

# Quick Start Guide for m0n0wall Gateways



**Version 1.0**  
**Copyright © 2006, Wifi-Soft Solutions**  
**All rights reserved.**

## Purpose of this document

1. This document should be used in conjunction with m0n0wall user guide for configuring your m0n0wall gateway in WiFiLAN. Please refer to WiFiLAN administrator guide and m0n0wall user guide for detail documentation
2. It assumes that the user has basic knowledge of networking including configuring subnet mask, RADIUS setting, default gateway and DNS configuration
3. In order to configure m0n0wall you will need a static IP address, subnet mask, default gateway and DNS information given to you by your Internet Service Provider. Please keep this information handy while setting up your gateway
4. Configuring WiFiLAN you will need the WAN MAC address, RADIUS secret, serial number (if any) and public IP address of your m0n0wall gateway
5. Finally, you need an active WiFiLAN account. Please contact Wifi-soft's sales to create your WiFiLAN account

# m0n0wall Setup

We have assumed that you have properly connected your m0n0wall gateway a broadband connection that has a static public IP address. Additionally, your m0n0wall gateway admin interface is accessible either via the LAN interface or via the public WAN interface as shown in the figure below.

The screenshot shows the m0n0wall webGUI Configuration page. The left sidebar contains a navigation menu with categories: System (General setup, Static routes, Firmware, Advanced), Interfaces (assign) (LAN, WAN, DMZ, WLAN), Firewall (Rules, NAT, Traffic shaper, Aliases), Services (DNS forwarder, Dynamic DNS, DHCP server, DHCP relay, SNMP, Proxy ARP, Captive portal, Wake on LAN), VPN (IPsec, PPTP), and Status (System, Interfaces, Traffic graph, Wireless, Diagnostics). The main content area is titled "System: General setup" and contains the following fields:

- Hostname:** m0n0wall. Description: name of the firewall host, without domain part e.g. *firewall*.
- Domain:** neon1.net. Description: e.g. *mycorp.com*.
- DNS servers:** Two empty input fields. Description: IP addresses; these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients. A checkbox is checked: **Allow DNS server list to be overridden by DHCP/PPP on WAN**. Description: If this option is set, m0n0wall will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). They will not be assigned to DHCP and PPTP VPN clients, though.
- Username:** admin. Description: If you want to change the username for accessing the webGUI, enter it here.
- Password:** Two empty input fields with "(confirmation)" next to the second. Description: If you want to change the password for accessing the webGUI, enter it here twice.
- webGUI protocol:** Radio buttons for HTTP (selected) and HTTPS.
- webGUI port:** Empty input field. Description: Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS).
- Time zone:** Dropdown menu showing "Europe/Zurich". Description: Select the location closest to you.
- Time update interval:** Input field with "300". Description: Minutes between network time sync.; 300 recommended, or 0 to disable.
- NTP time server:** Input field with "pool.ntp.org". Description: Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!

A "Save" button is located at the bottom of the form. The footer of the page reads: "m0n0wall is © 2002-2005 by Manuel Kasper. All rights reserved. [view license]"

Configure the relevant parameters for gateway as shown above.

Next, you need to click on the DHCP Server link under the Services menu. Assuming that your APs are connected on LAN interface, enable the DHCP server as shown below.

- System**
  - General setup
  - Static routes
  - Firmware
  - Advanced
- Interfaces** (assign)
  - LAN
  - WAN
  - DMZ
  - WLAN
- Firewall**
  - Rules
  - NAT
  - Traffic shaper
  - Aliases
- Services**
  - DNS forwarder
  - Dynamic DNS
  - DHCP server
  - DHCP relay
  - SNMP
  - Proxy ARP
  - Captive portal
  - Wake on LAN
- VPN**
  - IPsec
  - PPTP
- Status**
  - System
  - Interfaces
  - Traffic graph
  - Wireless
- ▶ **Diagnostics**

### Services: DHCP server

LAN **DMZ**

**Enable DHCP server on LAN interface**

**Deny unknown clients**

If this is checked, only the clients defined below will get DHCP leases from this server.

<b>Subnet</b>	192.168.1.0
<b>Subnet mask</b>	255.255.255.0
<b>Available range</b>	192.168.1.0 - 192.168.1.255
<b>Range</b>	<input type="text" value="192.168.1.100"/> to <input type="text" value="192.168.1.199"/>
<b>WINS servers</b>	<input type="text"/> <input type="text"/>
<b>Default lease time</b>	<input type="text"/> seconds <small>This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.</small>
<b>Maximum lease time</b>	<input type="text"/> seconds <small>This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.</small>

Save

**Note:**

The DNS servers entered in [System: General setup](#) (or the [DNS forwarder](#), if enabled) will be assigned to clients by the DHCP server.

The DHCP lease table can be viewed on the [Diagnostics: DHCP leases](#) page.

MAC address	IP address	Description
■■■■■■■■■■	192.168.1.90	Notebook

⊕ ⊗  
⊕

Unless you need to customize your lease time, leave the default and maximum lease time blank so that default values are taken. Adjust the Range of your IP addresses according to your subnet.

Next, click on the Captive Portal link under the Services menu. The following page will be displayed:

**System**

 General setup  
 Static routes  
 Firmware  
 Advanced

**Interfaces** (assign)

 LAN  
 WAN  
 DMZ  
 WLAN

**Firewall**

 Rules  
 NAT  
 Traffic shaper  
 Aliases

**Services**

 DNS forwarder  
 Dynamic DNS  
 DHCP server  
 DHCP relay  
 SNMP  
 Proxy ARP  
 Captive portal  
 Wake on LAN

**VPN**

 IPsec  
 PPTP

**Status**

 System  
 Interfaces  
 Traffic graph  
 Wireless

 ▶ **Diagnostics**
**Services: Captive portal**
**Captive portal** | **Pass-through MAC** | **Allowed IP addresses** | **Users**
 **Enable captive portal**
**Interface**

LAN

Choose which interface to run the captive portal on.

**Idle timeout**
 minutes

Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

**Hard timeout**

60 minutes

Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

**Logout popup window**
 **Enable logout popup window**

If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

**Redirection URL**


If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.

**MAC filtering**
 **Disable MAC filtering**

If this option is set, no attempts will be made to ensure that the MAC address of clients stays the same while they're logged in. This is required when the MAC address of cannot be determined (usually because there are routers between m0n0wall and the clients).

**Authentication**

- No authentication  
 Local user manager  
 RADIUS authentication

 IP address: 

 Port: 

 Shared secret: 

 Accounting:  send RADIUS accounting packets

 Accounting port: 

 Reauthentication:  reauthenticate connected users every minute

- no accounting updates  
 stop/start accounting  
 interim update

Since m0n0wall configuration supports only one RADIUS server. You need to add the primary RADIUS Server in m0n0wall. In future, when a backup server is supported, you can enter the IP address of our backup server.

Server Name	IP Address	Port
Primary RADIUS server	74.208.78.152	1812
Secondary RADIUS server	174.143.144.224	1812

Enter the desired secret key. Please remember this key since you will need it while configuring your gateway in WiFiLAN.

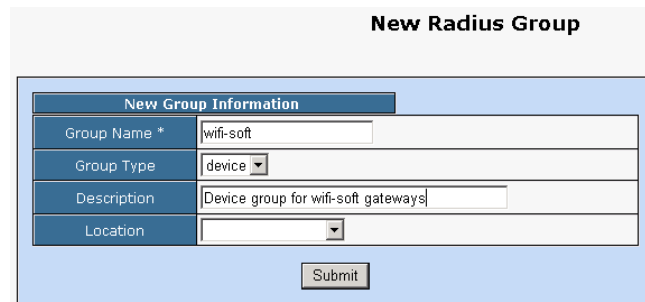
Next check the Enable Accounting check box. For RADIUS servers enter the same information and for port number, please enter **1813**.

If you create your own login portal page, then you need to follow the instructions listed below to correctly authenticate your users. If the redirect URL is configured, then your users will be redirected to this URL after they successfully login.

<b>Portal page contents</b>	<p><input type="button" value="Choose File"/> no file selected</p> <p>Upload an HTML file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "\$PORTAL_ACTIONS\$") with a submit button (name="accept") and a hidden field with name="redirurl" and value="\$PORTAL_REDIRURL\$". Include the "auth_user" and "auth_pass" input elements if RADIUS authentication is enabled. If RADIUS is enabled and no "auth_user" is present, authentication will always fail. If RADIUS is not enabled, you can omit both of these input elements. Example code for the form:</p> <pre>&lt;form method="post" action="\$PORTAL_ACTIONS\$"&gt;   &lt;input name="auth_user" type="text"&gt;   &lt;input name="auth_pass" type="password"&gt;   &lt;input name="redirurl" type="hidden" value="\$PORTAL_REDIRURL\$"&gt;   &lt;input name="accept" type="submit" value="Continue"&gt; &lt;/form&gt;</pre>
<b>Authentication error page contents</b>	<p><input type="button" value="Choose File"/> no file selected</p> <p>The contents of the HTML file that you upload here are displayed when a RADIUS authentication error occurs.</p>
<input type="button" value="Save"/>	

## WiFiLAN Setup

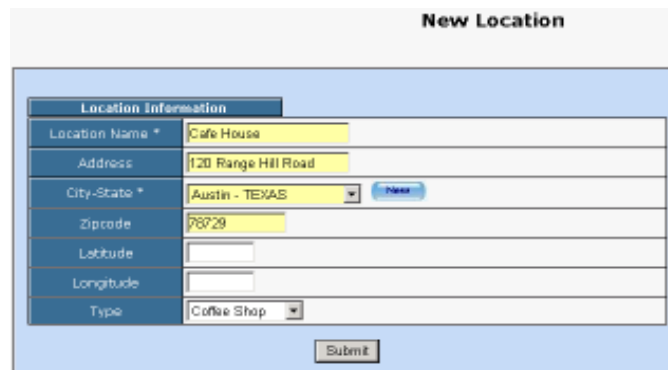
1. You need to log into WiFiLAN by pointing your browser to <https://www.wifi-soft.net/wifilan/>
2. Before you add your first gateway in RADIUS section, you need to create a device group to organize your gateways. To create a new device group, click on the RADIUS menu option and then on the Groups submenu.



New Group Information	
Group Name *	wifi-soft
Group Type	device
Description	Device group for wifi-soft gateways
Location	

Submit

3. Next you can a location entry for your new hotspot location. Although this step is optional, we highly recommend that you create a location entry since it helps you organize your hotspot locations and generate various location specific reports. To create a new location entry, click on RADIUS menu and then on the Location submenu. You need to click on New Location tab to enter a new location.



Location Information	
Location Name *	Cafe House
Address	120 Range Hill Road
City-State *	Austin - TEXAS <span>New</span>
Zipcode	76729
Latitude	
Longitude	
Type	Coffee Shop

Submit

4. Once the location entry for your hotspot is created, you may proceed to add your first gateway entry. To add a new gateway, click on the RADIUS menu and then on the Gateway submenu. Click on the New Gateway tab to add a new gateway.

The description of each parameter is as follows:

## New Radius Gateway

Gateway Information	
Device Name *	Cafe House
Device UserName	
Device Password	
IP Address *	82.165.211.54
Secret *	wifi-soft
Device Group *	wifi-soft
Device Type *	m0n0wall
MAC Address	00-0C-34-A8-E2-89
Description	Cafe House Gateway
Location	Cafe House

- Device Name: A friendly name for the gateway
- UserName & Password: Needed for gateways that fetch their configuration from RADIUS server. Optional
- IP Address: Public IP of the gateway
- Secret: The RADIUS secret configured in the gateway
- Device Group: The device group that we created in the previous step
- Device Type: Type of Device
- MAC Address: The MAC address of the WAN port
- Location: The location where the gateway is installed

You may add more information about the gateway in the Network section. Additionally, you can also configure the gateway for 24x7 monitoring by specifying the monitoring parameters as shown below:

Monitoring Information	
Is Monitored	<input checked="" type="checkbox"/>
Monitoring Type	<input checked="" type="radio"/> Ping <input type="radio"/> HTTP <input type="radio"/> SNMP
Monitor Modem	<input checked="" type="checkbox"/>
Modem IP	59.192.181.32 (If different than device IP)
Modem Monitor Type	<input checked="" type="radio"/> Ping <input type="radio"/> HTTP <input type="radio"/> SNMP
Monitoring Interval	15 minutes Custom Interval (10 mins or more)
Notify Enabled	<input checked="" type="checkbox"/>
Notify After	3 failures
Email Notifications	notify@wifi-soft.com

- **Is Monitored** : Device is monitored if checked
- **Monitoring Type** : Type of protocol used for monitoring
- **Monitoring Interval** : Frequency of monitoring
- **Monitor Modem** : DSL or Cable modem is monitored if checked
- **Modem IP** : The IP address of the modem if different from device IP
- **Modem Monitor Type** : Type of protocol used for monitoring
- **Notify Enabled** : Whether monitoring notification is enabled
- **Notify After** : Number of failure before sending notifications
- **Email Notifications** : List of email address for notification

That's it. Your newly configured m0n0wall gateway is ready for RADIUS authentication. You may configure the login and welcome URL for your gateway so that user can enter username and password that will be sent to our RADIUS server for authentication.

Please make sure that you use [username@realm](#) as username on your login pages so that it would be easier for you to support roaming in the future.

For more information on creating user accounts, please refer to the WiFiLAN administrator guide.