenWrt:~# wifi
```

Configure WPA2 Enterprise Client, PEAP-GTC using One Time Password (OTP)

The default `-mini` packages for Atheros hardware will not work with Enterprise mode. (See the table above.)

- Enter the following:

```
root@OpenWrt:~# uci set wireless.@wifi-iface[0].encryption=wpa2
root@OpenWrt:~# uci set wireless.@wifi-iface[0].mode="sta"
root@OpenWrt:~# uci set wireless.@wifi-iface[0].ssid="SET_AS_NEEDED"
root@OpenWrt:~# uci set wireless.@wifi-iface[0].encryption=wpa2+ccmp
root@OpenWrt:~# uci set wireless.@wifi-iface[0].eap_type=peap
root@OpenWrt:~# uci set wireless.@wifi-iface[0].auth=gtc
root@OpenWrt:~# uci set wireless.@wifi-iface[0].identity="SET_AS_NEEDED"
root@OpenWrt:~# uci commit wireless
root@OpenWrt:~# wifi
```

- Modify the generated wpa_supplicant.conf file in the /var/run folder to remove the *password=""* line using your favorite editor.
- Enter the following:

```
root@OpenWrt:~# wpa_cli -p /var/run/wpa_supplicant-wlan0
>status
```

- note the id of your interface (usually 0 in single interface systems)
- Enter the following at the wpa_cli prompt

```
>reconfigure
>reassociate
```

- When prompted for you OTP PIN enter the following at the wpa_cli prompt (if necessary replace the *0* with your desired interface id):

```
>otp 0 YOUR_PASSWORD_HERE
```

WEP encryption (NOT recommended)

Some notes for the WEP key format:

- The format for the WEP key for the key1 option is HEX

If you wish to use raw hex keys then you can skip to the UCI commands paragraph below. Raw hex keys have 10 hex digits (`0`..`9`, `a`..`f`) for 64-bit WEP keys and 26 hex digits for 128-bit WEP keys.

If you do not wish to use raw hex keys then follow the instructions below.

- The length of a 64bit WEP key must be exact 5 characters
- The length of a 128bit WEP key must be exact 13 characters
- Allowed characters are letters (upper and lower case) and numbers

Generate a 64bit WEP key:

```
root@OpenWrt:~# echo -n 'awerf' | hexdump -e '5/1 "%02x" "\n"'
6177657266
```

Generate a 128bit WEP key:

```
root@OpenWrt:~# echo -n 'xdhdkkewioddd' | hexdump -e '13/1 "%02x" "\n"'
786468646b6b6577696f646464
```

Now use UCI to configure WEP encryption with the hex key you just generated.

```
root@OpenWrt:~# uci set wireless.@wifi-iface[0].encryption=wep
root@OpenWrt:~# uci set wireless.@wifi-iface[0].key1="786468646b6b6577696f646464"
root@OpenWrt:~# uci set wireless.@wifi-iface[0].key=1
root@OpenWrt:~# uci commit wireless
root@OpenWrt:~# wifi
```

You can configure up to four WEP keys.
