

The KWiFiManager Handbook

Stefan Winter



The KWiFiManager Handbook

Contents

1	Introduction	1
2	Using the KWiFiManager suite	2
2.1	The KWiFiManager application	2
2.1.1	Main window	2
2.1.1.1	Signal quality display	2
2.1.1.2	Connection speed	3
2.1.1.3	Current configuration	3
2.1.1.4	Access Point information (bottom area)	4
2.1.1.5	Information about available networks	4
2.1.2	Statistics Viewer	5
2.1.3	Configuration Editor	5
2.1.4	Miscellaneous	6
2.1.4.1	Acoustic Scanning	6
2.1.4.2	Network logging	6
2.1.4.3	Disabling the wireless network	6
2.2	The system tray icon	6
2.3	The Control Center module	7
2.3.1	The Configuration Tabs	7
2.3.1.1	General settings	7
2.3.1.2	Cryptography settings	8
2.3.1.3	Power saving settings	9
2.3.2	Auto-configuration on KDE Control Center Module startup	9
2.3.3	Autodetecting your device	9
3	License and contributors	11

The KWiFiManager Handbook

A Further Information	12
A.1 Notes on the MAC address display in Ad-hoc mode	12
A.2 Security considerations on WEP cryptography	13
B Compilation and Installation	14

Abstract

The KWiFiManager suite can be used to configure and monitor wireless LAN cards. It consists of a stand-alone application and a module for the KDE Control Center.

Chapter 1

Introduction

The KWiFiManager suite is a set of tools which allows you to manage your wireless LAN Network Interface card (PC-Card, PCI or miniPCI) under the K Desktop Environment. It provides information about your current connection and lets you set up up to ten independent configurations and use up to four configurations that are pre-configured by distribution-specific scripts. If you are in a place where none of your preconfigured networks is available, you can also dynamically switch to an available network with almost no configuration effort. KWiFiManager supports every wireless LAN card that uses the wireless extensions interface. This includes virtually all wireless LAN cards that are operational at all under the Linux® operating system.

Chapter 2

Using the KWiFiManager suite

2.1 The KWiFiManager application

Purpose of the main KWiFiManager application is to show the currently active network configuration and to display connection quality and access points.

The main application is launched by either typing `kwifimanager` at the command prompt of a console window or via the K Menu, where it is located by default in the Applications group. If KWiFiManager is already running but minimised to the system tray then it can be restored by clicking once on the [system tray icon](#). If there is more than one wireless LAN card in your system, just open more than one instance of KWiFiManager: every instance will show information about a different card automatically. The GUI elements of the application are explained in the following subsections.

2.1.1 Main window

The KWiFiManager main window consists of five parts:

2.1.1.1 Signal quality display

Here you can see the quality and type of the active connection. The uppermost icon displays the general state of the wireless network via a set of pictograms:

- a wireless LAN card with a question tag means that no card was detected or its state could not be determined

The KWiFiManager Handbook

- a single laptop means that a wireless LAN card is inserted and in Infrastructure mode, but there is no radio signal from access-points. The card is out of range and can not communicate to the infrastructure network.
- a laptop that is connected to an access point means that a connection to an access point is established.
- two laptops mean that your system is in Ad-Hoc mode without access points. It may or may not have established a Peer-to-Peer connection.

Below these pictograms is a small quality meter. It displays, in a cellular-like manner, the quality level of the current connection. This information is only available in Infrastructure mode. In Ad-Hoc mode, the level is always 0.

This graphical information is supplemented by an integer value below the icon. It shows the signal quality, and is computed in one of two ways:

- a directly reported value from the card if the card supports 'Quality' reporting
- $(\text{signal strength in dBm}) - (\text{noise level in dBm})$ for cards that do not support that.

You can manually change the method used by turning File, Use alternate strength calculation on or off. Turning the option on means to use the second method. If your card is out of range, the value is 0; if no card is inserted or your card is in Ad-Hoc mode it will show N/A.

2.1.1.2 Connection speed

An indicator for the current connection speed is shown at the right-hand side of the main window above the configuration info. If the speed settings are set to AUTO, the value will change once in a while as the card adjusts the connection speed according to the signal quality. The scale of the bar graph will automatically adjust to up to 108 MBit/s when the current connection speed exceeds 11 MBit/s.

2.1.1.3 Current configuration

Here you can find information about your card configuration. It displays the following information:

- the network with which the card is connected to / tries to connect to (Searching for network: or Connected to network:)
- the MAC address of the access point to which the card is connected.

If the card is in Infrastructure mode but out of range, an appropriate warning (- no access point -) is displayed to indicate that no connection is established.

The KWiFiManager Handbook

In Ad-Hoc mode, the field shows an address that is associated with one of the cards in the Ad-Hoc network. It displays a MAC address that has a non-global scope: its second bit is set to 1, which often results in a prefix of '02:' instead of '00:'. Many people think this is an error, but in fact it is done on purpose to show that the cell you are connected to is not an actual physical device, but rather an imaginary access point without a real physical address.

Your card is the first card that enters Ad-Hoc mode with a given SSID. Then all other cards entering Ad-Hoc mode with the same SSID will see your MAC-address, slightly modified: instead of `00:xx:yy:zz:aa:bb` it will show `02:xx:yy:zz:aa:bb`. This behavior is intentional.

- on most cards (those that have the capability to report it), the frequency on which the card is transmitting data and the corresponding channel number is displayed.
- your local IP (version 4) address, if available. If no address could be retrieved from the networking subsystem, the word `unavailable` is displayed.
- encryption status (only if you have started KWiFiManager `asroot`). The display will only show `off` or `active`, but never the real key. This is intentional in order to not reveal the WEP key to people passing by the users screen.

2.1.1.4 Access Point information (bottom area)

The last line of the main window shows information about your `AccessPoint`. This requires that your system administrator provided a list of MAC addresses with a corresponding information. An example for such a list can be found in `$KDEDIR/share/apps/kwifimanager/locations/DE_BW_Karlsruhe_University.loc`

If you want to set up a new list, simply create a file in the same format and copy it into the folder `$KDEDIR/share/apps/kwifimanager/locations/`

It will be automatically parsed at the next start of KWiFiManager. If you have a list and want to have it included in future releases of KWiFiManager, simply send it to the author or current maintainer.

2.1.1.5 Information about available networks

The lower-left area of the main window contains a button named `Scan for networks....` If you click on this button, KWiFiManager will attempt to retrieve a list of all networks that are in range of your card. The outcome of this scan depends on two factors:

- the overall ability of your card and driver to perform network scans
- if you have root permissions or not

If your card or driver arent able to scan the network, your scanning results will always be empty. If you are not the root user, the list may be incomplete or outdated.

The KWiFiManager Handbook

In order to receive a reliable, current list of access points you will need to start the scan with root privileges, for example by using the KDE su utility to start KWiFiManager

If at least one network was found, you are presented with a table showing details of the network. It has four columns that inform you about

- the network name (or the string (hidden cell) if the name is not disclosed by the access point during the scan)
- the type (whether is a Managed or an Ad-Hoc network)
- the signal strength of the network
- and whether or not WEP encryption is used

In case of an active WEP encryption, you can click on that column and enter the network key. KWiFiManager will automatically try to guess if the key is a hexadecimal number or a string.

If the network information for the highlighted network is complete (i.e. all columns contain meaningful information), you can use the button Switch to network to enter the selected network. If KWiFiManager has no root privileges, you will be prompted with a password prompt to enter the root password in order to change the network.

Clicking on Close dismisses the network information screen without changes to the existing settings.

2.1.2 Statistics Viewer

Optionally, by selecting Connection statistics in the File menu, a separate window can be shown which displays the signal level and noise level graphs of the last 240 seconds. The signal level is displayed in blue and the noise level in red. The difference (SIGNAL minus NOISE) is the connection quality which is displayed in the main window.

Some cards do not report meaningful noise information. If this is the case for your card and you get annoyed by the irrelevant red line, you can disable showing the noise level in the statistics window by unselecting Config → Show noise level in statistics in the KWiFiManager main window.

2.1.3 Configuration Editor

By selecting Config → Configuration Editor you are taken to the [control center module](#) of KWiFiManager. In case you are not the `root` user, a window will pop up requesting the `root` password. This is because the configuration module allows you to change network connectivity and uses `ifconfig` to make changes, which requires root privileges.

2.1.4 Miscellaneous

There are some minor additional features worth of being mentioned.

2.1.4.1 Acoustic Scanning

First, there is a feature named Acoustic Scanning. If this option is enabled, the connection quality is converted into an acoustic signal. A higher signal quality leads to a higher frequency of the 'beep' output and to a more rapid beeping. If you've ever seen the Star Trek(tm) series you will see some parallels to their 'tricorders'

2.1.4.2 Network logging

A second feature is network logging. It just means that KWiFiManager will log the name of the network you are connecting to every time your network changes. This option is most useful when searching for the special network name 'any'. In this mode, the card will log into any network it finds. The logfile's position is `$HOME/.kde/share/apps/kwifimanager/wireless-log`

2.1.4.3 Disabling the wireless network

You can completely disable the card by selecting the option File Disable radio. Using this option will turn off the cards transmitter which effectively turns it off and saves a little bit of energy. This will only work for your card if it accepts changes to its `txpower` property.

2.2 The system tray icon

When KWiFiManager is launched, it installs a small icon in the system tray. The icon contains parts of the information of the main window, namely the bar graph and optionally the signal strength number. If you hover over the icon with the mouse for a few seconds, a tooltip will appear that contains the currently connected network name. Whether or not the strength number shall be shown can be configured via Config, Show Strength Number in System Tray.

If you have configured KWiFiManager to stay in the system tray when clicking on the X button, the icon will stay in the tray persistently unless you really exit the application by clicking on File, Quit.

You can always hide the main application to the system tray by clicking on the tray icon. Similarly, to restore the main application from the tray, just click on it once.

2.3 The Control Center module

The configuration module in the KDE Control Center is perhaps the most useful part of the KWiFiManager suite. Here you can actually change the basic settings of your wireless LAN card. The module can manage up to ten independent configurations for the card. If you don't need that many configurations, you can reduce the number of configs shown at any time by changing the Number of Configurations entry. If you have configured your wireless settings with a distribution-specific tool, chances are good that the KDE Control Center module will automatically detect this and also read in and show that configuration. In any case these configurations will be read-only, because it is the distribution's job to handle updating these settings and the module should not interfere with their internal magic. Up to five additional preset configurations can be shown in addition to the ten that are self-definable. These configurations will have the name Vendor x to distinguish them from the others. The KDE Control Center can even automatically set your card up whenever you start the module. Since establishing (or bringing down) a network connection is a security sensitive operation, any changes to the configuration can only be done by `root`.

2.3.1 The Configuration Tabs

The configurations are split up in three parts:

- general configuration settings (like the network name)
- encryption settings
- power saving settings

These parts are explained in the following sections.

2.3.1.1 General settings

The upper part of the control center module consists of one to ten tabs labelled Config 1 through Config 10. Each of these tabs can hold a configuration for your WLAN card. In addition (as explained above) up to five vendor-specific configurations may be visible, labelled Vendor 1 through Vendor 5.

The most important settings are always visible, the cryptography and power management options are only shown when activated. The perhaps most important element in each configuration tab is the fieldNetwork name. Here you can specify which network you would like to log into. You can either specify the name of your network directly, or you can try a scan on all available networks by setting the network name to `any`.

In addition to the network name, you have to specify the type of network to log into. That's the purpose of the button `groupOperation mode`. The option `Managed` means that the network consists of designated base stations, so-called

‘access points’ or sometimes ‘residential gateways’. This is the most common operation mode for company networks. The second option, Ad-hoc means that your network is just a direct connection between computers, without access points. The three other options (Repeater, Master and Secondary) are only very seldomly used. If you want to use them, please be aware that these settings are simply passed to the iwconfig program and have not been tested extensively. In case something doesn't work as expected, you are welcome to send a bug report.

You can optionally set the connection speed for your connection. The setting auto should do for most uses, since the card will determine the appropriate speed itself. However, if you find that the speed changes every few seconds, for example when you have a weak connection, you can set the speed manually.

Below these configuration items you will find a field named Execute script on connect:. Here you can enter the name of a script to execute after setting up the network connection. It will be executed whenever you hit the Activate configuration button and, optionally, automatically when you start the Control Center module. The script will have root rights. This may lead to problems if you want to start an X application in the script and the X server belongs to someone else than root. You can make such scripts work correctly if you execute the X application via `kdesu -u USERNAME -c COMMAND`. Or, you can instruct your X server to also allow connections coming from root. You can do this with the `xhost` program.

2.3.1.2 Cryptography settings

The checkbox Use encryption determines whether or not encryption shall be activated. If it is checked, a button labelled Configure... becomes available which allows you to configure the details of encryption. After pushing the button, you are presented the following settings in a new dialog:

Key to use: You can define up to four secret keys for each configuration; in this field you can set which one you want to use to send encrypted packets. The card can always receive packets that are encrypted with *any* of the keys.

TIP

You can achieve asymmetrical encryption (different keys for sending and receiving) if you configure your access point to send packets with a different key than the card. Just make sure that the partner station has the required key in any one of its key slots.

Crypto mode: When encryption is activated, there are two ways to deal with incoming non-encrypted packets: discard or allow. When you set your card for Open, the card will also listen to non-encrypted packets. Restricted will only allow encrypted network packets, any other packets are discarded.

Crypto keys: This box lets you specify the secret keys to use for cryptography. To protect your passwords, only asterisks will be shown when you enter a password. The KDE Control Center module will automatically try to guess whether you want to set an encryption string or a hexadecimal number by checking the input length: string keys are usually 5 or 13 characters long (for 64- or 128-Bit key lengths) whereas hex values are 10 or 26 characters long (please do not put a '0x' in front of hex keys).

Be aware that the built-in cryptography support (named WEP for Wired Equivalent Privacy) is not very safe at all. See Section [A.2](#) for details.

2.3.1.3 Power saving settings

The last configuration element that remains to be described is the power management. When checking the box Enable Power Management a button for the configuration of the setting will become active. After clicking this button, a new dialog will open and you will be presented some options that can help you save energy. The first two input fields named Sleep timeout and Wakeup period describe the periodicity of network online times for your wireless LAN card. The card will turn the radio antenna off for the time period (in seconds) specified in Sleep timeout. Afterwards it will be active for Wakeup period and will in that time establish the network connection and send/receive packets that queued up during the sleep time. If no network connection is found, it will go to sleep again immediately and the cycle begins again. The box named Receive packets below lets you specify which packets the card should listen to when awoken. You can either select Unicast only (which will only let your card listen to packets sent specifically to your card), Multi/Broadcast only (will only listen to packets sent to multiple machines and discard packets directed to your card) or Both. Most people should select the default value Both.

2.3.2 Auto-configuration on KDE Control Center Module startup

If you wish, you can make KWiFiManager initialize your wireless LAN card whenever you start the KDE Control Center module. To do so, check the box Load preset configuration on startup and select the configuration you want to use in the listbox below. If you want to set the card to these settings at once, push the button Activate configuration.

2.3.3 Autodetecting your device

KWiFiManager needs to know the interface name of your wireless LAN card to apply any settings. You can either enter the information (e.g. eth1 or wlan0) manually in the input field on the right-hand side of Settings apply to interface:, or let KWiFiManager auto-detect the interface. To do so, push the button Autodetect interface. This will perform a scan on all interfaces listed in `/proc/net/dev` to find your card. The result of the scan will show up in the input

The KWiFiManager Handbook

field beside the button. If the field remains empty, no card was found. Please note that KWiFiManager uses the wireless extensions to detect cards. If you use a card controlled by the wlan-ng package, KWiFiManager only shows correct results if your driver has a compatibility layer for the wireless extensions built-in. In the case that there are multiple wireless LAN cards present on the system, scanning stops after the first card found. So, if you want to apply the settings to a different card than the one that was detected during the scan, you need to enter its interface name by hand.

Chapter 3

License and contributors

Documentation copyright (c) Stefan Wintermail@stefan-winter.de.

This documentation is licensed under the terms of the [GNU Free Documentation License](#).

This program is licensed under the terms of the [GNU General Public License](#).

Appendix A

Further Information

This appendix contains some extra information of items concerning wireless LAN that are not directly related to KWiFiManager.

A.1 Notes on the MAC address display in Ad-hoc mode

At first glance, the MAC address in the field Access Point seems to be wrong in Ad-hoc mode because it changes the first two digits of the MAC address to 02. But actually, this is a hardcoded feature in wireless LAN cards.

Usually a card is connected to a 'real' access point. Then the correct MAC address is shown. If you change to Ad-hoc (or 'Peer-to-peer') mode, one of the computers must act as a server for the other computers. The first computer that enters a network will set itself as server. So, all other computers connecting to the same Ad-hoc network will see that first computer as network server. But since this computer is not a 'real' server (that is, it is not a permanently available access point), clients should be aware that the network they are connecting to is not a permanent one. IEEE standards for MAC addresses have a place reserved for such (rare) occasions: MAC addresses that are not globally valid have a bit set to one that shows that these addresses are 'locally administered'. This bit is the second bit in transmit order, and the seventh bit in logical order and will hence raise the number of the MAC's first digit block from 00 to 02.

You can compare this sort of address to the non-global IP addresses like '192.168.*.*'.

So, the implementors of wireless networking agreed to give these 'virtual' network servers a MAC address that is within the 'locally administered' scope. To keep this virtual MAC address unique, they used a little trick: they only changed the first segment of the MAC address of the wireless LAN card, and since the remaining segments are still unique in the world, they have a unique address to use as network server.

A.2 Security considerations on WEP cryptography

WEP cryptography is not very secure at all. A paper from cryptography analysts called the encryption algorithm 'kindergarten cryptography'. Actually, software exists that exploits a huge security hole in the encryption standard. This software listens to the encrypted network traffic, analyzes it, and after only a few hours it reveals the password to enter the network in clear text. The more traffic on the network, the easier it is to find out the password because some packets are particularly weak because they carry a bad so-called initialisation vector (IV). Recent access points try to avoid these bad IVs, so it is getting harder to exploit the hole.

If you are truly concerned about your security, *do not* use plain WEP. If you are just setting up a two-computer home network, well, then I guess WEP should do.

There are many alternatives to WEP encryption. Its successors WPA and WPA2 are better designed and do a better job protecting your traffic, for example by dynamically changing the keys after a while. If you don't want to rely on the basic safety of the network link you could use SSH to communicate over the network. SSH is a program suite that encrypts data with its own algorithm, which is very secure. Another option is to use PPTP, the Point-to-Point-Tunneling protocol. However, even PPTP seems to be a bit leaky concerning encryption security. And finally, you could set up an IPSec tunnel (VPN connection) for your encrypted connections. As of yet, this encryption seems to be very safe and flexible.

Appendix B

Compilation and Installation

KWiFiManager is part of the KDE project <http://www.kde.org/> .

KWiFiManager can be found in the kdenetwork package on <ftp://ftp.kde.org/pub/kde/> , the main FTP site of the KDE project.

In order to compile and install KWiFiManager on your system, type the following in the base directory of the KWiFiManager distribution:

```
% ./configure
% make
% make install
```

Since KWiFiManager uses **autoconf** and **automake** you should have no trouble compiling it. Should you run into problems please report them to the KDE mailing lists.