How This Reference Guide is Organized

**Scope of this Reference Guide**
This multi-volume reference guide has been designed to cover all 3.x versions of HotView and HotView Pro, as well as 4.x versions of HotView and HotView Pro. It is also applicable to all Series 3000 nodes, Series 6000 nodes, Series 4000 access points, Series 2000 CPE, and the Firetide Controllers.

Feature sets vary. Older versions do not have all of the features described in this manual, but in general the features they do have work as described herein. There may be minor differences.

Screen shots vary slightly among different versions of HotView. In general these differences are not significant to mesh operation. Where a feature is specific to certain classes of hardware, this is also called out (e.g. Auto Channel Assignment for Series 6000 only). Last but not least, certain functions are specific to HotView Pro only. These are also identified as such.

This manual is organized into Volumes, Sections, and Chapters. The Volumes are:

**Volume One: Wireless Mesh Basics**

- Wireless Mesh Basics describes the theory of wireless mesh operation, and explains the Firetide architecture. It explains how to plan deployments and how to assess RF conditions before deployment.

  This volume should be read and understood by planners, installers, system architects, and operators.

  It also describes the use of HotView Pro in managing a basic Firetide Mesh.

**Volume Two: Advanced Applications for Wireless Mesh**

- This volume explains the many advanced capabilities in the Firetide mesh architecture, and shows how and where to use them.

**Volume Three: Access Points & ISP Platforms**

- This volume explains the features and uses of Firetide’s unique, enterprise-class 802.11 WiFi access point product. Firetide’s access point products can be used alone or in combination with other Firetide products; both applications are covered.

  It also explains how the HotClient family can be used to deliver DSL-equivalent Internet access to residential and small-business subscribers.

**Volume Four: Mobility Controllers**

- Mobility is the short-hand expression for Firetide’s system for providing uninterrupted connectivity to all types of mobile users, including police and fire vehicles and well as commuter trains and busses and individual mobile 802.11 users.

**Volume Five: Reference Materials**

- This volume contains numerous appendices with useful reference information.

Within each Volume are Sections on the features and capabilities of the Firetide Mesh architecture, and chapters that describe specific operating techniques.

**Document Revisions**

The HotView Pro Reference Guide is updated frequently as new features are added. The multi-volume document as a whole has a three-digit revision number: A.B.C. The individual volumes have a four-digit revision number: A.B.C.D, where A.B.C is the same as the parent revision. Whenever any volume is revised, digit D is incremented for that volume, and digit C is incremented for all volumes.
Short Table of Contents

Section V Managing 802.11 Access Points ................................................................. 4
  Chapter 31 Firetide HotPoint Access Points .............................................................. 5
  Chapter 32 The Firetide WLAN Controller ............................................................... .28
  Chapter 33 Managing Third-Party APs ................................................................. .34

Section VI Managing HotClient CPE Systems ......................................................... 36
  Chapter 34 HotClient/HotPoint Auto-Configuration Setup ........................................ .37
  Chapter 35 HotClient Standalone Setup ................................................................... .42
  Chapter 36 HotClient Browser-based Setup .............................................................. .47
Section V Managing 802.11 Access Points

HotView Pro can manage both Firetide’s own HotPoint series of 802.11 access points as well as third-party access points connected to the Firetide mesh.

Firetide’s HotPoint AP family includes the HotPoint 4500 Indoor AP and HotPoint 4600 Outdoor AP. These are full-function enterprise-class APs. The family also includes the HotPoint 4100 indoor AP and the HotPoint 4200 Outdoor AP. These are also enterprise-class APs, and when used with the Firetide WLAN Controller deliver all the same functions as the HotPoint 4500 and HotPoint 4600 AP family. They also operate as thin APs in standalone mode, with a slightly more limited feature set.

In general, setup and operation of all types of APs is very similar. This manual shows various setup and configuration steps on various HotPoint models; the procedures are essentially the same on all models.

Chapter 31 will show you how to manage Firetide’s HotPoint series of enterprise-class access points.

Chapter 32 shows how Firetide’s WLAN Controller enhances the functionality of both regular and thin APs. It also shows you how to manage client mobility across access points.

In some cases you may wish to use the Firetide mesh network in conjunction with access points made by other vendors. HotView Pro supports this. Chapter 33 will show you how to manage third-party access points (that is, non-Firetide) which are connected to Firetide mesh nodes.

Firetide HotClient CPE for Internet Service Delivery

Firetide offers a solution for ISPs and other organizations who wish to deliver DSL-equivalent Internet service to consumers, businesses, or for any other application that needs an Ethernet connection and megabit-level speed. The HotClient family of affordable customer-premises equipment uses Firetide wireless technology to maintain the WAN connection, and delivers familiar 10/100 Mbps service via an RJ-45 jack on the customer premises.

HotClient 2100 and 2200 models work with Firetide APs to deliver this service. A single Firetide AP supports dozens of HotClients in its neighborhood.

Chapter 34 describes the setup and operation of a HotClient-based Internet access network.
Chapter 31 Firetide HotPoint Access Points

Firetide's HotPoint AP family offer similar capabilities. All are enterprise-grade APs with support for virtualization. All operate as independent APs, or under the control of a Firetide WLAN Controller. The 4100 and 4500 are for indoors; the 4200 and 4600 are for outdoors.

Table 20. HotPoint Family Models and Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>4100 alone</th>
<th>4200 alone</th>
<th>with WLAN ctrl</th>
<th>4500 alone</th>
<th>4600 alone</th>
<th>with WLAN ctrl</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Radio Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>400 mW transmitter</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Manual xmit power control</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Auto channel select</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>2.4 GHz band</td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>4.9 GHz band</td>
<td>√</td>
<td>√</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.0 GHz band</td>
<td>√</td>
<td>√</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11d</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11b/g</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11a</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Turbo mode (for supported clients)</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WMM QoS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WDS server</td>
<td>-</td>
<td>-</td>
<td>√</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>WDS client</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rogue AP Detection</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>802.11i; 40/128 WEP, 128/256 AES, TKIP</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WPA/WPA2 encryption</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES encryption</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.1X authentication</td>
<td>-</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login-based authentication</td>
<td>-</td>
<td>-</td>
<td>√</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL re-direction</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>IP walled garden</td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11f IAPP security handoff</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11r fast handoff</td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Layer 2 / Layer 3 Roaming</td>
<td>-</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intercell blocking</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intracell blocking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC address access control</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSID suppression</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLANs</td>
<td>4</td>
<td>4</td>
<td>16</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controller to AP tunnel</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Network Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP client</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP server</td>
<td></td>
<td>1/VAP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAT</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN Tunneling / Filtering</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtualized APs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP Management Groups</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtualized AP Management Groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fairness among connected STAs (to client level)</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per-user rate limiting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per-VAP rate limiting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum clients per AP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Management Features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS access for management</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP v2/v3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supports pre-configured 2100/2200 HotClients</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supports auto-configured 2100/2200 HotClients</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Further information on the Firetide WLAN Controller can be found in Chapter 32.
Modes of AP Operation

Firetide Hotpoint access points can be used as standalone APs or as companions to Firetide Mesh Routers, or a combination of the two. HotPoint access points can be managed in a number of ways, depending on your overall network and requirements. The management options are:

- ‘Integrated’ operation - each HotPoint is connected directly to a HotPort mesh router via an Ethernet span.
- ‘Standalone’ operation - there are no HotPorts in use, and the HotPoints are connected directly to the enterprise LAN.
- ‘Mixed’ - a combination of the above.

Note that the features and capabilities of the HotPoints are not affected by this, nor are any aspects of WLAN Controller operation. AP operational mode affects only the method by which you initially set up the AP.

Integrated Operation

Connect the HotPoint access points to their respective HotPort mesh routers. Configure and manage them using either HotView or HotView Pro. The HotPort node will discover the HotPoint automatically. This can be disabled via a right-click command on the HotPort node.

Standalone Operation

Connect the HotPoint access points to your enterprise LAN. You will want to connect them one by one and assign each an IP address. You can then configure them and manage them using HotView or HotView Pro.

HotPoint nodes can acquire IP addresses from a DHCP server; if you use this option, you will need to get the assigned IP addresses from the DHCP server. It may be easier to assign addresses manually.

Mixed Operation

Some deployments may have both integrated and standalone APs. In such cases, you can still manage all of the HotPoints and HotPorts using HotView or HotView Pro.

You may wish to avoid this configuration if you are planning on supporting mobility in your mesh. The Firetide Mobility Controller can support mobility across either integrated or standalone HotPoint arrays, but cannot do both at the same time.

Understanding the ’Association’ Process

The HotPort mesh routers run a discovery protocol to determine if there is a HotPoint access point connected to them. This protocol operates at layer 2, below IP, and it will discover HotPoints which are connected to HotPorts via Ethernet, regardless of the number of switches or hubs between the HotPort mesh router and the HotPoint access point.

This means that if you connect one or more HotPoint access points to your enterprise LAN, and then connect a HotPort mesh router, that mesh router will discover the HotPoints and associate with them. Specifically, it will associate with, and remember, the first four HotPoints it discovers.

If you wish to prevent this, place the HotPoints on a different LAN segment and assign them to a different IP subnet.

It’s possible to have more than four APs connected to a single HotPort, but this is not recommended. HotPort nodes use the same basic radio mechanism as the HotPoint AP. A HotPort has two radios, and can easily handle the load of two APs, or even four if the APs are not heavily loaded. Beyond that, there is not enough backhaul capability. To deal with the situation where you need different APs for different functions, HotPoints offer AP Virtualization.

AP Virtualization

Firetide’s HotPoint system is an enterprise-class 802.11 a/b/g wireless access system. As such, it has been engineering with management capabilities not found in consumer-grade products.

- Each HotPoint can be configured with up to 16 Virtual Access Points, or VAPs. Each VAP behaves like an independent access point. Thus, you can have one VAP configured for guest access and a second VAP configured for secure employee wireless access. A third VAP can support wireless security cameras (with full privacy), while a fourth VAP can be assigned a higher QoS to support mobile VoIP.
- VAPs can be grouped. This makes it easy to change the password or security settings, for example, for all employee wireless access across all access points with just a few clicks.
- Physical access points can also be grouped. This makes it easy to change hardware settings (such as radio channel) system wide with just a few clicks.

The options and capabilities of the Firetide HotPoint system are covered in detail later in this chapter. You should study this information carefully when planning your AP deployment.
Basic Setup Sequence

The basic sequence of steps in setting up a Firetide HotPoint access point are summarized here, then shown in detail in the following pages.

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 4.7.X.X or later. Use your existing version of HotView to upgrade all mesh nodes, then use HotView 4.7.X.X to configure HotPoint APs.

Then:

1. Depending on whether you are using your HotPoints as Associated or Standalone, configure your management tool (HotView, HotView Pro, or a browser) to access the HotPoint.
2. Assign a management IP address to each HotPoint. The default address options are shown in Table 21. The IP address you pick should be reachable from the computer running HotView, or a browser. It does not need to be on the same subnet as the management address of the Firetide mesh.

Note that if you are using DHCP for Standalone access points, you will need to capture the IP address assigned by the DHCP server to each HotPoint. Because this complicates management, Firetide recommends that you not use DHCP to assign IP addresses to HotPoint nodes, but it is a supported option.

3. Log in to the AP.
5. Change the default password.
6. Rename the AP. A name based on the AP’s location is a good choice.
7. Set the radio settings (channel, etc) for each physical AP.

Repeat these steps for all access points. Before proceeding with the details of setup, you should understand the interrelationship between physical nodes and virtual access points. This is discussed on the next page. Read this material before proceeding.

(Note that VAP Groups and AP Groups are not supported on the HotPont 4100 and 4200 unless you are using the WLAN Controller.)

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. Use the AP Group command to group all of APs into a management 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 in most cases this is not required.)

<table>
<thead>
<tr>
<th>HotPoint Connection Method</th>
<th>DHCP Server</th>
<th>Default IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>via HotPort node</td>
<td>don’t-care</td>
<td>none</td>
</tr>
<tr>
<td>Standalone</td>
<td>DHCP available</td>
<td>as assigned by DHCP</td>
</tr>
<tr>
<td></td>
<td>no DHCP available</td>
<td>192.168.224.160</td>
</tr>
</tbody>
</table>
Understanding APs, AP Groups, VAPs, & VAP Groups

Before you begin software configuration, you should understand your choices for management. You may use Firetide’s HotView Network Management System to manage HotPoint Access Points, or you can manage individual access points via a web browser or via SNMP. Regardless of the method, the essential management is the same.

An AP is a physical system - 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 37 shows how the various domains relate to each other. Figure 38 shows a more complex arrangement of multiple APs and multiple Virtual APs. Figure 39 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 37. Matrix of Physical and Logical APs - Simple

Figure 38. Three-AP Network

Figure 39. Large AP Matrix
Table 22 gives a summary of all of the major commands and options available on the HotPoint APs, organized by logical group. Note that some features may only be available on Model 4100 and 4200 HotPoints when used with the Firetide WLAN Controller.

### Table 22. Summary of Commands by Logical Group

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

### 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.

- **AP 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.

### Subnetting

Users with large numbers of HotPoint access points in relationship to the number of HotPort mesh routers should consider placing Standalone HotPoints on a separate IP subnet and a separate LAN segment. This will prevent HotPorts from discovering and associating with HotPoints.
HotPoint Configuration

The Firetide HotPoint access point family requires either HotView or HotView Pro software, version 4.7.X.X or newer, on your computer, or a browser. In addition, the HotPort nodes to which the access points will be connected must be upgraded to firmware version M3.5.X.X. Access Points should have firmware version A2.0 installed.

If you’ve connected your HotPoints as integrated nodes, launch HotView Pro and log in. Your screen will look like Screen 123.

Screen 123. Access Points on a Firetide Mesh

New or factory-reset APs default to IP address 192.168.224.160. You should right-click on each AP and change its IP address to a unique value suitable for your overall enterprise IP addressing system.

Firetide mesh nodes look for APs and associate them. This is usually the desired response, but in some cases a mesh node may discover and associate an AP that you wish to use as a standalone node. (This can happen if they are both plugged into the same Ethernet switch, for example.) To force an associated AP to dis-associate, right-click on the mesh node to which it is associated, and select the Disable Integrated Access Points command. Then add the APs as described in the following section.

Note that this operation can be reversed the same way.
**Adding Standalone HotPoints to HotView**

If you’re operating your access points as Standalone units and you are using HotView, launch it and check the Manage Standalone APs box in the login screen. If you’re using HotView Pro, just launch it and log in. In either case, your screen will be blank. You will add the APs next.

To add Standalone HotPoints to HotView or HotView Pro, use the **Standalone Access Point Configuration** command under the Access Point menu to add the IP address of each HotPoint to the system, as shown in Screen 124.

**Screen 124. Access Point Menu Commands**

![Access Point Menu](image1)

Enter the IP addresses of each node, and click the **Add** button, as shown in Screen 125. The IP address will appear in the list. When you’ve added all APs, click **Save**.

**Screen 125. Adding HotPoint IP Address to HotView**

![Adding IP Address](image2)

When you’ve finished adding the IP addresses, HotView will automatically discover the APs. Your screen should look like Screen 126. Regardless of whether your nodes are Associated or Standalone, you can now proceed with configuration.

**Screen 126. Access Point Display - Standalone Mode**

![Access Point Display](image3)
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.

Table 23. Summary of AP Node Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename AP</td>
<td>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.</td>
</tr>
<tr>
<td>HotPoint Location</td>
<td>Allows you to assign a location string to the unit.</td>
</tr>
<tr>
<td>IP Settings (includes Management VLAN)</td>
<td>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.</td>
</tr>
<tr>
<td>Release Lock</td>
<td>Releases management control lock on APs. Normally all APs are locked by one instance of HotView; this command allows others to manage the AP.</td>
</tr>
<tr>
<td>View Write Access</td>
<td>When you don’t have write access, this command allows you to see who does.</td>
</tr>
<tr>
<td>Login</td>
<td>The default user ID and password is admin and firetide.</td>
</tr>
<tr>
<td>Apply Policy</td>
<td>Applies a previously-defined policy (for bandwidth, access, etc) to this AP. Note that this command is not available for Model 4100/4200 HotPoints when no WLAN Controller is deployed.</td>
</tr>
<tr>
<td>Statistics</td>
<td>Shows performance for a given VAP.</td>
</tr>
<tr>
<td>Upgrade Firmware</td>
<td>Upgrades firmware. Operation is essentially identical to upgrading HotPort nodes.</td>
</tr>
<tr>
<td>AP Configuration (Radio)</td>
<td>Allows you to specify the radio parameters, firewall configuration, and VPN.</td>
</tr>
<tr>
<td>VAP Configuration</td>
<td>Allows you to define DHCP service for the VAP.</td>
</tr>
<tr>
<td>VAP Group Configuration</td>
<td>Allows you to define radio and security options for a group of Virtual Access Points.</td>
</tr>
<tr>
<td>Access Point Controller Configuration</td>
<td>Allows you to define and access Firetide Mobility Controllers and Firetide WLAN Controllers.</td>
</tr>
<tr>
<td>Country Code</td>
<td>Set once at initial startup.</td>
</tr>
<tr>
<td>Reboot, Reset</td>
<td>Allows you to reboot or reset to factory defaults.</td>
</tr>
<tr>
<td>Move HotPoint</td>
<td>Moves the icon on the screen.</td>
</tr>
<tr>
<td>Import, Apply</td>
<td>Allows you to save and restore node settings.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Forces HotView to re-acquire the status of the AP.</td>
</tr>
<tr>
<td>Refresh Configuration</td>
<td>Gets the config from the AP.</td>
</tr>
<tr>
<td>Summary</td>
<td>Gives a summary of HotPoint node information.</td>
</tr>
</tbody>
</table>
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 in Screen 127.

Basic radio settings are under the AP Setup tab. Proxy ARP and range settings are under the Advanced tab. Setting options for Firewall, VPN, and SNMP are described later in this chapter.

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. Note that the HotPoint 2200 has only a single (built-in) antenna.

HotPoint 4500 and 4600s offer Rogue AP Detection. This enables the AP to detect other, “unknown” APs operating in the area, and report them. You may specify how often the AP stops and scans for rogue APs, as well as the level of search. This features in only available with the HotPoint 4100/4200 family if you are using the WLAN Controller.

Screen 127. AP Radio Settings
Proxy ARP

Proxy ARP (Address Resolution Protocol) is a technique by which a network host answers to the ARP queries for the network address that it does not have configured on the receiving interface. Proxying ARP requests on behalf of another host effectively directs all LAN traffic destined for that host to the proxying host. The “captured” traffic is then typically routed to the destination host via another interface or via a tunnel.

The advantage of Proxy ARP over other networking schemes is simplicity. A network can be extended using this technique without the knowledge of the upstream router. Definition of Proxy ARP can also be a process where a border device (a device connecting between two networks) answers ARP requests on behalf of a remote host.

For example, suppose a host, say A, wants to contact another host B, where B is on a different subnet/broadcast domain than A. For this, host A will send an ARP request with an Destination IP address of B in its ARP packet. The multi-homed router which is connected to both the subnets, responds to host A's request with its MAC address instead of host B's actual MAC address, thus proxying for host B. In the due course of time, when host A sends a packet to the router which is actually destined to host B, the router just forwards the packet to host B. The communication between host A and B is totally unaware of the router proxying for each other. The process which results in the node responding with its own MAC address to an ARP request for a different IP address for proxying purposes is sometimes referred to as ‘publishing’.

Proxy ARP can be enable for each physical AP, as shown in Screen 128.

Range

The range setting does NOT extend the range of the AP. Rather, it alters the timing of packet transmission slightly to allow time for distant clients to receive RF signals. This optimizes the CSMA/CD algorithm and increases throughput by reducing collisions. If you expect to support clients at ranges over one-half mile (0.8 km), adjust this accordingly. When in doubt, set it to a higher range.

Screen 128. Advanced AP Settings
VAP Configuration & VAP Group Configuration

VAPs are virtualized access points. In an enterprise environment, you are likely to have dozens or even hundreds of VAPs spread across the enterprise. To simplify management, Firetide offers VAP Groups. VAP Groups are the collections of Virtual Access Points that form the user-visible ‘logical layer’ overlaid on the physical collection of Access Points.

VAP Groups are offered on the HotPoint 4500/4600 platform, and via the WLAN Controller on the HotPoint 4100/4200. The HotPoint 4100/4200 platform itself does not support VAP Groups.

Because of this difference, the arrangement of VAP Configuration commands and VAP Group Configurations commands varies slightly. The commands and their locations are shown in Table 24.

Table 24. VAP Configuration and VAP Group Configuration Commands

<table>
<thead>
<tr>
<th>Command Tab</th>
<th>Individual Commands</th>
<th>HotPoint 4500/4600 WLAN Controller</th>
<th>HotPoint 4100/4200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Setup</td>
<td>SSID, VLAN, misc</td>
<td>VAP Group</td>
<td>VAP Configuration</td>
</tr>
<tr>
<td>Security</td>
<td>WEP, WPA, AES</td>
<td>VAP Group</td>
<td>VAP Configuration</td>
</tr>
<tr>
<td>Access Control</td>
<td>MAC addresses</td>
<td>VAP Group</td>
<td>VAP Configuration</td>
</tr>
<tr>
<td>Advanced</td>
<td>Intracell, rates, IAPP, WMM</td>
<td>VAP Group</td>
<td>VAP Configuration (no IAPP)</td>
</tr>
<tr>
<td>Network</td>
<td>IP, DHCP, DNS, NAT</td>
<td>VAP Configuration</td>
<td>VAP Configuration</td>
</tr>
<tr>
<td>Radio</td>
<td>multicast rate, power</td>
<td>VAP Configuration</td>
<td>VAP Configuration</td>
</tr>
</tbody>
</table>

The individual command tabs operate in the same manner for all HotPoints; they are just located in slightly different places. This manual will use screen shots based on the assumption that you are configuring HotPoint 4500/4600s. For HotPoint 4100/4200s, all command tabs are located in the VAP Configuration command window.
VAP Group Creation & Editing

When using the HotPoint 4500 or 4600, or any HotPoint in conjunction with the WLAN Controller, you must create at least one VAP Group, with at least one VAP in it. The HotPoint 4100 and 4200 do not support VAP groups without a WLAN Controller.

Do this by selecting **VAP Group Configuration** command from the Access Point menu. You will see the **Manage VAP Groups** screen, as shown in Screen 129.

---

Screen 129. Managing VAP Groups

Click on the **New VAP Group** button. The New VAP Group screen appears, as shown in Screen 130.

---

Screen 130. Creating a New VAP Group

(Note: if there is a default group in existence already, you can use the Edit VAP Group button to remove it altogether.)

Enter a VAP Group Name. This is **NOT** the same as the SSID; it is just the name you will use for management purposes. Select one (or more) APs which will participate in this VAP group. Note that APs can be (and usually are) members of more than one VAP group. Typically, all APs are members of all VAP Groups.

Select a VAP group type. The most common type is ‘client’ - this is the usual mode of operation for most APs - the AP will support standard 802.11 wireless clients.

You can also select CPE as a group type. This is for use with Firetide’s HotClient family of CPE equipment. If you are going to deploy CPEs, you must create at least one CPE-type VAP group.
You can use HotPoint APs to create Wireless Distribution Service (WDS) networks. However, there are two limitations. First, APs which are members of a WDS-enabled VAP Group cannot be members of any other VAP Group.

Second, and more critically, **do not use WDS to bridge two APs which are connected to the same Firetide mesh. This creates a packet loop.** WDS connections between meshes can create loops as well, depending on configuration. If you need a wireless connection between two meshes, use Firetide’s Mesh Bridge configuration.

When you have finished creating VAP groups, your screen should look something like this:

Screen 131. VAP Group Creation - Final

There are two remaining basic setup steps: VAP Configuration and VAP Group Configuration. As discussed previously, the tab location for these commands varies slightly, but command operation is the same. If you are configuring HotPoint 4500/4600, or WLAN Controller, the order in which you do these is not critical; this manual will perform the individual VAP configuration next, and then the VAP Group configuration.
VAP Configuration

VAP Settings

As shown in Screen 132, 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. Some radio settings are VAP-specific, as well.

To modify the VAP 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. The VAP IP address is the one that DHCP clients interact with. You must assign an IP address before enabling DHCP. If desired, configure DHCP service. For DHCP, each VAP Group should have every VAP in that group configured to serve addresses to clients. Each VAP must have a unique range of assignable IP addresses. The DHCP range must be on the same subnet as the VAP IP address.

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. Firetide's WLAN Controller can function as this DHCP server.

NAT may be enabled here, if desired.

Screen 132. VAP Network Settings

Radio power can be configured per VAP. This can be useful in certain applications for minimizing interference and enhancing security.

Screen 133. VAP Radio Settings
VAP Group Settings

You must enable each VAP Group by checking the box. VAP groups can be turned off and on if desired, to limit access to certain times.

The SSID defaults to the VAP Group name, but this can be changed if desired. The SSID can be suppressed if desired for high-security applications.

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.

Screen 134. VAP Group Basic Settings
VAP Group Security Settings

VAP Group security options depend on whether the VAP Group is intended to support general 802.11 clients, or is intended to work exclusively with HotPoint CPE equipment. For general client use, a wide range of wireless security options are supported. Authentication choices include:

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

Begin by selecting an authentication type using the first drop-down menu. The other menus will change to reflect the options available for each method.

Screen 135. VAP Group Security Settings

If you are configuring a CPE-type VAP Group, you must use WPA and Radius. The configuration shown in Screen 136.

Screen 136. Security Setup for CPE-type VAP Groups
MAC Address Access Control

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

Screen 137. VAP Group Access Control Settings
Understanding Advanced Settings

There are a number of advanced settings which allow you to maximize security and optimize traffic loading for various usage scenarios.

Intracell Blocking

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

Note: Intercell blocking is accomplished with VLANs. To implement it, configure a VLAN for each VAP. Refer to the HotView Pro User Guide for details on VLAN configuration.

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 multivendor systems. If you have other APs which support it, you can enable its operation and set the port used for control.

Fast roaming is also supported for clients which support PMKID.

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.

Screen 138. VAP Group Advanced Settings
**AP Group Commands**

HotPoint Access Points can be grouped for management purposes. HotPoint 4500/4600s can be grouped directly; HotPoint 4100/4200s can be grouped when using the WLAN Controller. 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.

**Screen 139. AP Group Management**

**Screen 140. New AP Group**
Advanced Features

Firetide HotPoint APs support several advanced features. These include:

- NAT
- Firewall
- VPN
- SNMP

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.

Screen 141. Enabling NAT

![VAP Configuration Screen](image)
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.

Screen 142. Firewall

![Firewall Configuration Screen]

Backhaul via VPN

The Firetide AP family permits you to backhaul the AP traffic over a VPN. Specify the VPN parameters in this screen.

Screen 143. AP VPN Backhaul

![VPN Backhaul Configuration Screen]

SNMP

APs can be monitored and managed via SNMP. To activate SNMP access, use the SNMP tab in the AP Configuration window.

Copies of the MIBs can be found on the CD, or obtained from Firetide.

Screen 144. Enabling SNMP Management

![SNMP Configuration Screen]
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:

Screen 145. Country Code Warning
Chapter 32 The Firetide WLAN Controller

The Firetide WLAN Controller adds a number of enterprise-class features to the Firetide HotPoint AP product family. The WLAN Controller manages a collection of HotPoint APs. It is an optional system but offers a number of advantages over HotView Pro.

HotView Pro alone allows you to group HotPoints and manage them by groups. Channel assignments and all other parameters are configurable via HotView Pro. The Virtual AP capability of the HotPoint AP is fully exploited by HotView Pro. However, HotView Pro does not automatically and independently manage APs; it is static.

The WLAN Controller offers a number of important capabilities that are especially useful in larger access point deployments. In particular, it does a number of these things automatically.

- **Coverage Analysis** - the Firetide WLAN Controller calculates a coverage map of all APs, and informs you of coverage holes.
- **Channel Assignment** - the Firetide WLAN Controller automatically manages the channel assignments of all HotPoint APs, insuring minimum interference. Because it knows the coverage map, it can pick channels to maximize coverage.
- **DHCP Server** - the WLAN Controller provides AP-wide DHCP address assignment of all 802.11 clients.
- **Radius Authentication** - the WLAN Controller supports Radius authentication for wireless clients. It can use its own built-in Radius server or an external server. The WLAN Controller includes an instance of PostgreSQL to support this.
- **Client Mobility** - the WLAN Controller supports 802.11 client mobility across a collection of standalone HotPoint APs. With the Firetide Mobility Controller providing 802.11 client mobility across integrated HotPoint APs, this makes a complete solution.

The Firetide WLAN Controller also supports client mobility across HotPoint APs. Setup for this is in the Mobility chapter. The Controller includes a Radius server and a PostgreSQL database as well.
The WLAN Controller commands are shown via a right-click on the icon, as in Screen 147.

**Screen 147. WLAN Controller Right-Click**

<table>
<thead>
<tr>
<th>“cmd [234]” Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename Controller...</td>
</tr>
<tr>
<td>Controller Location...</td>
</tr>
<tr>
<td>Controller ID...</td>
</tr>
<tr>
<td>Controller Configurations...</td>
</tr>
<tr>
<td>Controller Management VLAN...</td>
</tr>
<tr>
<td>WLAN Controller Services...</td>
</tr>
<tr>
<td>WLAN Controller VLAN Config</td>
</tr>
<tr>
<td>View HotPoint(s) associated to this Controller</td>
</tr>
<tr>
<td>HotPoint(s) Station History</td>
</tr>
<tr>
<td>Hotpoint Channel Allocation</td>
</tr>
<tr>
<td>Hotpoint Coverage Gap Detection</td>
</tr>
<tr>
<td>Upgrade Controller Software</td>
</tr>
<tr>
<td>Refresh configuration for this Controller ...</td>
</tr>
<tr>
<td>Reboot this Controller ...</td>
</tr>
<tr>
<td>Factory reset this Controller ...</td>
</tr>
<tr>
<td>Backup Configuration from Controller</td>
</tr>
<tr>
<td>Restore Configuration to Controller</td>
</tr>
<tr>
<td>Controller Summary</td>
</tr>
</tbody>
</table>

---

### VLAN Configuration

VLANs should be configured on the Controller so that HotPoint APs on VLANs can reach the Controller. Use the WLAN Controller VLAN Configuration command (and the management VLAN command, if needed), as shown in Screen 148.

**Screen 148. Configuring WLAN Controller VLANs**

![VLAN Configuration Screen](image)
Associated APs

You can view a list of APs under management by a WLAN Controller. Typical results are shown in Screen 149.

Screen 149. List of APs Associated with WLAN Controller

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Serial Number</th>
<th>IP Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>test1</td>
<td>A04165677418650253</td>
<td>192.168.224.253</td>
<td>✔️</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>A04165677418650210</td>
<td>192.168.224.210</td>
<td>✔️</td>
</tr>
<tr>
<td>test2</td>
<td>A04165677418650205</td>
<td>192.168.224.205</td>
<td>✔️</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>F000000000000000000</td>
<td>192.168.224.72</td>
<td>✔️</td>
</tr>
<tr>
<td>test2</td>
<td>F000000000000000000</td>
<td>192.168.224.72</td>
<td>✔️</td>
</tr>
<tr>
<td>test2</td>
<td>A042165677418650224</td>
<td>192.168.224.44</td>
<td>✔️</td>
</tr>
</tbody>
</table>

AP History

The history of clients associated with each AP can also be viewed, as shown in Screen 150. This can be used to track user patterns, adjust coverage and placement, and help detect improper use.

Screen 150. Clients Associated with AP
Channel Allocation

HotPoint Channel Allocation is an automatic process that assigns channels across a collection of HotPoints in order to maximize coverage and minimize interference. To allocate channels, begin by creating a Channel Allocation Group, or CA Group. This is a collection of APs over which the allocation algorithm will run. Add only those APs that are within radio range of each other. You can use the coverage tool to help determine this.

Screen 151. Creating a Channel Allocation Group

(Note: CA groups have nothing to do with the various AP and VAP groups you created for AP management.)

Next, specify the AP Group and channels. You can view results when done.

Screen 152. HotPoint Channel Allocation
**Coverage Gaps**

The WLAN Controller can compute the coverage effectiveness of the HotPoint APs. To do so, select the command and specify the parameters, as shown in the lower left in Screen 153.

**Screen 153. Setup for Calculating WLAN Coverage**
The WLAN Controller offers a range of services for APs and 802.11 clients. These services can be enabled and disabled via the Services control panel, as shown in Screen 154.

**Screen 154. Enabling WLAN Services**

![Services Panel](image)

<table>
<thead>
<tr>
<th>Service</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Running</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Running</td>
</tr>
</tbody>
</table>

Background services are started once and run in the background. On-demand services are started on demand and end when there is nothing more to do.
Chapter 33 Managing Third-Party APs

Access Point Configuration

HotView offers two ways to manage third-party access points which are connected to HotPort nodes. You can manually add an access point to an existing node, using the Access Point command in the Node Command list (right-click the node). This is convenient if you are adding just a few access points. In the window, specify the access IP address or URL, and HotView will allow you to open a browser window that will control the specified access point.

Mobility Support

You don’t need to add third-party access points to HotView Pro, but it does provide a convenient, unified management interface. However, if your mesh supports mobility (that is, mobile users), all access points must be added.

Screen 155. Adding a Third-Party Access Point to HotView Pro

When an access point has been configured, it is shown in the HotView mesh diagram:

Screen 156. HotView Pro Mesh Screen with Third-Party Access Point
The second method is recommended when you are adding a larger number of access points. In this method, the MAC addresses and IP addresses of each access point are entered into HotView. The system then auto-discovers the access points after they are installed.

Begin by using the Access Point menu command to bring up this window, then add the MAC and IP addresses.

**Screen 157. Entering MAC Addresses and IP Addresses for Third-Party APs**

The Auto Discover command can then be used to identify all of the access points once they're installed. A summary list is available:

**Screen 158. Third-Party Auto-Discover Results**
Section VI Managing HotClient CPE Systems

The Firetide Mesh system includes a powerful system for delivering Internet service to clients. The offering is built around Firetide's HotClient family of Customer-Premises Equipment (CPE). These units work with Firetide's HotPoint wireless access points to deliver controllable, billable Internet access to your user community.

You can use Firetide's mesh technology to backhaul the data, or used a wired or fiber infrastructure. In either case, HotClient configuration can be completely automated.

A key advantage of the Firetide system is its flexible ability to define and enforce Service Level Agreements (SLAs). Service Providers can offer guaranteed or best-effort service, and can set maximum data rates per subscriber.

In addition to controlling bandwidth and access priority with SLAs, a Policy Manager lets you define the behaviors to be taken when bandwidth is exceeded or other defined events occur.

**Firetide Access Points**

When HotClient CPEs are used with Firetide's HotPoint AP family, configuration can be automatic, based on a centralized Radius Server. A Radius implementation is included with Firetide's HotView Pro, or you can use an existing Radius server.

Firetide' Automatic Configuration mode means that neither your installers nor your clients need to perform any configuration or setup operations. The HotClient will acquire its configuration automatically from HotView Pro.

In this mode, each HotClient is made known to the system by entering its serial number into HotView Pro prior to deployment. The HotClient, when installed, will power up, find the Firetide AP, and automatically configure itself. Setup for Auto-Configuration is covered in Chapter 34.

**Manual Configuration**

Use of Auto-Configuration is optional. You may, if you wish, manually configure your HotClient units via HotView Pro. This is done my connecting directly to the HotClient (with a cat-5 cable) and setting the configuration parameters. This is described in Chapter 35.

Alternately, either you or your customers can configure the HotClient via a standard web browser. This is described in Chapter 36.

**Non-Firetide Access Points**

HotClient CPEs can also be used with third-party access points. In this mode, configuration is not automatic. You must manually configure each HotClient, as described in Chapter 35 or via a browser as described in Chapter 36.
Chapter 34 HotClient/HotPoint Auto-Configuration Setup

When used together, HotPoint APs and HotClient CPEs support an Auto-Configuration method of deployment. With Auto-Configuration, the HotClient automatically gets its configuration information from a Radius server. This can be the Radius Server included with HotView Pro, or a Radius server you are already running.

If you have not already installed Radius, do so now. Directions can be found in the Appendices.

Access Point Configuration

You should configure and deploy all of your Firetide HotPoint access points before proceeding with HotClient deployment. Firetide HotPoint configuration is covered in detail in other sections of this manual. There is one key step you must perform when configuring HotPoints which will support HotClient devices, and that is to create a VAP group that is explicitly declared as a CPE VAP group, as shown in Screen 159.

**Screen 159. Declaring a VAP Group for CPE**

![Screen 159. Declaring a VAP Group for CPE](image)

**Enabling VAP Groups**

After you’ve created your VAP groups, be sure to enable them, as shown in Screen 160. VAP groups can be enabled and disabled, which provides a quick method of enabling and disabling classes of users or applications.

**Screen 160. Enabling a VAP Group**

![Screen 160. Enabling a VAP Group](image)
When defining your CPE VAP group, you must select AES security, as shown in Screen 161. AES is the only security mode supported by the HotClient family in this Auto Configuration mode.

You must also specify the IP address of the Radius server, so that the HotPoints and HotClients can access it. Note that even though you may have Radius on the same machine that is hosting HotView Pro, you cannot use the local address (127.0.0.1), because the HotPoints and HotClients need the actual IP address of the Radius server.

Screen 161. Configuring AES for CPE VAP Groups
Service Level Agreements

A key feature of the Firetide system is the ability to define multiple Service Level Agreements (SLAs). You can define as many as you want, and then assign users to them.

SLA parameters include upstream and downstream bandwidth limits, and a choice of shared or dedicated access.

You may wish to define one or more SLA configurations now, but it is not required. They can be defined later, and HotClients can be configured with the new SLAs at that time. You can change a HotClient's SLA configuration at any time, and you can also override a HotClient's SLA setting and give it custom settings.

If you wish to specify SLA configurations now, select SLA Definitions from the CPE menu. You will see a screen similar to Screen 162.

Give each SLA a name, then select either Dedicated or Shared access.

Next, select an upstream and a downstream data rate.

Finally, click Add to add the definition to the list.

If you wish to edit an existing definition, click on it and change its settings in the field below.

If you don’t want to configure SLAs now, go to the next page.
Adding HotClients

When you have finished configuring your HotPoint access points to support your HotClient CPE units, you must next add the HotClients to the system. Use the Add HotClient command from the CPE menu. You’ll see a screen similar Screen 163.

Enter the HotClient’s serial number (found on the bottom) and give it a name. You may also enter three fields of identity information. This can be a street address or any other information useful in identifying the unit.

Screen 163. Adding HotClients

![Screen 163: Adding HotClients](image)

When you have finished adding the HotClients, you should see a display similar to the results shown in Screen 164.

Screen 164. Typical Display - HotClients associated with HotPoints.

![Screen 164: Typical Display - HotClients associated with HotPoints](image)
Monitoring HotClient Performance

You can monitor the performance of HotClient nodes with the HotClient Performance screen, accessed via the HotClient Performance tab, as shown in Screen 165.

For best performance, be sure the RSSI (signal strength) is -70 dBm or greater. If it is weaker (i.e., more negative) adjust the HotClient’s antenna or unit placement to improve the signal. If the signal is strong and the data rate is slow, check for interference, which may be caused by other devices operating on the same channel.

Screen 165. Monitoring HotClient Performance
Chapter 35 HotClient Standalone Setup

Specifying Standalone Operation

To use HotClient nodes with third-party access points, you must first add the HotClients to the system, then configure them as 'Pre-Configured' nodes. From the CPE menu, select the Standalone HotClient Configuration option. Adding HotClient nodes to the system is shown in Screen 166.

Enter each HotClient as shown. The default login is admin and the default password is firetide.

Screen 166. Adding Standalone HotClient Configurations

Screen 167. Results of Adding a Standalone HotPoint
When you have finished adding the HotClients, you must specify, for each standalone HotClient, that it is a pre-configured unit. Do this via a right-click on the selected HotClient node, as shown in Screen 168.

**Screen 168. Specifying Pre-Configured Operation for Standalone HotClients**

This will bring up a configuration dialog, as shown in Screen 169.

**Screen 169. Changing the HotClient Configuration Mode**

When you select the Pre-Config option and click Save the HotClient will reboot. This takes about a minute. When the unit is rebooted, you must log into it again.

You must then set the Country Code. (It may already be set.)

You will want to assign a new IP address to each HotClient as you go; you cannot have all HotClients at the default address of 192.168.1.1. To change the IP address, add the node, then right-click on it. Log in, then select LAN settings. Change the node's IP address.
You can then configure the WAN and LAN settings on each HotClient, as shown in Screen 170 and Screen 171. Right-click on the HotClient you’ve just added and select LAN or WAN settings.

**Screen 170. Configuring WAN Settings for a Standalone HotClient**

**Screen 171. Configuring LAN Settings for a Standalone HotClient**
**HotClient Wireless Settings**

You must also configure the radio settings. Right-click on the HotClient you have just added and select Radio settings. You must tell the HotClient the SSID of the AP to which it is to connect. Specify the wireless security as well.

**Screen 172. Specifying Wireless Settings for Standalone HotClient**

There are optional radio settings under the Advanced tab. In most cases you will not need to alter any of these. You may need to change the range setting if the HotClient is more than 800 meters (about 1/2 mile) from the AP. Changing this settings does not increase the range of the radio. It alters the Ethernet timing slightly to reduce the collision rate.

If your AP is a lower-power unit (100 mW/20 dBm units are common) you may wish to reduce the power level of the HotClient to avoid needless interference.

**Screen 173. Optional Wireless Settings for Standalone HotClients**
Other Standalone Settings

The HotClient identifier (name) and other settings can be configured. Right-click on the HotClient you have just added and select HotClient settings.

Use the Identity tab to give the HotClient a name for management purposes. You may also specify up to three lines of additional information. This can be a street address or any other information you wish to display in management screens.

Screen 174. Standalone HotClient Settings - Identity

Use the Administrator tab to change the administrative login settings. You can also restrict or disable entirely the web (http) interface.

Screen 175. Standalone Settings - Administrative Access Controls

If you wish, you may also limit access to the network via MAC address, on the MAC Filters tab.
Chapter 36 HotClient Browser-based Setup

Introduction

You can manually configure HotClient units using a standard browser, such as Firefox. A new (or factory-reset) HotClient has an address of 192.168.224.165. Begin by setting your computer’s IP address to an address in the 192.168.224.x subnet. (Consult the documentation for your OS if you are unsure how to do this.) Connect your computer to the HotClient with an Ethernet cable. (You must use a wired connection to configure the HotClient; it cannot be done wirelessly.

Next, launch your browser and type http://192.168.1.1. You should see a screen similar to Screen 176. Log in, using the name login for the login and password for the password.

Screen 176. Initial Login Page

A successful login will take you to a screen where you can change the operating mode of the HotClient, as shown in Screen 177. When you do this, you will see a warning message, as shown in Screen 178. This is normal. Click through.

Screen 177. Changing the HotClient Operating Mode

Screen 178. Warning Message When Changing the HotClient

Your HotClient will reboot. This will take about a minute. When it is done, you will need to log in again as you did before.
After you have logged in again, select the LAN Settings screen. This screen, shown in Screen 179, allows you to configure the IP addressing system used on the local network supported by the HotClient. The HotClient is capable of performing NAT and functioning as a DHCP Server.

If you are unsure what to enter, use the values shown in Table 25.

### Table 25. Typical HotClient LAN-side Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.1.1</td>
<td>Use this as the default gateway address for all client machines on this network</td>
</tr>
<tr>
<td>IP Mask</td>
<td>255.255.255.0</td>
<td>Up to 254 nodes on this network</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Enable</td>
<td>Set client machines on this network to acquire an address automatically.</td>
</tr>
<tr>
<td>Client Lease</td>
<td>3600</td>
<td>Provides a 1-hour lease. Longer times are permissible; many installations use 14400, which provides a 4-hour lease.</td>
</tr>
<tr>
<td>Start IP Addr</td>
<td>192.168.1.101</td>
<td>This defines the start of the pool of addresses available to clients on this network.</td>
</tr>
<tr>
<td>End IP Addr</td>
<td>192.168.1.31</td>
<td>This defines the end of the range. This example supports up to 63 clients. You may wish to restrict the range to a smaller set.</td>
</tr>
</tbody>
</table>

Note: you can use any LAN address values you wish. Once you change the IP address value, that becomes the new IP address to which you must connect your browser. Thus, if you change it to something other than 192.168.1.1 you will need to log in again. If you change it to a different subnet, you may need to reconfigure your PC’s network settings as well.
CPE Settings

The CPE Basic Settings screen allows you to configure certain management-visible parameters, such as the name of the HotClient node. These settings are for management only, and do not affect HotClient operation.

**Screen 180. CPE Settings**

![CPE Basic Configuration](https://example.com/image1.png)

### CPE Basic Configuration

- **Node Name:** CPE-Pre-config
- **Query String 1:**
- **Query String 2:**
- **Query String 3:**

[Apply]

---

WAN Settings

The WAN Settings screen is where you define the settings that the HotClient will use to connect to your wide-area distribution network.

You must give the HotClient the correct SSID name so that it can find the access point to which it will connect. Make sure the spelling and case are correct; note that spaces are not permitted.

You have the choice of manually assigning an IP address or allowing the HotClient to acquire an address from the ISP's DHCP Server. Note that this setting is independent of whether you choose to have the HotClient function as a DHCP Server on the LAN side.

You can also configure your system’s DNS Server addresses here.

**Screen 181. WAN Settings**

![WAN Configuration](https://example.com/image2.png)

### VAP Configuration

- **VAP SSID:** ISP-name

### VAP Security Configuration

- **Encryption Settings:** Enable Disable
- **Authentication:** WPA2-PSK
- **Cipher:** AES-CCM
- **Key Input Type:** ASCII
- **Key Options:** Passphrase

[Apply]
Wireless Settings

The Wireless Settings page is used to tell the HotClient to which AP it should connect. The VAP SSID value that you enter must exactly match that of the access point which will provide service to the HotClient.

Likewise, you must specify the security settings that the HotClient will need in order to connect to its access point.

Note that there is no radio channel setting. The HotClient will automatically scan for an access point with the SSID value you specified, and connect to it on whatever channel that AP is on.

Screen 182. Wireless Settings

Changing the Default Password

To change the default password, click on the CPE Management tab. Enter the default user name and password, and then enter your new password twice. This is shown in Screen 183.

Screen 183. Changing the Default Password
Glossary

These terms are useful to an understanding of wireless mesh technology in general and Firetide products in particular.

- **802.11** - a family of protocols developed under IEEE guidelines for sending Ethernet packets over radio links. 802.11a, 802.11b, and 802.11g are currently the most widely used.
- **Bandwidth damping** - a speed-limiting effect which can occur in half-duplex networks.
- **dB, or decibel** - the commonly-used measure of power in RF systems.
- **Ethernet Direct** - a wired connection within one mesh. An Ethernet direct connection is visible to the mesh routing algorithm, which considers its capacity and speed when routing packets within a mesh. Thus, Ethernet Direct links increase the capacity of the mesh in which they are contained.
- **Fresnel Zone** - the area surrounding an RF signal that must remain largely free of interfering objects.
- **Full-duplex** - some radio systems support simultaneous transmission and reception.
- **Gateway Group** - a collection of nodes configured to offer multiple egress points from the mesh. When a Gateway Group is used, it is usually also the Head Node, but this is not required.
- **Half-duplex** - many radio systems can either transmit or receive, but cannot do both at the same time. Thus in a group of nodes all within radio range of each other, at any given time only one node can be transmitting.
- **Head Node** - the node on the mesh which is logically closest to the NMS. Typically this is the node which is plugged into the enterprise backbone, and from there to the NMS system.
- **Integrated AP** - A Firetide HotPoint Access Point that is connected to a Firetide mesh node.
- **Interoperability** - in the Firetide context, use of Series 6000 nodes and Series 3000 nodes in the same mesh.
- **Link** - a connection between two nodes within a single mesh. Also known as a path. Links are generally wireless RF connections, but can be wired connections in some cases. (See Ethernet Direct.) The key point is that the connection is between two nodes within the same mesh; that is, within the same mesh-routing domain.
- **Mesh Bridge** - a wired connection between two distinct meshes. The meshes can be near each other, or even physically overlapping if they are logically isolated. They can also be arbitrarily far apart. Because a Mesh Bridge connection is between two meshes, it is not part of any mesh-routing algorithm.
- **Mobile node** - a Firetide mesh node installed in a vehicle or any other place where it moves relative to the other nodes.
- **Multipath** - the condition where a radio receiver receives two versions of the same signal, because one signal took a more direct path and the other signal a reflected path.
- **Network Management System (NMS)** - another name for HotView or HotView Pro, the system for configuring and monitoring network behavior. Note that the NMS is NOT required for network operation; only for initial configuration.
- **Node** - one of the elements of a mesh. It has one or more radios, and a CPU which implements the packet-switching algorithm. Nodes also offer wired-Ethernet ports as entry points to the wireless mesh.
- **QoS/Class of Service** - mechanism used to insure that time-critical traffic (e.g. VoIP) gets delivered promptly
- **Roaming** - the ability to support 802.11 clients as they move from access point to access point.
End of Volume 3 of the HotView Pro Reference Guide