

Quick Start Guide for DD-WRT Firmware



Version 1.0
Copyright © 2007, Wifi-Soft Solutions
All rights reserved.

Purpose of this document

1. This document should be used in conjunction with DD-WRT guide for configuring your DD-WRT firmware in WiFiLAN. Please refer to WiFiLAN administrator guide and DD-WRT 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 DD-WRT 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 DD-WRT gateway
5. Finally, you need an active WiFiLAN account. Please contact Wifi-soft's sales to create your WiFiLAN account

DD-WRT Setup

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

Log into DD-WRT and then go to Setup -> Basic Setup screen. Enter the details in network setup. The connection type should be configured correctly for your Internet connection. Please make sure that you disable the DHCP server under Network Address Server Setting section on this page. We will be using the DHCP server provided by Chillispot. (see later)

The screenshot displays the DD-WRT Basic Setup page. The top navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. The 'Setup' tab is active, and sub-tabs for Basic Setup, DDNS, MAC Address Clone, Advanced Routing, and VLANs are visible. The 'Internet Setup' section is expanded, showing 'Internet Connection Type' set to 'Automatic Configuration - DHCP' and 'STP' set to 'Enable'. Below this, 'Optional Settings' includes fields for Router Name (DD-WRT), Host Name (wifi-soft.com), Domain Name (wifi-soft.com), and MTU (Auto). The 'Network Setup' section shows 'Router IP' with fields for Local IP Address (192.168.1.100), Subnet Mask (255.255.255.0), Gateway (192.168.1.1), and Local DNS (0.0.0.0). The 'Network Address Server Settings (DHCP)' section shows 'DHCP Type' set to 'DHCP Server', 'DHCP Server' set to 'Disable', and 'Start IP Address' set to 192.168.1.100. On the right side, a 'Help' section provides instructions for 'Automatic Configuration - DHCP', 'Host Name', 'Domain Name', 'Local IP Address', 'Subnet Mask', 'DHCP Server', 'Start IP Address', 'Maximum DHCP Users', and 'Time Settings'.

Next, go to Administration tab and click on the Hotspot sub-tab. You need to enable Chillispot on this page. Chillispot is a software program that redirects the unauthenticated users to the login page. This program should be running on the router for the login page to work correctly.

Next you need to configure Chillispot with the Radius server settings as shown below:

Chillispot

Chillispot Enable Disable

Separate Wifi from the LAN Bridge Enable Disable

Primary Radius Server IP/DNS

Backup Radius Server IP/DNS

DNS IP

Redirect URL

Shared Key

DHCP Interface

Radius NAS ID

UAM Secret

UAM Any DNS

UAM Allowed

MACauth Enable Disable

Additional Chillispot Options

Chillispot Local User Management

User List

User Name	Password

HTTP Redirect

HTTP Redirect Enable Disable

HTTP Destination IP

HTTP Destination Port

HTTP Source Network

If you need to separate the LAN portion of the router from WLAN, enable the “Separate Wifi from LAN bridge” option.

Enter the primary and secondary Radius server IP addresses as shown.

Primary server: 173.224.125.185
 Secondary server: 74.208.78.152

DNS IP should be the IP address of the ISP’s DNS server

Redirect URL should be URL of the login page. Please contact Wifi-soft to design custom portal page designs for your hotspots.

If the portal/login page is hosted on your server, you will also need to include your web server in the UAM allowed list

Shared key is the secret key between the Radius server and the router. It should match the one configured in the router.

If you want to enable login page redirection for WLAN (wireless) only, then select WLAN from the drop-down list for DHCP Interface.

Enter the NAS Id for the router. NAS Id is the friendly name used to identify the router.

Leave the UAM secret and DNS settings as shown.

Under UAM allowed, enter the following values (comma separated):

www.wifi-soft.net,www.wifi-soft.com,74.208.78.152,173.224.125.185

Next enable HTTP Redirect option and leave the default setting.

Save the above settings.

If chillispot is configured correctly, then you should get an IP address in the following subnet when you connect to WLAN:

192.168.182.X

Troubleshooting DD-WRT:

If you enable SSH (secure shell) access to DD-WRT, then you should be able to directly log into the firmware installed on the router. The username and password is same as the one for your admin page. Please make sure that you connect to the router using the wired port.

To determine whether Chillispot is working correctly, please execute the ps command. The login page will only work if "chilli" process is running in the router and chilli.conf file is created in the /etc directory.

If the 'chilli' process is not running, then you need to verify your chillispot configuration once again.

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 Radius Group

New Group Information	
Group Name *	wifi-soft
Group Type	device
Description	Wifi-soft device group
Location	

- 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.

New Location

Location Information	
Location Name *	Cafe House
Address	120 Range Hill Road
City-State *	Austin - TEXAS <input type="button" value="New"/>
Zipcode	78729
Latitude	
Longitude	
Type	Coffee Shop

- 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:

Edit gateway : mikrotik test	
Device Name *	<input type="text" value="mikrotik test"/>
Device UserName	<input type="text" value="123456"/>
Device Password	<input type="text" value="123456"/>
IP Address *	<input type="text" value="65.65.110.170"/>
Secret *	<input type="text" value="secret"/>
Device Group *	<input type="text" value="FreeTest"/>
Device Type *	<input type="text" value="Microtik Gateway"/>
MAC Address	<input type="text" value="00-0B-6B-32-17-F4"/>
Description	<input type="text"/>
Location	<input type="text" value="Wifi-soft Office"/>

- 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	<input type="text" value="69.192.181.32"/> (If different than device IP)
Modem Monitor Type	<input checked="" type="radio"/> Ping <input type="radio"/> HTTP <input type="radio"/> SNMP
Monitoring Interval	<input type="text" value="15 minutes"/> Custom Interval <input type="text"/> (10 mins or more)
Notify Enabled	<input checked="" type="checkbox"/>
Notify After	<input type="text" value="3"/> failures
Email Notifications	<input type="text" value="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. You newly configured DD-WRT 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.

These instructions will help you get started with DD-WRT compatible routers. For advanced configuration, please refer to DD-WRT and Chillispot documentation.