

HotPoint

# Installation & Setup Guide HotPoint 5000 Access Point FWC2050 WLAN Controller



HotPoint 5200 MIMO Outdoor Access Point



HotPoint 5100 MIMO Indoor Access Point

## Safety Instructions

Firetide 5200 units must be installed by a qualified professional. Failure to install this equipment properly may result in equipment damage, personal injury, or death.

### Explanation of Graphic Symbols



This symbol alerts the user to the presence of non-insulated dangerous voltage that may be of sufficient magnitude to constitute a risk of lethal electric shock to persons.



This symbol alerts the user to important operating, maintenance, and servicing instructions. Failing to comply with instructions may result in electrical shock.



This symbol alerts the user to the presence of important operating, maintenance, and servicing instructions. Failing to comply with this instruction may result in a hazard.



### Caution! Risk of electric shock!

#### POWER LINES CAN BE LETHAL

Do not install Firetide products where possible contact with power lines can be made. Antennas, poles, towers, guy wires, or cables may lean or fall and contact these lines. People may be injured or killed if they are touching or holding any part of equipment when it contacts electric lines. Make sure there is NO possibility that equipment or personnel can come in contact directly or indirectly with power lines.

#### ASSUME ALL OVERHEAD LINES ARE POWER LINES

The horizontal distance from a tower, pole or antenna to the nearest power line should be at least twice the total length of the pole/antenna combination. This will ensure that the pole will not contact power if it falls either during or after installation.

#### SURVEY THE SITE

Look over the entire site before beginning any installation and anticipate possible hazards. Never assume anything without checking it out for yourself! Don't take shortcuts!

#### TO AVOID FALLING, USE SAFE PROCEDURES WHEN WORKING AT HEIGHTS ABOVE GROUND

- Select equipment locations that will allow safe and simple installation.
- Don't work alone. A friend or co-worker can save your life if an accident happens.
- Don't attempt repair work when you are tired. Not only will you be more careless, but your primary diagnostic tool - deductive reasoning - will not be operating at full capacity.
- Use approved non-conducting ladders, shoes, and other safety equipment. Make sure all equipment is in good repair.
- If a tower or pole begins falling, don't attempt to catch it. Stand back and let it fall.
- If anything such as a wire or pole does come in contact with a power line, DON'T TOUCH IT OR ATTEMPT TO MOVE IT. Instead, save your life by calling the power company.
- Don't attempt to erect antennas or towers on windy days.
- MAKE SURE ALL TOWERS AND POLES ARE SECURELY GROUNDED, AND ELECTRICAL CABLES CONNECTED TO ANTENNAS HAVE LIGHTNING ARRESTORS. This will help prevent fire damage or human injury in case of lightning, static build-up, or short circuit within equipment connected to the antenna. The HotPoint access point has built-in lightning protection. Be sure that any other equipment connected to the HotPoint access point also has the same level of protection.
- The base of the antenna pole or tower must be connected directly to the building protective ground or to one or more approved grounding rods, using 10 AWG ground wire and corrosion-resistant connectors.
- Refer to the National Electrical Code for grounding details.

#### IF AN ACCIDENT SHOULD OCCUR WITH THE POWER LINES

- DON'T TOUCH THAT PERSON, OR YOU MAY BE ELECTROCUTED.
- Use a non-conductive dry board, stick, or rope to push or drag them so they no longer are in contact with electrical power.
- Once they are no longer contacting electrical power, administer CPR if you are certified.
- Immediately have someone call for medical help.

### Do not open the cover

- Dangerous voltages inside.
- No serviceable parts inside.
- Refer to qualified service personnel.



# Table of Contents

---

|   |    |
|---|----|
| The MIMO HotPoint Family . . . . .                  | 4  |
| Setting Up Your Equipment . . . . .                 | 5  |
| Setting Up Your FWC2050 . . . . .                   | 5  |
| Setting Up Your Access Points . . . . .             | 5  |
| Use with Firetide HotPort 7000 Mesh Nodes . . . . . | 5  |
| Logging In . . . . .                                | 6  |
| System Requirements . . . . .                       | 6  |
| Logging In . . . . .                                | 6  |
| Access Point Tab . . . . .                          | 7  |
| Discovery . . . . .                                 | 7  |
| Configuration Tab. . . . .                          | 9  |
| System Menu. . . . .                                | 9  |
| Wireless . . . . .                                  | 14 |
| Security . . . . .                                  | 18 |
| Profiles. . . . .                                   | 23 |
| WLAN Network. . . . .                               | 26 |
| Captive Portal . . . . .                            | 26 |
| Monitoring . . . . .                                | 27 |
| Controller . . . . .                                | 27 |
| WLAN . . . . .                                      | 31 |
| Clients . . . . .                                   | 31 |
| Maintenance . . . . .                               | 32 |
| User Management. . . . .                            | 32 |
| Upgrade . . . . .                                   | 33 |
| Backup/Restore . . . . .                            | 34 |
| Reboot/Reset . . . . .                              | 34 |
| Remote Management . . . . .                         | 34 |
| Logs & Alerts . . . . .                             | 35 |
| HotPoint 5000 Specifications . . . . .              | 38 |
| FWC2050 Specifications. . . . .                     | 39 |
| Reset Procedure . . . . .                           | 39 |
| Regulatory Notices . . . . .                        | 40 |
| Limited End User Product Warranty . . . . .         | 41 |

# Chapter 1 The MIMO HotPoint Family

---

The Firetide MIMO HotPoint Wireless Access Point System delivers a complete access solution for indoor and outdoor wireless mesh networks. Firetide's MIMO HotPoint family consist of three components:

**The FWC2050 Wireless LAN Controller:** Each FWC2050 can control and manage up to 50 Firetide MIMO Access Points.

**The HotPoint 5100 Indoor Access Point:** A dual-radio system support 2.4 and 5 GHz operation in 802.11a, b, g, and n modes.

**The HotPoint 5200 Outdoor Access Point:** A dual-radio system support 2.4 and 5 GHz operation in 802.11a, b, g, and n modes.

To ease management of multiple access points in enterprise applications, a virtual AP model is offered. Each FWC2050 WLAN controller can support up to 8 'group' definitions, and each group supports 8 profiles per radio - 16 total. Almost any combination of groups and profiles can be applied to individual access points, making it easy to support multiple classes of users and applications on the same hardware.

## Dual Radio, Dual-Band Support

---

Each 5000 Series MIMO unit has two radios; one operates on the 2.4 GHz band and the other on the 5 GHz band.

## Outdoor and Indoor Operation

---

Outdoor HotPoint 5200 access points have NEMA 4X/IP67-rated cast aluminum enclosures and a weatherproof connector for attaching to a Firetide HotPort wireless mesh node or a conventional Ethernet port. These units can receive power directly from a HotPort mesh node, eliminating the need for an external power supply.

Indoor HotPoint 5100 access points provide wireless access within buildings and moving vehicles. Each indoor access point has a UL2043 plenum-rated enclosure and an RJ-45 connector for attaching to a Firetide HotPort wireless mesh node or a conventional Ethernet port.

## Complete Stand-Alone System

---

The HotPoint 5000 Series Access Points, under the control of an FWC2050, are a complete stand-alone system for wireless access service delivery. No other equipment is required.

## Integration with Firetide HotPort Mesh Networks

---

Firetide's HotPoint 5000 Series Access Points can use Firetide's HotPort 7000 Series wireless mesh equipment for backhaul to the wired infrastructure.

# Chapter 2 Setting Up Your Equipment

---

## Setting Up Your FWC2050

---

The FWC2050 can be set up in any indoor location, but the best option is to place the unit in the data center, wiring closet, or other location with access to UPS-protected power and the enterprise backbone network.

The FWC requires AC power and a wired Ethernet connection. Refer to the specifications section for details.

Figure 1. FWC2050 Controller



## Setting Up Your Access Points

---

The HotPoint 5100 can be installed in any indoor location. The location should be selected based on antenna and coverage plans - best RF performance is obtained with antennas connected directly to the HotPoint AP, or with short, good-quality cables.

The HotPoint 5200 can be installed in any outdoor location. Again, location should be determined by antenna and coverage needs, not by Ethernet or power availability.

Figure 2. Firetide HotPoint 5100 Indoor and 5200 Outdoor MIMO Access Points



## Use with Firetide HotPort 7000 Mesh Nodes

---

In locations where access to Ethernet or power is limited, the HotPoint 5100 and 5200 can be paired with a HotPort 7000 Mesh Node for backhaul. The HotPort 7201/7202 Series is also capable of powering the HotPoint 5100/5200 Series.

# Chapter 3 Logging In

---

## System Requirements

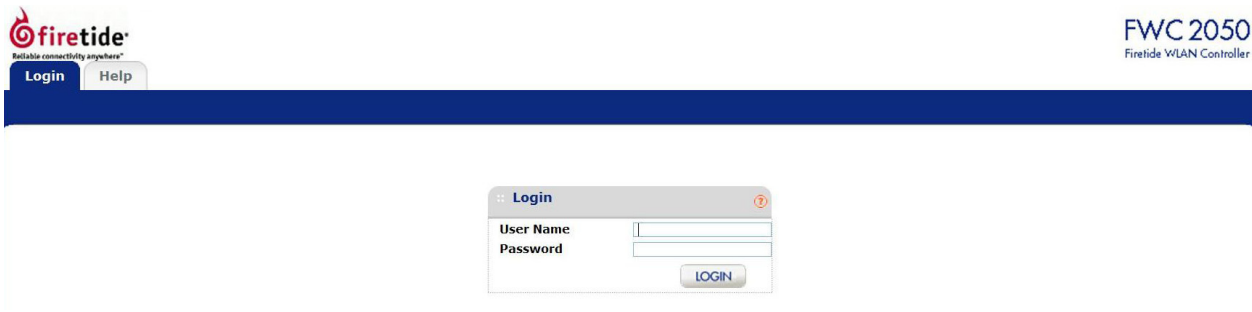
---

The FWC2050 Controller, if used, must have layer 2 or layer 3 connectivity to all Firetide 5000 series Access Points.

The system requires a DHCP server. If your network has one, it can be used. If desired, you can use the DHCP server built into the FWC2050.

## Logging In

---



The default IP address for the FWC2050 is 192.168.224.250.

Log in to your FWC2050 Wireless Management System administrative interface for the first time at <http://192.168.224.250>, using the default username (admin) and password (password)

Firetide recommends that you change the user name and password, and the default IP address.

# Chapter 4 Access Point Tab

## Discovery

Firetide HotPoint 5000 Access Points can operate as stand-alone devices, or be associated with Firetide Wireless Controllers. Controller-based operation, called Managed Mode, offers many additional features, including roaming. The Controller can auto-discover and manage the access points in the same layer-2 domain, or across a layer-3 domain, but certain conditions must be met

## Discovery for Initial Setup

New or factory-reset APs operate in stand-alone mode, unaware of the existence of the Controller. The Controller can discover these units as long as they are on the same layer-2 subnet. Once an AP is discovered, it switches into Managed Mode. APs in Managed Mode will look for a Controller whenever they reboot, using IP multicast.

Access Points in stand-alone mode (including any factory-reset APs) can only be discovered within the local subnet.

At the end of the discovery process, each discovered AP will be running a controller-based software image and will have attached itself to the controller that discovered it. It will be ready to accept client connections.

## Re-Discovery

Once an AP has been discovered, it remains a Managed AP until it is factory reset. Managed APs will actively look for the Controller after a reboot. This process uses IP multicast, and can work across multiple subnets, if you enable multicast routing for address 224.0.100.250 between controller and the APs. Alternately, you can enable DHCP option 43 on the DHCP server and provide the controller's IP address. APs will get their address via this DHCP server and get the controller's IP as part of the option 43.

For the discovery process to work, the FWC 2050 and the APs must be running compatible firmware versions. Contact Firetide for details on firmware levels. In addition, DHCP service must be available, either from a system-wide DHCP server or via the DHCP service offered by the FWC2050.

## Last Discovered



The screenshot shows the Firetide FWC 2050 web interface. The 'Discovery' menu is expanded, and the 'Last Discovered' page is active. A table displays the results of the auto-discovery process.

| Model        | IP         | MAC               | Name        |
|--------------|------------|-------------------|-------------|
| HOTPOINT5100 | 10.0.3.150 | 00:18:c2:00:20:03 | Firetide-AP |

The results of the auto-discovery are shown in the “Last Discovered” page under Discovery menu. Access Points can also be added manually.

## Configuration and Image Upgrade on the AP

After each reboot of an access point AP, the AP will look for its Controller, using multicast. Upon reconnecting, the AP and Controller will re-synchronize on firmware levels and AP settings. As part of this state machine, the AP will load any new firmware image posted to the controller. It will also synchronize to any configuration changes that were done on the controller while the AP was offline.

## Managed AP List



The screenshot shows the Firetide FWC 2050 web interface. The 'Discovery' menu is expanded, and the 'Managed AP List' page is active. A table displays the list of APs currently under management.

| Edit                             | IP         | MAC               | Model        | Name        | Status        | Group Name |                          |
|----------------------------------|------------|-------------------|--------------|-------------|---------------|------------|--------------------------|
| <input checked="" type="radio"/> | 10.0.3.141 | 00:18:c2:00:20:01 | HOTPOINT5100 | Firetide-AP | Connected     | basic      | <input type="checkbox"/> |
| <input type="radio"/>            | 10.0.3.103 | 00:18:c2:00:20:02 | HOTPOINT5100 | Firetide-AP | Not connected | basic      | <input type="checkbox"/> |

This displays a list of APs currently under management, and allows you to edit their settings.

## Discovery Wizard

If all APs were not discovered, run the Discovery Wizard.

The image displays three sequential screenshots of the Firetide FWC2050 Discovery Wizard interface. Each screenshot shows the 'Discovery Wizard' window with a sidebar on the left containing 'Discovery Wizard', 'Last Discovered', and 'Managed AP List'. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Plans', and 'Diagnostics'. The top right corner shows 'FWC 2050 Firetide WLAN Controller' and a 'LOGOUT' button.

**Step 1 of 3 : Choose state of Access Points**  
In simple steps FWC2050 can discover your supported Access Points in the network.  
Please select the state of the Access Points

- Access Points are already installed
- I am not sure

**Step 2 of 3 : Choose Network Layout**  
Select how the access points are connected to the controller

- Access Points and Controller are connected directly or through a backend in same L2 network
- Access Points and Controller are in different L3 Network(different VLAN or behind router)

**Step 3 of 3 : Select Access Points to manage**

| <input type="checkbox"/> | Model | IP | MAC |
|--------------------------|-------|----|-----|
| No Access Points Found.  |       |    |     |

CANCEL BACK ADD

## Manual Additions

You will be asked to choose between two options:

**Option 1 - Add new factory-defaulted APs:** Add new factory defaulted AP. This option should be chosen during staging the process. Here the controller and APs are going to be taken out of the box and configured for deployment.

**Option 2 - Add existing installed APs:** Add existing installed APs. This option should be chosen in scenarios where APs are already deployed and running, and need to be attached to a controller. Depending upon the network topology, you may need to provide the controller with a range of IP addresses to search during discovery.

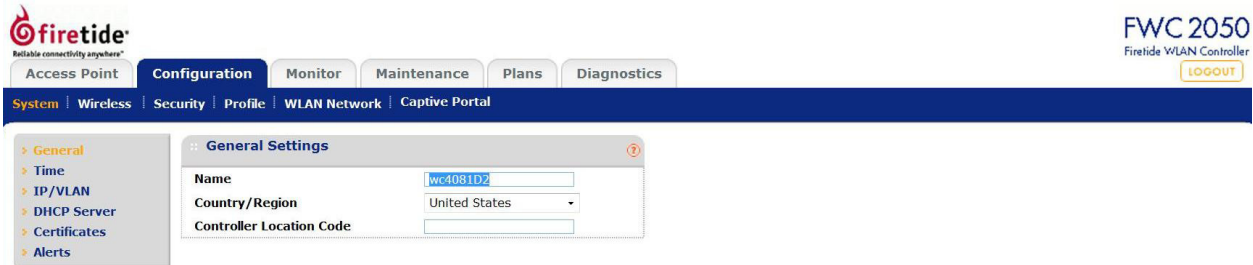
When the process finishes, you will be presented with a list of APs, their model numbers, their IP and their Ethernet MAC addresses. You can then choose the APs to be managed under this controller. Once this is done, the AP will be upgraded to the controller-based image.



# Chapter 5 Configuration Tab

## System Menu

### General Settings

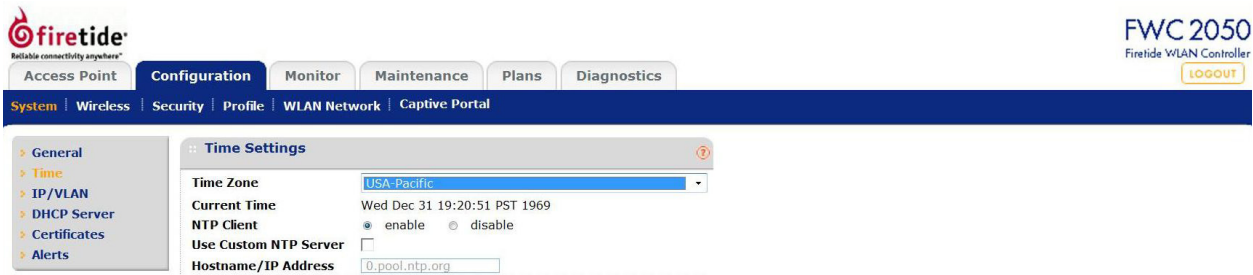


**Name:** This is the FWC2050 name. By default, the name is FWC2050. Firetide recommends changing the name as soon as possible after setting up. The name must contain only alphabets, numbers, and hyphens, and must be 31 characters or less.

**Country/Region:** This field displays the region of operation for the FWC2050 and the Access Points managed by the FWC2050. You must select a country or region.

**Controller Location Code:** This field defines the identifying code for the controller.

### Time Settings



This page lets you configure the time-related settings of your FWC2050 and managed Access Points.

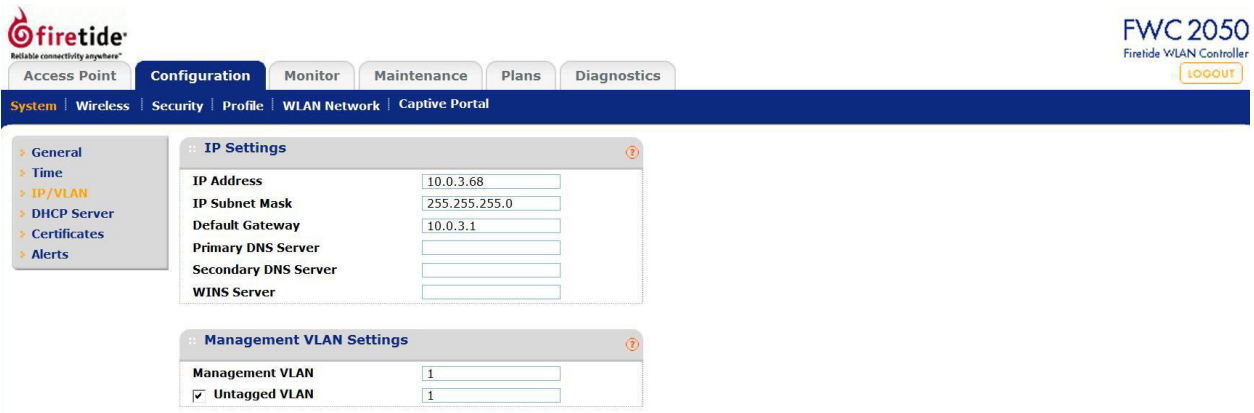
**Time Zone:** Select the appropriate local time zone for your region or country.

**Current Time:** Shows the current time. You cannot set the time; you must use an NTP server.

**NTP Client:** Defines the Network Time Protocol (NTP) server used to synchronize the clock of the FWC2050 and managed Access Points.

**Use Custom NTP Server:** Check this box if you wish to use an alternate NTP Server. By default, the Firetide NTP server (time.firetide.com) is used by the Access Point. Further information about NTP servers can be found at <http://support.ntp.org/bin/view/Servers/WebHome>

**Hostname / IP Address:** Provide the host name or IP address of the NTP server, if you are using a custom NTP server.



This page lets you to configure the Management IP address setting of the FWC2050. It has the following options:

**IP Address:** This is the IP address of the FWC2050. The default IP address is 192.168.224.250. To change it, enter an available IP address from the address range used on your LAN.

**IP Subnet Mask:** Enter the subnet mask value used on your LAN. The default value is 255.255.255.0.

**Default Gateway:** Enter the IP address of the gateway for your LAN.

**Primary DNS Server:** Enter the IP address of the Primary Domain Name Server (DNS) that you want to use.

**Secondary DNS Server:** Enter the IP address of the Secondary Domain Name Server (DNS) that you want to use.

**WINS Server:** Enter the IP address of the WINS server that you want to use.

**Management VLAN:** Management VLANs are used for managing traffic (Telnet, SNMP, and HTTP) to and from the FWC2050 and managed Access Points. Frames belonging to the Management VLAN are not given any 802.1Q header when sent over the trunk. If a port is in a single VLAN, it can be untagged, but if the port needs to be a member of multiple VLANs, it must be tagged. The Management VLAN value must be between 1 and 4094.

**Untagged VLAN:** When checked, this option allows one VLAN to be configured as an “untagged VLAN”. When the FWC2050 sends frames associated with the untagged VLAN out the Ethernet interface, those frames will be untagged. When the FWC2050 receives untagged traffic from the Ethernet interface, those frames are assigned to the untagged VLAN.

If unchecked, the FWC2050 tags all outgoing Ethernet frames, and only accepts incoming frames that are tagged with known VLAN IDs.

**Note:** The untagged VLAN checkbox should only be unchecked if the hubs or switches on your LAN support the 802.1Q VLAN standard. Likewise, the untagged VLAN value should only be changed if the hubs and switches on your LAN support the 802.1Q standard.

Changing either of these values will result in a loss of IP connectivity if the hubs and switches on your network have not yet been configured with the corresponding VLANs.

## DHCP Server List

The screenshot shows the Firetide FWC2050 web interface. The top navigation bar includes 'Access Point', 'Configuration', 'Monitor', 'Maintenance', 'Plans', and 'Diagnostics'. Below this, a secondary bar shows 'System', 'Wireless', 'Security', 'Profile', 'WLAN Network', and 'Captive Portal'. On the left, a sidebar menu lists 'General', 'Time', 'IP/VLAN', 'DHCP Server', 'Certificates', and 'Alerts'. The main content area is titled 'DHCP Server List' and displays a table with columns: 'Select', 'VLAN', 'IP Network', 'Subnet Mask', 'Default Gateway', 'Start IP', 'End IP', 'Primary DNS Server', 'Secondary DNS Server', and 'WINS'. The 'DHCP Server' menu item is highlighted in orange.

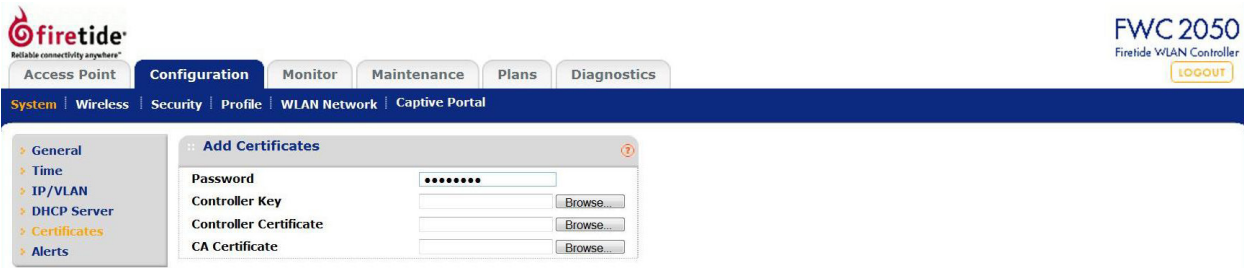
Displays a list of DHCP Servers configured on the FWC2050.

The screenshot shows the 'Add DHCP Server' dialog box overlaid on the DHCP Server List page. The dialog box has a title bar 'Add DHCP Server' and contains the following settings:

- DHCP Settings**
- Use VLAN Interface:**
- VLAN:**
- IP Network:**
- Subnet Mask:**
- Default Gateway:**
- Start IP:**
- End IP:**
- Use Default DNS Server:**
- Primary DNS Server:**
- Secondary DNS Server:**
- Use Default WINS Server:**
- WINS Server:**

At the bottom of the dialog box are three buttons: 'CANCEL', 'CLEAR', and 'ADD'.

- Use VLAN Interface:** Enable this option to provide IP addresses to clients in a specified VLAN.
- DHCP Server VLAN ID:** Enter DHCP server VLAN ID. The VLAN ID range is between 1 and 4094.
- IP Network:** This option is enabled only when "Use VLAN Interface" is enabled. This provides the IP address for the FWC2050 in specified VLAN; when VLAN is not selected the FWC2050 management IP/VLAN is used.
- Subnet Mask:** Enter the subnet mask that will be assigned to clients by the Server.
- Gateway IP Address:** Enter the IP address of the default gateway.
- Starting IP Address:** Enter the starting IP address of the range that can be assigned by the Server.
- Ending IP Address:** Enter the ending IP address of the range that can be assigned by the Server.
- Use Default DNS Server:** This option allows the FWC2050 DNS server to be provided to the clients of the specified VLAN.
- Primary DNS Server:** Enter the IP address of the primary DNS server for the network.
- Secondary DNS Server:** Enter the IP address of the secondary DNS Server for the network.
- WINS:** This displays WINS server configuration on the FWC2050 for all configured VLANs.



This option lets you add security certificates to your system. There are three elements:

- Password:** Encrypts the Controller Key.
- Controller Key:** The private key used by the Controller to decrypt messages.
- Controller Certificate:** The public key of the Controller. The default key is signed by Firetide.
- CA Certificate:** The signed certificate of the Certificate Authority.

All keys and certificates are in PEM format.

## Alerts

### Syslog Configuration

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 left sidebar shows a tree view with 'Alerts' expanded to 'SysLog'. The main content area is titled 'Syslog Settings' and contains the following fields:

- Enable Syslog:** A checked checkbox.
- Syslog Server IP Address:** An empty text input field.
- Server Port Number:** A text input field containing the value '514'.

This page lets you configure the settings to connect to a Syslog server.

**Enable Syslog:** Enable the Syslog settings, if you have a Syslog server on your network.

**Syslog Server IP Address:** Enter the IP address to which the FWC2050 and managed Access Points will send all SysLogs, if SysLog option is enabled.

**Port:** Enter the port number at which your Syslog server is configured to listen to requests.

### Alarm Actions

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 left sidebar shows a tree view with 'Alerts' expanded to 'Alarms'. The main content area is titled 'Alarm Actions' and contains a table with the following structure:

| Severity | Action        | Email Address |
|----------|---------------|---------------|
| Minor    | No Action     |               |
| Normal   | No Action     |               |
| Major    | Add To Syslog |               |
| Critical | Add To Syslog |               |

The 'Action' dropdown for the 'Critical' severity is open, showing the following options: 'Add To Syslog', 'No Action', 'Add To Syslog', and 'Send E-mail'.

This screen lets you define actions to be taken for the four defined alarm conditions. For each condition, you can do nothing, write to syslog, or generate an email to a defined email address.

### Alarm Email Configuration

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 left sidebar shows a tree view with 'Alerts' expanded to 'Email Setup'. The main content area is titled 'Email Configuration' and contains the following fields:

- Server Address:** An empty text input field.
- Port:** A text input field containing the value '25'.
- Sender E-Mail Address:** An empty text input field.
- UserName:** An empty text input field.
- Password:** An empty text input field.

Alarm messages via email require that a mail server be defined.

**Server Address:** Enter the address or name of the mail server (e.g. smtp.firetide.com)

**Port:** Enter the port on which the mail server receives mail.

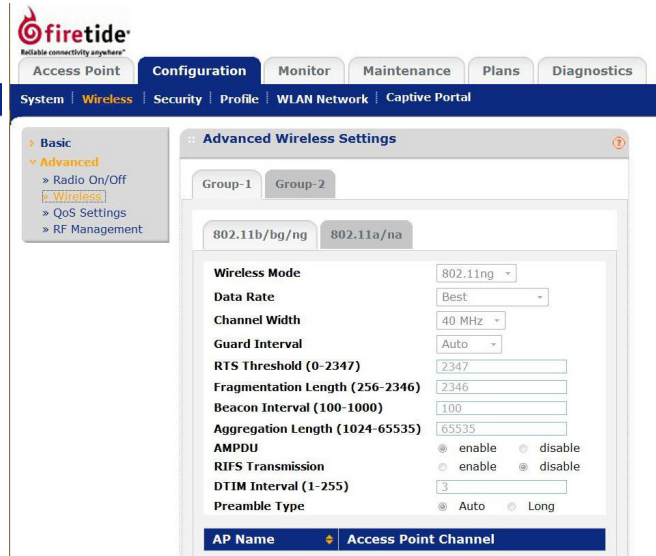
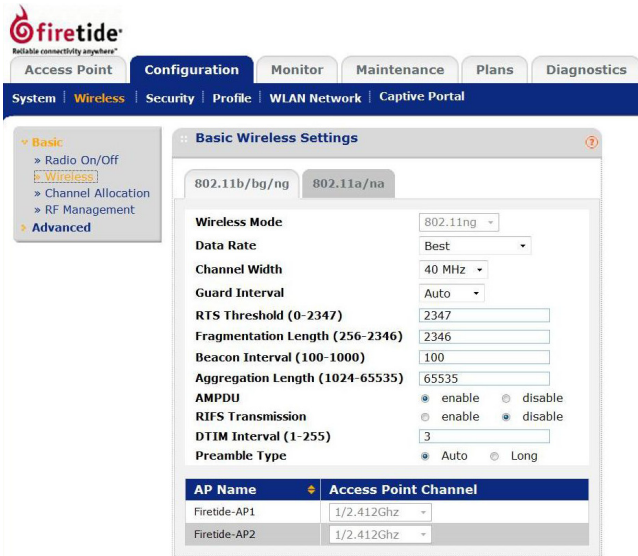
**User Name:** Enter the 'user name' that identifies the Controller that is sending the message.

**Password:** Enter the email system password defined for the account.

# Wireless

## Wireless - Basic and Advanced

Wireless Settings for Basic and Advanced are similar; except that Advanced allows you to configure settings per Group.



### Wireless Mode:

This option is enabled when Channel Allocation is disabled. In addition to the default 802.11ng mode, you can also choose 802.11b or 802.11bg. In 802.11bg mode, both 802.11n and 802.11g compliant devices can be used with the AP. If you select this option and other settings on this screen are disabled, select the Turn Radio On radio button to enable options on this screen.

### Data Rate:

This configuration specifies the rate of data frames from AP towards clients. Selecting any value other than best means that the rate will adapt up to the configured rate. Selecting a lower rate is helpful in scenarios where the radio environment is very noisy resulting in high bit errors. A lower rate may impact data throughput negatively.

### Channel Width (11n):

This configures the width of operation of the selected channel and is valid only in 802.11ng or 802.11na modes. The default value is 40 MHz. A wider channel improves the performance, but some legacy devices can only operate on either 20 MHz.

### Guard Interval (11n):

This is the interval between two consecutive symbols in a radio transmission. Legacy devices (802.11b or 802.11g) operate with a long guard interval while 802.11n devices can move between short and long. The default is Auto. Firetide recommends leaving this setting at Auto.

### RTS Threshold:

If the packet size is equal to or less than this threshold, the data frame is transmitted immediately. If the size is larger than the specified value, then the transmitter must send out an RTS packet, and then must wait for the receiving station to send back a CTS before sending the actual packet data.

### Fragmentation Length:

This is the maximum packet size used for fragmentation. Packets larger than this size will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value.

### Beacon Interval:

Sets the time period between transmissions of the AP beacon signal.

### Aggregation Length:

Specifies the maximum permitted length of aggregated frames.

### AMPDU:

Enables aggregation of several MAC frames into a single large frame to achieve higher throughput. Enabling AMPDU may sometimes lead to better network performance.

### RIFS Transmission:

Enables Reduced Interframe Space option. Enabling RIFS may lead to better network performance.

### DTIM Interval:

This sets the desired Delivery Traffic Indication Message or the data beacon rate. It indicates the message period in multiples of beacon intervals. This value must be between 1 and 255.

### Preamble Type:

Long transmit preambles provide a more reliable connection or longer range. Short transmit preamble gives better performance. Auto handles both long and short preambles. The default is Auto.

### Access Point Channel:

Each Managed Access Point channel can be individually selected. The Access Point mode is either set to the one enabled for the group, or, if the selected mode is not available on the Access Point, to the mode providing highest performance.

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 'WLAN Network' sub-tab is selected. The left sidebar shows a tree view with 'Basic' expanded to 'Channel Allocation'. The main content area is titled 'Channel Allocation' and contains the following settings:

- Automatic channel allocation:**  enable  disable
- Valid corporate channels:**
  - 2.4 Ghz:** Channels 1, 6, and 11 are checked.
  - 5 Ghz:** Channels 36, 40, 44, 48, 128, 132, 136, 149, 153, 157, and 161 are checked.
- Prevent channel change during:**
  - Active voice call:**  enable  disable
  - High Traffic Load:**  enable  disable
- Schedule channel allocation:**
  - Run channel allocation at:** hr: 0, min: 0
  - Run channel allocation every:** m, t, w, t, f, s, s (all checked)

Automatic Channel Allocation (ACA), when run, tries to optimize the channel allocation for access points based on clients, user data traffic load and observed nearby RF environment of access points in order to reduce interference. The algorithm takes into consideration interference, traffic load on the AP and neighborhood maps to come up with the best channel for an Access Point. This information, collected over the last 24 hours, is used by the controller to determine the best possible channel for the Access Point.

For this reason, Automatic Channel Allocation should be re-run 24 hours (or more) after an initial deployment, so that the algorithm has a good base of performance data for analysis. You can also schedule the algorithm to run at a specified time, or periodically.

ACA can be configured to allow allocation of only the specified channels. This ensures that the Access Points only use the channels allowed according to Administration policies. ACA can also be configured to not change channels on any Access Point through which there is data traffic or voice-call traffic (identified by the traffic in WMM voice priority queues).

## Recommendations

- Selecting non-overlapping channels for channel allocation is a good practice e.g. for 2.4 GHz use channels 1,6,11.
- Having channel allocation scheduled once a day allows better management of available bandwidth during the day. It is best to schedule at times when least number of clients are expected to be connected.

**Automatic Channel Allocation:** Enables this mode.

**Valid Corporate Channels:** Lets you select permitted channels. The first check box allows all channels to be for either 2.4GHz or 5GHz to be selected.

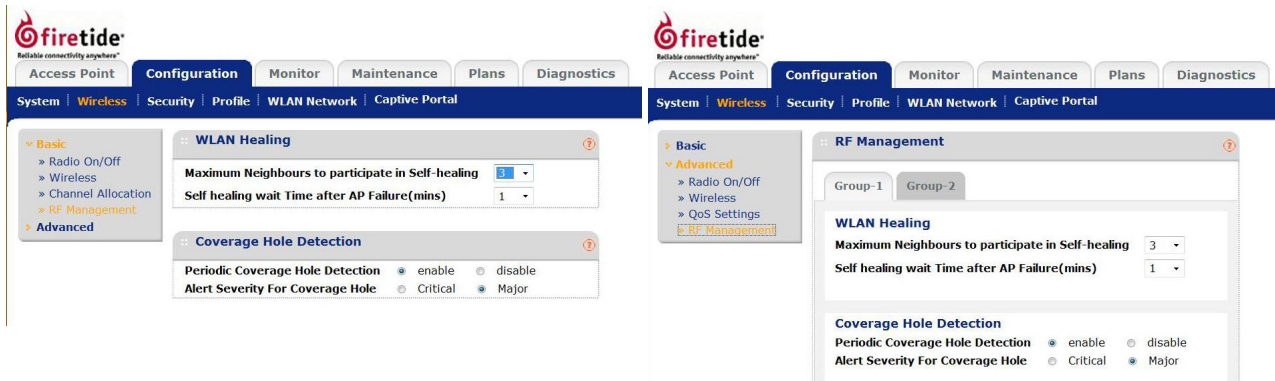
**Prevent Channel Changing During:** Lets you delay changes for certain critical traffic. Enabling “Active voice call” or “High Traffic Load” prevents a channel change on an Access Point if the respective condition is true.

**Run Channel Allocation at:** Specify at what time of the day the channel allocation can modify access point RF configuration.

**Run Channel Allocation every:** Specify weekly schedule for running channel allocation.

## RF Management

Basic and Advanced RF Management settings are similar, but Advanced allows you to configure settings per Group.



Automatic WLAN Healing increases the transmit power of nearby Access Points to cover for an AP losing connection to the controller, or other loss. It works by periodically looking at the radio neighborhood maps and detecting any changes happening in the maps. This feature can be configured to wait for a specified time before any transmit power changes are done on neighboring Access Points to avoid short intermittent changes happening owing to surrounding environment. Configuration also allows selecting the number of neighboring Access Points which should increase Transmit power to cover for the down Access Point.

This feature is configured per Security Profile group and runs between the access points in the same group.

**Maximum neighbors to participate in Self-Healing:** Maximum Number of neighboring access points which increase or decrease power to cover for a failing Access Point. Selecting “0” disables this feature. The number of neighbors to participate in healing should not be very large. Three to four usually suffices in most deployments. This avoids too many access points located close to increase power for a single failed Access Point.

**Self healing wait time after AP failure (in mins):** Number of minutes to validate i.e. wait before confirming a failed Access Point and increasing transmit Power to cover the area. Self healing wait time should be configured to a value greater than AP reboot time usually two minutes. This allows for fluctuations in the power of nearby Access Points when Access Points are rebooted.

## Radio On-Off Times

Radio On Settings can be set for the unit as a whole, or per Group.



- Current Time:** Enter the correct current time. If NTP service is enabled, this field displays the local time.
- Schedule Radio On/Off:** Enables and disables this feature.
- Schedule at:** Specifies the time.
- Schedule On:** Specifies the days of the week.
- Duration:** Specifies the length of on time.



The screenshot displays the 'Advanced QoS Settings' configuration page for a Firetide FWC 2050. The interface is divided into a navigation sidebar on the left and a main configuration area. The sidebar shows a tree view with 'Advanced' expanded to 'QoS Settings'. The main area has tabs for 'Group-1' and 'Group-2', with '802.11b/bg/ng' selected. Below this, there are two tables: 'AP EDCA parameters' and 'Station EDCA parameters'. Each table has five columns: Queue, AIFS, cwMin, cwMax, and Max Burst/TXOP Limit. The 'AP EDCA parameters' table has rows for Data 0 (Best Effort), Data 1 (Background), Data 2 (Video), and Data 3 (Voice). The 'Station EDCA parameters' table has rows for Data 0 (Best Effort), Data 1 (Background), Data 2 (Video), and Data 3 (Voice). Each row contains numerical values in input fields and dropdown menus.

| AP EDCA parameters   |      |       |       |           |
|----------------------|------|-------|-------|-----------|
| Queue                | AIFS | cwMin | cwMax | Max Burst |
| Data 0 (Best Effort) | 3    | 15    | 63    | 0         |
| Data 1 (Background)  | 7    | 15    | 1023  | 0         |
| Data 2 (Video)       | 1    | 7     | 15    | 3008      |
| Data 3 (Voice)       | 1    | 3     | 7     | 1504      |

| Station EDCA parameters |      |       |       |            |
|-------------------------|------|-------|-------|------------|
| Queue                   | AIFS | cwMin | cwMax | TXOP Limit |
| Data 0 (Best Effort)    | 3    | 15    | 1023  | 0          |
| Data 1 (Background)     | 7    | 15    | 1023  | 0          |
| Data 2 (Video)          | 2    | 7     | 15    | 3008       |
| Data 3 (Voice)          | 2    | 3     | 7     | 1504       |

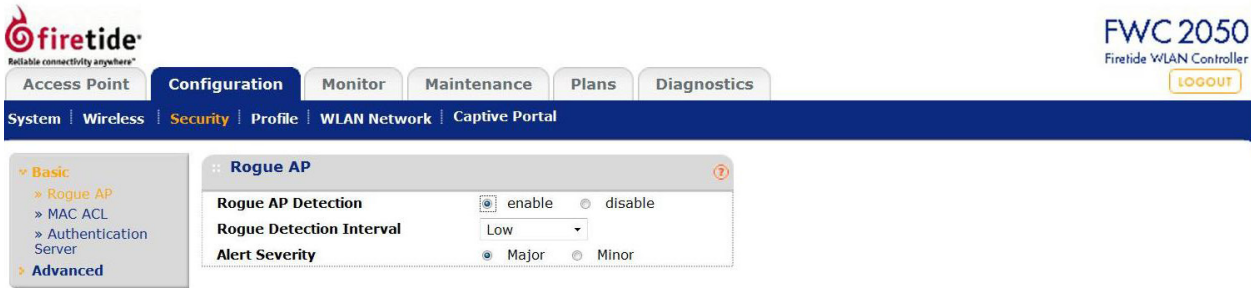
QoS settings on the access point control downstream traffic flowing from the AP to client (AP EDCA parameters) and the up-stream traffic flowing from the client to the AP (station EDCA parameters).

- Data 3 (Voice):** The highest priority queue, minimum delay; ideal for VOIP and streaming media.
- Data 2 (Video):** The second highest priority queue, low delay. Video applications are routed to this queue.
- Data 1 (Background):** Low priority queue with high throughput. Applications which are not time-sensitive but require high throughput can use this queue.
- Data 0 (Best Effort):** The medium priority queue, medium delay. Most IP applications use this queue.

# Security

## Basic

### Rogue AP Detection



Unidentified access points that use the SSID of a legitimate network can present a serious security threat. Detecting rogue access points involves scanning the wireless environment on all available channels, looking for unidentified access points. These settings are applied to all managed APs.

An AP is defined as rogue if all of the following are true:

1. AP's Radio BSSID is observed by any of the managed APs,
2. AP is seen transmitting on the Ethernet side on the same L2 as the APs.
3. At least one client is connected to the AP.

Any AP not meeting all of the conditions above is classified as a neighbor. Neighbor APs can be rogue; until a client connects it is not possible to determine whether the AP is rogue or not.

Neighbor APs as well as rogue APs will be detected and maintained in the controller. The controller also maintains current count of the rogue APs as well as rogue APs seen in the last 24 hours. All Neighbor as well as rogue APs will be displayed, up to a maximum of 512 APs.

Neighbor and rogue APs are detected by scanning, and the AP is off-channel during this time. Because the detection interval is long, it will take at least one such interval (and possibly more) for a rogue or neighbor AP to be detected and appear.

**Rogue AP Detection:** Disabled by default.

**Rogue Detection Interval:** The interval at which Rogue Detection required on run on FWC2050. The default Rogue Detection Interval is "Low".

**Alert Severity:** Sets the severity of the alarm when Rogue APs are detected.

This is a sample rogue and neighbor screen:

**firetide**  
Reliable connectivity anywhere™

FWC 2050  
Firetide WLAN Controller  
LOGOUT

Access Point | **Configuration** | Monitor | Maintenance | Plans | Diagnostics

System | Wireless | **Security** | Profile | WLAN Network | Captive Portal

Basic  
Advanced  
» Rogue AP  
» MAC ACL  
» Authentication Server

**Rogue AP**

Import Known List    Merge  Replace

**Rogue List**

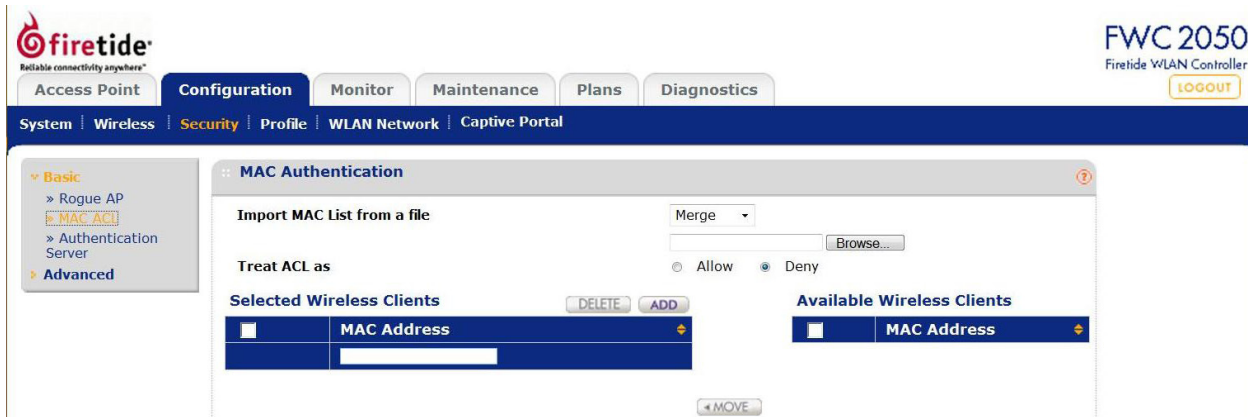
| <input type="checkbox"/> | MAC Address       | SSID               | Channel | Privacy   | Last Beacon              | Type     | Rogue Type | Name |
|--------------------------|-------------------|--------------------|---------|-----------|--------------------------|----------|------------|------|
| <input type="checkbox"/> | 00:26:f2:8b:20:30 | NG_11a             | 40      | Unsecured | Wed Dec 31 16:28:19 1969 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | 00:26:f2:8b:2c:00 | NG_11g_LoadBalance | 6       | Unsecured | Wed Dec 31 16:28:19 1969 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | 00:26:f2:8b:20:37 | NG_11a-7           | 40      | Unsecured | Wed Dec 31 16:28:19 1969 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | 00:26:f2:8b:20:20 | NG_11g             | 1       | Unsecured | Wed Dec 31 16:28:19 1969 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | 00:26:f2:8b:2c:10 | NG_11a_LoadBalance | 153     | Unsecured | Wed Dec 31 16:28:19 1969 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | 00:26:f2:8b:20:21 | NG_11g-1           | 1       | Unsecured | Wed Dec 31 16:28:19 1969 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | 00:26:f2:8b:20:22 | NG_11g-2           | 1       | Unsecured | Wed Dec 31 16:28:19 1969 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | 00:26:f2:8b:20:26 | NG_11g-6           | 1       | Unsecured | Wed Dec 31 16:28:19 1969 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | 00:26:f2:8b:20:27 | NG_11g-7           | 1       | Unsecured | Wed Dec 31 16:28:19 1969 | Neighbor | Unknown    |      |
| <input type="checkbox"/> | 00:26:f2:8b:26:00 | NG_11g_LoadBalance | 6       | Unsecured | Wed Dec 31 16:28:19 1969 | Neighbor | Unknown    |      |

PREVIOUS | NEXT

Move to:

## MAC Address Access Control Lists

MAC ACL Restrictions can be applied to the unit, or per Group.



**Import MAC List from file:** Allows you to import a list of MAC addresses.

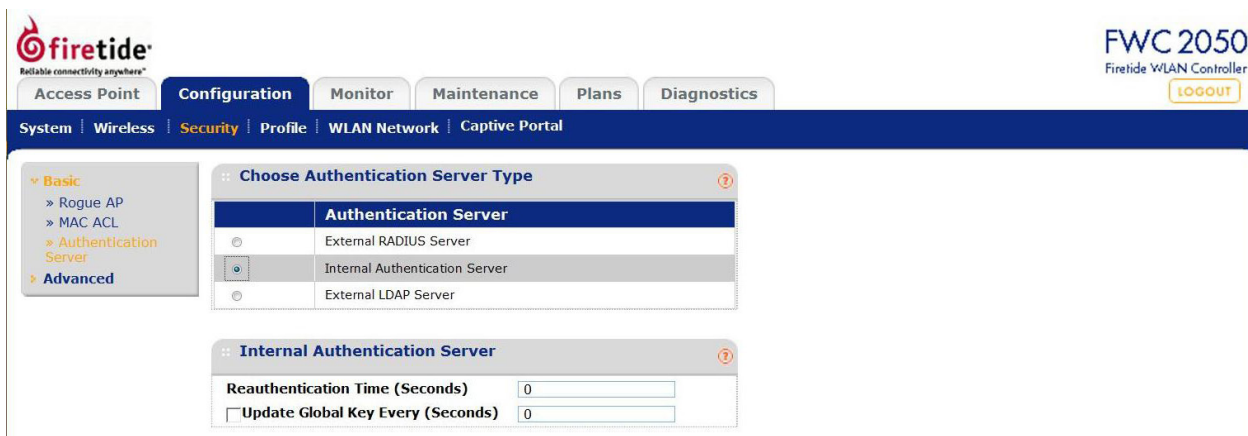
**Treat ACL as:** Lets you specify whether the imported list is allow or deny.

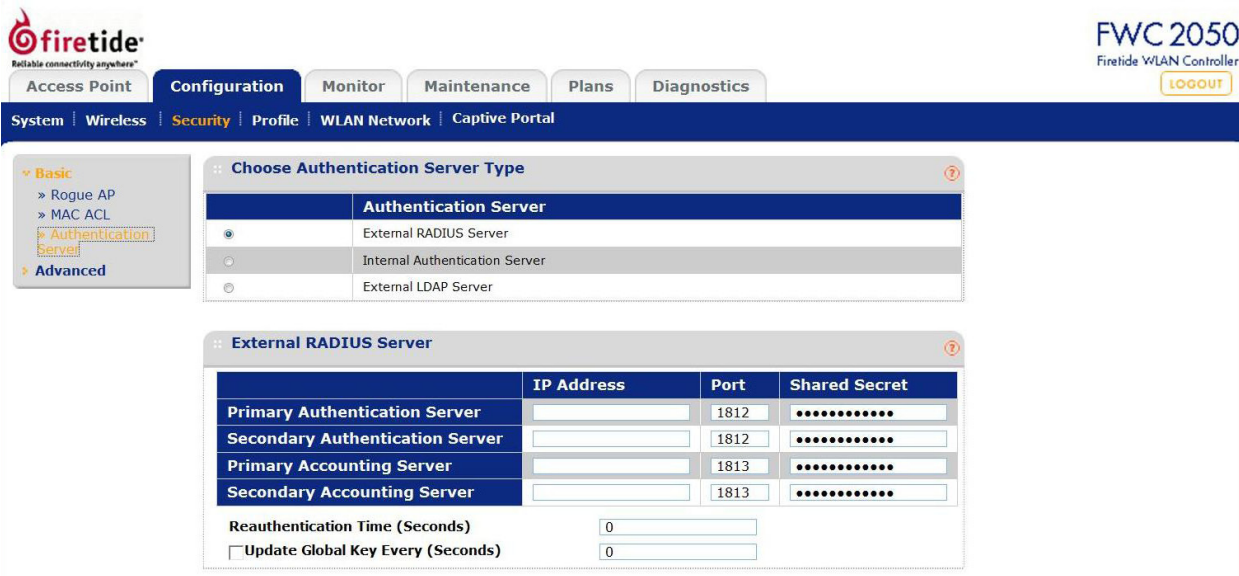
**Selected Wireless Stations:** This table lists the stations that have been allowed access to the network through this Access Point. Click **Delete** to delete a wireless station from the Selected wireless clients table list. Enter a MAC address and Click **Add** to add the MAC address of the wireless stations to the Selected wireless clients table list.

**Available Wireless Stations:** This table lists the Wireless stations that are present in the vicinity of the Access Point. Click **Refresh** to update this list in the table. Select a station in the Available Wireless Stations table and click **Move** to move the station to the Selected wireless clients table.

## Authentication Server Selection

This lets you select one of three authentication servers.





**Primary Authentication Server:** The Primary Authentication Server is the main Radius server used for authentication. The IP Address, Port, and Shared Secret information is required to communicate with Radius Server. The Shared Secret is shared between the Wireless Access Point and the Radius Server while authenticating the Wireless client.

**Secondary Authentication Server:** A Secondary Authentication Server can be configured for use if the Primary Authentication Server fails or is unreachable. The IP Address, Port, and Shared Secret information is required to communicate with the Radius Server. The Shared Secret is shared between the Wireless Access Point and the Radius Server while authenticating the Wireless client.

**Primary Accounting Server:** The Primary Accounting Server is used for accounting on the network. The IP Address, Port No., and Shared Secret information is required to communicate with Radius Server. The Shared Secret is shared between the Wireless Access Point and the Radius Server while authenticating the Wireless client.

**Secondary Accounting Server:** A Secondary Accounting Server can be configured to use if the Primary Authentication Server fails or is unreachable. The IP Address, Port No., and Shared Secret information is required to communicate with Radius Server. The Shared Secret is shared between the Wireless Access Point and the Radius Server while authenticating the Wireless client.

**Re-authentication Time (Seconds):** This is the time interval in seconds after which the supplicant will be authenticated again with the RADIUS Server. The default interval is 3600 seconds.

**Update Global Key Every (Seconds):** Enable this option to have the Global Key changed according to the time interval specified. If enabled, enter the desired time interval. The default is enable, and the default interval is 1800 Seconds.