

Quick Start Guide for Gemtek 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 Gemtek P-560 gateway user guide for configuring your Gemtek gateway in WiFiLAN. Please refer to Wi-FiLAN administrator guide and Gemtek 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 Gemtek 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 Wi-FiLAN you will need the WAN MAC address, RADIUS secret, serial number (if any) and public IP address of your Gemtek gateway
5. Finally, you need an active Wi-FiLAN account. Please contact Wifi-soft's sales to create your Wi-FiLAN account

Gemtek Setup

We assume that you have properly connected your Gemtek gateway to a broadband connection with static IP address. Additionally, your Gemtek admin interface is either accessible via a HTTP connection (WAN or LAN) or through a command line interface. This document explains the Gemtek configuration using a HTTP interface.

1. First you need to configure your RADIUS server setting on the gateway. To configure RADIUS server click on the RADIUS settings menu under the network interface. You will see the RADIUS setting screen.
To edit any parameter on this page, click the edit button. The following screen will be displayed to you. Enter the authentication IP, accounting IP and port numbers and backup IP of our RADIUS server

The RADIUS server settings are as follows:

Server Name	IP Address	Authentication Port	Accounting Port
Primary RADIUS server	74.208.78.152	1812	1813
Backup RADIUS server	69.64.34.236	1812	1813

RADIUS Servers	
description	value
name	BRO4200
default	<input checked="" type="checkbox"/>
authentication ip	74.208.78.152
authentication port	1812
authentication secret	secret
accounting ip	74.208.78.152
accounting port	1813
accounting secret	secret
backup on	<input checked="" type="checkbox"/>
backup ip	69.64.34.236
backup port	1812
backup secret	secret
reverse accounting	disabled ▼
user password md5sum secret	disabled ▼
strip WISP	enabled ▼
UAM authentication method	chap ▼

You can select either PAP or CHAP as UAM authentication method. CHAP is preferred since the authentication information is transmitted in encrypted format.

- Next you need to set different RADIUS attributes for your user session. This configuration is optional. For NAS server id, enter a unique name. For example: WS_001 (first gateway of wifi-soft).
If you need bandwidth control, then set the bandwidth up and bandwidth down parameters to the desired values.

RADIUS settings		
setting	value	action
RADIUS retries	5	edit
RADIUS timeout (seconds)	2	edit
NAS server id		edit
user session timeout (seconds)	72000	edit
user accounting update interval (seconds)	600	edit
user accounting update retry (seconds)	60	edit
user idle timeout (seconds)	900	edit
location ISO country code	us	edit
location E.164 country code	1	edit
location E.164 area code	408	edit
location network	GEMTEK_SYSTEMS	edit
hotspot operator name	GEMTEK_SYSTEMS	edit
location	Terminal_Worldwide	edit
bandwidth up	1.00 Mbps	edit
bandwidth down	1.00 Mbps	edit

- Set the Domain policy for WISP to [Username@Domain](#) under the Network Interface -> RADIUS -> WISP section.

Domain Policy			
Domain Policy	Prefix Length	Action	
Username@Domain ▼	4 ▼	save	cancel
Username@Domain			
Domain/UserName			
use name prefix			
RADIUS name	bound to	action	

Next you need to setup the login page for your hotspot. Gemtek allows you to configure an internal as well as an external login page. Using external login page is more convenient since it allows you to customize the look-and-feel of the web page to your specifications. You can also put custom branding (logo, images, etc) on the login page.

The image below shows how to configure the external login page. Replace the login and logout URL with the respective URLs on your server.

Customize Page Status		
Description	Status	Action
Customize Page	enabled	edit
Pop Logout Page	enabled	edit
Logout Page width size: 760 Logout Page Height size: 600		edit
Use External Page	enabled	edit
External login page url:	http://60.244.104.172/login.htm	
External Logout page url:	http://60.244.104.172/logout.htm	edit
Update external page interval(Sec.):	7200	edit
Update external login and logout url page immediately		done

See example external login html page [here](#) and See example external logout html page [here](#)

If you want a popup logout window, then enable the “Pop Logout Page” option. The HTML code below explains how to configure the login page. The code in red is needed for the authentication to work correctly. You can embed the HTML form inside your customized login page.

```

<td width="100%" height="18" colspan="2">
<p align="center"></td>
</tr>

<tr>
<td width="100%" colspan="2" height="62">
<table border="0" width="100%">
<tr>
<form method="POST" action="/login.user">
<td width="50%" align="right"><b><font size="2">Account:</font></b></td>
<td width="50%">
<input type="text" name="username" size="20">
</td>
</tr>
</tr>
<tr>
<td width="50%" align="right"><b><font size="2">Password:</font></b></td>
<td width="50%">
<input type="password" name="password" size="20">
</td>
</tr>
</table>
</td>
</tr>

<tr>
<td width="100%" colspan="2" height="27">
<p align="center">
<input type="submit" value="Login" size="20">
</td>
</tr>

```

If your login page contains links to other websites, then we need to add passthrough or wall garden links in the Gemtek controller. The user will be able to access the wall garden links or IP addresses without logging into the hotspot. Generally the company URL or free links are provided to the user so s/he can browse through the provider’s website before purchasing hotspot access.

network interface user interface system connection built-in AAA				
configuration administrator start page walled garden web proxy				
Walled Garden URLs				
URL for user	string to display			action
no free site (or walled garden) URL is specified				
				<input type="button" value="new URL"/>
Walled Garden hosts				
type	host	netmask	port	action
no free site (or walled garden) host is specified				
				<input type="button" value="new host"/>

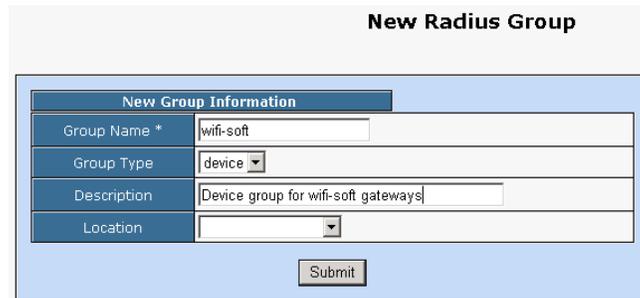
To add new Wall Garden Link, click on the “New URL” button.

Lastly you can configure the welcome or post-login URL. The user will be redirected to this URL after he logs in successfully.

network interface user interface system connection built-in AAA				
configuration administrator start page walled garden web proxy				
Start Page				
setting	value			action
start page URL	http://www.gemtek-systems.com			<input type="button" value="edit"/>

WiFiLAN Setup

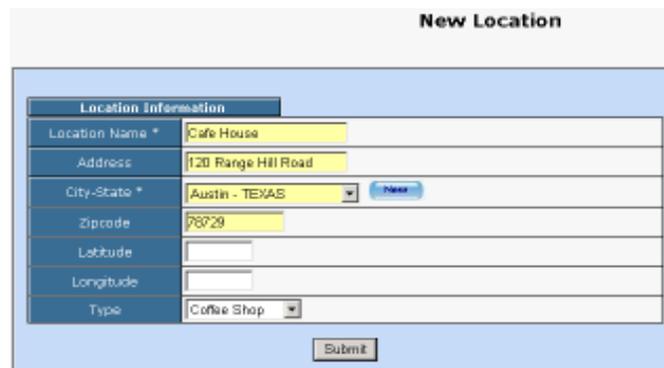
1. You need to log into WiFiLAN by pointing your browser to <https://www.wifi-soft.net/wifilan/>
2. Before you add your first gateway in RADIUS section, you need to create a device group to organize your gateways. To create a new device group, click on the RADIUS menu option and then on the Groups submenu.



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
Zipcode	78729
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 *	24.198.234.8
Secret *	wifi-soft
Device Group *	wifi-soft
Device Type *	Gemtek P-560
MAC Address	00-0C-2F-45-A8-29
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. You newly configured Gemtek 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.