HotPort™

HIGH PERFORMANCE MESH NETWORK

Wireless Access Point User Guide

HotPoint 4500 Indoor Access Point

HotPoint 4600 Outdoor Access Point

firetide™

instant mesh networks™

Safety Instructions

The HotPoint node 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 is intended to alert the user to the presences of non-insulated dangerous voltage that may be of sufficient magnitude to constitute a risk of lethal electric shock to persons.

This symbol is intended to alert the user to the presence of important operating, maintainance, and servicing instructions. Failing to comply with this instruction may result in electrical shock.

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

Do not open the cover

- Dangerous voltages inside.
- No serviceable parts inside.
- Refer to qualified service personnel.
- Unit must be disconnected from power prior to servicing.
- Unit has tamper-evident labeling that indicates when the cover has been removed.

Caution! Risk of electric shock!

POWER LINES CAN BE LETHAL

Do not install the HotPort outdoor mesh node 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.

SURVEYING 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 HotPort outdoor node has built-in lightning protection. Be sure that any other equipment connected to the HotPort node 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.

Firetide Limited End User Product Warranty

Pursuant to all provisions described herein, Firetide products are warranted for one (1) year 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. 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 antennas and the AC power adapter.

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.

Indoor Manual Contents

Introduction

Firetide HotPoint Wireless Access Point Family

Firetide's HotPoint family of wireless access points are the newest addition to the company's HotPort line of high performance wireless mesh networking products. The HotPoint access points provide an enterprise-class wireless access solution and can be used as full-function standalone access points, or as part of an integrated, triple-play wireless mesh network. Available in indoor and outdoor models, they include a high power, multi-spectrum extended range radio, multiple antenna options, robust security features, and multiple ESSID support.

The Firetide™ HotPoint™ Wireless Access Points (AP) are companion units to the Firetide HotPort™ High-Performance Mesh Network. Each AP allows 802.11b and 802.11g wireless clients to connect to the Firetide Wireless Mesh network. Such clients include laptops, wireless security cameras, VoIP phones, and portable terminal and POS devices.

The Firetide mesh network itself provides a high-capacity, self-healing wireless mesh for indoor and outdoor networks. The HotPort system allows standard Ethernet devices to operate on the wireless backbone, creating secure and reliable wireless networks for video surveillance, voice, and data. HotPoint APs and HotPort nodes can be managed together as a system with Firetide's HotView mesh management software.

HotPoint 4500 indoor APs are plenum-rated and can be mounted securely to a wall, ceiling, or countertop using an optional mounting bracket. Each HotPoint indoor node includes antennas.

HotPoint 4600 Outdoor APs feaure NEMA4X/IP66-rated aluminum enclosures, and can be powered over Ethernet.

Firetide's modular access point design offers several benefits. Among them are:

- A HotPoint access point can be mounted to a Firetide mesh node to provide enterprise class Wi-Fi access to any indoor or outdoor location, without the need for backhaul cabling.
- A HotPoint access point can connect directly to a conventional wired infrastructure. This eliminates the need to install a Firetide mesh node in locations where wired connectivity is readily available, while preserving the unified management capabilities for all access points.
- Because the access points and mesh nodes are kept in separate enclosures, they can be independently positioned for optimum RF connectivity. For example, in a multi-building mesh network, mesh nodes should be placed in areas that enable the best connectivity between buildings, while the APs can be mounted for best interior coverage.
- A HotPoint access point can share a Firetide mesh node with other devices for true triple-play networking at any mesh node location. This can include a second HotPoint access point operating on a different channel, a video camera, a VoIP device, or even a third party access point.
- All HotPoint access points, as well as all Firetide mesh nodes, can be managed across the network from a central location regardless of whether the access points are connected to wireless mesh nodes, to a wired infrastructure, or both. This integrated approach also allows network broadcasts to all access clients anywhere on the network.

HotPoint Access Point Features

- Wireless features include:
  - Frequency ranges 2.400—2.484 GHz
  - Transmit up to 400 mW with 802.11h Automatic XMIT Power Control
  - Manual Transmit Power Control with 802.11d Auto Channel Select

- Network features include:
  - Up to 16 independent VLANs
  - Up to 16 ESSIDs per HotPoint
  - Up to 64 clients per HotPoint
  - WDS
  - DHCP client and server, separate DHCP range per SSID
  - NAT
  - 802.1p (Quality of Service)
  - 802.11e (WMM) (Quality of Service)
  - Inter Access Point Protocol (IAPP) enabled per 802.11f
  - Fast handoff enabled per draft of 802.11r
  - Intercell blocking – blocks communication between APs
  - Intracell blocking – blocks communication between BSSIDs

- Security and Encryption features include:
  - 802.11i with 40 bit or 104 bit WEP keys; 128 bit or 256 bit AES keys, TKIP
  - 802.1x authentication
  - WPA2
  - VPN tunneling and filtering
  - ESSID suppression
  - Firewall
  - MAC access control
  - Rogue AP detection

- Management & Configuration features include:
  - SNMP v2/3
  - FTP firmware upgrade
  - Virtual AP Grouping- uniform SLAs
  - Physical AP Grouping – uniform parameters
  - Per-user and per-VAP data rate limiting
  - Per-user based accounting

HotPoint + HotPort Network Applications

Wi-Fi Networks

Together, HotPoints and HotPorts allow you to quickly deploy Wi-Fi service anywhere. The Firetide mesh provides more flexibility for Wi-Fi deployment than other mesh solutions because it can support existing third-party APs as well as Firetide HotPoint APs. Each HotPort can support up to four APs, so high-density Wi-Fi can be deployed at a lower cost than using mesh nodes that are limited to a single access point.

Voice over IP

The HotPort mesh network enables clear VoIP traffic over the wireless backbone. Both wired and wireless VoIP phones support Class-of-Service prioritization which enables you to assign high priority to voice traffic to ensure the best quality voice transmission.

Video

The high capacity and sustained throughput of the HotPort network makes it ideal for IP video networks and video surveillance applications, especially those requiring multiple cameras or faster frame rates. Wi-Fi cameras are not needed because any camera with an Ethernet interface can connect directly to a HotPort mesh node. HotPort outdoor mesh nodes also support Power over Ethernet, allowing the use of a single power connection to power both the node and the camera.

Data

The HotPort mesh network also provides direct connectivity for computers and servers via a cable to the Ethernet ports on each node.

Point-of-Sale

HotPoint APs and the HotPort network make it easy to deploy Point-of-Sale terminal support at trade shows, fairs, and other temporary locations, as well as to support handheld wireless devices in inventory, tracking, and other logistics applications.

Printing

With the HotPort mesh network network printers become wireless printers, without additional setup, drivers, or software, simply by connecting to one of the Ethernet ports on a HotPort mesh node. This wireless capability allows network printers to operate anywhere, including mobile carts and in temporary settings.

HotPoint + HotPort Features

Security

HotPort mesh networks feature multiple layers of security, including 40 and 104 bit WEP key and 128 and 256 AES key encryption. The mesh also provides packet filtering, based on MAC addresses, to limit access to the mesh. For additional security, a proprietary mesh protocol prevents non-HotPort devices from participating on the mesh.

VLANs

The HotPort mesh network includes support for virtual local area networks (VLANs) to enable traffic to be separated into smaller groups and application-specific LANs. The HotPort mesh supports 802.1q VLAN tagging of packets entering and exiting the mesh. You can assign Ethernet ports to different VLANs; only ports belonging to the same VLAN can switch traffic among themselves. You can define up to 4093 VLAN IDs and create up to 16 multiple, logically separated VLANs within a single mesh. The HotPort mesh also supports VLAN trunks.

Traffic Prioritization (class of service)

The HotPort system provides traffic prioritization levels to prioritize traffic on the mesh. This helps ensure that certain types of traffic requiring high throughput or continuous service, such as voice, take precedence over other forms of traffic.

Intuitive Network Mesh Management with HotView™ Software

HotView™ mesh management software provides live monitoring and management of Firetide HotPort wireless mesh networks, including HotPoint AP nodes. The software features a graphical user interface and provides access to all mesh and node settings, including security, VLAN, class of service, radio power controls, and network gateway interconnects. Live monitoring features include mesh and node statistics.

HotView Pro extend the management features of HotView across multiple meshes. Thus, an enterprise can manage all of its HotPort meshes worldwide from anywhere.

HotView and HotView Pro operate on virtually any workstation or server that is connected to the mesh, either directly or remotely via WAN connection or the Internet.

Radio Settings

HotPort wireless mesh supports 2.4 GHz OFDM and DSSS radio modes, as well as 5 GHz OFDM. When combined with 802.11b/g APs, the backbone can be run at 5 GHz, thus avoiding interference.

HotPort 3100 and 3500 Series Mesh Routers

HotPort 3100 series mesh nodes provide fast and easy indoor network deployment. They connect wirelessly to other indoor and outdoor HotPort nodes to form a mesh network. Ethernet packets are automatically switched across the mesh, in a manner analogous to an Ethernet switch, using AutoMesh™, a proprietary protocol developed by Firetide. AutoMesh has been optimized for efficiency in wireless mesh environments. HotPort nodes are plenum-rated and feature a built-in four-port 10/100 Ethernet switch for connecting networking devices a fully wireless mesh backbone. Models are available for operation at 2.4 GHz for high capacity and maximum range or at 5 GHz for high capacity and minimal interference from 2.4 GHz devices.

The HotPort 3100/PS supports the public safety band, used in the US.

The HotPort 3500 Series feature band-specific high-power radios, but are otherwise identical to the 3100 Series Models.

Outdoor Nodes

In addition to the indoor models, Firetide offers a range of HotPorts for outdoor use. These are similar to the 3100 and 3500 Series units, but are packaged in NEMA-4 enclosures suitable for outdoor use.

The full model range is shown in this table: (Data rates are typical for a single hop operation.)

Table 1. Summary of Firetide Mesh Router Models

Model & SKU	Use	Band	RF Output Power	TCP Data Rate	Default Channel
3101	Indoor	2.4, 5 GHz	standard	10 Mbps	2.462 GHz DSSS, Ch 11
3103	Indoor	2.4, 5 GHz	standard	25 Mbps	2.462 GHz DSSS, Ch 11
3100/PS	Indoor, Public Safety	2.4, 4.9, 5 GHz	standard	25 Mbps	4.962 GHz DSSS, Ch 5
3500-2401	Indoor	2.4 GHz	high	10 Mbps	2.462 GHz DSSS, Ch 11
3500-5001	Indoor	5 GHz	high	10 Mbps	5.805 GHz OFDM, Ch 161
3500-2403	Indoor	2.4 GHz	high	25 Mbps	2.462 GHz DSSS, Ch 11
3500-5003	Indoor	5 GHz	high	25 Mbps	5.805 GHz OFDM, Ch 161
3203	Outdoor	2.4, 5 GHz	standard	25 Mbps	2.462 GHz DSSS, Ch 11
3200PS	Outdoor, Public Safety	2.4, 4.9, 5 GHz	standard	25 Mbps	2.462 GHz DSSS, Ch 11
3600-2400	Outdoor	2.4 GHz	high	25 Mbps	2.462 GHz DSSS, Ch 11
3600-5000	Outdoor	5 GHz	high	25 Mbps	5.805 GHz OFDM, Ch 161

Indoor Unit - Unpacking and Installation

Unpacking and setup are straightforward. The HotPoint 4500 requires AC power, but can be mounted almost anywhere indoors. Brackets are available to facilitate wall or ceiling mounting. You will need a cat-5 cable to connect the AP to its companion Firetide mesh node. This cable can be any length permissible for 10/100 Mbps Ethernet.

Your AP includes a power supply and three different AC line cords, as shown in Figure 1. Use the one appropriate for your region.

Figure 1. Indoor AP Power Supply

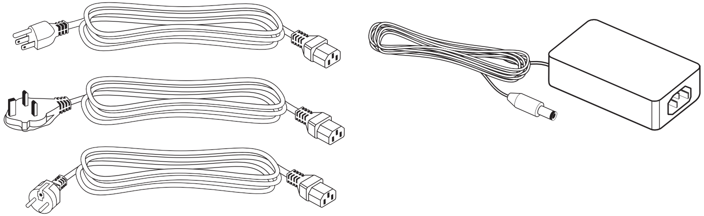
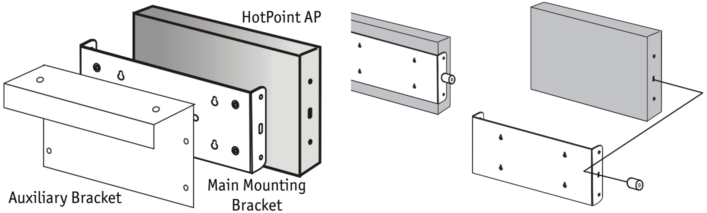


Figure 2. Optional Mounting Brackets



Wall/Ceiling Mounting Bracket (optional) with Auxiliary bracket for cube-wall applications.

Bracket Lock Mechanism Detail

Mount your HotPoint in a location that will give the best wireless coverage of AP clients. The access point does NOT have to be close to its companion HotPort node; in fact, it is better to mount each unit in a location that is optimum for the RF needs of that unit.

Figure 3. Firetide HotPoint 4500 Series - Front View

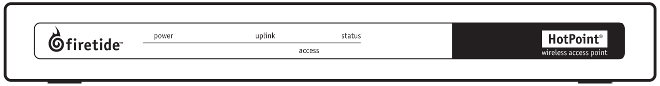
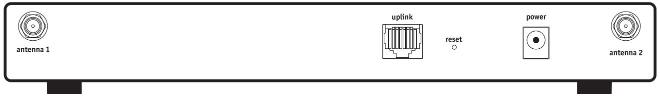


Figure 4. Firetide HotPoint 4500 Series - Rear View



After the units are installed, connect the access point to its companion HotPort node with a cat-5 cable. Then apply power to the access point.

Outdoor Unit - Unpacking and Installation

Unpacking and setup are straightforward. Included with your HotPoint 4600 are:

- Mounting bracket and hardware
- 2.4 GHz omnidirectional antennas (2)
- Weatherproof Ethernet cable, 10-pin to 10-pin, PoE-compatible. This cable will power your HotPoint when connected to port 2 of a Firetide 3200 Series or 3600 Series outdoor node.

You may wish to configure your HotPoint 4600 before installation. Refer to the software section of this manual for details on initial setup.

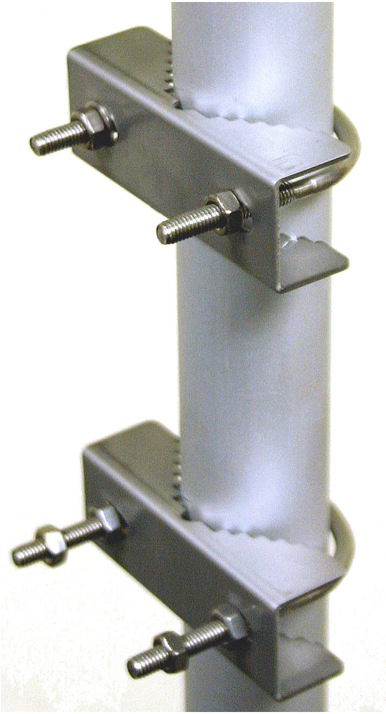
Note: a Firetide outdoormesh node can support up to two access points, but it can only power 1 unit via PoE. In addition, there are constraints on overall bandwidth and on VLAN support. In most cases, you will want to use only one HotPoint per HotPort.

Pole Installation

Installation on any pole up to 2 inches is easy. Begin by mounting the supplied U-bolts, and 'claw' pieces to the pole, using two nuts, as shown in Figure 5. Make the nuts just finger-tight.

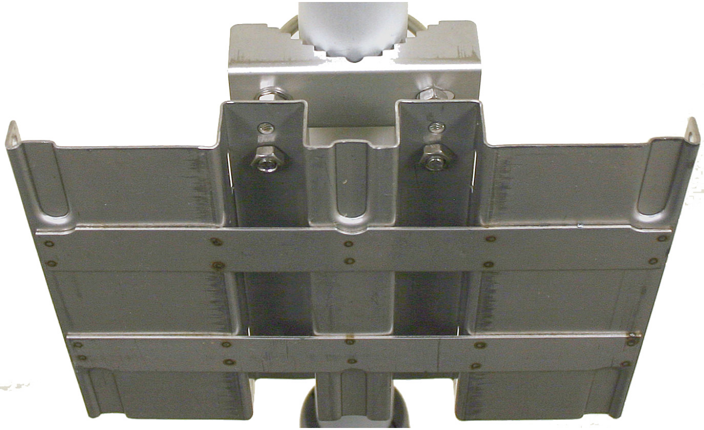
Depending on the pole diameter, you may need additional nuts, as shown on the lower clamp of Figure 5. The purpose of the extra spacer nuts is to prevent the U-bolt legs from protruding too far out beyond the mounting plate. This will interfere with the AP. If required, place two more spacer nuts on the U-bolts.

Figure 5. Pole Clamps



Next, attach the plate, using two more nuts, as shown in Figure 6. Adjust the spacer nuts to insure that the U-bolts do not protrude out of the fold in the plate. The exact adjustment will depend on pole diameter.

Figure 6. Mounting Plate



When the plate is mounted and aligned, tighten all the nuts with a 7/16-inch wrench. Then slide the HotPoint onto and downward slightly, so that its tabs on its backing plate (Figure 7) engage the mounting plate, as shown in Figure 8. Tighten the four knurled nuts on the sides.

The supplied antennas can be used for initial deployment, but should be replaced after initial testing with outdoor-rated units of suitable gain and pattern.

Figure 7. AP Bracket Mounting Tabs

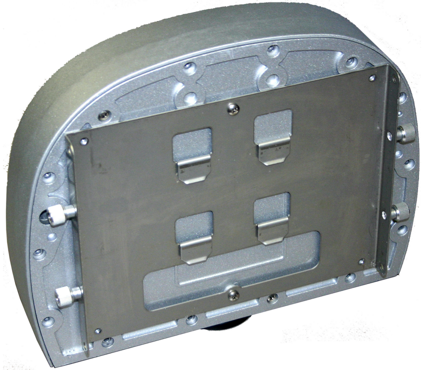
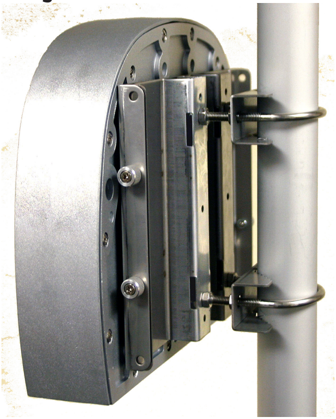


Figure 8. AP Mount - Finished



Understanding APs, AP Groups, VAPs, & VAP Groups

Before you begin installation, you should understand how Firetide's HotView Network Management System views HotPoint Access Points.

An AP is a physical box - a computer and a radio - which can implement up to 16 "virtual" access points. Virtual access points are the things that wireless clients actually see and connect to.

Each HotPoint node offers a range of network as well as radio configuration options. The commands which control these features and options are grouped logically. This makes it easy to manage large collections of physical nodes and virtual APs, once you understand the concepts.

Access Points (AP) - certain parameters, such as radio settings, are specific to the hardware on each particular physical node.

Virtual Access Points (VAP) - HotPoint nodes support Virtual Access Points. In general, each physical HotPoint can support up to 16 VAPs. (A HotPoint which is the server node of a WDS cluster can only belong to one VAP.)

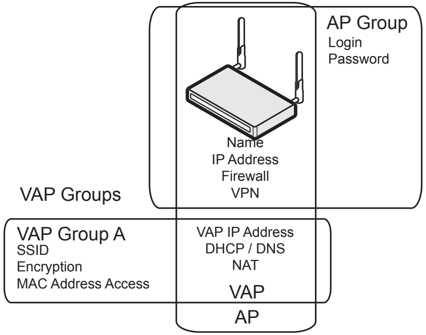
VAP Groups - VAPs are grouped together for management purposes. You will create at least one VAP group, with SSID, encryption, and other parameters. This is the 'access point' that will appear to wireless clients.

Access Point Groups - In some cases, you may want to grant management access to some nodes to one person or persons, and other nodes to other persons. This can be done using Access Point Groups. Each HotPoint may be assigned to an Access Point Group, or AP group. You can specify different user names and passwords for each group.

All HotPoint commands are grouped according to whether they affect settings on a physical node, a VAP Group, an AP Group, or an individual VAP.

Figure 9 shows how the various domains relate to each other.

Figure 9. Matrix of Physical and Logical APs - Simple



Figures 10 and 11 show more complex arrangements of multiple APs and multiple Virtual APs.

Figure 10. Three-AP Network

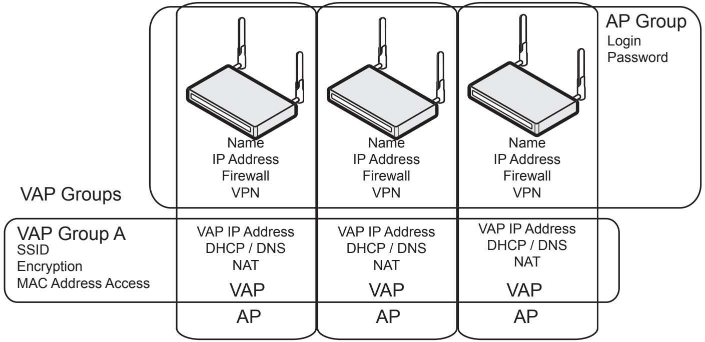


Figure 11 shows a three-AP, three-VAP configuration. You can have up to 16 VAPs per physical AP. You can have as many AP Groups as needed, and there is no limit to the number of APs in any one AP Group.

Figure 11. Large AP Matrix

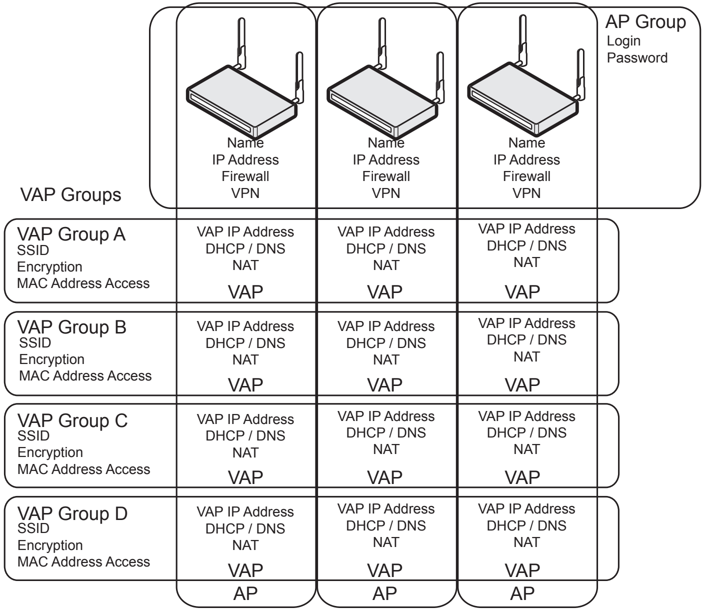


Table 2 gives a summary of all of the major commands and options available on the HotPoint APs, organized by logical group.

Table 2. Summary of Commands by Logical Group

Physical AP	AP Group	VAP Configuration	VAP Group Configuration
AP Name	Membership	DHCP Server DHCP Service IP address	WDS (new group creation only)
AP Mgmt IP address / DHCP client	Guest Login Admin Login	DNS	Broadcast SSID SSID suppression
Performance Statistics		NAT	VLAN
Radio Settings: ch, mode, RF power, beacon, rogue detection			DTIM, RTS/CTS, fragmentation
Firewall			Encryption
VPN			MAC address access
Country Code			Intracell blocking
Reboot / Reset			User data rate control
Import & Apply			IAPP
Refresh			WMM

Software Installation

If you are installing a new Firetide-based wireless network, begin by installing the HotPort Mesh nodes, and the HotView or HotView Pro mesh management software, before installing any HotPoint APs. Refer to the documentation supplied with those products for details.

If you are adding HotPoint APs to an existing network, begin by upgrading the existing mesh nodes to version 3.4.X.X or later. Use your existing version of HotView to upgrade all mesh nodes, then use HotView 3.4.X.X to configure HotPoint APs.

Basic Setup Sequence

Several steps are involved in configuring a HotPoint AP. These steps are summarized here, then shown in detail in the following pages.

1. Assign a management IP address to each AP. This address should be reachable from the computer running HotView. It does not need to be on the same subnet as the management address of the Firetide mesh.
2. Log in to the AP.
3. Set the Country Code.
4. Rename the AP. A name based on the AP's location is a good choice.
5. Set the radio settings (channel, etc) for each physical AP.

Repeat these steps for all access points. Then:

1. Create one or more VAP Groups, using the VAP Group Configuration command. You must have at least one group, even if you only have one AP.
2. Use the VAP Configuration command to configure those VAP features which are controlled per physical AP. (DHCP, DNS, NAT)
3. Use the VAP Group configuration command to assign the SSID, security, and other features for the entire VAP group.
4. Use the AP Group command to group all of APs into a managment group. (This is not necessary if you only have one AP. Also, you can create more than one group if you require multiple management domains, but it most cases this is not required.)

IP Address Planning

You should plan out your IP addressing scheme prior to deployment. You will need several ranges of IP addresses. All of these IP addresses are in addition to the management IP address (aka mesh IP address) assigned to your Firetide mesh network.

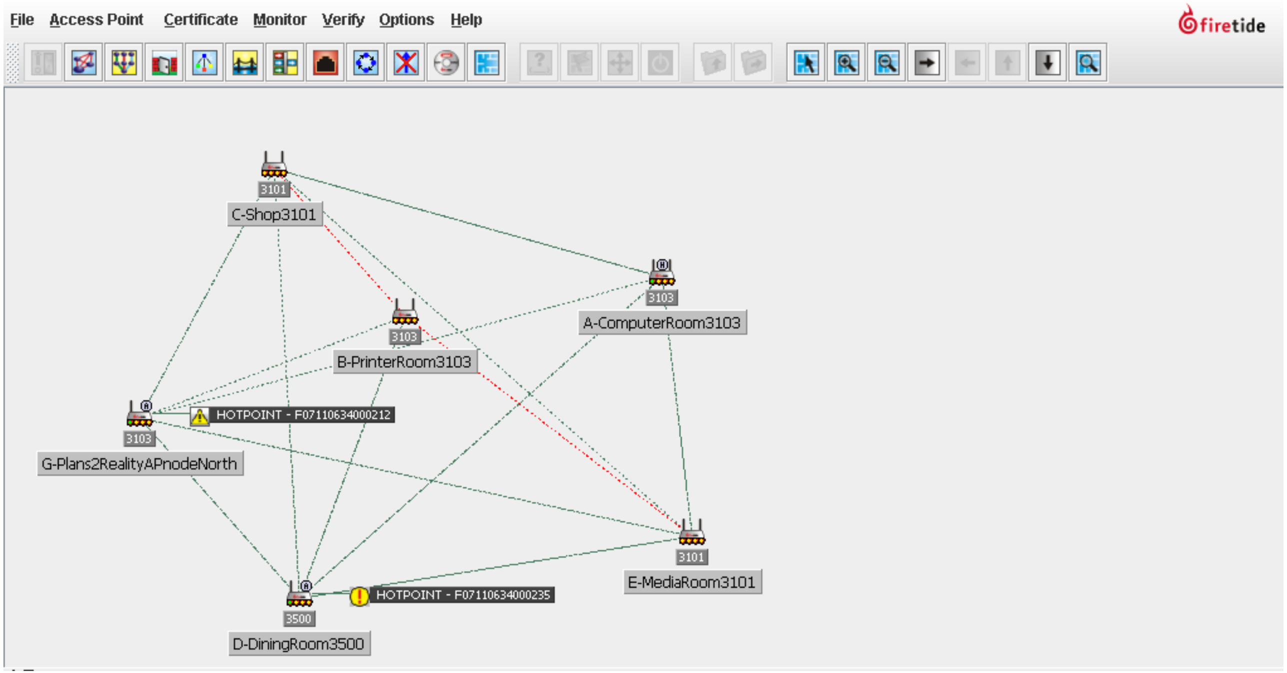
In general, you may assign AP IP addresses independently of the IP addressing scheme you use for the Firetide mesh. The only constraint on AP IP address assignment is that the IP addresses must be routable within your overall IP addressing scheme.

- A**P Management IP Address** - this is the IP address assigned to the physical access point, and is used for management purposes. An AP is capable of acquiring this address from a DHCP server, or it may be manually assigned. This address must be reachable from the HotView management workstation.
- **VAP Management / DHCP Server IP Address** - Each VAP requires an IP address. It is used for NAT, if enabled, and for DHCP, if the AP is configured to assign IP addresses to clients. It must be different from the AP Management IP address. Note that each AP can be a member of as many as 16 VAP Groups.
- **DHCP Address Range** - this is the pool of addresses available to be assigned to wireless clients.

It is permissible for an AP to acquire its AP Management address via DHCP, yet also serve DHCP addresses to clients. The addresses do not need to be on the same subnet, but all must be routable over the enterprise LAN.

Software Configuration

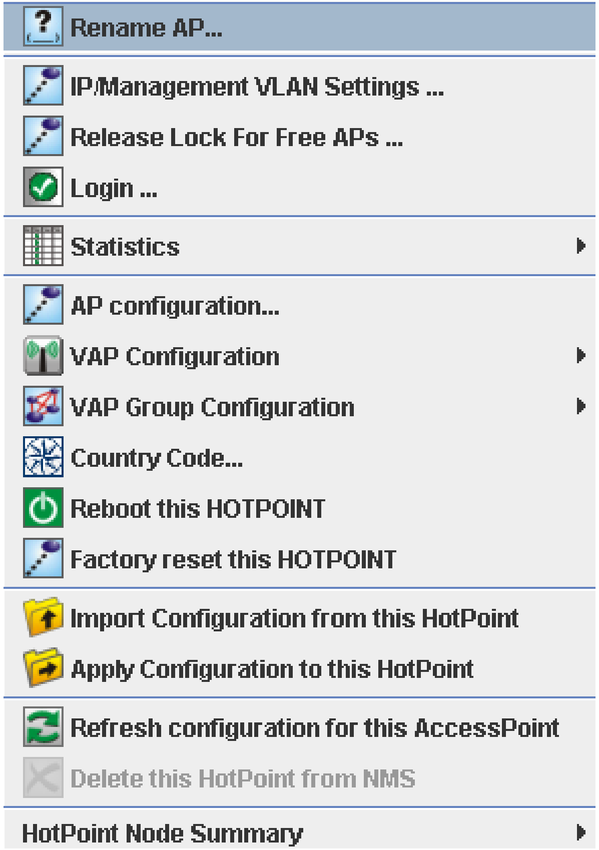
The Firetide HotPoint access point family requires HotView or HotView Pro software, version 3.4.X.X or newer, on your computer. In addition, the Firetide HotPort nodes to which the access points will be connected must be upgraded to firmware version M3.4.X.X. Access Points should have firmware version A3.4.X.X installed. After you've physically installed your access point, launch HotView (or HotView Pro). You will see a screen similar to this one:



AP Node Commands

These commands are accessed by right-clicking the AP icon. Begin by assigning an IP address to each node, and logging in to the node. You must then set the Country Code. Finally, you should rename each node.

Command	Function
Rename AP	Assigns the management screen name to the physical node. Note: this is NOT the SSID of the node; that is specified under the VAP Group Configuration command.
IP Settings (includes Management VLAN)	Assigns the IP address that will be used by the AP for management access. This command also allows you to assign a management VLAN, if desired.
Release Lock	Releases management control lock on APs.
Login	The default user ID and password is **admin** and **firetide**.
Statistics	Shows performance for a given VAP.
AP Configuration (Radio)	Allows you to specify the radio parameters, firewall configuration, and VPN.
VAP Configuration	Allows you to define DHCP service for the VAP.
VAP Group Configuration	Allows you to define radio and security options for a group of Virtual Access Points.
Country Code	Set once at initial startup.
Reboot, Reset	Allows you to reboot or reset to factory defaults.
Import, Apply	Allows you to save and restore node settings.
Refresh	Forces HotView to re-acquire the status of the AP.
Delete HotPoint	Removes 'stale' HotPoint icons from HotView.
Summary	Gives a summary of HotPoint node information.


Rename AP...
IP/Management VLAN Settings ...
Release Lock For Free APs ...
Login ...
Statistics
AP configuration...
VAP Configuration
VAP Group Configuration
Country Code...
Reboot this HOTPOINT
Factory reset this HOTPOINT
Import Configuration from this HotPoint
Apply Configuration to this HotPoint
Refresh configuration for this AccessPoint
Delete this HotPoint from NMS
HotPoint Node Summary

Physical AP Radio Settings

Each physical AP has certain radio settings which are common to all virtual APs on that node. These are set using the AP Configuration command, as shown at right.

Auto Channel allows the AP to find the clearest channel, or you may set the channel manually.

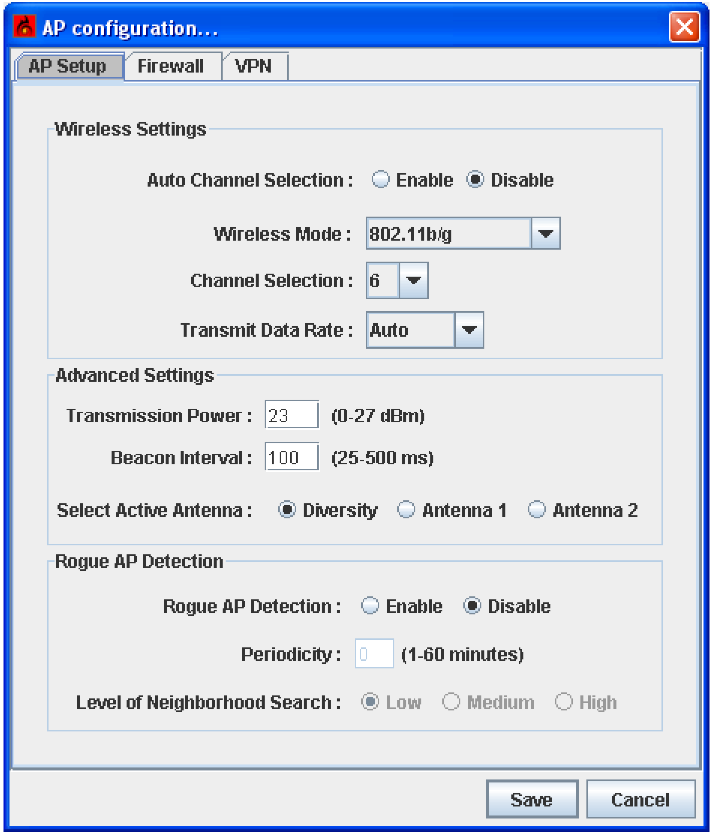
The **Wireless Mode** can be set to b, b/g, g-only, or 108g Static Turbo.

The raw **Transmit Data Rate** of the wireless link can also be specified.

Transmitter power and beacon can be controlled.

Antenna Diversity is supported. This control determines which antenna the unit listens on; transmit is always on Antenna 1. In most cases, **Diversity** is the best choice, but if you are only installing one antenna, set this to Antenna 1.

Rogue AP Detection enables the AP to detect other, “unknown” APs operating in the area, and report them. You may specifiy how often the AP stops and scans for rogue APs, as well as the level of search.



Wireless Settings

Auto Channel Selection : ○ Enable ● Disable

Wireless Mode : 802.11b/g

Channel Selection : 6

Transmit Data Rate : Auto

Advanced Settings

Transmission Power : 23 (0-27 dBm)

Beacon Interval : 100 (25-500 ms)

Select Active Antenna : ● Diversity ○ Antenna 1 ○ Antenna 2

Rogue AP Detection

Rogue AP Detection : ○ Enable ● Disable

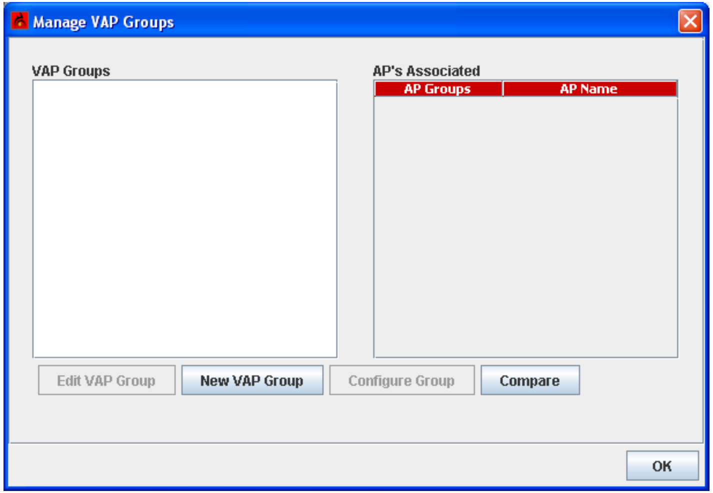
Periodicity : 0 (1-60 minutes)

Level of Neighborhood Search : ● Low ○ Medium ○ High

VAP Group Configuration

VAP Groups are the collections of Virtual Access Points that form the user-visible 'logical layer' overlaid on the physical collection of Access Points.

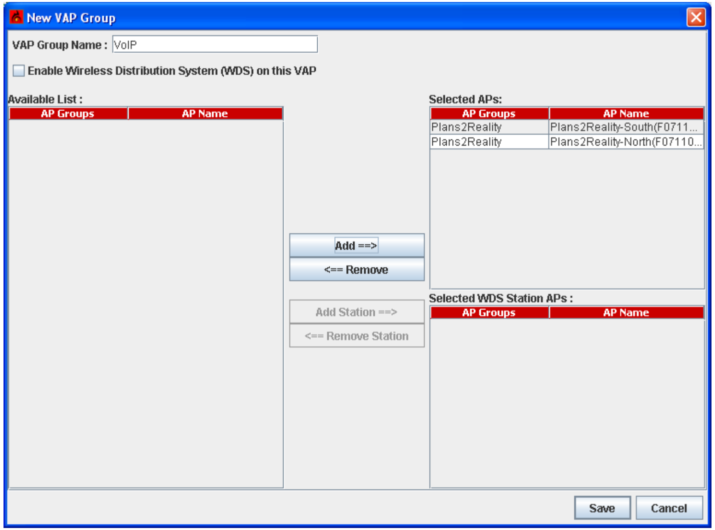
You must create at least one VAP Group, with at least one VAP in it. Do this by selecting **VAP Group Configuration** command from the Access Point menu. You will see the **Manage VAP Groups** screen, as shown on the left. Click on the **New VAP Group** button. The New VAP Group screen appears, as shown on the right. Enter a VAP Group Name. This is NOT the same as the SSID. Select one (or more) APs which will support this VAP group. Note that APs can be members of more than one VAP group. Typically, all APs are members of all VAP Groups.



You can also create Wireless Distribution Service (WDS) networks. However, there are some limitations:

- APs which are members of a WDS-enabled VAP Group cannot be members of any other VAP Group.
- Do not use WDS to bridge two APs which are connected to the same Firetide mesh. This creates a routing loop. Set the SSID and radio data rates.

There are two remaining basic setup steps: VAP Configuration and VAP Group Configuration. The order in which you do these is not critical; this manual will configure each VAP next.



New VAP Group

VAP Group Name : VoIP

☐ Enable Wireless Distribution System (WDS) on this VAP

Selected APs:

AP Groups	AP Name
Plans2Reality	Plans2Reality-South(F0711...
Plans2Reality	Plans2Reality-North(F07110...

VAP Settings

As shown in Figure 11, VAP Groups logically intersect with APs to form VAPs. Certain settings are specific to each VAP. These settings include the IP address of the VAP, the DHCP Server settings, the DNS settings, and the optional NAT capability.

To modify these settings, right-click on the AP icon and select the **VAP Configuration** command. This command will reveal a second drop-down menu which lists all of the available VAPs. Select the VAP you wish to configure. You will see a screen like the one at right.

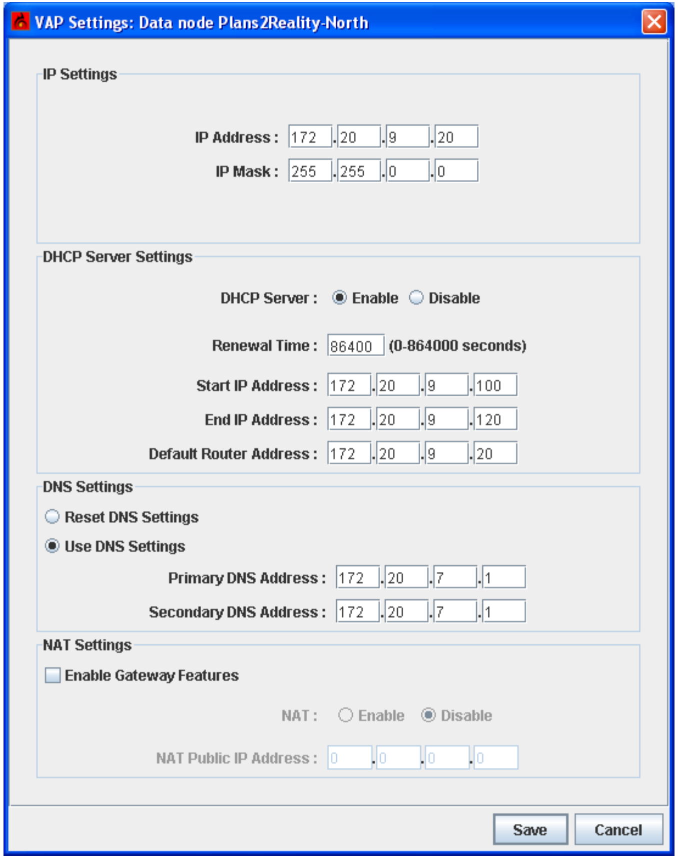
Enter the VAP IP address. This must NOT be the same as the management IP address of the AP.

If desired, configure DHCP service. For DHCP, each VAP Group should have every node in that group configured to serve addresses to clients. All nodes must be configured, and each node must have a unique range of assignable IP addresses.

Note: it is possible, using VLANs, to insure that each client receives its IP address from the VAP with which it physically associates, rather than the first DHCP server within the VAP Group to respond. This is useful in multi-tenant applications. Each node will need a VLAN; refer to your HotView Pro manual for assistance in VLAN configuration.

You may also use an independent DHCP server. The HotPoint AP will forward DHCP requests if it is not configured to serve DHCP addresses.

NAT may be enabled here, if desired.



VAP Settings: Data node Plans2Reality-North

IP Settings

IP Address : 172.20.9.20

IP Mask : 255.255.0.0

DHCP Server Settings

DHCP Server : ● Enable ○ Disable

Renewal Time : 86400 (0-864000 seconds)

Start IP Address : 172.20.9.100

End IP Address : 172.20.9.120

Default Router Address : 172.20.9.20

DNS Settings

○ Reset DNS Settings

● Use DNS Settings

Primary DNS Address : 172.20.7.1

Secondary DNS Address : 172.20.7.1

NAT Settings

□ Enable Gateway Features

NAT : ○ Enable ● Disable

NAT Public IP Address : 0.0.0.0

VAP Group Settings

Basic VAP Group Settings

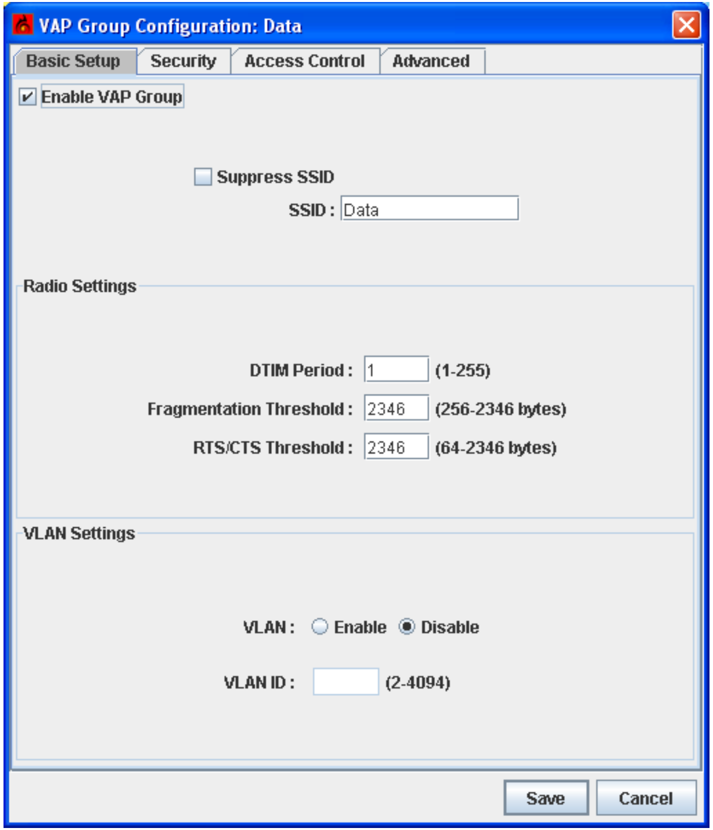
The SSID defaults to the VAP Group name, but this can be changed if desired. You must also enable the VAP Group by checking the box.

DTIM is the Delivery Traffic Indication Message. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pick-up.

The DTIM period you specify here indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup.

Fragmentation and **RTS/CTS** Thresholds can be used to tune wireless performance in some specialized applications.

A **VLAN** can be created for this VAP Group. This can be useful for security and privacy purposes.



VAP Group Configuration: Data

☑ Enable VAP Group

□ Suppress SSID

SSID : Data

Radio Settings

DTIM Period : 1 (1-255)

Fragmentation Threshold : 2346 (256-2346 bytes)

RTS/CTS Threshold : 2346 (64-2346 bytes)

VLAN Settings

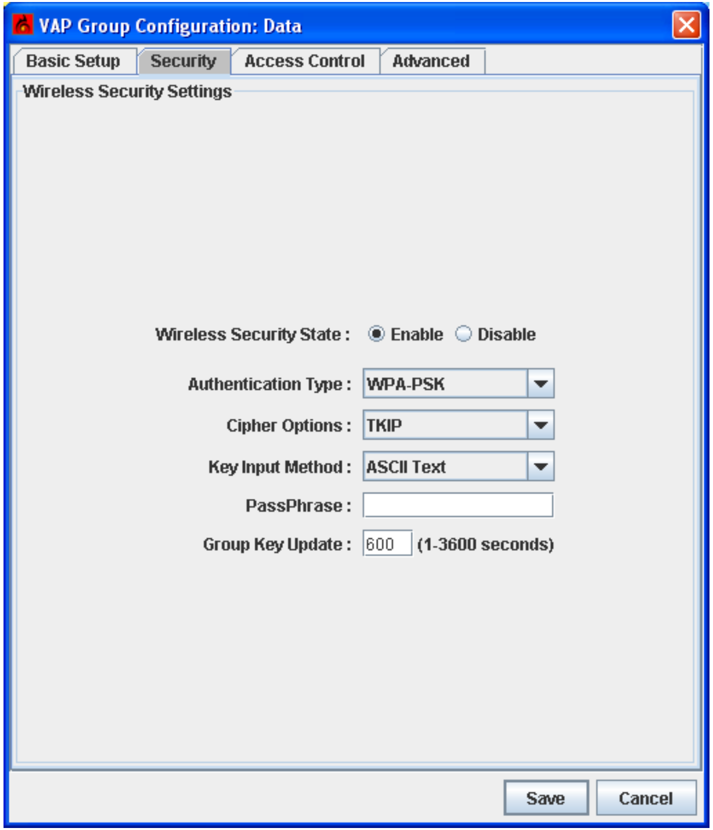
VLAN : ○ Enable ● Disable

VLAN ID : (2-4094)

VAP Group Security Settings

A wide range of wireless security options are supported. Select the one you prefer. Authentication choices include:

- 802.1X
- Auto
- Open
- Shared Key
- WPA
- WPA-Auto
- WPA-Auto-PSK
- WPA-PSK
- WPA2
- WPA2-PSK



Wireless Security State : ● Enable ○ Disable

Authentication Type : WPA-PSK

Cipher Options : TKIP

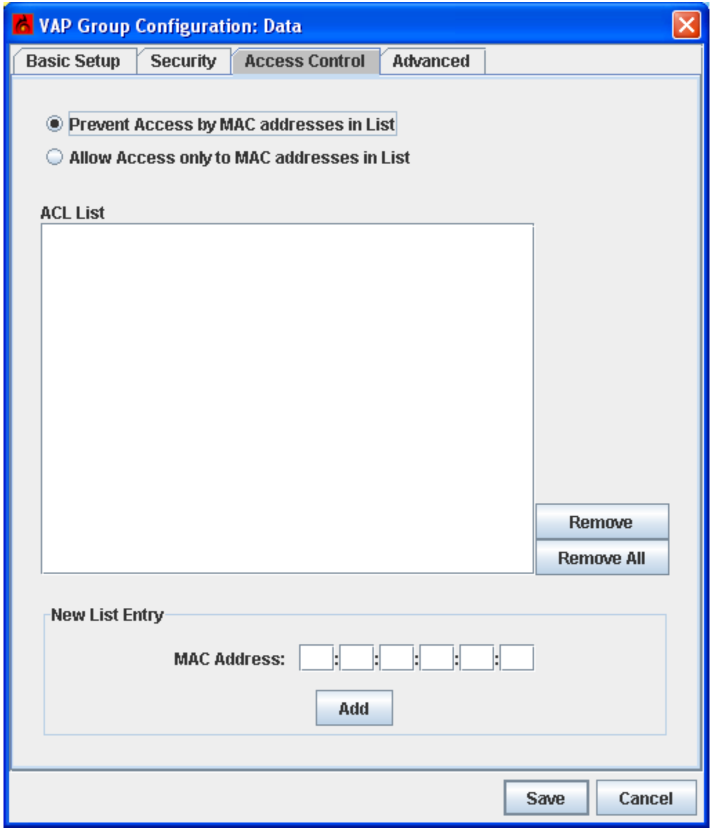
Key Input Method : ASCII Text

PassPhrase :

Group Key Update : 600 (1-3600 seconds)

MAC Address Access Control

If desired, VAP Group access can be limited to an explicit group of MAC addresses, or denied.



● Prevent Access by MAC addresses in List

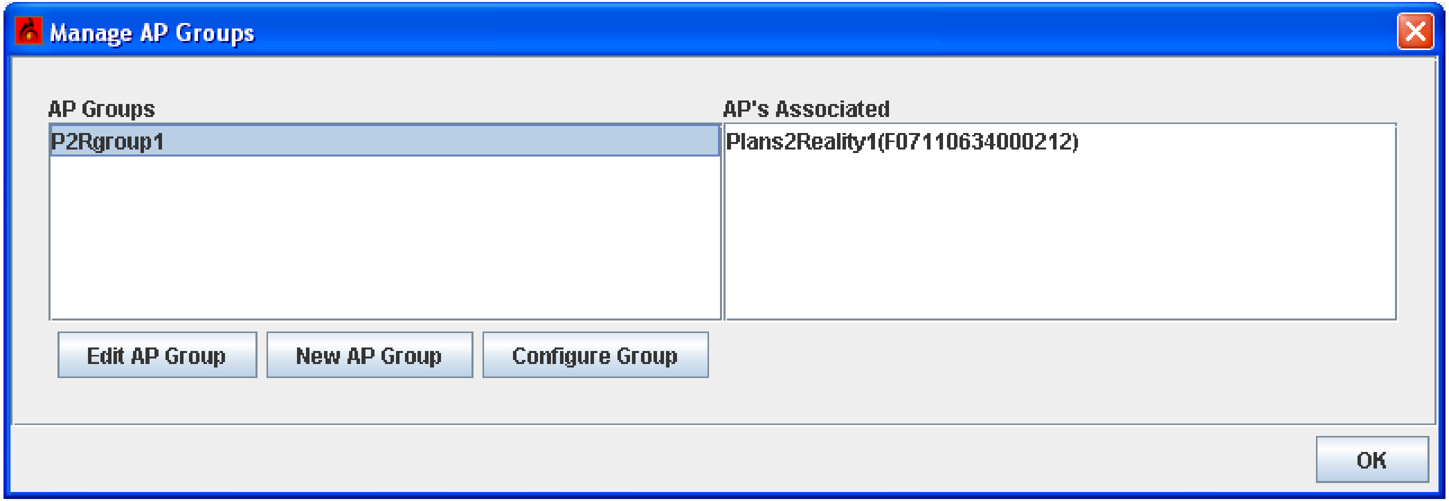
○ Allow Access only to MAC addresses in List

AP Group Commands

HotPoint Access Points can be grouped for management purposes. Each group shares a set of administrative accounts and passwords. The AP Group Configuration command, under the Access Point menu, opens a dialog box, in which you can create new groups and edit existing groups.

The Configure button lets you re-define the user ID and password for all APs in a group. There is an account name for read-write privileges, and a second, 'guest' account with read-only privileges. The defaults are **admin** and **firetide**, but these should be changed for security reasons.

Most small installations will find a single AP group for all APs to be the most convenient to manage. Larger installations which have APs for security purposes as well as user data networking may wish to divide the management functions (and access privileges) by creating multiple groups with unique user IDs.


Manage AP Groups

AP Groups

P2Rgroup1

AP's Associated

Plans2Reality1(F07110634000212)

Understand Advanced Settings

Intracell Blocking

Intracell blocking allows you to prevent users of a given VAP from seeing each other. When enabled, all users can use the AP to reach the network, but no user can access other computers on that VAP.

Note Intercell blocking is accomplished with VLANs.

User Data Rate

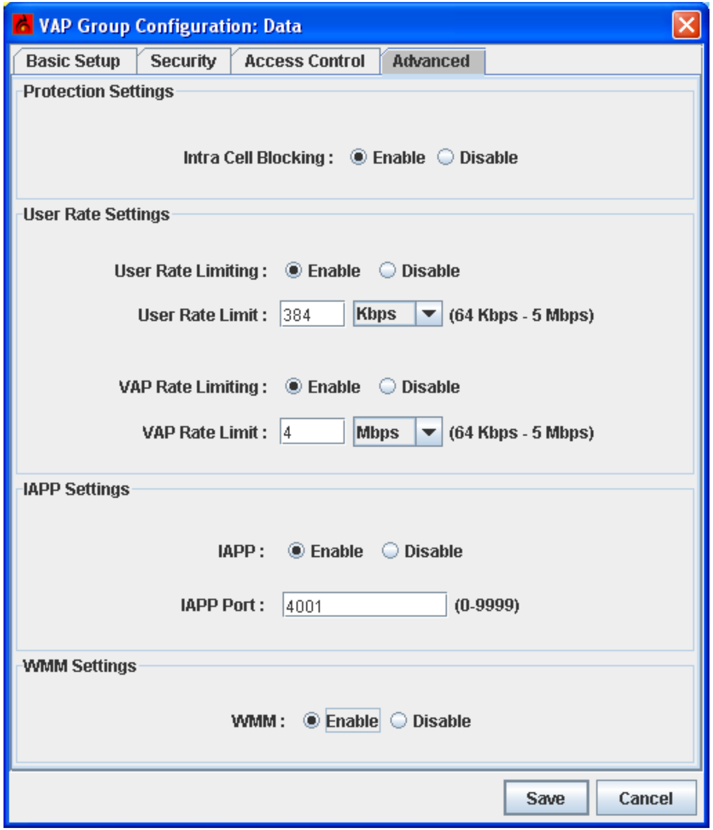
In order to prevent one user from consuming excess bandwidth on the backbone, you can limit the data rate for each user. You can also limit the aggregate rate for each VAP Group.

IAPP and Roaming

The Inter-Access Point Protocol describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multi-vendor systems. If you have other APs which support it, you can enable its operation and set the port used for control.

WMM

WMM, also known as WME, allows clients which support the Wireless Multimedia Extensions protocol to prioritize VoIP and video traffic. If your clients support it, enable it here.


VAP Group Configuration: Data

Protection Settings

Intra Cell Blocking : ● Enable ○ Disable

User Rate Settings

User Rate Limiting : ● Enable ○ Disable

User Rate Limit : 384 Kbps (64 Kbps - 5 Mbps)

VAP Rate Limiting : ● Enable ○ Disable

VAP Rate Limit : 4 Mbps (64 Kbps - 5 Mbps)

IAPP Settings

IAPP : ● Enable ○ Disable

IAPP Port : 4001 (0-9999)

WMM Settings

WMM : ● Enable ○ Disable

Advanced Features

Firetide HotPoint APs support several advanced features. These include:

- NAT
- Firewall
- VPN

NAT

Network Address Translation is configured per VAP; that is, each physical node has a NAT setting for each VAP Group to which it belongs. Use the **VAP Configuration** command (in the right-click menu) to configure it.

Firewall

The Firewall features is configured per physical AP, and is common to all VAP Groups on that AP. The Firewall blocks ports coming from the AP's wired connection, going to the wireless clients.

By default, all ports are open. Enabling the Firewall closes all ports; individual ports can then be opened as needed. Use the **AP Configuration** command (in the right-click menu) to configure it.

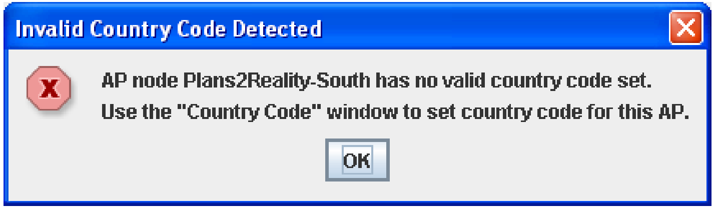
VPN

APs can be tunneled directly to a remote network by using the VPN feature. The VPN will tunnel all traffic from a physical AP, regardless of VAP Group. Use the **AP Configuration** command (in the right-click menu) to configure it.

Country Code Assignment

Firetide HotPoint APs are designed to be compliant with all applicable regulations for their country of operation. In order for this to work, the AP needs to know which country it is in.

You MUST set the Country code in order for the HotPoint AP to work correctly. If the Country Code has not been set, you may see the following warning:



Invalid Country Code Detected

AP node Plans2Reality-South has no valid country code set.
Use the "Country Code" window to set country code for this AP.

Appendix A - HotPoint Features and Specifications

Wireless

- IEEE 802.11b/g
- Frequency ranges 2.400—2.484 GHz
- Transmit power up to 400 mW
- 802.11h (Automatic Transmit Power Control)
- Manual Transmit Power Control
- 802.11d (Auto Channel Select)
- Receive sensitivity measured at N connector:
  - 2.4 GHz, DSSS
    - 1 Mbps: -96 dBm
    - 11 Mbps: -90 dBm
  - 2.4 GHz, OFDM
    - 6 Mbps: -93 dBm
    - 54 Mbps: -74 dBm
- Media Access Protocol: CSMA/CA with ACK
- Modulation techniques: DSSS, OFDM, CCK, DQPSK, DBPSK
- Range up to 200 meters depending on client
- WDS

Networking

- Up to 16 independent VLANs
- DHCP client and server, separate DHCP range per SSID
- Up to 16 ESSIDs per HotPoint

Security and Encryption

- 802.11i
- 40 bit, 104 bit WEP keys
- 128 bit, 256 bit AES keys
- 802.1x authentication
- TKIP
- WPA2
- VPN tunneling and filtering
- ESSID suppression
- Firewall
- MAC access control
- Rogue AP detection

Management & Configuration

- Integrated mesh and access management
- Web-based management
- SNMP v2/3
- CLI
- FTP firmware upgrade
- 802.1p (Quality of Service)
- 802.11e (WMM) (Quality of Service)
- NAT
- Virtual AP Grouping – uniform SLAs
- Physical AP Grouping – uniform parameters
- Per-user and per-VAP rate limiting
- Per-user-based accounting

Performance

- Up to 54 Mbps
- Up to 64 concurrent users simultaneously per HotPoint
- Inter Access Point Protocol (IAPP) enabled per 802.11f
- Fast handoff enabled, per 802.11r draft recommendation
- Intercell blocking – blocks communication between APs
- Intracell blocking – blocks communication between BSSIDs
- Auto discovery
- Configurable web portal
- Broadcasted advertising
- No user configuration

Network Port

- One 10/100 Base-T (RJ-45) ports IEEE 802.3, 802.3u compliant
- CSMA/CD 10/100 auto-sense

Indoor Unit - Power

- Input voltage: 5 VDC @ 2.0 A
- External power supply: 100-240 VAC, 50/60 Hz
- Power consumption: 10 W

Outdoor Unit - Power

- Input voltage requirement: 5 VDC @ 2.0 A
- PoE-compatible - will operate PoE supplied by Firetide 3200/3600 Series Outdoor Mesh Router
- Optional external power supply: 100-240 VAC, 50/60 Hz
- Power consumption: 10 W

Indoor Unit Enclosure

- System indicator LEDs (power, status, mesh, fault)
- Ethernet indicator LEDs (link status, activity)
- Two antenna connectors: SMA, reverse polarity
- Power connector
- One Ethernet data connectors (RJ-45)
- Reset button (recessed)
- Security slot for physical locking device
- Weight: 2.1 lbs (.95 Kg) without external transformer
- Dimensions: 9.00 in x 5.84 in x 1.07 in (22.85 cm x 14.83 cm x 2.71 cm)

Outdoor Unit Enclosure

- NEMA-rated die-cast aluminum
- Two antenna connectors, type N
- Weatherproof power connector
- Weatherproof Ethernet connector

Regulatory agency certifications

- Plenum rated UL2043
- FCC Part 15

Environmental specifications

- Operating temperature: -20º C to +60ºC
- Storage temperature: -20º C to +70º C
- Humidity (non-condensing): 10% to 90%
- Storage humidity (non-condensing): 10% to 90%

Appendix B - Regulatory Notices

USA

FCC Class A Notice

This device complies 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 Part 15 Note

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 in an office installation. 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/television technician for help.

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.

FCC Radiation Exposure Statement

The antenna used for this transmitter must be installed to provide a separation distance of at least 35 cm from all persons and must not be co-located or operated in conjunction with any other antenna or transmitter. OEM Integrators, end-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

Installation

Antenna(s) for this 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.

Approved antennas are:

Maxrad / PCTel	MFB24008
NCG Coment	SF-245W
Firetide	C812-510010-A

Canadian Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations. Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur du Canada. This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

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

Firetide HotPoint 4500 and 4600 wireless access points 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.

HotPoint Wireless Access Point

www.firetide.com

APUG001 082206

firetide™
instant mesh networks™