

Configuring RADIUS per Group

RADIUS server parameters can also be configured per Group. Settings are the same as for a system-wide RADIUS server.

The screenshot shows the Firetide FWC 2050 configuration interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Plans', and 'Diagnostics'. The 'Configuration' tab is active, and the 'Security' sub-tab is selected. The main content area is titled 'Authentication Server' and shows a configuration window for 'Auth-1'. The 'Group Name' is set to 'Auth-1'. Below this is a table for 'External RADIUS Server' with columns for 'IP Address', 'Port', and 'Shared Secret'. The table has four rows: 'Primary Authentication Server' (Port 1812), 'Secondary Authentication Server' (Port 1812), 'Primary Accounting Server' (Port 1813), and 'Secondary Accounting Server' (Port 1813). Below the table are fields for 'Reauthentication Time (Seconds)' (set to 0) and a checkbox for 'Update Global Key Every (Seconds)' (set to 0).

Configuring an LDAP Authentication Server

The screenshot shows the Firetide FWC 2050 configuration interface. The top navigation bar is the same as in the previous screenshot. The 'Configuration' tab is active, and the 'Security' sub-tab is selected. The main content area is titled 'Choose Authentication Server Type' and shows three radio button options: 'External RADIUS Server', 'Internal Authentication Server', and 'External LDAP Server'. The 'External LDAP Server' option is selected. Below this is a configuration window for 'External LDAP Server' with the following fields: 'Server IP', 'Server Port' (set to 389), 'User Base DN', 'Workgroup Name', 'Admin Domain', 'Domain Admin User', and 'Domain Admin Password'.

- Server IP:** Enter the LDAP Server IP address.
- Server Port:** Enter the server's port number.
- User Base DN:** Enter the DN for the base of users.
- Admin Domain:** Defines the administrative domain.
- Domain Admin User:** User name for administering domain.
- Domain Admin Password:** Password for Domain Admin User.

Profiles

Profiles are the basic building blocks of HotPoint AP configurations. They represent the settings of a virtual machine that can be instantiated on any HotPoint unit. Profiles are a set of configuration that can be applied onto an AP. These configurations include radio parameters, load balancing and rate limit parameters. Each access point under the control of the FWC2050 is capable of supporting 8 profiles per radio, or 16 profiles in total.

Small Networks

For small scale WLAN networks, you can use the basic configuration, and you don't need to create additional profile groups. All APs will belong to the same group and have the same configuration.

Larger Networks

For larger deployments, comprised of different sets of WLAN networks, you will need to use the advanced profile option. Under the Advanced profiles tab, you can create, edit, and delete profile groups. Editing a profile group will take the user to a profile edit page similar to the one under basic setting.

The Delete button, at the bottom of the screen, will delete the selected profile.

Once the creation of the profiles are done, you can go to the Configuration->WLAN Network page to assign profile groups to the APs.

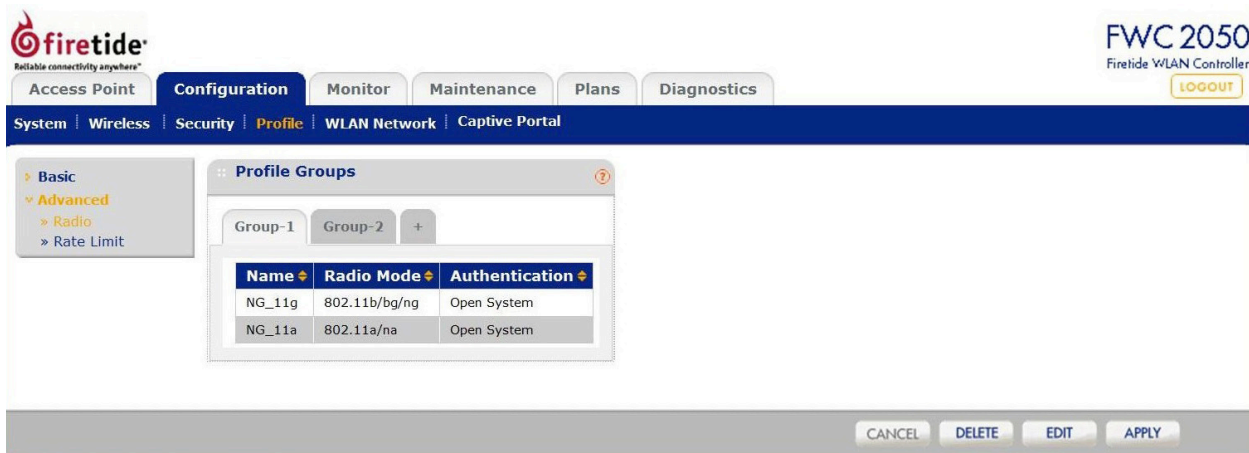
For ease of use, during a profile add, an option is given to the user to clone a profile. Cloning of a profile copies all the settings except the name and SSID.

Configuration templates for Authentication Server Settings in case of LDAP/Radius and MAC ACL list configuration needs to be done separately in their respective pages under Security. Once done, you can assign one of the created security profiles to a particular profile.

Profile Groups

Complex deployments may require multiple sets of profiles. Groups are a way of managing large numbers of profiles. The controller supports configuration of up to 8 distinct set of grouped profiles. Each profile group can contain up to 16 profiles. You can configure these profiles and profile groups without worrying about the state of the APs. Once the APs connect to the controller these profile configuration will be pushed onto the AP. This is the method used to configure the WLAN network offline and then push the configuration once the WLAN network is up and running.

Two groups are defined by default. Additional groups can be created by clicking on the + tab next to the groups, in the Configuration - Profile - Advanced - Radio section, as shown below.



Basic and Advanced - Radio

Settings for Basic and Advanced are similar, except that the Advanced option allows you to configure settings per Group.

The screenshot shows the Firetide configuration interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Plans', and 'Diagnostics'. Below this is a secondary navigation bar with 'System', 'Wireless', 'Security', 'Profile', 'WLAN Network', and 'Captive Portal'. The main content area is titled 'Edit Profile (Basic)' and contains several sections: 'Profile Definition' (Name: SP_11g, Wireless Network Name (SSID): HotPoint5100g, Broadcast Wireless Network Name (SSID): Yes), 'Client Authentication' (Network Authentication: Open System, Data Encryption: None, Wireless Client Security Separation: Disable, Vlan: 1), 'Authentication Settings' (Mac Ad Group: basic, Captive Portal: unchecked), and 'Wireless QoS' (Wi-Fi Multimedia (WMM): enable, WMM Powersave: enable). At the bottom of the window are buttons for 'CANCEL', 'DELETE', and 'APPLY'.

- Name:** Displays user-assigned name of profile.
- SSID:** Displays the SSID of access point.
- Broadcast SSID:** Enables broadcasting of the SSID in the clear.
- Network Authentication:** Displays type of authentication required.
- Data Encryption:** Displays encryption type.
- Wireless Client Security Separation:** Controls security among clients connected to AP.
- VLAN:** Specifies VLAN for traffic to/from this Profile.
- MAC ACL Group:** Defines MAC address Access Control List preferences.
- Captive Portal:** Defines which, if any, captive portals are being managed.
- Wi-Fi Multimedia (WMM):** Enables WMM mode. Select this option to ensure that applications that require better throughput and performance are provided special queues with higher priority. WMM defines the following four queues in decreasing order of priority:
- Voice:** The highest priority queue, minimum delay; ideal for VOIP and streaming media.
 - Video:** The second highest priority queue, low delay. Video applications are routed to this queue.
 - Best Effort:** The medium priority queue, medium delay. Most IP applications use this queue.
 - Background:** Low priority queue with high throughput. Applications which are not time-sensitive but require high throughput can use this queue.

With WMM enabled, QoS prioritization and coordination of wireless access is on. Disabling WMM will deactivate QoS control of station EDCA parameters on upstream traffic flowing from the station to the access point.

- WMM Powersave:** Enables Powersave option for WMM.

Load Balancing

The screenshot shows the Firetide FWC 2050 configuration interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Plans', and 'Diagnostics'. Below this, a secondary navigation bar shows 'System', 'Wireless', 'Security', 'Profile', 'WLAN Network', and 'Captive Portal'. The main content area is titled 'Load Balancing' and is divided into two tabs: 'HOTPOINT5100' and 'HOTPOINT5200'. A table below the tabs shows the configuration for two radio types:

Radio	Max Client	RSSI
802.11b/bg/ng	64	100
802.11a/na	64	100

Max Client: The maximum number of clients that can connect to this profile.

RSSI: Defines the weakest signal that the APs in this profile will accept.

The controller supports balancing of load on the APs it manages. This is based on the number of clients connected to APs as well as signal quality of clients. At the time a client discovers APs (using probe requests) or sends association frames, AP decides whether to accept a client or not based on the number of clients already connected or the signal strength of the clients.

The two configurations are:

Max Clients: The maximum number of wireless clients that can connect to each radio of Access Point at one time. A value of 64 can be selected to specify to allow maximum supported by Access Point.

RSSI: The minimum signal quality in percentage (0 - 100) % expected from the wireless clients that connect to the Access Points. A value of 0 means this check is not enforced and load balancing is disabled.

Setting the Max. number of clients to a low value (compared to the total number of client in an office/floor) is recommended when there are several APs and the administrator would like a good distribution of clients between the access points.

Setting the RSSI to a high percentage would mean that only clients near to APs will be permitted to associate to the APs and is good in situation where the throughput expectation is high. In scenarios, where the clients can be expected to be far away (or the number of APs is less), this should be set to a lower value.

Basic and Advanced - Rate Limiting

The screenshot shows the Firetide FWC 2050 configuration interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Plans', and 'Diagnostics'. Below this, a secondary navigation bar shows 'System', 'Wireless', 'Security', 'Profile', 'WLAN Network', and 'Captive Portal'. The main content area is titled 'Rate Limit' and shows configuration for two radio types: '802.11b/bg/ng' and '802.11a/na'. A table below the tabs shows the configuration for a specific profile:

Profile Name	SSID	Rate Limit
NG_11g	HotPoint5100g	0

The Rate Limiting feature can be configured differently for each BSSID in security profile group. Rate limiting is done per BSSID and is configured as a percentage of available bandwidth. Available bandwidth is determined by the number of errors occurring during transmission and the amount of time a packet spends in the transmission queue.

The available bandwidth is distributed among the BSSIDs configured on the Access Points as a specified percentage. The percentage configured for a BSSID is shared among all the clients connected to it. The total of the percentages distributed among the BSSIDs can be up to 100%.

Rate Limiting can be disabled by setting the limit to 0%. This can be useful for having BSSIDs for management/administration/testing.

Rate Limit: The slider bar and value specify configured rate limit values.

WLAN Network

This screen allows you to assign each AP to a group.

The screenshot shows the Firetide FWC 2050 WLAN Controller interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Plans', and 'Diagnostics'. The 'Configuration' tab is active, and the 'WLAN Network' sub-tab is selected. Below the navigation bar, there is a 'Basic' tab and a 'WLAN Group Assignment' section. This section contains a table with the following data:

IP	MAC	Model	Name	Building	Floor	Status	Group Name
10.0.3.141	00:18:c2:00:20:01	HOTPOINTS100	Firetide-AP1	Building-1	Floor-1	Connected	basic
10.0.3.120	00:18:c2:00:20:02	HOTPOINTS100	Firetide-AP2	Building-1	Floor-1	Connected	basic

Captive Portal

The Captive Portal allows you to require the user to log in, and optionally accept a EULA, in order to use the wireless service.

The screenshot shows the Firetide FWC 2050 WLAN Controller interface with the 'Captive Portal' sub-tab selected. The 'Portal Settings' section is visible, showing the following configuration options:

- Portal Type:** Radio buttons for 'Guest' (selected) and 'Captive'.
- Select Placement:** Three preview windows showing the login form positioned in the center, bottom, and top of the background image. Below these are radio buttons for 'Center' (selected), 'Bottom', and 'Top'.
- Load Background Image:** A text input field and a 'Browse...' button.
- EULA:** A section titled 'EULA Text Required' with a checked checkbox and a text area containing the text: 'You can erase this, it is only a test.'

At the bottom of the interface, there are buttons for 'CANCEL', 'PREVIEW', and 'APPLY'.

- Portal Type:** Portals can be guest (open to all) or require an ID and password. In Guest mode, the user must enter an email address to gain access. In Captive mode, the user must enter a user name and password. These values are defined as shown in "Maintenance" on page 32.
- Select Placement:** Allows you to position the login in a location compatible with the background image.
- Load Background Image:** Allows you to place an image with logos, etc as required for your application.
- EULA Text Required:** You can optionally require a EULA. Enter the EULA text in place of the 'test' text, and tick the enable box.

Chapter 6 Monitoring

Controller

Summary

Network Status

Device	Total		Alarms	
	Up	Down	Critical	Major
Access Points	2	0	0	0
Clients	0	NA	NA	NA

Wireless Clients

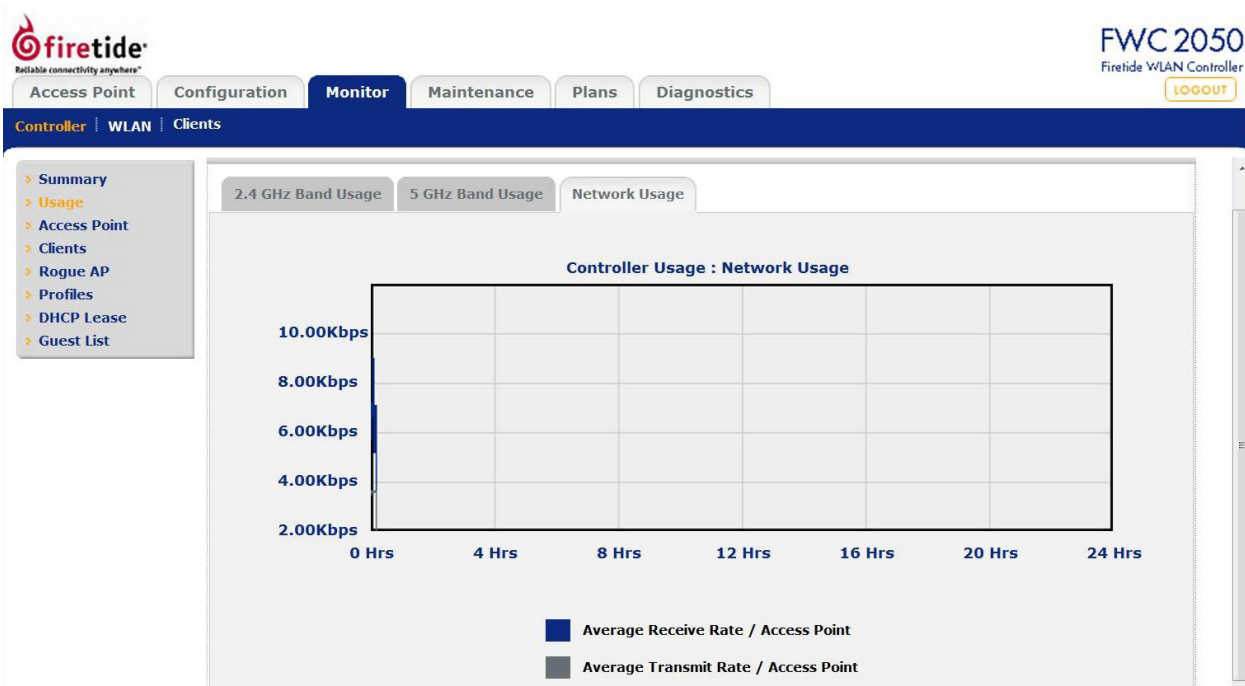
Open	WEP	WPA	WPA2
0	0	0	0

Network Info

Firmware Version	0.B.2_1684
Controller Uptime	44 mins, 27 secs
Last Reboot	Wed Dec 31 16:00:19 1969
Last Configuration Change	Wed Dec 31 16:16:24 1969
Last Channel Allocation	Wed Dec 31 16:05:19 1969
Last Admin Login	Wed Dec 31 16:13:11 1969

This screen displays a summary of the current managed Access Point status, rogue access points detected, current wireless stations connected, FWC2050 System Information and Network Usage. Clicking on the individual windows will lead to a new screen showing greater detail.

- Up:** Managed Access Points running properly.
- Down:** Number of managed Access Points which cannot be pinged.
- Critical:** Number of managed Access Points which can be pinged but cannot be logged in or device is different from the one which was configured.
- Major:** Number of managed Access Points whose configuration differs from the one which is set on the FWC2050. This is mostly owing to Access Point having an unsupported software version running or configuration changes were done on WMS when Access Point was Down/Offline.
- Rogue AP Current:** The number of unique rogue/neighbor Access Point bssid which can be observed now.
- Rogue AP Count 24hrs:** The number of unique rogue/neighbor Access Point bssid observed over the last 24 hrs.
- Wireless Clients:** This section displays count of Current Wireless Stations of managed Access Points.
- FWC2050 Firmware Version:** Current FWC2050 firmware version.
- Controller Uptime:** Time since last controller restart.
- Last Reboot:** When was the FWC2050 rebooted last time.
- Last Configuration Change:** When last configuration change was done on the FWC2050.
- Last Channel Allocation:** When last automatic channel Allocation was performed.
- Last Admin Login:** When Admin logged in last time.



This shows the transmit, receive, and network usage rates for the AP.

Access Point List

The screenshot shows the 'Access Point List' in the Firetide FWC 2050 interface. The table below lists the details for three managed APs.

Select	Name	Location	Status	MAC	IP	Model	Building	Floor	2.4 GHz Channel	5 GHz Channel	Uptime
<input checked="" type="checkbox"/>	Firetide-AP2		healthy	00:18:c2:00:20:02	10.0.3.160	HOTPOINTS100	Building-1	Floor-1	6 / 2.437Ghz	36 / 5.180Ghz	16 days, 22 hour
<input type="checkbox"/>	Firetide-AP		healthy	00:18:c2:00:20:0a	10.0.3.136	HOTPOINTS100	Building-1	Floor-1	6 / 2.437Ghz	36 / 5.180Ghz	4 days, 20 hours
<input type="checkbox"/>	Firetide-AP		healthy	00:18:c2:00:20:04	10.0.3.140	HOTPOINTS200	Building-1	Floor-1	6 / 2.437Ghz	36 / 5.180Ghz	14 days, 19 hour

This shows the status of each AP under management.

- Name:** Displays name of Access Point.
- Location:** Displays location of Access Point.
- Status:** Displays status of Access Point.
- MAC Address:** Displays MAC Address of Access Point.
- IP address:** Displays management IP address used by the FWC2050 to connect to Access Point.
- Model:** Displays Access Point Model.
- Building:** Displays building name where Access Point is located.
- Floor:** Displays floor where Access Point is located.
- 2.4 GHz channel:** Displays 2.4 GHz channel configured on Access Point.
- 5 GHz channel:** Displays 5 GHz channel configured on Access Point.
- Uptime:** Shows elapsed time since last AP reboot.

Clients

This shows connected clients.

Rogue AP List

Select	MAC	SSID	Channel	Privacy	Last Beacon	Category	Known/UnKnown
<input checked="" type="radio"/>	00:26:f2:8b:20:30	NG_11a	40	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:2c:00	NG_11g_LoadBalance	6	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:20:37	NG_11a-7	40	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:20:20	NG_11g	1	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:2c:10	NG_11a_LoadBalance	153	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:20:21	NG_11g-1	1	Unsecured	Wed Dec 31 16:33:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:20:22	NG_11g-2	1	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:20:23	NG_11g-3	1	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:20:24	NG_11g-4	1	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:20:25	NG_11g-5	1	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:20:26	NG_11g-6	1	Unsecured	Wed Dec 31 16:37:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:20:27	NG_11g-7	1	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:26:00	NG_11g_LoadBalance	6	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:26:f2:8b:26:10	NG_11a_LoadBalance	149	Unsecured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:18:c2:04:0b:3b	NewFTGuestAccess	11	Secured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown
<input type="radio"/>	00:18:c2:00:01:97	4500WPA2	1	Secured	Wed Dec 31 16:49:19 1969	Neighbor	Unknown

This shows a list of detected rogue APs. You can double-click on an AP to see a detailed view. The shaded region (at right in this example) shows the estimated location of the rogue AP.

Profiles

SSID	Security	Radio Mode	Status	Group Name
HotPoint5100g	Open	802.11b/bg/ng	Active	basic
HotPoint5100a	Open	802.11a/na	Active	basic
NG_11g	Open	802.11b/bg/ng	Inactive	Group-1
NG_11a	Open	802.11a/na	Inactive	Group-1
NG_11g-0	Open	802.11b/bg/ng	Inactive	Group-2
NG_11a-0	Open	802.11a/na	Inactive	Group-2

- SSID:** Wireless SSID configured for that Profile.
- Security:** Open/wep/wpa/wpa2 authentication mode of security.
- Mode:** 802.11 b/bg/ng or 802.11 a/na mode for security profile.
- Status:** Indicates usage of that profile.
- Group Name:** Name assigned to the group.

DHCP Lease

Host Name	MAC	IP	End Time	End Date	VLAN
-----------	-----	----	----------	----------	------

The DHCP Lease screen displays current DHCP clients which have been allocated IP addresses.

- Host Name:** The host name of the client, if possible to resolve.
- IP:** IP address allocated to DHCP client by the FWC2050.
- End Time:** The DHCP Lease End time for DHCP client.
- End Date:** The DHCP Lease End date for DHCP client.
- MAC:** The Ethernet MAC address of DHCP client.
- VLAN:** VLAN the Client is using to connect.

Use the **REFRESH** button to update client DHCP Lease display.

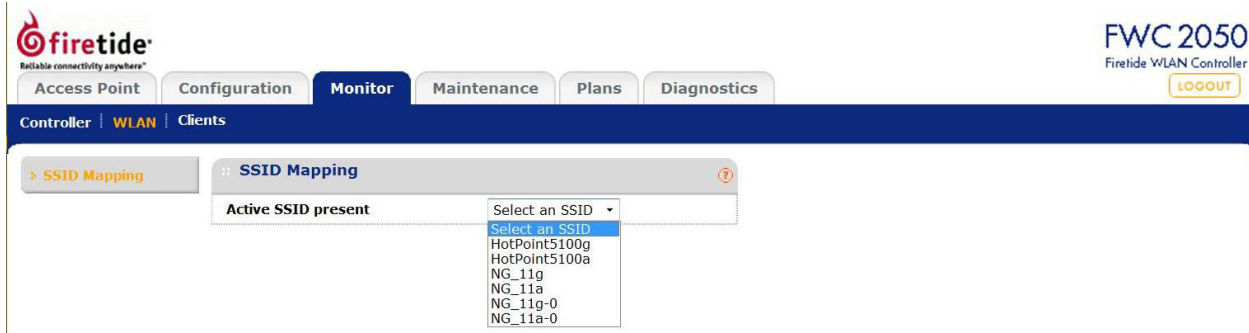
Guest List

IP	Email Address
----	---------------

This shows IP address and email addresses (obtained during guest access login).

WLAN

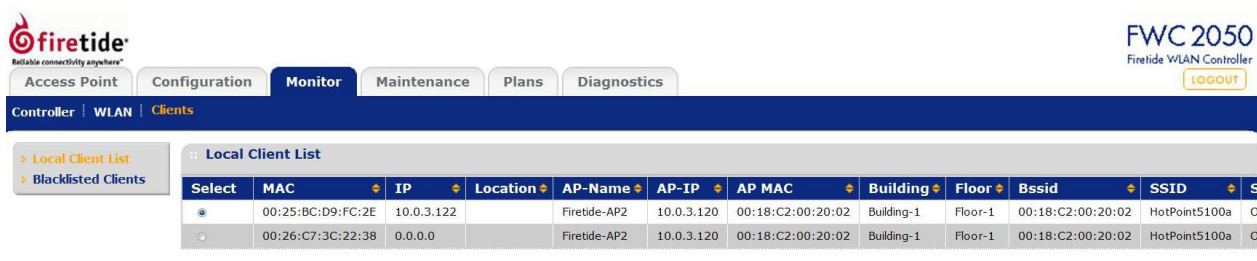
SSID Mapping



This shows the SSIDs detected within range of the AP network.

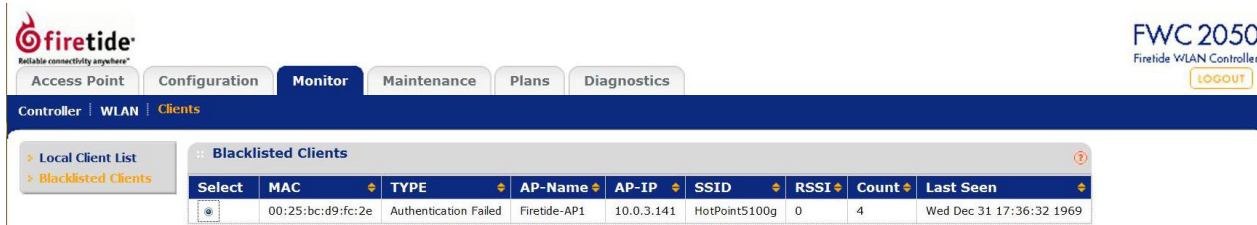
Clients

Local Client List



This screen shows connected clients.

Blacklisted Clients



This screen shows blacklisted clients.

Chapter 7 Maintenance

User Management

The top screenshot shows the Firetide FWC 2050 web interface. The 'Maintenance' tab is selected, and the 'User Management' sub-tab is active. A table lists the following users:

User Name	User Type
admin	Administrator
guest	Read Only
license	License Management Only

The bottom screenshot shows the 'Edit User' dialog box. The 'User Name' field is set to 'admin'. The 'User Type' dropdown is set to 'Administrator'. The 'Old Password', 'New Password', and 'Confirm New Password' fields are empty. The dialog has 'CANCEL', 'APPLY', and 'RESET' buttons.

This allows adding and removing FWC2050 administrative users. “admin” is the default user with administrative privileges and cannot be removed.

- User Name:** Add the name of the new user.
- Old Password:** Enter the old password to make changes.
- User Type:** Specify the type of access permitted to FWC2050 user Read-only/Administrative. A read-only user cannot make any configuration changes. He is allowed to see the all the statistics and configuration information.
- Password:** Type a new user password.
- Confirm Password:** Retype the new user password to confirm.

Upgrade

Upgrade FWC2050 Firmware

You can install a new version of the FWC2050 software using the Firmware Upgrade page. You have a choice of three methods. You can use a local file, or FTP or TFTP to access a remote file.


You can also set the upgrade to occur immediately, or at a scheduled time.

The screenshot shows the Firetide FWC2050 Firmware Upgrade page. The 'Local File' radio button is selected. The 'Schedule' section shows 'Scheduled Upgrade Status' set to 'None' and 'When to Upgrade?' set to 'Now'. The 'Server Parameters' section is not visible as it is only shown for remote file methods.

The screenshot shows the Firetide FWC2050 Firmware Upgrade page with the 'FTP' radio button selected. The 'Server Parameters' section is visible, containing fields for 'Server IP', 'File Name', 'User Name', and 'Password'. The 'Schedule' section shows 'Scheduled Upgrade Status' set to 'None' and 'When to Upgrade?' set to 'Now'.

The screenshot shows the Firetide FWC2050 Firmware Upgrade page with the 'TFTP' radio button selected. The 'Server Parameters' section is visible, containing fields for 'Server IP' and 'File Name'. The 'Schedule' section shows 'Scheduled Upgrade Status' set to 'None' and 'When to Upgrade?' set to 'Now'.

Go to the Firetide Web site (www.Firetide.com) customer service downloads section to get new versions of the FWC2050 software. Includes AP firmware.

 **IMPORTANT!** Once you click **Upload** do NOT interrupt the process of sending the software to the FWC2050 and restarting the FWC2050.

Backup/Restore

The screenshot shows the Firetide FWC 2050 web interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Plans', and 'Diagnostics'. The 'Maintenance' tab is selected, and the 'Backup/Restore' sub-tab is active. The main content area is titled 'Backup/Restore' and contains two sections: 'Backup' with a 'BACKUP' button and 'Restore' with a 'Browse...' button.

Backup: Allows you to save the settings of the FWC2050 to a file.

Restore: Configures the FWC2050 to the settings previously saved.

Reboot/Reset

The top screenshot shows the 'Reboot/Reset Controllers' page. It has tabs for 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Plans', and 'Diagnostics'. The 'Maintenance' tab is active, and the 'Reboot/Reset' sub-tab is selected. The main content area is titled 'Reboot/Reset Controllers' and contains a 'Reset/Reboot' section with radio buttons for 'reboot' and 'reset', and a 'Reset type' section with radio buttons for 'hard' and 'soft'.

The bottom screenshot shows the 'Reboot Access Points' page. It has the same navigation bar. The 'Maintenance' tab is active, and the 'Reboot/Reset' sub-tab is selected. The main content area is titled 'Reboot Access Points' and contains a search bar for 'Search Access Point by IP/MAC/Name' with 'SEARCH' and 'CLEAR' buttons. Below the search bar is a table titled 'List of Access Points'.

<input type="checkbox"/>	IP	MAC	Name	Building	Floor	Location
<input type="checkbox"/>	10.0.3.141	00:18:c2:00:20:01	Firetide-AP1	Building-1	Floor-1	
<input type="checkbox"/>	10.0.3.120	00:18:c2:00:20:02	Firetide-AP2	Building-1	Floor-1	

Both Controllers and Access Points can be rebooted or reset to factory parameters.

Remote Management

Session Timeout

The screenshot shows the Firetide FWC 2050 web interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Plans', and 'Diagnostics'. The 'Maintenance' tab is selected, and the 'Session Timeout' sub-tab is active. The main content area is titled 'Session Timeout' and contains a text input field for 'Timeout (minutes)' with the value '5'.

You can specify a time period for automatic disconnect if the management connection remains idle.

Logs & Alerts

Numerous Log Types are available.

System Alerts Log

The screenshot shows the Firetide FWC 2050 web interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance' (selected), 'Plans', and 'Diagnostics'. Below this is a secondary navigation bar with 'User Management', 'Upgrade', 'Backup/Restore', 'Reboot/Reset', 'Remote Management', and 'Logs & Alerts'. The main content area is titled 'System Alerts' and features a table with columns for Type, Severity, Description, and Raised Time. The table contains 16 rows of 'System UP' alerts. A left sidebar menu lists 'System Alerts', 'RF Events', 'Load Balancing', 'Rate Limit', and 'Save Logs'. At the bottom right of the table area are 'PREVIOUS' and 'NEXT' links, and at the bottom of the page are 'REFRESH' and 'CLEAR' buttons.

Type	Severity	Description	Raised Time
System	Normal	System UP	Wed Dec 31 16:00:29 1969
System	Normal	System UP	Wed Dec 31 16:00:18 1969
System	Normal	System UP	Wed Dec 31 16:00:18 1969
System	Normal	System UP	Wed Dec 31 16:00:18 1969
System	Normal	System UP	Wed Dec 31 16:00:18 1969
System	Normal	System UP	Wed Dec 31 16:00:18 1969
System	Normal	System UP	Wed Dec 31 16:00:18 1969
System	Normal	System UP	Wed Dec 31 16:00:18 1969
System	Normal	System UP	Wed Dec 31 16:00:18 1969
System	Normal	System UP	Wed Dec 31 16:00:23 1969
System	Normal	System UP	Wed Dec 31 16:00:23 1969
System	Normal	System UP	Wed Dec 31 16:00:19 1969
System	Normal	System UP	Wed Dec 31 16:00:20 1969
System	Normal	System UP	Wed Dec 31 16:00:18 1969
System	Normal	System UP	Wed Dec 31 16:00:20 1969
System	Normal	System UP	Wed Dec 31 16:00:19 1969

Shows logged events. The results can be filtered.

RF Events Log

The screenshot shows the Firetide FWC 2050 web interface with the 'RF Events' tab selected. The navigation and secondary navigation bars are identical to the previous screenshot. The main content area is titled 'RF Events' and features a table with columns for Type, Severity, Description, and Raised Time. The table contains two rows of 'Coverage Hole Detection' alerts. A left sidebar menu lists 'System Alerts', 'RF Events' (selected), 'Load Balancing', 'Rate Limit', and 'Save Logs'. At the bottom right of the table area are 'PREVIOUS' and 'NEXT' links, and at the bottom of the page are 'REFRESH' and 'CLEAR' buttons.

Type	Severity	Description	Raised Time
Coverage Hole Detection	Major	Coverage Hole detected around AP Firetide-AP in 5GHz frequency band in building Building-1 on Floor-1.	Wed Dec 31 20:35:15 1969
Coverage Hole Detection	Major	Coverage Hole detected around AP Firetide-AP in 2.4GHz frequency band in building Building-1 on Floor-1.	Wed Dec 31 20:45:15 1969

Shows logged RF events.

Load Balancing

The screenshot shows the Firetide FWC 2050 interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance' (selected), 'Plans', and 'Diagnostics'. Below this is a secondary navigation bar with 'User Management', 'Upgrade', 'Backup/Restore', 'Reboot/Reset', 'Remote Management', and 'Logs & Alerts'. On the left, a sidebar menu lists 'System Alerts', 'RF Events', 'Load Balancing' (selected), 'Rate Limit', and 'Save Logs'. The main content area displays a table titled 'Load Balancing' with the following data:

Type	Severity	Description	Raised Time
System	Normal	Load Balancing[Bad RSSI] Event for Client 60:33:4b:04:8a:5f	Wed Dec 31 20:32:00 1969
System	Normal	Load Balancing[Bad RSSI] Event for Client 60:33:4b:04:8a:5f	Wed Dec 31 20:32:06 1969
System	Normal	Load Balancing[Bad RSSI] Event for Client 60:33:4b:04:8a:5f	Wed Dec 31 20:32:56 1969
System	Normal	Load Balancing[Bad RSSI] Event for Client 60:33:4b:04:8a:5f	Wed Dec 31 20:34:34 1969
System	Normal	Load Balancing[Bad RSSI] Event for Client 00:26:08:ae:e5:4a	Wed Dec 31 20:41:44 1969
System	Normal	Load Balancing[Bad RSSI] Event for Client 00:26:08:ae:e5:4a	Wed Dec 31 20:41:50 1969
System	Normal	Load Balancing[Bad RSSI] Event for Client 00:26:08:ae:e5:4a	Wed Dec 31 20:41:59 1969

Shows occurrences of load balancing among APs.

Rate Limit Events

The screenshot shows the Firetide FWC 2050 interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance' (selected), 'Plans', and 'Diagnostics'. Below this is a secondary navigation bar with 'User Management', 'Upgrade', 'Backup/Restore', 'Reboot/Reset', 'Remote Management', and 'Logs & Alerts'. On the left, a sidebar menu lists 'System Alerts', 'RF Events', 'Load Balancing', 'Rate Limit' (selected), and 'Save Logs'. The main content area displays a table titled 'Rate Limit' with the following data:

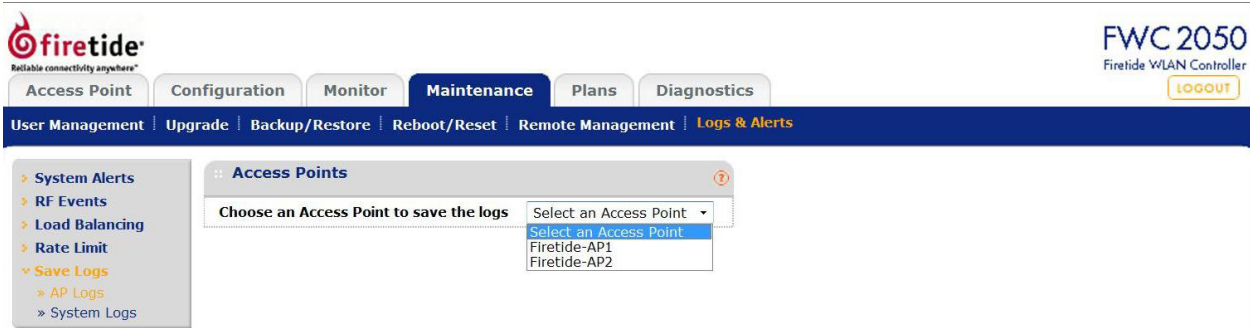
Type	Description	Severity	Raised Time
		All	All

Shows occurrences of rate-limit events on clients using excess bandwidth.

Saving Logs

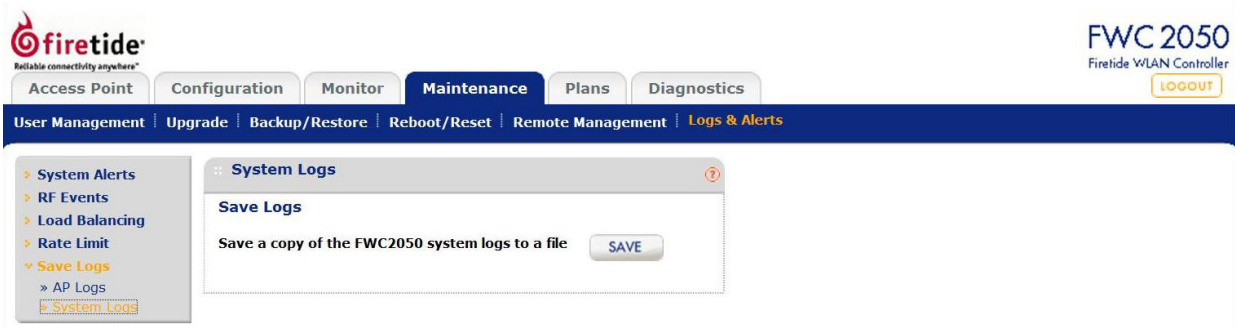
Logs from individual APs and the FWC2050 Controller can be saved.

AP Logs



Select an AP to save a log of events associated with it. You will be prompted to enter a file name and select a location.

System Logs



You will be prompted to enter a file name and select a location.

Appendix A HotPoint 5000 Specifications

Common Specifications

Wireless Interface

Model	Use
5100	Indoor, Worldwide. Radio 1: 2.4, Radio 2: 5 GHz
5200	Outdoor, Worldwide, Radio 1: 2.4, Radio 2: 5 GHz

Bands	Frequency (GHz)	Restrictions
802.11a	5.15-5.25	Indoor use only
802.11n	5.25-5.35 5.725-5.825	
	4.9-5.090	Japan only
	4.94-4.990	US Public Safety
	5.470-5.725	ETSI 301.893, U-NII
802.11b/g	2.412-2.484	
802.11n		

Bands (GHz)	Max TX Power
802.11a 5.725-5.825 UNII-3	20 dBm
802.11n	20 dBm 20 dBm 20 dBm 20 dBm
5.470-5.735 UNII	20 dBm
5.25-5.36 UNII-2	20 dBm
5.15-5.25 UNII-1	17 dBm
802.11b	20 dBm
802.11g, n	20 dBm

Supported Data Rates & Standards

- 802.11a 6/9/12/18/24/36/48/54Mbps
- 802.11a Capable of switching to 1/4 and 1/2 rates for 4.940 – 4.990 GHz Public Safety Band
- 802.11b 1/2/5.5/11Mbps
- 802.11g 6/9/12/18/24/36/48/54Mbps
- 802.11n 6.5/13/19.5/26/65/130 (20MHz LGB)
7.2/14.4/21.7/28.9/72.2/144 (20MHz SGB)
13.5/27/40.5/54/135/270 (40MHz LGB)
15/30/45/60/150/300 (40MHz SGB)
- Network Standards: IEEE 802.11a/b/d/g/e/f/h/i/n
- Dynamic Frequency Selection (DFS) capable in conjunction with FireTide Software application
- Security: WPA; 64/128/256 w/TKIP, AES

Power

- 48 VDC via DC connector or 802.3af PoE

Environmental

- Humidity (non-condensing): 10% to 90%
- Storage humidity (non-condensing): 5% to 95%
- Maximum altitude 15,000 feet (4600 meters)

Networking

- Up to 16 SSIDs (8 groups, 8 profiles) per HotPoint
- Up to 16 independent VLANs

Security, Authentication and Encryption

- 802.11i, WPA2
- 40-bit, 104-bit WEP keys
- 802.1x, RADIUS authentication
- SSID suppression
- MAC-address access control

Management and Configuration

- Integrated mesh and access management
- Multiple user interface options:
- Centralized management via HotView Pro
- Built-in web-based management
- Command line interface (CLI)
- Remote firmware upgrade
- Auto AP discovery
- Physical AP grouping

Hot Spot Services

- Virtual AP grouping
- User-based rate limiting
- Intercell/intracell blocking
- Captive portal management
- Walled garden
- Client-based policy management

Client Access Features

- Up to 128 concurrent users simultaneously per HotPoint
- L2 Fast Roam and L3 seamless mobility with controller
- Fast handoff enabled
- 802.11e (WMM) (Quality of Service)
- Auto configuration and image download

Network Ports

- One 10/100/1000 autosense Base-T port
- IEEE 802.3, 802.3 at based PoE

Warranty

- Hardware: one year limited warranty
- Software: 90 days limited warranty

5200 Outdoor Unit Specifications

Network Port

- One 10/100/1000 Mbps Ethernet port with weatherproof connector
- IEEE 802.3, 802.3u compliant
- CSMA/CD 10/100/1000 autosense

Enclosure

- Cast aluminum NEMA-4X/IP66 enclosure
- Six N-type antenna connectors
- Weatherproof 48VDC power connector
- Weight: 3.75 lbs (1.7 Kg) with bracket
- Dimensions: 8.2" x 8.6" x 2" (205 x 214 x 100 mm)

Environmental Specifications

- Operating temperature: -40° C to +60° C
- Storage temperature: -40° C to +85° C

Included Accessories

- Bracket for pole and wall mounting
- AC power adapter
- Three 2.4 GHz and three 4.9-5.8 GHz 3 dBi omni staging antennas, for indoor and temporary use only.

5100 Indoor Unit Specifications

Network Ports

- 10/100/1000 Mbps Ethernet port
- PoE PD on Port 1
- IEEE 802.3, 802.3u compliant
- CSMA/CD 10/100/1000 autosense

Enclosure

- Plenum-rated metal enclosure
- Six RP-SMA antenna connectors
- One DC power connector, 12 VDC \pm 15%, 3 A
- One Ethernet connector
- Weight: 0.9 lbs (.4 Kg)
- Dimensions: 7.3" x 6.8" x 1.4" (182 x 170 x 35 mm)

Environmental Specifications

- Operating temperature: 0° C to +60° C
- Storage temperature: -20° C to +70° C

Included Accessories

- AC power adapter
- Three 2.4 GHz and three 4.9-5.8 GHz 3 dBi omni staging antennas, for indoor use only.

Appendix B FWC2050 Specifications

Physical Specifications	<ul style="list-style-type: none">• Four GigE 10/100/1000 Mbps Ethernet ports with LEDs• IEEE 802.3, 802.3u compliant• CSMA/CD 10/100 autosense
Network Ports Enclosure	<ul style="list-style-type: none">• LEDs (power, 2.4 GHz, 5 GHz)• Reset button (recessed)• Weight: 2 lb 14 oz (1.3 kg)• Dimensions 9.4" X 5.9" X 1.6"
Power	<ul style="list-style-type: none">• DC Input: 12 VDC, 2.5 A• Port 1: IEEE 802.3at compliant PoE• External power supply: 100–240 VAC, 50/60 Hz
Environment Specifications	<ul style="list-style-type: none">• Operating temperature: 0° C to +60° C• Storage temperature: -20° C to +70° C• Humidity (non-condensing): 10% to 90%• Storage humidity (non-condensing): 5% to 95%• Maximum altitude 15,000 feet (4600 meters)
Included Accessories	<ul style="list-style-type: none">• AC power adapter with cord (non-North America power cord is separate orderable item)• Bracket for Rack Mounting

Appendix C Reset Procedure

Firetide Access Points may be reset to factory parameters. This is useful when returning a unit from field service or in recovering a unit you cannot communicate with. To reset a unit, apply power and wait for the unit to fully boot. This takes 60 to 90 seconds. Use a paperclip to press and hold the reset button for 15 seconds. Wait for the units to reboot before removing power.

Appendix D Regulatory Notices

FCC Part 15 Note

These devices comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Class A Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure

To ensure compliance with the FCC's RF exposure limits, the antenna used for this transmitter must be installed to provide a separation distance of at least 40 cm from all persons and must not be co-located or operated in conjunction with any other antenna or transmitter. Installers and end users must follow these installation instructions.

Modifications

Any modifications made to this device that are not approved by Firetide, Inc. may void the authority granted to the user by the FCC to operate this equipment.

Installation

Antenna(s) for the Model 5200 outdoor unit must be installed by a qualified professional. Operation of the unit with non-approved antennas is a violation of U.S. FCC Rules, Part 15.203(c), Code of Federal Regulations, Title 47.

Canadian Compliance Statement

This Class A Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.	Cet appareil numérique de la classe A respecte les exigences du Règlement sur le matériel brouilleur du Canada.
The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.	L'artifice pour l'opération dans la bande 5150-5250 MHz est seulement pour l'utilisation en salle pour réduire le potentiel pour l'interférence malveillante au radiotéléphone de co-canal les systèmes satellites.
The maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall comply with the EIRP limit.	L'augmentation d'antenne maximum permise pour les artifices dans les bandes 5250-5350 MHz et 5470-5725 MHz se pliera à la limite d'e.i.r.p.
The maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the EIRP limit specified for point-to-point and non point-to-point operation as appropriate.	L'augmentation d'antenne maximum permise pour les artifices dans la bande 5725-5825 MHz se pliera aux limites d'e.i.r.p. spécifiées pour le point-à-point et non l'opération de point-à-point comme appropriées.
Firetide 5100 and 5200 devices are certified to the requirements of RSS-210 for 2.4 GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.	Dispositifs Firetide 5100 et 5200 sont certifiés selon les exigences du CNR-210 pour les périphériques 2,4 GHz à étalement de spectre. L'utilisation de ce dispositif dans un système d'exploitation, partiellement ou complètement à l'extérieur peut obliger l'utilisateur à obtenir une licence pour le système en fonction de la réglementation canadienne. Pour de plus amples renseignements, communiquez avec votre bureau d'Industrie Canada.

NCC Statement

- 一、經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 二、低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Appendix E Limited End User Product Warranty

Pursuant to all provisions described herein, Firetide hardware products and Firetide antennas are warranted for one (1) year from the date of purchase against defects in the build materials and workmanship. Firetide does not warrant that the Products will meet any requirements or specifications of any End User Customer. This warranty applies to the entire Firetide product, including the AC power adapter.

Pursuant to all provisions described herein, Firetide software products are warranted for ninety (90) days from the date of purchase against defects in the build materials and workmanship. Firetide also warrants that the Software will materially conform to the documentation supplied by Firetide with the Software. In the event that the Software fails to materially conform to the documentation and an authorized Firetide reseller is notified in writing of such failure within the warranty period, Firetide or its reseller shall use commercially reasonable efforts to promptly correct the nonconformity. Firetide does not warrant that the use of the Software will be uninterrupted or error free.

The above warranties are void if the alleged defect cannot be verified by Firetide or if, as determined by Firetide, the product failure was due to tampering, abuse, misuse, accident, shipping, handling, or storage; or if the product has been installed, used, or maintained in a manner not described in the product user manual; or if the product has been altered in any way; or if product serialization has been altered. Any attempt to disassemble or repair the product by anyone other than Firetide immediately voids this warranty.

This warranty applies only to the original End User purchaser of the product and may not be transferred to any other individual or entity.

The foregoing are the exclusive warranties applicable to the product including the software, and the exclusive remedy for defects in the product. Firetide disclaims all other warranties, whether express, implied, statutory or otherwise, including but not limited to implied warranties of merchantability, non-infringement or fitness for a particular purpose. Some laws do not allow the exclusion of implied warranties so to that extent this limitation may not apply to you.

In no event will Firetide be liable for any special, incidental, consequential, punitive or indirect damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or other pecuniary loss) arising out of the use or inability to use the product or the performance, interruption or failure of the product, irrespective of the cause of action, even if Firetide has been advised of the possibility of such damages. Firetide's cumulative liability for all claims arising out of or in connection with this warranty will not exceed the amount paid by the original End User purchaser to purchase the product. The amounts payable for the product are based in part on these limitations and these limitations shall apply notwithstanding the failure of essential purpose of any remedy. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so to that extent the above limitations or exclusions may not apply to you.

By using the product the original End User purchaser agrees to and is bound by these terms and conditions.

In the event that a product fails to meet this warranty and Firetide's authorized reseller is notified in writing of such failure within the warranty period, Firetide shall, at its own discretion, either repair the product or replace it with the same or a functionally-equivalent product free of charge. Replacement products may contain refurbished materials in whole or in part. Firetide will honor this warranty provided the product is returned through an authorized Firetide reseller or dealer with shipping charges prepaid, along with a proof of purchase describing the original purchase date and product serial numbers if applicable. The authorized reseller must acquire a Return Materials Authorization (RMA) number from Firetide prior to returning any product. Firetide does not accept shipments of defective products without shipping charges prepaid.

Please contact your Firetide dealer for instructions on returning defective or damaged products for repair or replacement. Do not return products to Firetide, Inc. Please keep all original packaging materials in the event they are needed to return the product for servicing.



Firetide, Inc.
140 Knowles Avenue
Los Gatos, CA 95032 USA

Copyright Notice: ©2010 Firetide, Inc. All rights reserved. Trademarks: Firetide, the Firetide logo, Instant Mesh Networks, HotPort, HotPoint, and HotClient are trademarks of Firetide, Inc. All other trademarks are the property of their respective owners.