HotView Pro Version 10.17.0.0 & HotPoint Product Manual

HotView Pro® manages these Firetide products:

- HotPort™ 7010/7020 mesh nodes
- HotPort™ 7010-900/7020-900 mesh nodes
- HotPort™ 7100-FIPS/7200-FIPS mesh nodes
- FMC-2000
- HotPort™ 5020-M mesh nodes
- HotPort™ 5020-E/LNK nodes
- HotPoint™ 5100/5200 access points

Published March 2015
(Revised in 2016)

Firetide, Inc.

2105 S. Bascom Avenue, Suite 220
Campbell, CA 95008
USA

www.firetide.com

About this document

This section lists the audience, purpose, summary of information, and conventions used in this document.

Audience

This document is intended for qualified installers and administrators of Firetide products.

Purpose

This document has the information necessary to install, configure, troubleshoot, and maintain HotView Pro network management software in networks that use HotPort 7010/7020, FMC-2000, HotPort 5020 nodes, and HotPoint 5100/5200 access points. HotView Pro also manages HotPort 5020-LNK solutions.

Summary of information

This document contains information about HotView Pro Version 10.17.0.0. The next table lists the chapter names and summaries.

Section	Chapter name	Summary
HotView Pro software	HotView Pro introduction	Lists HotView Pro software features and benefits
	HotView Pro software installation	Lists the system and environmental requirements, third party software installation procedures, and installation procedure
	Hot View Pro server configuration	Contains information about HotView Pro Server and the procedures to configure the server
	Configuration of the network monitor server	Contains information about HotView Pro Monitor and the procedures to configure the monitor features
	Mesh node security	Contains information about radio and network security

Section	Chapter name	Summary
	Performance tools	Contains information and procedures for improving the performance of your network
	Network tasks	Contains upgrade procedures and gateway group procedures
	Ethernet Direct	Contains the procedures for setting up Ethernet Direct
	Transfer of licenses	Explains licensing requirements
	Client preferences	Contains information about how to customize the HotView Pro workspace
	Troubleshooting HotView Pro software and mesh issues	Lists problems and suggested solutions
HotPort mesh node configuration	Mesh-wide node configuration	Contains the procedures to configure HotPort mesh nodes
	Mesh node-specific settings	Contains HotPort mesh node-specific settings and feature information
	HotPort 5020-M Mesh node-specific settings	Contains feature information pertinent to the HotPort 5020-M mesh node
	5020-E settings	Contains HotPort 5020-E configuration information
Firetide Mobility	Mobile network solutions	Contains the procedures for administrative tasks, such as creating administrative accounts
Access point configuration	Initial access point configuration with HotView Pro	Contains the procedure for an initial software configuration and log in and access point load procedures
	Wireless LAN configuration	Contains the procedures to configure virtual access points (VAPs)
	Authentication and captive portal configuration	Contains the procedures for set up internal and RADIUS authentication and for custom portals
	Access point management	Contains the procedures related to access point (AP) groups
	Wireless feature configuration	Contains procedures and information related to wireless features to enhance user experience, manage resources, and satisfy special network requirements
	Wireless distribution stations	Contains the procedure for configuring a wireless distribution station (WDS) system

Section	Chapter name	Summary
	Monitoring and reporting with HotView Pro	Contains information that can be viewed, exported, or printed
	SNMP with HotPoint access points	Contains HotView Pro procedures related to SNMP integration
	HotPoint access point MIB list	Contains Firetide MIB names and descriptions
	Licenses	Contains information about required licenses for access point management and a procedure for using a field laptop without a HotView Pro management license
	HotPoint messages	Contains HotPoint access points messages
	Upgrade by script	Contains the procedures to use the Firetide AP FW Upgrade Utility
	Configuration with the web interface	Contains access point configuration procedures using the integrated web (HTTP) interface
Appendix	Worldwide default radio assignments	List radio defaults by country

Conventions

Certain information has special meaning for the reader. This information appears with an icon that indicates a particular condition, such as a warning or caution, or a label, such as “Note” or “Best Practice”.

Electrical hazards are those environments where the danger of electrocution is probable. This image appears before each electrical hazard statement.

Warnings contain safety information that you must obey. If you do not obey the instruction in a warning, the result might include serious injury or death. This image appears before each warning statement.

Cautions contain information that you should obey to avoid minor injury, inconvenience, and damage to equipment. This image appears before each caution statement.

Notes contain optional advice and information particular to a special case or application.

Best practices contain specific recommendations based on industry-standard expectations.

Document feedback

If you find an error or content missing from this document, we want to hear about it. You can send your feedback about any of our documents to techpubs@firetide.com.

Contacting customer support

If you need support, depending on the problem, you might be asked for this information:

- Description of the problem
- Computer with HotView Pro and an installed management license
- Channel and frequency plans
- Recent spectrum analysis
- Device topology in Google Earth (KMZ file)
- Network map or topology plan with the names and device information

A support case may be opened from http://www.Firetide.com/supportrequest following completion of the online form. To reach support by phone:

Worldwide customer support	Days/Hours	Contact
Americas	Monday to Friday 7:00 am to 5:30 pm PST (Pacific standard time)	http://www.firetide.com/requestsupport (877) FIRETIDE, extension 2 (408) 399-7771, extension 2 (408) 355-7271
Africa Asia Australia Europe	Monday to Friday 8:00 am to 5:30 pm IST (India standard time)	http://www.firetide.com/requestsupport +918040215111 Fax +1(408) 317-2257

Contents

HotView Pro software

This section contains these chapters:

- HotView Pro introduction
- HotView Pro software installation
- Hot View Pro server configuration
- Native SNMP configuration and use
- Configuration of the network monitor server
- Mesh node security
- Performance tools
- Network tasks
- Ethernet Direct
- Transfer of licenses
- Client preferences
- Troubleshooting HotView Pro software and mesh issues

HotView Pro introduction

HotView Pro is a centralized, network management software. It is a platform from which you can configure, monitor, and manage HotPort® mesh nodes and HotPoint® access points.

This version of HotView Pro supports networks that have these hardware platforms:

- HotPort 7010/7020 mesh nodes
- HotPort 5020 nodes

Note: HotPort 5020-LNK can be managed with HotView Pro.

- HotPoint 5100/5200 access points

Optimal network performance

HotView Pro software uses these features to support high throughput and low latency of voice, video, and data communications:

- Unique flow control mechanism to balance link-specific traffic loads and class-of-service priorities. With flow-based routing, the system balances traffic across the mesh to best optimize aggregate throughput and increase network performance.
- Traffic priority options and management capabilities.
- Bandwidth metrics to improve overall throughput for the best transmission paths based on link capacity, type, hop count, and retransmission count.

Network performance can be refined in crowded environments by manually removing redundant links from the mesh.

Management features

HotView Pro uses traditional client/server design. The server uses a database to store and export:

- Mesh and node configurations
- Operating statistics
- Fault and event logs
- Administrator access privileges and user preferences.

The client and server functions operate across a LAN or WAN, or can be collocated on a single platform.

Managing multiple mesh networks

Each local or remote HotView Pro client is capable of managing one or more HotPort mesh networks from a single screen. Real-time monitoring shows a graphical view of active connections in the mesh topology, and statistics and logs. You can insert a custom background image, such as a floor plan, map or drawing, to show the physical location of all nodes in the mesh. You can view multiple or individual meshes.

Multi-user management

HotView Pro lets multiple administrators have different management capabilities. To support good change management practices, however, only one user at a time has read and write capability for a mesh. HotView Pro also includes a default ID lockout feature that lets you change default user IDs to avoid brute-force attacks.

SNMP management

SNMP management lets network administrators customize and integrate management of individual or multiple HotPort mesh networks with a network management system, such as HP OpenView or IBM NetView.

Web-based client

The HotView web server feature enables network managers to use a web browser to connect to the HotView Pro Server.

Real-time management

HotView Pro has visual information of one or more wireless networks. The information includes:

- Network status
- Performance statistics
- Current/logged faults

Note: Statistics and log files can be exported for later analysis.

- Real-time inventory of all HotPort mesh nodes and HotPoint access points
- Scalable and secure software upgrades and updates

Note: Certificate-based firmware upgrades force devices to accept upgrades only from digitally signed sources.

- Different segment views of the network

Access features

HotView Pro network management software provides performance and statistics monitoring for HotPoint products. Access points can be connected to HotPort mesh nodes or directly to a wired infrastructure.

HotView Pro software installation

This chapter contains information to help you avoid problems when you install HotView Pro and contains the steps to install HotView Pro and apply license keys.

Installation options

You can choose to install HotView Pro or HotView Pro with HTTP.

Installation location

The HotView Pro software and licensing is intended to be installed on a specific system, and management via this software should be done from this system or another system that has network connectivity to this original device. If the original system with the Firetide software and licensing is no longer available, the software and licensing can be moved to a different device, but this transition will require assistance from Firetide Technical Support.

It is the customer's responsibility to maintain and secure license key information, since Firetide sells directly to the distributor and does not record integrator or end-user information. Applying Management directly to the mesh nodes is one way of accessing a mesh network from a non-licensed system. However, all nodes will require a Management license be installed and applying a Management license to a node does deplete the HotView Pro Management license count.

Ports that HotView Pro software uses

If there are firewalls between the various elements of the network, certain ports must be open. The next table lists the TCP ports that Firetide products use.

HotView Client to HotView Pro Server	Device ports
1921 to 1930	32000
6666	6610
—	6613

Table 1

Caution! If you change the JBOSS default port from 80 to another port, you must ensure that the port is reachable and is not blocked by a firewall.

Hardware requirements

The next table lists the minimum hardware requirements of the server.

Component	Minimum requirement
Operating system	• Windows® 8 Professional (32 and 64 Bit)/7 Professional (32 and 64 Bit)/ Vista, XP Professional SP2, Windows Server 2008 and 2012 Standard R2 (64 Bit), • Fedora FC 17 (32 Bit)
CPU	Intel i3 Dual Core or higher
RAM	4GB or more
Storage	250GB or more disk space
Network connection	10/100/1 Gig RJ45 Ethernet
Other	• (Optional) UPS back up • (Optional) Redundant power supplies • (Optional) One or more RAID arrays

Table 2

Client computers need to have a supported browser, such as Internet Explorer, Mozilla Firefox, or Google Chrome.

Software requirements

Refer to the following OS and Java compatibility table.

Operating System	Java Version (32 Bit)	DB version
Windows 7 Professional (32 Bit)	Java 1.7 update 14, 51, 60, and 67	PostgreSQL 9.1, PostgreSQL9.2 PostgreSQL9.3
Windows 7 (64 Bit)	Java 1.6 update 34 Java 1.7 update 45, 147 Java 1.8 update 25	PostgreSQL9.4
Windows 8 Professional (64 Bit)	Java 1.7 update 71	PostgreSQL9.2
Windows Server 2008 (64 Bit)	Java 1.7 update 21	PostgreSQL9.2
Windows Server 2012 (64 Bit)	Java 1.8 update 25	PostgreSQL9.2
Fedora 17 (32 Bit)	Java 1.8 update 25	PostgreSQL9.2

Table 3

Make sure you have a 32-bit version of Java 7 or 8 installed on the server. For a copy of Java 7 or 8, visit www.java.com.

Caution! If you use another version of Java, you might experience unpredictable results.

Caution! HotView Pro is not supported in virtual environments. If you run HotView Pro in a virtual environment you void your product warranty.

To be able to use all HotView Pro features, you must install the database software. Install the database support software before you install the HotView Pro software. By default, the HotView Pro software does not detect the database.

HotView Pro uses the PostgreSQL database for long-term storage of performance data. Firetide supplies a database schema.

Installing the PostgreSQL database

Prerequisites:

- Server that meets the software requirements. See "Software requirements".
- Database software (in the software package). If you do not have access to the database software, we recommend that you download a copy of PostgreSQL version 9.x from http://www.postgresql.org/download/windows (See Table 3 above)
- You are the Administrator or have Administrative rights to the system to which you are installing this software.

To install the PostgreSQL software:

1. Double-click the application file.
2. Specify the location for the program or accept the default location, and then click **Next**.
3. Specify the location for the data files, which can be a drive on the network, and then click **Next**.
4. Specify a password, and then click **Next**. This is the authentication password used by HotView Pro to access the database.

   Best practice: Use a unique password.
5. Click **Next** to accept the default network access port setting (Port 5432).
6. Select the language support, and then click **Next**.
7. Remove the check from Stack Builder application.
8. Click **Finish**.

For HotView to work with a remote server, you need to edit pg_hba.conf and postgresql.conf.

If HotView is on the same server as the database software, the process is complete.

Editing PostgreSQL configuration files

If you want the database to reside on a remote server (separate from where HotView Pro is installed), you need to point to the remote server location.

Prerequisite: PostgreSQL software is installed on the server.

To edit the PostgreSQL configuration files:

1. Browse to the PostgreSQL folder, click on PostgreSQL version (specific version of PostgreSQL installed), and open the data folder.
2. In a text editor, such as Notepad, open pg_hba.conf

3. Modify the file (pg_hba.conf).
    a. Search for"IPv4 local"
    b. Change the encryption type from md5 to password. For example: "host all all 127.0.0.1/32 md5" to "host all all 127.0.0.1/32 password"
    c. Save the file.
4. Open postgresql.conf
5. Modify the file (postgresql.conf).
    a. Change #ssl = off to ssl = off
    b. Change #default_with_oids = off to default_with_oids = off
    c. Save the file.
6. Run the SQL script to build the database.
7. Expand the database, schema, and public structures.
8. Click **Execute Arbitrary SQL Query**.
9. Select **File > Open** and navigate to the Firetide installation directory.
10. Expand folders until you can select the nmspro_create file.
11. On the Query screen, click the green arrow to do the query.

Setting up the database

Prerequisite: PostgreSQL configuration files are modified.

To set up the database:

1. Select the database you just created (for example, FiretideDB).
2. Click **Refresh Object**.
   Database setup is complete.

Installing HotView Pro software

Prerequisites for a test environment:

- Server that meets the software requirements
- Correct version of Java installed on the server
- (Optional) database software installed on the server

Prerequisites for a production environment:

- Server that meets the software requirements
- Correct version of Java installed on the server
- Database software installed on the server

To install HotView Pro software:

1. Download the executable software file.
2. If you want to install HotView Pro with HTTP, download jdk and jboss.
3. Double-click the file to run it.

4. Click through the installation wizard to:
   - Make a language selection
   - Select the location of the installation
   - Select the installation option (HotView Pro or HotView Pro with HTTP)
   - Enter selections and paths to third party software.
   - Review your selections.
5. Click **Install**.

   The installation takes two to three minutes.
6. Click **Done** to exit the wizard.

If the installation process does not finish, see "Troubleshooting HotView Pro software and mesh issues" on page 90.

Next steps: Install the licenses, and then enable the databases.

Using HotView Pro launcher to access applications

After you install the software, you have to configure the HotView Pro server. Double-click the HotView Launcher icon.

From the launch screen you can open specific applications, such as the client application, server application, or both (quick launch).

Single-click the item to launch the software.

Caution! Double-clicking launches the program two times and causes an error.

The next table lists the items on the HotView Pro launch screen and when to use them.

Item	Action and use
Quick Launch 	Action: Launches the server application and the client application at the same time. When the client application closes, the server application also stops. Use: For tests and to debug. **Note:** Do not use in a production environment.
Server 	Action: Launches the server application. It runs until it is manually stopped. If the LED is red, the server is not running; if it is green, the server is running. Use: For production environments.

Item	Action and use
Client 	Action: Launches the client application. Use: For production environments.
Server Configuration 	Action: Launches the Server configuration functionality. Use: For initial server setup and to manage users and system-wide settings.

Table 4

License registration

The HotView Pro Server operates with licenses. Each license applies to one server.

You can purchase licenses for the following purposes:

- Management

  You can enter an alphabetic key to create a temporary license. The system lets you configure some items while you request a permanent license. If you do not get a permanent license key the software stops working after 30 days.

- Mobility

  A mobility license is required when one or more nodes travel within a mesh.

Note: For mobility across multiple meshes additional hardware and software configuration are required.

- Dual radio

  If your Firetide product has a second radio, you must activate it through software with a license key.

- Wireless-n

  802.11n (MIMO) operation is also activated through software and a license key.

Note: Without a permanent dual radio license you cannot configure the second radio.

Note: During a new installation, several warning messages appear during the configuration process.

1. From the HotView Launcher, click the Server Configuration icon.
2. At the login prompt enter the default user name and password:

   Database user name: hv_admin

   Database password: firetide
3. When a warning message to inform you that the server cannot be reached appears, click **Yes**.
4. When a warning message to inform you that the database cannot be reached appears, click **Yes**.
5. When a warning message to inform you that there is no valid license appears, click **OK**.

Entering a temporary license key

Prerequisite: Temporary license key for each license you need.

Repeat these steps until you enter all of the licenses that your network requires.

To enter a temporary license key:

1. Enter the license key you were given. The license key is not case-sensitive.
2. Click **Add License Key**. The key you entered appears in the list.
3. Click **EULA**, and read the end user license agreement (EULA).
4. Close the window.
5. Check the check box to accept the agreement.
6. Click **Activate License**.
7. Add another next license if necessary.

Requesting a permanent license key

A temporary license is good for 30 days. When a temporary license expires, you cannot use the software. You must request a permanent license.

Prerequisite: temporary license key

Best practice: Enter all license keys, enter the information in the License To tab, and then generate the request for a permanent license key.

To request a permanent license key:

1. Select the temporary license for which you want to request a permanent license. (Optional) Check **Apply Online** to use the online method or requesting a key.

Note: Apply online option can only be used for new licenses, not re-issues.

2. Click the Licensed To tab.
   a. Enter all of the account's contact information.
   b. Click **Save**.
3. Click **Request Permanent License**.
4. After you have all of the key requests, make an email request and attach all of the key requests to the same email.

5. Send the email to licensing@firetide.com

Caution! You must save the License To information. If this information is not saved, you cannot import your permanent license.

6. Click **Save**.

Permanent license key failure

If you select to apply for a permanent license key by Internet (online), the request for permanent license button starts the license request process. If an SMTP server is running on your HotView Pro server, the system sends an e-mail request automatically.

If the system cannot send the license request because SMTP is not available, choose the appropriate option when prompted. Select **No**.

If you accidentally select **Yes**, an error message will appear. Save the generated file to the system, and then send it by e-mail.

Installing a permanent license key

Prerequisite: Permanent license key from Firetide

To install a permanent license key:

1. Copy the file to your desktop.

Go to **Server Administration > Configure HotView Server > Licensing > License Information** tab

2. Select the license that you want to make permanent, and then select **Import Permanent License**.
3. Browse to the file and then click **Open**.

Viewing the licensee

You cannot make changes to the licensee information, but you can view it.

To view the licensee information:

1. Launch HotView Pro or HotView Pro Server Configuration.
2. Click **Licensing > Licensed To** tab.

Enabling the databases

The database feature is disabled by default.

Note: Enable the databases after you enter the licenses.

Note: When the server cannot reach the databases and when the databases are not configured, the system sends logged in users warning messages.

To enable the PostgreSQL database:

1. Select **Use Database**.
2. Click **Apply**.

Field access without a management license

When you set up a new mesh, you have the option of pushing a management license to each node. Pushing a management license to each node will allow one to manage the mesh nodes from a system that does not have a management license. For instructions on how to push the management license, see page 83. The following paragraph describes the process after you have pushed the management license to the nodes.

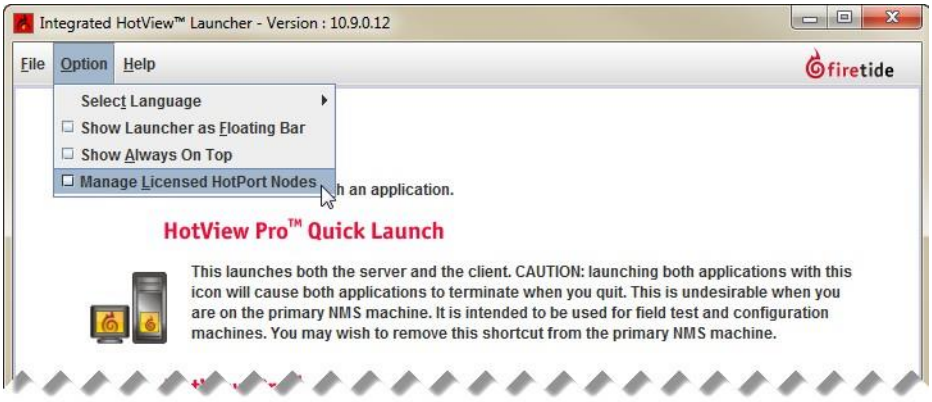
Using HotView Pro without a license key

Caution! You need to apply a management license to all nodes in a mesh. If one of the nodes in a mesh does not have a management license, then the system sends an error message and prevents access to all nodes in the mesh.

To use HotView Pro without a license key after the management license key is assigned to the appropriate set of mesh nodes:

1. Install HotView Pro on a system that does or does not have a temporary or a permanent license.
2. Start the HotView Pro Launcher, and then select the Server Configuration icon.

3. Accept the prompts to access the Server Configuration, and remove the check from Use Database and Use Database for Radius.
4. Click **Save**.
5. From the HotView Pro Launcher, go to **Options > Manage Licensed HotPort Nodes**



You can now log into and manage the mesh from a different computer.

Software upgrade and downgrade considerations

If you have an existing mesh and want to upgrade to HotView Pro 10.17.0.0:

- Carefully evaluate the feature set for your needs.
- Make sure that the HotPort 6000 node interoperability feature set meets your needs.
- Make sure that any HotPort 7000 mesh nodes are configured to use channels available in the release to which you want to upgrade. Refer to the release notes for the supported channels list.

Caution! Refer to the 10.17.0.0 release notes, located at http://www.firetide.com/support/support-resources for details in regards to upgrade and downgrade considerations.

HotView Pro server configuration

This section contains server configuration information. You do not have to start the server to configure it.

The next table lists the HotView Pro server configuration choices and tasks.

Menu item	Tasks
Database Management	Lets you configure authentication for a database • Configure a database name, host name, username, password • Clean (delete) log files • Delete "older than" statistics
Network Management	Lets you configure the Mesh, AP Group, and Firetide Mobility Controller network ID and login information
Service Manager	Lets you stop and start the HotView server, the SNMP agent and monitor server
HotView Management	Lets you configure HotView users, Windows services, SNMP, Upgrade, Logs, syslog, NTP, and Network monitor server
Licensing	Lets you enter your License To information, add a license key, access the Firetide privacy policy and FAQs, import a permanent license and request a permanent license
Alarm Management	Lets you configure an SMTP server, define alarms, severity, and actions
Security	Lets you configure high or low security
Network Monitor ACL	Lets you set the security level for the network monitor server

Table 5

Server management and firmware configuration options include:

- "Accessing HotView Pro server" on page 19
- "Starting HotView Pro server" on page 19
- "Stopping HotView Pro server" on page 19
- "Stopping the server manager" on page 20

Other configuration options include:

Accessing HotView Pro server

To access the HotView Pro server:

1. Start HotView Pro.
2. Go to **Server Administration > Configure HotView Server**

Note: Use the shortcut icon from the Quick Launch software. Single mouse-click on the icon that has a nut, screw, and server.

Starting HotView Pro server

To start the HotView Pro Server:

1. Click the HotView Pro shortcut **> Server Configuration > Configure HotView Server > Service Manager**
2. Click **Start HotView Server**.

Stopping HotView Pro server

To stop the HotView Pro server:

1. Go to **Server Administration > Configure HotView Server > Service Manager**
2. Click **Stop HotView Server**.
3. Click **Apply**, and then click **Save**.

Stopping the server manager

To stop the server manager:

1. Go to **Server Administration > Configure HotView Server > Service Manager**
2. Click **Stop HotView Server**.
3. Click **Apply**, and then click **Save**.

Starting the server manager

To start the server manager:

1. Go to **Server Administration > Configure HotView Server > Service Manager**
2. In the HotView Pro Server Manager section, click **Start HotView Server**.
3. Click **Apply**, and then click **Save**.

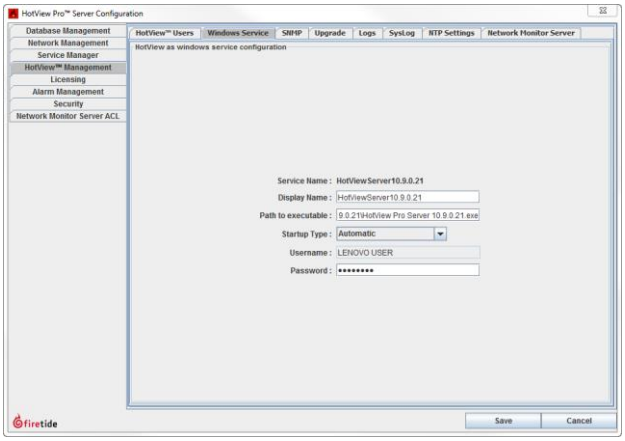
Configuring HotView Pro as a Windows Service

A Windows Service Application can run for a long time and does not interfere with someone who uses the computer for other tasks. You can also run the service application under a different user account than the account of the person who regularly uses the computer. For more information, refer to the MSDN Library. You must make Windows configuration changes and HotView configuration changes for this feature to work.

Note: The Linux version of HotView Pro does not support this feature.

To enable HotView Pro to run as a Windows Service Application:

1. Go to **Server Administration > HotView Management > Windows Service**
2. Enter the name you want to appear (display name).
3. Select the startup type: automatic, manual, or disabled.
4. Enter the user name and password.
5. Click **Save.**



Changing the chunk size and retry count for a firmware upgrade

Mesh nodes receive firmware upgrades over a wireless connection, which consumes bandwidth. When a mesh is heavily loaded or bandwidth is limited, you can configure smaller chunk sizes to be sent to each node. Small chunks increase the time required for an upgrade, but they reduce the impact on mesh traffic in a production environment.

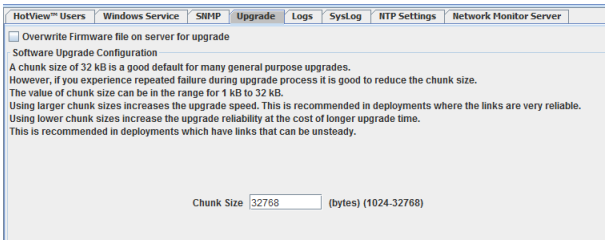
The default chunk size in bytes is 32768. The range of acceptable values is 1024 to 32768.

Note: In environments with high levels of interference, Firetide recommends smaller chunk sizes. Smaller chunk sizes reduce sensitivity to interference.

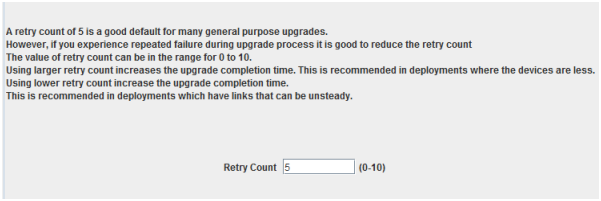
You can also enter the number of retry attempts during a firmware upgrade. The default number of retries is 5. If you experience upgrade failures, reduce the retry count. The range of acceptable values is 0 to 10.

To change the upgrade chunk size and retry count:

1. Go to **Server Administration > Configure HotView Server >** Select the **Upgrade** tab
2. Enter a chunk size in bytes.



3. Enter a retry count number: 0 to 10 (5 is the default value).



4. Click **Save**.

Enabling the overwrite firmware file option

If you enable "Overwrite Firmware file on server for upgrade," the system overwrites the firmware saved in cache with each upgrade. By default, the system uses the firmware image in cache for multiple upgrades.

To enable the overwrite firmware file option:

1. Go to **Server Administration > Configure HotView Server >** Select the **Upgrade** tab
2. Make a check the "Overwrite Firmware file on server for upgrade" box.
3. Click **Save**.

SNMP and alarm configuration

The HotView Pro system can send messages when trigger events occur to give you information about the health of the network. The system has SNMP and SMTP features.

If you want to use an SNMP management software without a HotView Pro server, see"Native SNMP configuration and use" on page 38.

SNMP support

The system supports SNMP versions 1, 2, and 3. To use SNMP you need to start and then configure the SNMP agent manager.

Note: SNMP management from HotView Pro is not available for these products:
- HotPort 5020-E
- HotPort 5020-LNK

SNMP agent manager tasks include:

- "Starting the SNMP agent manager" on page 25
- "Stopping the SNMP agent manager" on page 25
- "Configuring the SNMP agent manager" on page 25

SMTP support

SMTP is a way to receive email notifications of log events. When several events happen in a 10 second period, HotView Pro puts all of the events in one email.

If the database is configured to work with HotView Pro, the system uses the database to keep the alarm history. If no database is configured, save a local file on the HotView Pro server. Alarm history can be kept for trend analysis of individual node performance.

For the alarm management feature to work:

1. Set up an SMTP server in your network. See "Configuring an SMTP server in HotView Pro" on page 26.
2. Set up a HotView Pro SMTP server entry.

3. Configure the alarms in HotView Pro. See “Adding an alarm” on page 27.

Alarm severity levels

HotView Pro has these alarm levels:

- Critical: This event affects service. The system requires immediate action.
- Major: An error occurred and will require attention.
- Minor: This event might be an error.
- Informational: This is an expected event. No action is required.
- Custom: An administrator can create their own levels.

By default HotView Pro has a default assignment of alarm types and level, but you can change the alarm severity level.

Alarm types

The next table lists the pre-configured alarm types and events.

Alarm Type	Event
Access Point	HotPoint Down
	HotPoint Up
	Station Association
	Station Disassociation
FMC	FMC Down
	FMC Up
	Mesh Down
	Mesh Up
	Mobile Node Authentication Fail
	Mobile Node Authentication Success
	Mobile Node Down
	Mobile Node Roam
	Mobile Node Up
	Standby FMC Down
	Standby FMC Up
	Static Node Down
	Static Node Up

Alarm Type	Event
Mesh	Bridge Link Down
	Bridge Link Up
	Faults (Port Up/Down)
	HotPort Link Up
	HotPort Node Down
	HotPort Node Up
PTP	Faults (Port Up/Down)
	HotPort Link Up
	HotPort Node Down
	HotPort Node Up

Table 6

Alarm identifier

You can select an alarm identifier on a node or device type basis, such as all access points, or on a per device basis by serial number.

Alarm actions

When an event happens, you can configure HotView Pro to do different actions for each alarm. For example, for critical alarms, you can configure HotView Pro to immediately send you or other administrators email messages.

The next table lists the actions HotView Pro supports and a description of each action.

Action	Description
Alert sound	By default, the HotView Pro server machine makes the sound. You can enable client machines to make a sound when you select the check box **Enable alerting at HotView Client**.
Execute a system command	You can configure the system to run a Linux shell command. For example, you might want to run a script every time a link breaks.

Action	Description
Send an email	The system immediately sends a custom email message. The message can be different for each alarm.
Do nothing	This action tells the system to record the event for later.
Ignore	This action tells the system to not keep information about this event.

Table 7

Starting the SNMP agent manager

To start the SNMP agent manager:

1. Go to **Server Administration > Configure HotView Server > Service Manager**
2. In the SNMP Agent Manager section, click **Start SNMP Agent**.

Stopping the SNMP agent manager

To stop the SNMP agent manager:

1. Go to **Server Administration > Configure HotView Server > Service Manager**
2. In the SNMP Agent Manager section, click **Stop SNMP Agent**.

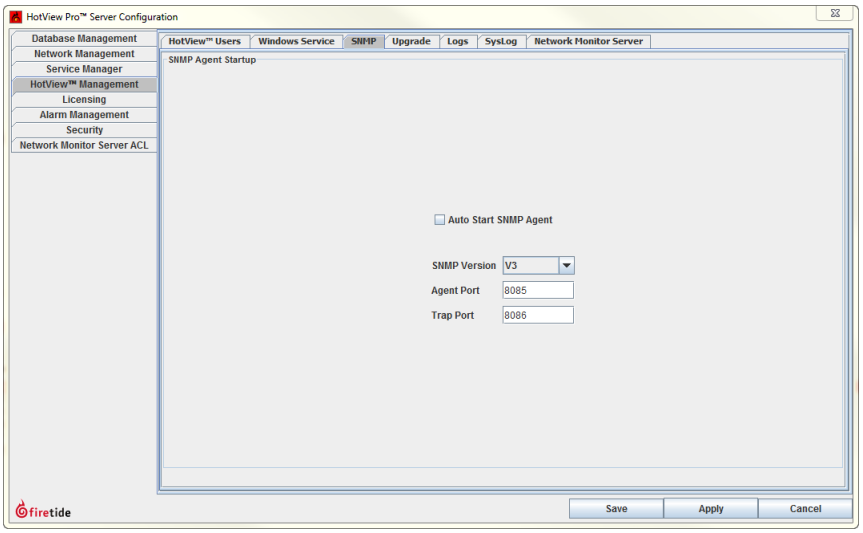
Configuring the SNMP agent manager

You need to set the SNMP version (v1, v2, or v3), agent port, and trap port. Optionally, you can choose to have the system auto start the SNMP agent. By default, the SNMP Agent does not start automatically. The agent port is set to 2000 by default. If you need to change this setting, open the server configuration, select HotView management option and in the SNMP tab, provide the SNMP startup information:

Click on the **Auto Start SNMP Agent** checkbox, select SNMP version and type in the port value of your choice-- between 1 and 65535 (see instructions below).

Prerequisite: You must enable the SNMP agent manager.

1. Go to **Server Administration > Configure HotView Server > HotView Management>SNMP** tab
2. Make these changes:
   - (Optionally) Select **Auto Start SNMP Agent**.
   - Select the SNMP version.
   - Enter an agent port.
   - Enter the trap port.
3. Click **Save**.

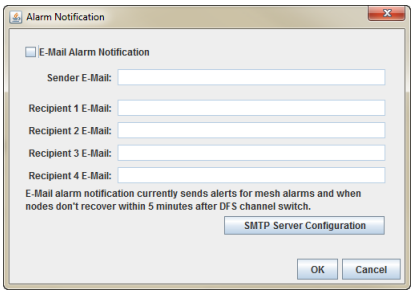


Configuring an SMTP server in HotView Pro

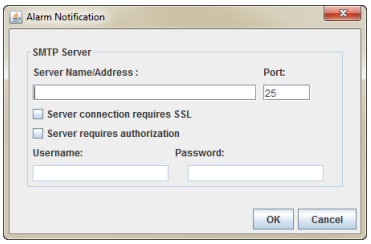
To use the alarm management features, you have to configure the SMTP server within HotView Pro.

To configure an SMTP server:

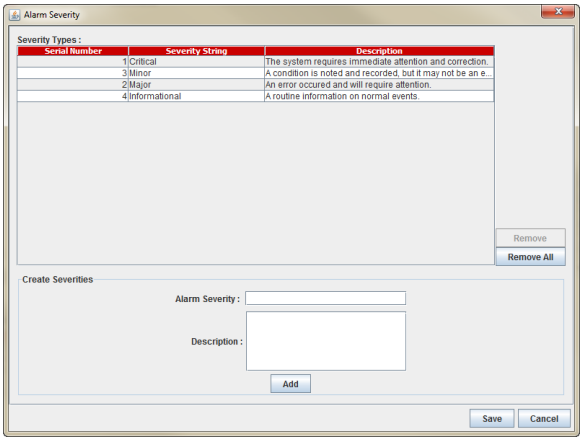
1. Go to **Server Administration > Configure HotView Server > Alarm Management**
2. Click **Configure SMTP Server**.
   a. (Optional) Click email notification box, and then enter the email for the sender and up to four recipients.



   b. Click **SMTP Server Configuration**.
   c. Enter the server name/IPv4 address and port number.
   d. (Optional) Select Server connection requires SSL.
   e. (Optional) Select Server requires authorization.
   f. Enter the user name and password.



3. Configure alarm severity levels.



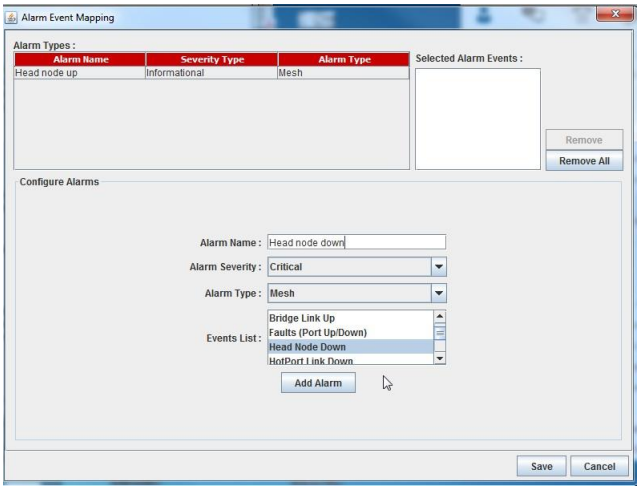
4. Click **Save**.

Adding an alarm

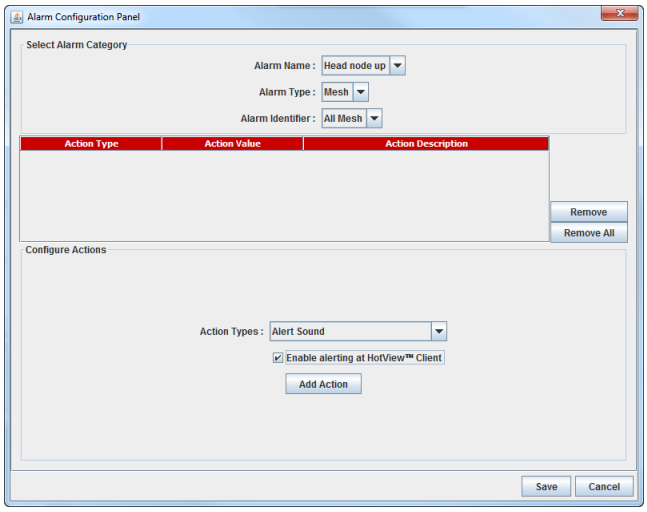
To configure an alarm:

1. Go to **Server Administration > Configure HotView Server > Alarm Management**

2. Click **Define Alarm**.
   a. Enter a name for the alarm. The name can be up to 30 characters long. The character count includes spaces and special characters.
   b. Select a severity from the drop-down list.
   c. Select the alarm type: PTP, Mesh, FMC, or Access Point.
   d. Select the event from the event list.
   e. Click **Add Alarm**.



3. Click **View Alarms/Configure Actions**.
   a. Click **Add Action**.
   b. From the drop-down menus, select the alarm name, type and alarm identifier.
   c. From the drop-down menu, select an action:
      - Alert sound: makes a sound from the HotView server or client
      - Execute a system command: enter a Linux shell command
      - Ignore
      - Report no action
      - Send an email: enter the receiver's email ID and message
   d. Click **Add Action**.
   e. Click **Save**.



The system adds the action to a table in the middle of the workspace.

Clearing an alarm

To clear an alarm from the alarm history:

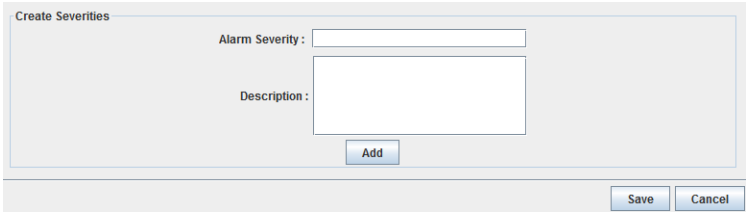
1. Go to **Server Administration > Configure HotView Server > Alarm Management > View Alarms/Configure Actions**

2. Highlight the alarm that you want to remove.
3. Click **Remove**.

Creating a custom alarm severity level

To create a custom alarm severity level:

1. Go to **Server Administration > Configure HotView Server > Alarm Management > Add Severity**



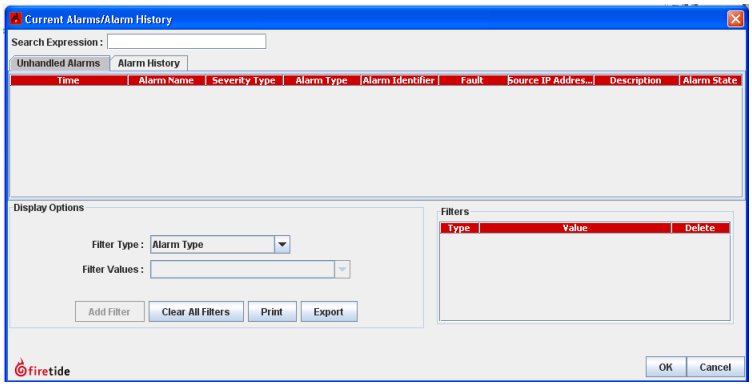
2. Enter a name (up to 30 characters long) for the severity level.
3. Add a description.
4. Click **Add**.

Viewing alarm history

You can view unmanaged and managed alarm histories.

To view and filter alarm entries:

1. Go to **Server Administration > View Alarm Logs/Alarm History**
2. (Optional) Add an alarm filter.
   a. Select a filter type: Alarm Type, Alarm Type Identifier, or Date.
   b. Select the field values.
   c. Click **Add Filter**.
3. (Optional) To print out the results, click **Print**. To export to a spreadsheet application, such as Microsoft Excel, click **Export**.
4. Click **OK** to exit the window.



User account configuration

This section contains tasks related to user account management:

- "Configuring an administrative user"
- “Deleting an administrative user” on page 31

Configuring an administrative user

You can add, edit privileges, or reset the passwords for administrative accounts so that you can have people log into the system to monitor, configure new nodes, or troubleshoot network events.

The system has two default accounts:

- hv_admin: a superuser with privileges to all meshes
- hv_guest: a read only account

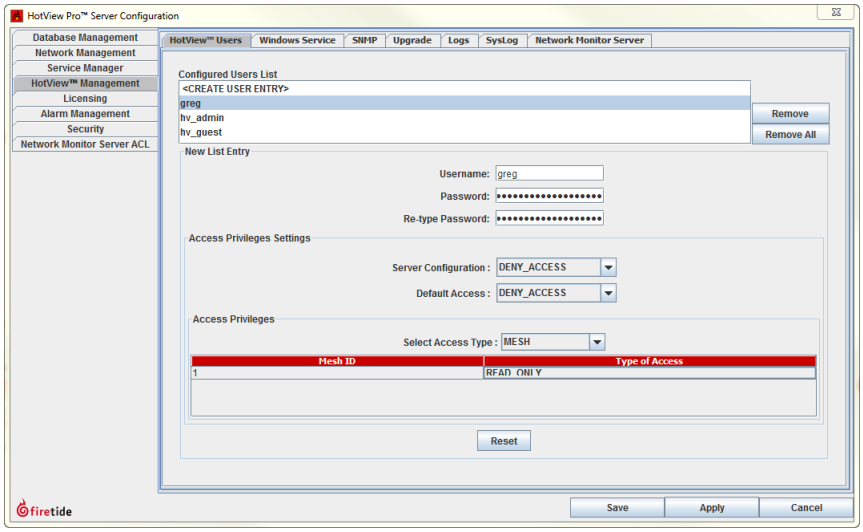
When you make a new user account, you have these options:

- Server Configuration:
  - Deny access (default setting)
  - Admin access (equivalent to hv_admin)
- Default Access is the access level given to the user for all new meshes that are not already in the mesh list.
  - Deny access (default setting)
  - Read-only
  - Read-write
- Access Privileges:
  - Mesh
  - Controller
  - FMC
  - AP group

To configure an administrative user:

1. Go to **Server Administration > HotView Management > HotView Users**

2. Select <Create User Entry> or select an existing account.
3. Enter or modify this information:
   - User name
   - Password
   - Password (to verify)
   - Select access privileges to the server and default settings.
   - Set the access privilege type.
4. Click **Save**.



Deleting an administrative user

Note: If you cannot see the Remove or Remove All buttons, expand the window.

To delete a user-configured administrative account:

1. Go to **Server Administration > HotView Management > HotView Users**
2. Select the account you want to delete.
3. Click **Remove.**
4. Click **Save**.

To delete all user-configured accounts:

1. Go to **Server Administration > HotView Management > HotView Users**
2. Select one system default account.
   A confirmation message appears.
3. Click **OK**.
4. Click **Remove All**.
5. Click **Save**.

Setting a user lockout

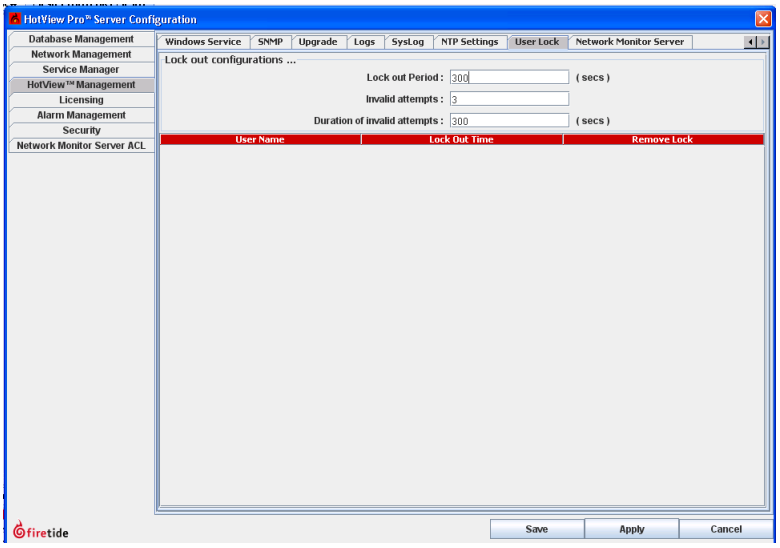
A user lockout entry lets you configure how many tries a user has to enter the correct login credentials. This feature is available for networks that use high security.

The default values for this feature are:

- Lock out period is 300 seconds
- Number of invalid login attempts is 3
- Duration of invalid attempts is 300 seconds

To set a user lockout entry:

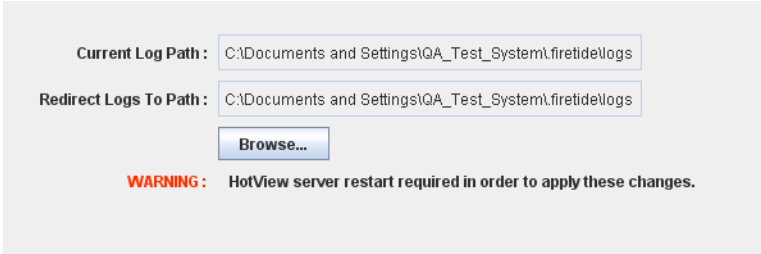
1. Go to **Server Administration > HotView Management > User Lock** tab
2. Enter the lock out period, number of invalid login attempts, and duration of invalid attempts.
3. Click **Save**.



Redirecting NMS logs

To change the place where you receive logs:

1. Go to **Server Administration > Configure HotView Server > HotView Management > Logs** tab
2. Click **Browse** to select a network location for logs.

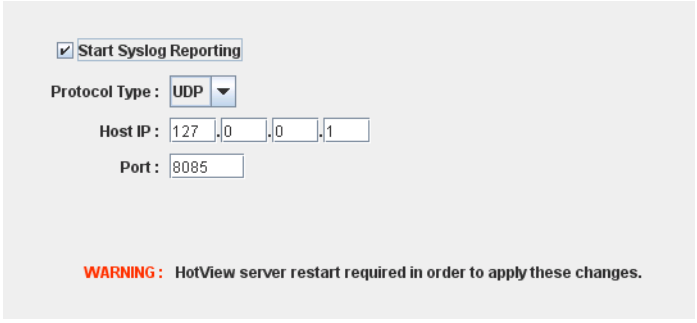


3. Click **Save**.
4. Restart the HotView server.

Configuring a syslog server

To configure a syslog server:

1. Go to **Server Administration > Configure HotView Server > HotView Management > SysLog** tab
2. Select Start Syslog Reporting.
3. Select the connection protocol: UDP or TCP.
4. Enter the host IP address and port number.



5. Click **Save**.
6. Restart the HotView server.

Mesh account and membership configuration

This section contains tasks related to mesh account and membership configuration:

- "Saving login credentials"
- "Deleting network objects"
- “Restricting node membership in a mesh network” on page 35

Saving login credentials

Each mesh network, access point group, and FMC device has a user name and password. HotView Pro system keeps a record of login credentials of each object.

To save the machine login credentials for a network, device group, or device:

Mesh tab > Configure Mesh > User Accounts

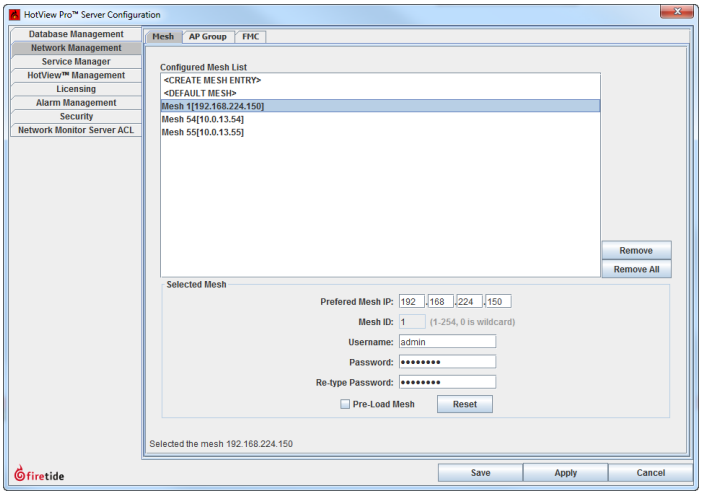
Note: You can also make password changes from **Server Administration > Configure HotView Server > Network Management** tab.

Deleting network objects

You can delete a mesh network, and access point group, and FMC device from network management tab of the HotView Pro Server Configuration window.

To delete a mesh network from the HotView Pro server:

1. Go to **Server Administration > Configure HotView Server > Network Management** tab
2. Select the Mesh tab.
3. Select the name of the mesh to delete from the Configured Mesh List.
4. Click **Remove**.
5. Click **Apply**
6. Click **Save**.



To delete an access point group from the HotView Pro server:

1. Go to **Server Administration > Configure HotView Server > Network Management** tab
2. Select the AP Group tab.
3. Select the name of the AP group entry to delete from the Configured AP Group List.
4. Click **Remove**.
5. Click **Apply**
6. Click **Save**.

To delete an FMC device from the HotView Pro server:

1. Go to **Server Administration > Configure HotView Server > Network Management** tab
2. Select the FMC tab.
3. Select the FMC ID of the FMC to delete from the Configured FMC List.
4. Click **Remove**.
5. Click **Apply**
6. Click **Save**.

Restricting node membership in a mesh network

By default, all mesh networks are trusted (low security). You can restrict network membership with the security feature. Without security features, any node with the correct mesh settings can join the mesh.

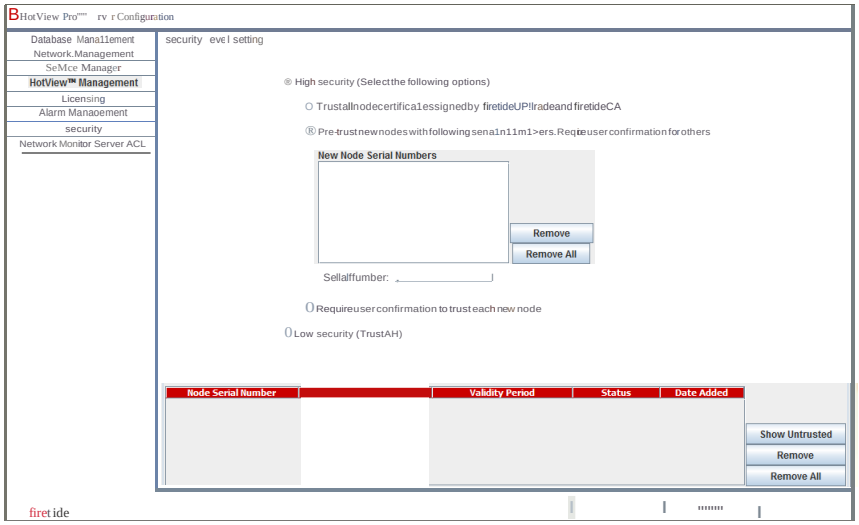
If the mesh has high security enabled, when you do future firmware upgrades you must use the digitally signed (.bin2) file.

You can set different kinds of security:

- Require a digital certificate signed by Firetide
- Trust nodes that have serial numbers that appear in a table that you make
- Require an administrator to approve each new node

To restrict node membership in a mesh network:

1. Go to **Server Administration > Security** tab
2. Select high security.
    a. Select one option.
    b. For the Pre-trust certain nodes option, enter the serial number of a node to be trusted, and then click **Add**.
    c. Repeat step “b” until all nodes are in the pre-trusted list.
3. Click **Save**.


HotView Pro rv r Configuration
Database Manallement
Network Management
SeMce Manager
HotView™ Management
Licensing
Alarm Manaoement
security
Network Monitor Server ACL
security eve l setting
High security (Select the following options)
TrustallInodecertifica1essignedby firetideUP!lradeand firetideCA
Pre-trustnewnodeswithfollowingsena1n11m1>ers.Requeuserconfirmationforothers
New Node Serial Numbers
Remove
Remove All
Sellalffumber:
Requireuserconfirmation to trusteachnew node
Low security (TrustAH)
Node Serial Number
Validity Period
Status
Date Added
Show Untrusted
Remove
Remove All
firet ide

Native SNMP configuration and use

Simple Network Management Protocol (SNMP) includes these components: managed devices, a SNMP agent, and a network management system. This content is about SNMP v1 and SNMPv2 support within Firetide mesh products.

Firetide native SNMP support includes these components:

- Managed device: a HotPort mesh node that has an SNMP agent and resides in a managed network
- SNMP agent: a software module inside a HotPort mesh node that translates information into an SNMP-compatible format
- HotView Pro Network Management System to configure the SNMP interfaces and agents
- SNMP manager (MIB browser), such as iReasoning

SNMPv1

RFC 1157 describes SNMPv1 and obsoletes RFC 1067 and RFC 1098. Security is based on community strings.

SNMPv2

SNMPv2 includes these enhancements:

- SMI
- Manager-to-manager capability
- Protocol operations

SNMPv2c (RFC 1901 to RFC 1908) combines the community-based approach of SNMPv1 with the protocol operation of SNMPv2 and supports only SNMPv2c security features.

SNMP default behavior

The SNMP interface and SNMP agent are disabled by default. The default SNMP agent port is 161. A maximum of four trap IP addresses can be configured. GET operations are supported. SET operations are not supported.

Compatibility

SNMPv1 and v2 are not directly compatible with each other. You must select one version through the HotView Pro interface to use in your mesh.

MIBs and OIDs

MIB stands for Management Information Base (MIB) is a collection of information organized hierarchically. SNMP provides access to MIBs.

A MIB can be:

- Scalar, which define a single object instance
- Tabular, which define multiple related object instances grouped in MIB tables

Object Identifiers (OIDs) uniquely identify managed objects in a MIB hierarchy. This can be depicted as a tree, the levels of which are assigned by different organizations. Top level MIB object IDs (OIDs) belong to different standard organizations. Vendor-defined private branches include managed objects for their own products.

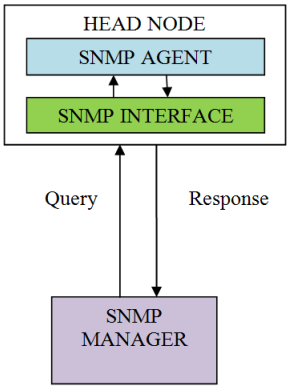
SNMP agent

For an SNMP browser to be able to communicate directly or indirectly connected mesh nodes, each node in the network must have a virtual network interface dedicated to the SNMP agent and each node needs a unique IP address that the SNMP browser can use to query the SNMP agent running on a particular node.

Communication between SNMP managers and SNMP agents

Communication flow happens differently depending on how the SNMP manager is connected to the mesh node.

The next figure shows the data communication flow between an SNMP manager and a directly connected mesh node (head node).

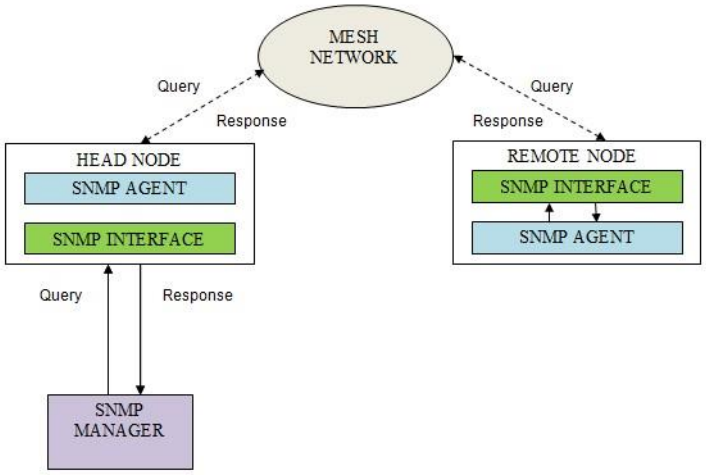


When the SNMP manager is directly connected to a mesh node (head node), the communication sequence is:

1. The SNMP manager sends a query to the IP address of the head node.

2. The SNMP interface receives the query.
3. The SNMP agent, which is listening on SNMP interface IP/SNMP agent port, receives the query.
4. The SNMP agent processes the query and then sends a response to the SNMP interface. The SNMP interface forwards the response to the SNMP manager.

The next figure shows an indirect connection between an SMNP manager and a remote mesh node.



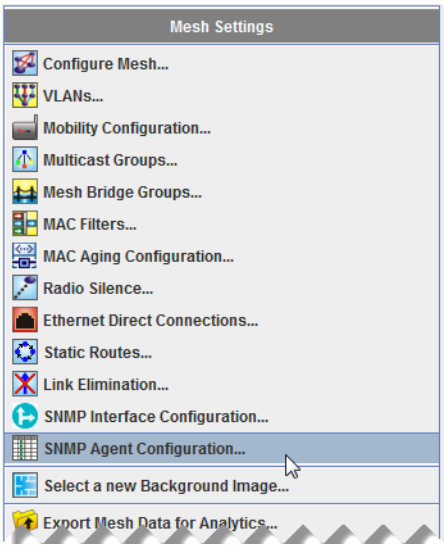
When the SNMP manager is indirectly connected to a mesh node (remote node), the communication sequence is:

1. The SNMP manager sends a query to the IP address of the remote mesh node.
2. The head node receives the query and forwards it to the mesh network.
3. The remote node receives and sends the query to its SNMP interface.
4. The SNMP agent, which is listening on SNMP interface IP/SNMP agent port, receives the query.
5. The SNMP agent processes the query and then sends a response to the SNMP interface. The remote node SNMP interface sends the response through the mesh network to the head node. The head node forwards the response to the SNMP manager.

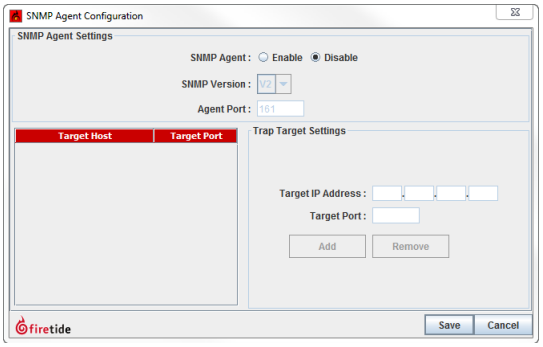
Configuring an SNMP agent on a node

To configure the SNMP agent on a node:

1. Right-click the mesh **> Mesh wide configurations > SNMP Agent Configuration**



2. In the SNMP Agent Configuration window, click **Enable**.



3. In the SNMP Agent Settings area:
   a. select the SNMP Version: v1 or v2
   b. Enter the Agent Port. The default value is port 161.
   c. (Optional) Enter up to four Trap IP Addresses and listener ports. The trap IP address field lets the user configure the trap listener's machine IP address. The trap IP port field allows the user to configure the trap listener to listen on the particular port.
4. Click **Save**.

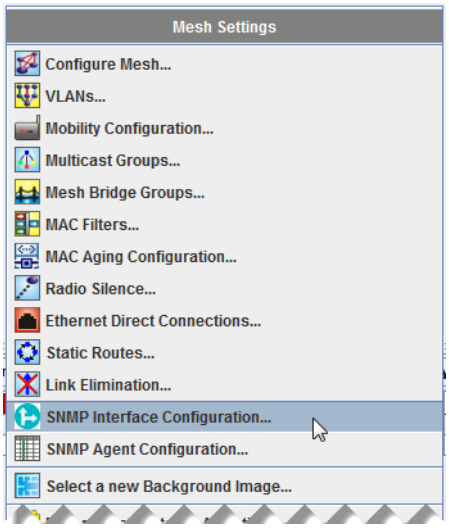
SNMP Interface

An SNMP interface is a virtualized representation of a network interface that might not correspond directly to a physical network interface. An SNMP interface of a mesh node is accessible within a heterogeneous network whether or not it is directly connected to that node.

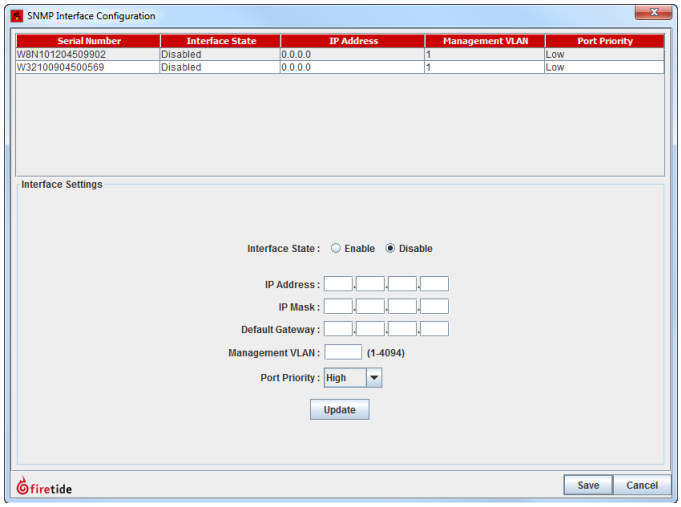
Configuring an SNMP interface

To configure an SNMP interface:

1. Right-click the mesh > **Mesh wide configurations > SNMP Interface Configuration**



2. Select the node on which the system is to apply the configuration.



3. Click **Update**.
4. Configure the state of the interface. By default SNMP interface state is disabled.
5. Enter the IP Address, IP mask, and default gateway address for the SNMP address.

Caution! The SNMP IP Address should not be in same subnet as NMSIP Address.

6. Enter the management VLAN. All the packets going out from this SNMP interface port will be tagged with configured VLAN. Default VLAN ID is 1. The VLAN range is 1 to 4094.
7. Enter the port priority: high, medium, or low. The default value is low. All packets that leave this port are assigned the configured priority.
8. Click **Save**.

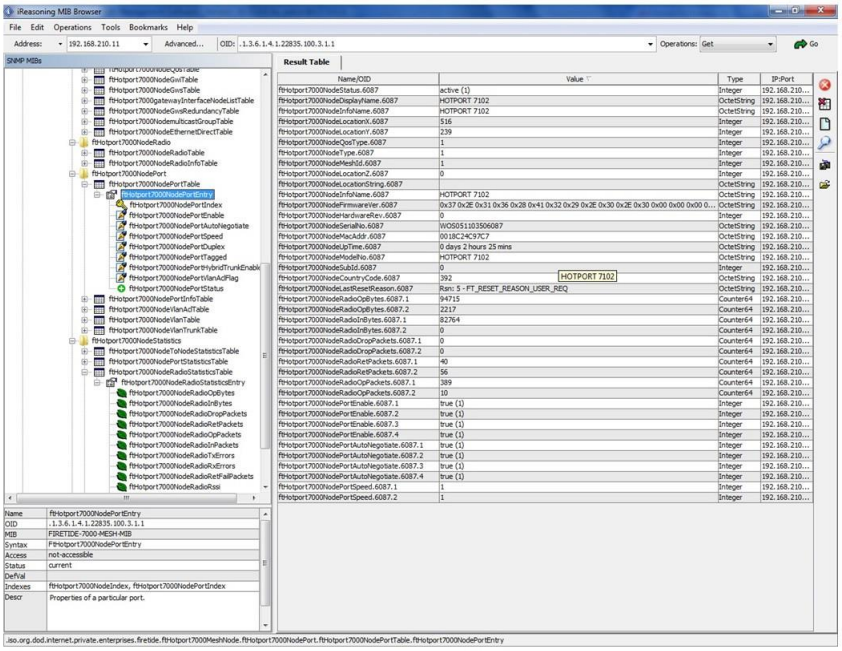
MIB browser use

This section contains basic examples of using different MIB browsers. This section is not a substitute for the MIB browser documentation or training to use a specific MIB browser.

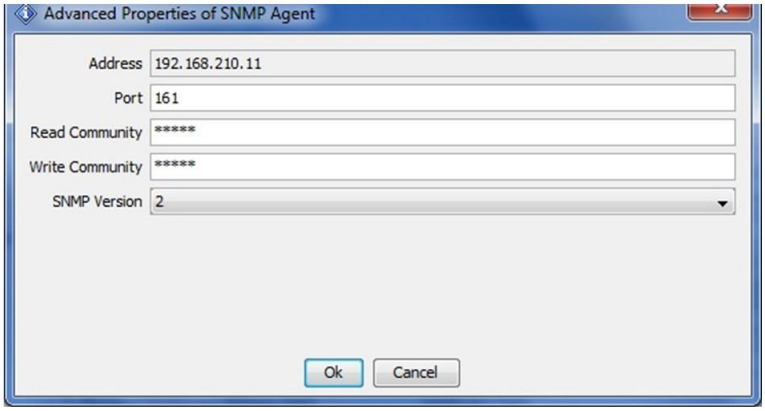
Using iReasoning MIB browser

The screen captures in this section show how to load and access the MIBs with the iReasoning MIB browser.

1. Load the MIB file FIRETIDE-7000-MESH-MIB.mib or FIRETIDE-5000-MESH-MIB.mib
2. Perform GET / GET BULK operation.



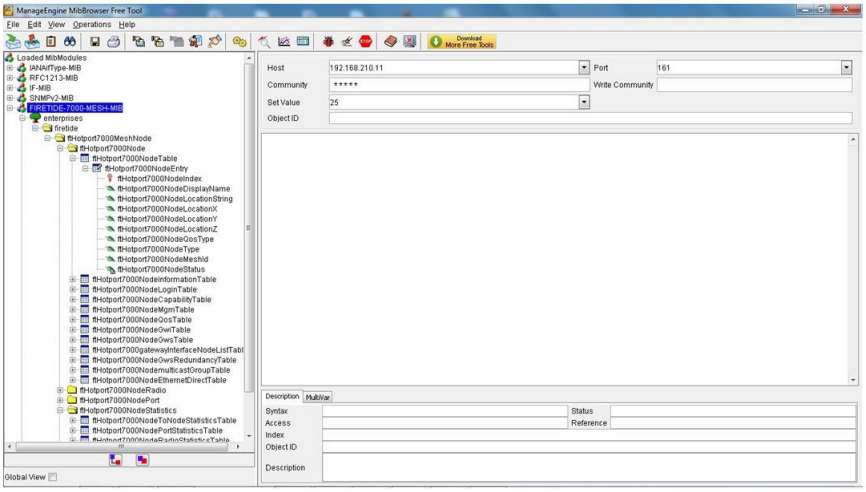
3. Configure Read community as guest.

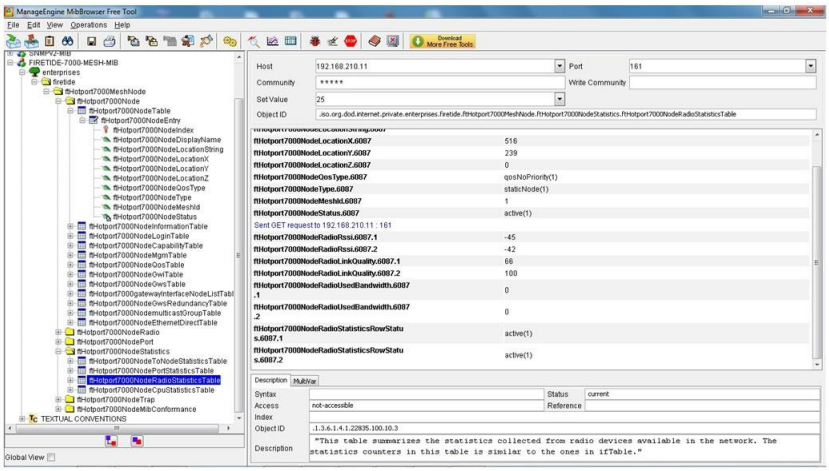


Using ManageEngine MIB browser:

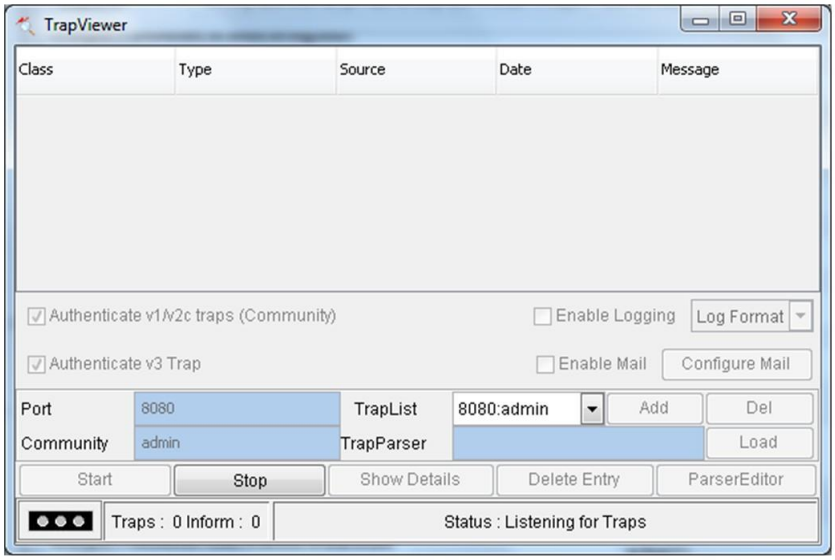
The screen captures in this section show how to load and access the MIBs with the ManageEngine MIB browser.

1. Load the MIB file FIRETIDE-7000-MESH-MIB.mib or FIRETIDE-5000-MESH-MIB.mib
2. Configure Read community as guest. Write community is not required.
3. Perform GET / WALK operation.

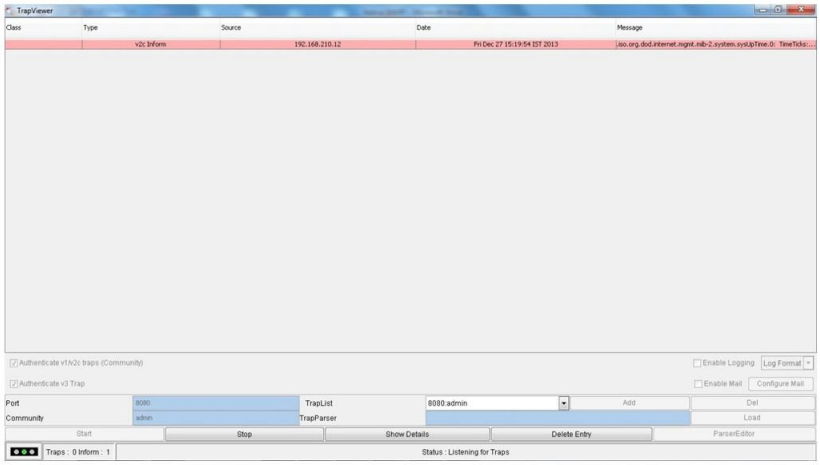




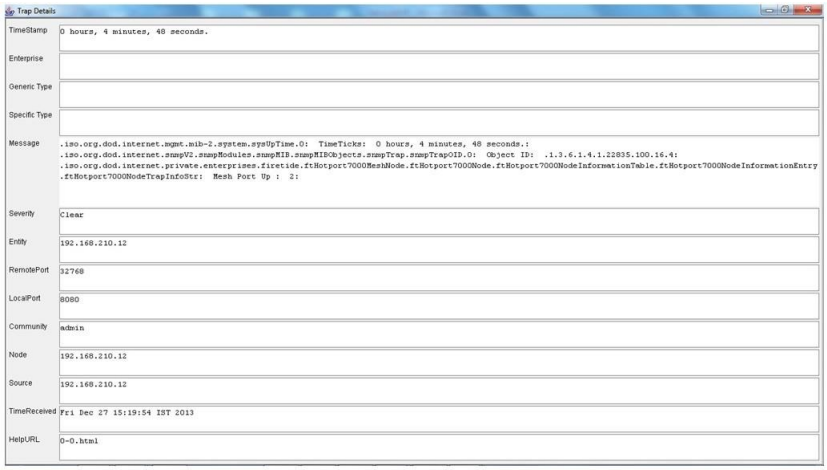
4. Configure the trap viewer
   Community String for Traps: admin



Trap viewer



Trap Details



Configuration of the network monitor server

The network monitor feature is an effective monitoring tool for customers who manage large networks, such as a multi-site carrier Wi-Fi HotSpot network.

This tool lets you monitor the status of access points in a hierarchical manner. The tool can be used in your OCC (Operations Command Center) to get a global status view of your network. A global view can lead to faster responses to events, network connectivity issues, and so on. Network monitor does not support the configuration of access points. To make configuration changes, you have to explicitly log into an AP group.

By default, network monitor is disabled. To use this feature you have to enable it with HotView Pro. When you upgrade to a software version with network monitor functionality, you must enable the feature.

Network Monitor Server can monitor 4000 or more access points in a network.

This chapter explains:

Configuring the Network Monitoring Server startup settings

You can set the Network Monitor Server to:

- Start every time HotView Pro Server starts
- Set a specific port on which Network Monitor starts

The network monitor server listens to port 10000 (default). The range is 1 to 65000. If port 10000 is not available on your network, select an available port. Ports above 2000 are usually available. The port value that you set must be the same value on each access point.

Specify a keep alive message time delay and a timeout to manage network overhead. The keep alive delay specifies in seconds how long that the Network

Monitoring Server waits to receive keep alive messages from the access points. The default value is 20 seconds.

The keep alive timeout specifies the number of successive keep alive messages that the Network Monitoring Sever misses before the server reports the access point down. The default value is 3.

To configure startup settings:

1. Go to **Server Administration > HotView Management > Network Monitor Server** tab
2. (Optional) Check the option Network Monitoring server is started when HotView server starts.
3. Enter the port number on which Network Monitoring Server starts.

Caution! You must restart the server for port changes to update.

4. (Optional) Enter a keep alive delay and timeout.
5. Click **Save**.

Starting and Stopping Network Monitoring Server

From the HotView Server Configuration panel you can select the option to start or stop the Network Monitoring Server.

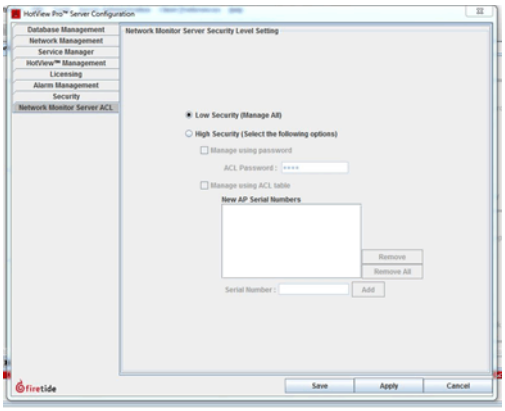
1. Click the HotView Pro shortcut > **Server Configuration > Configure HotView Server > Service Manager**
2. Click the button to stop or start the monitoring server.
3. Click **Save**.

Network Monitoring Server security level settings

Note: HotView View only shows managed access points.

When an access point connects to the Network Monitoring Server, the server enforces a particular security level to that access point. All new devices (no configuration) enter the system as unmanaged devices. Based on the settings you configure, the system applies low or high security settings to the device:

- Low security. The system converts unmanaged devices to managed devices.
- High security. The system applies a credential process to all unmanaged devices:
  - The system permits devices that appear in the Managed ACL list or devices with an ACL password that matches the HotView ACL password or serial number in the pre-approved AP list.
  - The system blocks devices that appear in the Blocked ACL.



Low security level

If you select low security, unmanaged access points become managed access points.

High security level

If you select high security, you can choose to use an ACL password, or an ACL password and a list of pre-approved nodes.

If you select the ACL password option, the password must match on both the AP and HotView Pro for the access point to become a managed access point.

If you use an ACL table, you must add the serial number of the node to the ACL table for the access point to be a managed access point.

The user lockout feature is available for networks that use

Setting the security level

To set the security level:

1. Click the HotView Pro shortcut > **Select Server Configuration** > **Security**
2. Select low or high security.
   If you selected high security, configure the security settings:
   a. (Optional) Check **Manage using password** and enter an ACL password.
   b. Check **Manage using ACL table** and enter the serial numbers of the nodes that you want to be monitored.
3. Click **Save**.

Managing the Network Monitor Server ACL

You can enter the serial number and security access level (Managed or Blocked) into an ACL table to manage access points. Alternatively, if you have no pre-configured setting requirements, when you load a new access point, by default it becomes an unmanaged access point.

Note: HotView View only shows managed access points.

Each list contains the serial number of the node and the status.

To change the status of a device:

1. Select a setting from the drop-down menu.
2. Click **OK**.

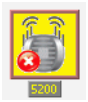
Viewing access points using HotView

The access point group panel shows all the access point groups. Access point group icons indicate the status of the group:

	Group WARNING icon One or more access points are not running.
	Group UP icon All access points are running, and you are logged in.
	Group DOWN icon You are not logged into the AP group.

You can only see managed access points. Access points that are not working correctly have a small red mark in the lower left corner of the icon.

Managed AP (UP)

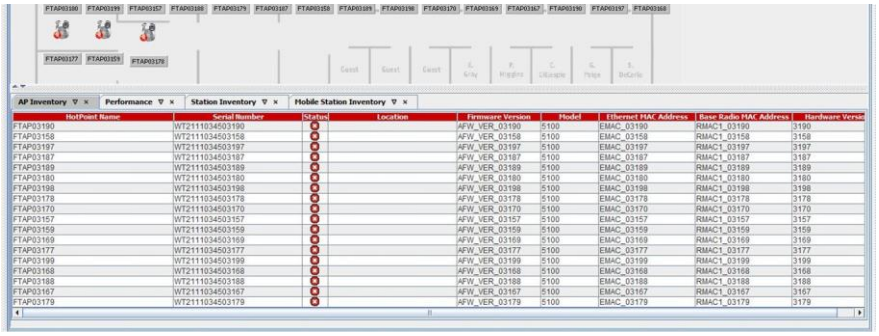


Managed AP (DOWN)

Alternatively, you can view the same access points with the AP Inventory panel which shows a list of all the access points and the status of each one.

The Station Inventory panel shows a list of all stations attached to the access point.

The next figure shows the Performance Panel where you can see the wired and wireless statistics for each AP.



Statistics for each access point include:

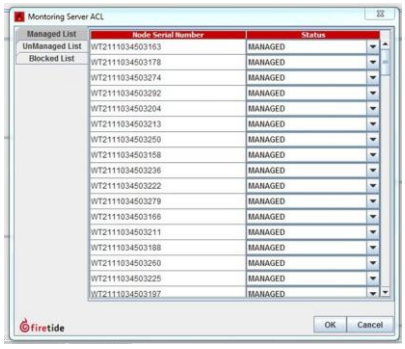
- HotPoint name
- Serial number
- Status
- Location
- Firmware version
- Model
- Ethernet MAC address
- Base radio MAC address
- Hardware version

Configuring ACL password use with access points

Prerequisite: You have to enter some settings on each access point to be able to add access points to the ACL:

- IP address of the network monitor server
- Port on which the network monitoring server accepts connections from AP
- Password

When you select the high security and option for using ACL passwords to manage access points, HotView Pro uses a password to load approved access points. The default password is firetide. If the passwords in HotView Pro and the access point are the same, the access point becomes a managed access point.



1. Go to **Access Point > Monitoring Server ACL Configuration**
2. Enter the following information:
   - IP address of the network monitoring server
   - Port on which the network monitoring server accepts connections from access point. If you made a change to the port, then you need to enter the same port for the access point. (The default value is 10000.)
   - The same password that is configured on the Network Monitor Server
3. Click **Save**.

Mesh node security

Firetide offers a number of features that let you to implement various levels of security. The security domains applicable to a mesh network are:

- Physical access
- Access control systems
- Telecommunications and network security

You should always change the basic mesh parameters:

- Mesh ID number
- Mesh name
- Mesh IP address
- Mesh ESSID

Note: You should also enable radio encryption.

Best practice: Change all machine and administrator passwords from the default values to something more secure.

Physical access

Prevent physical access to network devices:

- Disable all ports that are not in use.
- Put gateway servers and controllers in secure environments.

You can configure to receive an e-mail alert if an Ethernet port is tampered with. For more information, see "Configuring an SMTP server in HotView Pro" on page 26.

The status of every port on the mesh is visible on each node in HotView Pro.

Access control systems

You can prevent access through HotView Pro through careful configuration of passwords and user account management:

- HotView Pro server configuration. Change the default start-up password for the HotView Pro server.
- Mesh network configuration. Change the default user names and passwords of the read only and read/write accounts.
- User account management.
  - Use different classes of HotView Pro users to monitor the health of the network

- Assign correct read and write privileges.
- If using the high security options, configure the login attempt lockout feature.

• Configure and use self-signed certificates.

Telecommunications and network security

This section lists software security features that you can configure to prevent application and wireless access.

Note: You cannot prevent the mesh nodes from forming links to each other. You can prune or eliminate poor links.

Preventing access through telnet and SSH

From HotView Pro and HotPort Users (Mesh option), telnet and SSH access can be disabled.

To block access to telnet or SSH:

1. Go to **Mesh > HotPort Users Configuration**
2. Remove the check from the check box for the correct service (telnet or SSH) to block all access to traffic from either service.
3. Click **Save**.

For more information, see "HotPort Users Configuration" on page 125.

Changing the telnet or SSH password

It is recommended that you change the default passwords to make your system more secure.

To change the passwords for accounts authorized to use telnet or SSH:

1. Go to **Mesh > HotPort Users Configuration**
2. Edit the password for users and root as appropriate.
3. Click **Save**.

For more information, see "HotPort Users Configuration" on page 125.

MAC address filtering

MAC address filtering can be used to block specific MAC addresses. For more information, see "Configuring MAC filters" on page 120.

Radio security

Enable 256-bit AES encryption over the radio links to prevent eavesdropping. End-to-end encryption is also available. Encryption is hardware-based, and the use of end-to-end encryption does not significantly impact performance.

The ESSID can be encrypted to prevent someone from detecting the presence of equipment.

Blocking Unauthorized Nodes

You can prevent unauthorized nodes from joining the mesh. To do this, you must enable the high security mode in HotView Pro. This is system-wide setting; you cannot have some meshes at high security and other meshes at low security.

If you enable high security, when you do future firmware upgrades you must use the digitally signed image (.bin2) file.

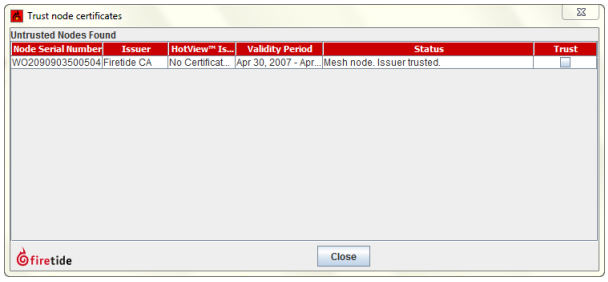
High security options include:

- Trust all
- Pre-trust existing
- Require confirmation for all

For the pre-trust option, you must enter the serial numbers for each existing node.

Note: Configure the mesh network and just before it is ready for a production environment, enable high security and manually enter the serial numbers.

The next image shows the display when you use high security with require confirmation for all.



Disabling an Ethernet port

To disable an Ethernet port:

1. Right-click the node.
2. Select **Configure Node Port > Port Configuration**.
3. Modify the port settings.
4. Click **Save**.

Performance tools

HotView Pro software has tools to help you analyze, troubleshoot, and optimize the performance of your system.

RF signal quality

The key to good RF signal quality is good signal-to-noise ratio. For 802.11a and 802.11g operating modes, a received signal strength indicator (RSSI) of -70 dBm is the minimum strength required for reliable operation at full link speed. In RF-noisy environments, a stronger signal might be required.

Best practice: Design links to achieve -50 dBm or better to provide a reasonable fade margin.

For 802.11n, the RSSI must be -60 dBm or better.

Best practice: Links should be -40 dBm or better.

Rarely, strong signals can overload radio receivers. Avoid RSSI values in excess of -20 dBm.

Antenna placement and alignment, RF channel plan and interference, a congested wireless domain, mesh configuration or individual radio settings are some of the reasons why dropped packets and retries are high and wireless performance is affected in a negative way.

Possible sources of interference include:

- Other devices
- Another radio inside the node. Dual-radio nodes should have antennas placed so that their radiation patterns do not overlap.
- An incorrectly-set range parameter or multi-hop optimization. Make sure multi-hop optimization is turned on for all meshes with more than two nodes.

Make sure the range setting is larger than the longest RF link in the mesh. Set the range parameter larger than necessary to see if it solves the problem.

To view the common RSSI threshold value, hysteresis value, extended range setting, and noise floor RSSI value, go to **Mesh > Configure Mesh > Advanced** tab.

Node statistics window

You can reset the statistics for each link and chart them over time. Statistics refresh automatically; you can also refresh the statistics manually.

The next tables shows each column and lists its purpose.

Table 1. Node statistics window columns and purposes

Column	Purpose
1	Each radio has a one-line entry for each neighbor with which it communicates. Columns 1, 2, and 3 identify the link.
2	
3	
4	Shows if the system eliminated a link. The system eliminates marginal links.
5	Show the RSSI value and Signal-to-Noise ratio.
6	
7	Data Rate, shows the current modulation rate of the link. Until traffic moves over the link, this value stays at a low value. Use the Run Diagnostics command to generate traffic if the mesh is not busy.
8	Show traffic in (received) and out (transmitted) for each link.
9	
10	
11	
12	
13	Show dropped packets and total retries. It is normal to have a few. If either parameter exceeds one percent of total traffic, look for sources of interference.
14	

Table 8

Spectrum analysis tool

HotPort mesh nodes have a spectrum analysis tool. You can use it to monitor the RF environment, such as the usage of each channel around a specific node.

Run the spectrum analysis tool when you notice lots of dropped packets, which indicate that the link is overloaded.

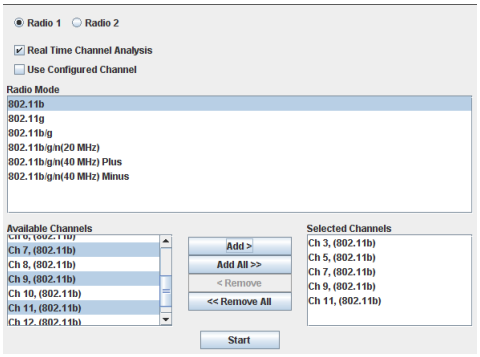
Spectrum analysis works by using one radio in the node to sequentially scan through the list of selected channels, recording the duration and power of any RF signals it finds. The other radio in the node sends the result back to HotView Pro,

which stores the result and shows the information in a graph. The radio that scans is out of service and cannot carry mesh traffic.

Note: Use an extra HotPort 7000 Series mesh node at a mesh site for spectrum analysis work, instead of using a radio on a mesh that is carrying production traffic.

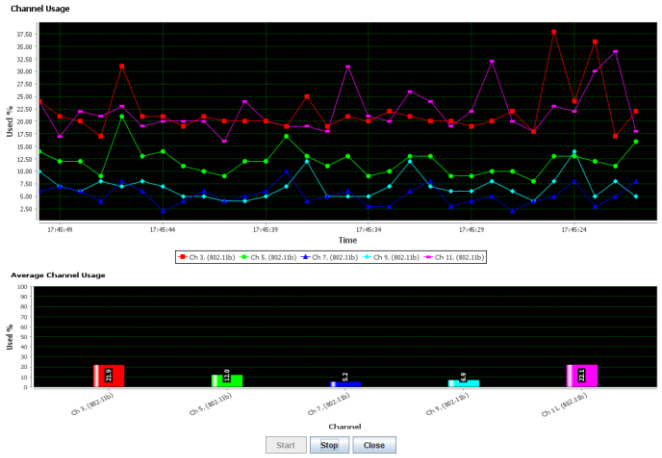
To access the spectrum analysis feature:

1. Right-click a node **> Advanced Tools**



2. Select the options:
   - Type of analysis: channel usage or power meter
   - Radio: 1 or 2
   - Real-time channel analysis
   - Use configured channel on node
   - Radio mode
   - Available channels
3. Click **Start**.

   The system makes a graph based on the settings you selected. The next image shows an example spectrum analysis.



Link throughput tests

HotPort mesh nodes have a built-in link throughput tool.

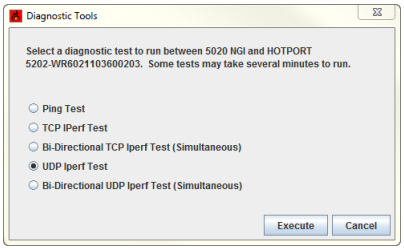
The Iperf test is a deployment diagnostic tool and is not a performance benchmark test. The results are indicative of baseline performance, but actual throughput performance can be higher.

To measure link throughput performance:

1. Right-click on one of the two nodes between which you want to measure performance.
2. Select **Run Diagnostics Tools**, and select the second node from the menu.

   A window appears from which to select a test:

   - Ping. A ping test checks for a link between the nodes. It does not generate enough traffic to affect mesh operation. The ideal result is a low, consistent, ping response time. Highly inconsistent times indicate RF signal problems.
   - TCP Iperf and bi-directional TCP Iperf. Both tests send a large amount of TCP traffic between the nodes on one link. The bi-directional test runs the test traffic in both directions simultaneously.
   - UDP Iperf and bi-directional UDP. Both tests run a large amount of UDP traffic between the nodes on one link. The bi-directional test runs traffic in both directions simultaneously.
3. Select the type of test.
4. Click **Execute**.



Note: Iperf tests flood a link with as much traffic as it can carry. This can disrupt other traffic on the mesh. Iperf sends a large, fixed amount of traffic. If iperf cannot complete the transfer in a fixed period of time, it stops. If you receive a failure message, run the test again. If the test fails consistently, substantial interference exists on the RF link.

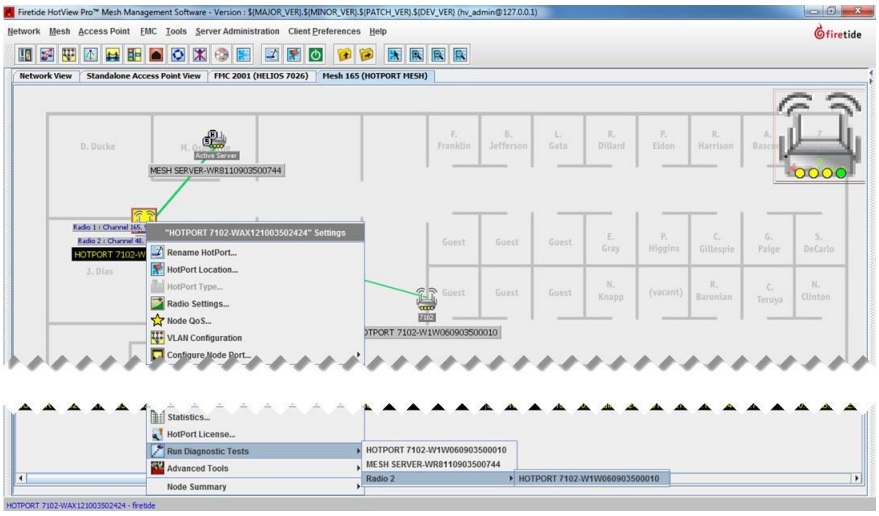
Lightweight Link Capacity Estimation Tool

The lightweight link capacity estimation tool is designed to estimate the bandwidth of a wireless link between two mesh nodes.

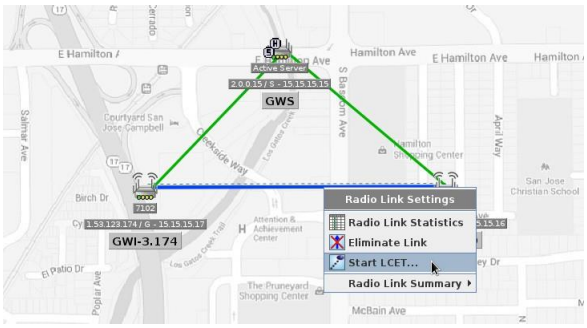
Estimating link capacity

To estimate the capacity of a radio link capabilities between two mesh nodes:

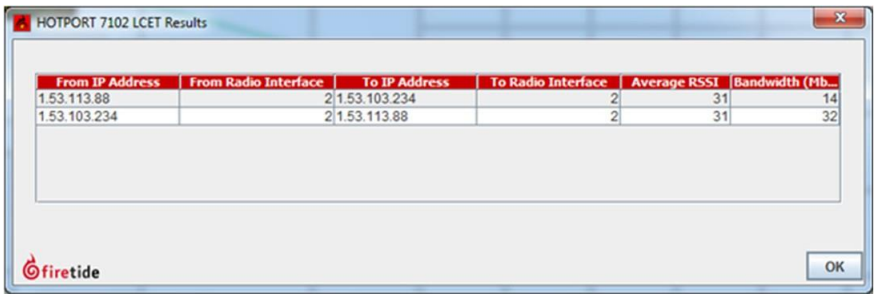
1. Right-click the node **> Run Diagnostic Tests >** Select **Radio 1** or **Radio 2 >** Select HotPort Node



Note: Alternatively, you can right-click the radio link between two nodes **> Start LCET**



2. Wait until the results appear.



3. Click **OK** to exit the results.

Antenna Alignment Tool

The antenna alignment tool gives you real-time signal strength data, so that you can orient an antenna for optimal performance. One person can hold an antenna up and move it from side to side, while another installer can read the data.

The antenna alignment tool is designed to report bearing and antenna tilt information. It also reports the dynamic RSSI value, which is independent from the bearing, tilt, and GPS information.

Use this tool with static nodes, and check the azimuth settings from both ends of the wireless link.

Note: Do not use this tool from mobile nodes or a single node.

Configuring the antenna alignment tool

Prerequisite: HotPort location information (GPS and height/elevation) is complete and consistent for all nodes in the mesh network. See "Entering a location for a mesh node" on page 129.

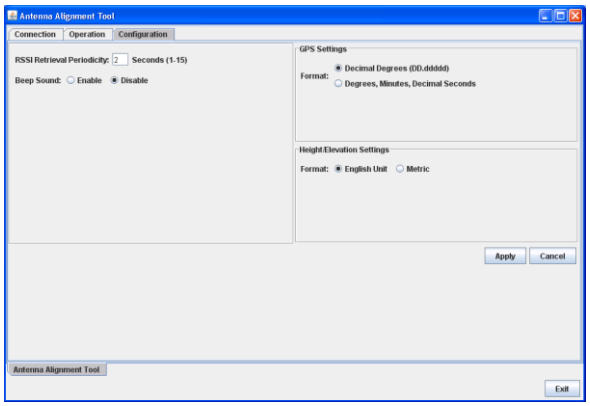
To configure the antenna alignment tool:

1. Connect an Ethernet cable from a node in the mesh to an administrator computer.

   The system detects the connection and reports the node as the head node. The letter H appears near the node in Network View.

2. Go to **Tools > Antenna Alignment Tool**

3. Make sure that the IP address is for the correct mesh.
4. Click **Connect**.
5. Click the Configuration tab.
6. Enter the RSSI retrieval period, which is a value from 1 to 15 seconds. The default value is 2 seconds.
7. Select format for GPS settings and measurements to be the same as the formats configured in the mesh nodes.
8. Click **Apply**.



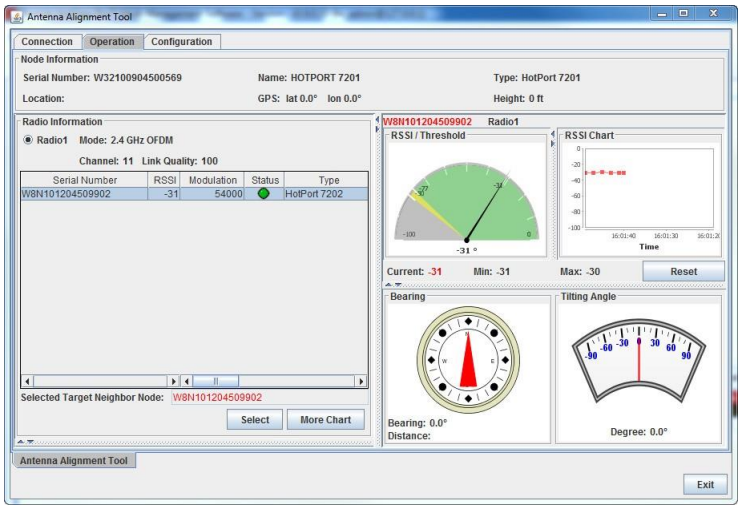
Using the antenna alignment tool

Prerequisites:

- You need to configure the antenna alignment tool before you run it.
- HotPort location information (GPS and height/elevation) is complete and consistent for all nodes in the mesh network. See “Entering a location for a mesh node” on page 129.

To use the antenna alignment tool:

1. Go to **Tools > Antenna Alignment Tool**
2. Make sure that the IP address is for the correct mesh.
3. Click **Connect**.
4. Click the Operation tab.



a. Select the radio.

b. Click **Select**.

The system sends real-time bearing and tilt data.

c. To view the information for a different neighbor node, select **More Chart**.

5. When you are finished, click the Connection tab.
6. Click **Disconnect**.
7. Click **Exit**.
8. Remove the Ethernet cable from the node.

Repeat this procedure on the far end of the link to confirm the accuracy of the azimuth settings.

Restore Node Configuration

Restore Node Configuration restores the node settings to the node. It does the same action as the node-specific menu item.

View Historical Diagnostic Data

View Historical Diagnostic Data gets the results of past diagnostics test from the database. You can choose to view up to 1000 records of one kind at a time.

The ping option shows ping results.

The iperf option shows:

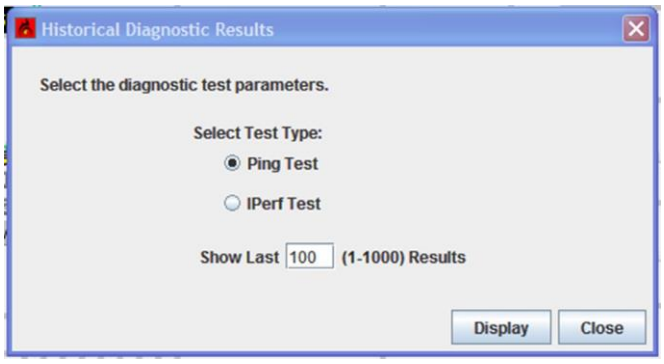
- TCP Iperf Test
- Bi-Directional TCP Iperf Test (simultaneous)
- UDP Iperf Test
- Bi-Directional UDP Iperf Test (simultaneous)

If the database is disabled, the system keeps no test results.

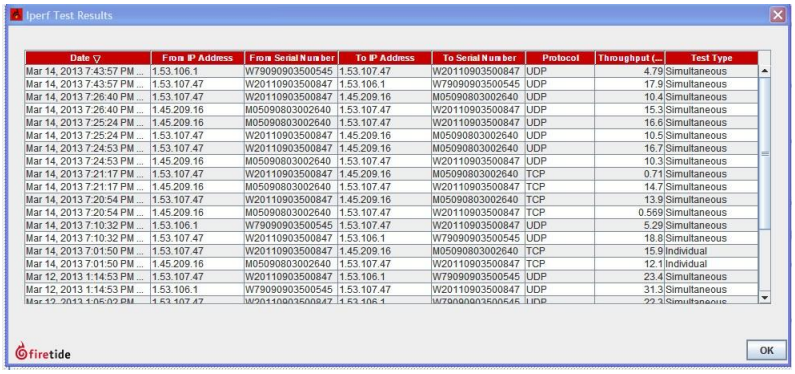
Prerequisite: You must install and enable the database functions.

To view past test results from the database:

1. Got to **Tools > View Historical Diagnostic Data**
2. Select the data type to show: ping or iperf.
3. Enter the number of records to show: 1 to 1000.



4. Click **Display**.



Graph Statistics

Graph Statistics lets you graph statistics for up to four parameters.

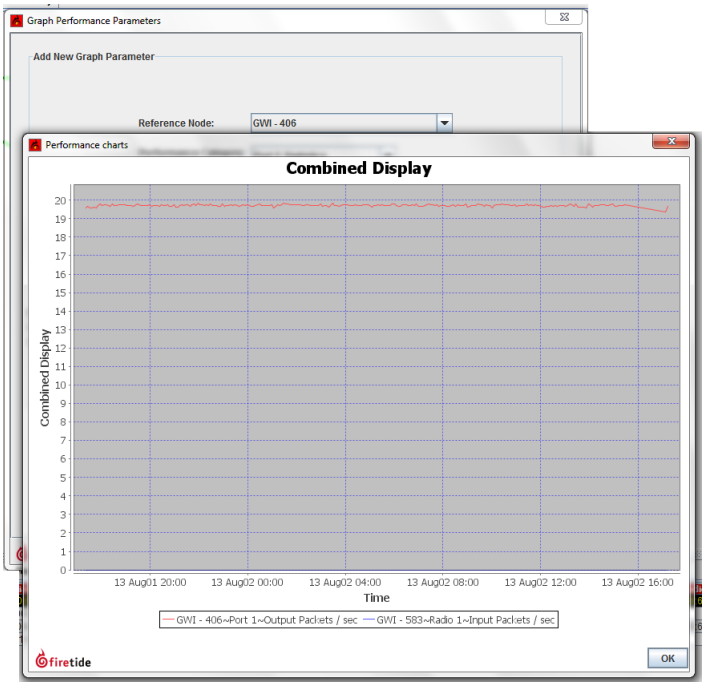
The next table lists the parameter elements and the choices associated with it.

Element	Notes
Reference node	All of the nodes in the mesh by Mesh ID
Performance category	You can select to view: - Port (1 to 4 depending on the HotPort model) - Radio (1 or 2 depending on model) - Neighbor statistics for radio 1 or 2 (as available) You can also select to view all neighbor statistics or you can select a specific neighbor from the drop-down list).
Individual statistic	Select on of these parameters: - Output packets per second - Input packets per second - Output bytes per second - Input bytes per second - RSSI (dBm) - Data rate (Kbps) - Packets dropped per second - Total number of retries

Table 9

To make a graph:

1. Go to **Tools > Graph Statistics**
2. Enter up to four graph parameters:
   a. Select a reference node.
   b. Select a performance category.
   c. Select the statistics setting for one neighbor or all neighbors.
   d. Select the individual statistic (type and unit of measure).
3. Select a start and end time.
4. Select whether you want all of the data on one graph or if you want individual graphs.
5. Click **Display Graphs**.



Network tasks

This chapter explains specific network tasks:

Upgrade process

This upgrade process is for mesh nodes, 5020-Es, access points, and FMC devices.

When you upgrade firmware for a production static or mobile mesh network, the system copies the new firmware image to all of the nodes in the mesh. Next, the system activates the firmware as configured in the upgrade scheduler. All nodes must run the same version of firmware.

The system verifies firmware images by checksum. The system does not let you activate or reboot a node that has corrupt or invalid firmware.

If the network has one or more unreliable links over which the system has to send a copy of the new firmware image, the upgrade over the unreliable link might fail. In this case HotView Pro tries to send the firmware image again. The system tries five times by default.

If one or more links fail to upload the firmware to the remote nodes, the system does not activate the firmware image even if the job scheduler indicates immediate activation. The system sends a message to let you know that the upgrade failed. After the system verifies that the new firmware image is on all nodes in the network, then the image can be activated.

You can change the retry count and chunk size to make the upgrade process more efficient for your network conditions. To change the default retry count and chunk size, see "Changing the chunk size and retry count for a firmware upgrage" on page 21.

Image file names

Image file names have a specific format:

- Product type
- Numerical family number
- Version number

Suffixes can be .bin or .bin2. Digitally signed images have the .bin2 suffix and are for mesh networks that have high security enabled.

Upgrading firmware with HotView Pro

This procedure is for upgrading the firmware of mesh nodes, 5020-Es, access points, and FMC devices.

Caution! If the mesh has high security enabled, you must upload the .bin2 file. If you try to load the .bin file, the upgrade will fail.

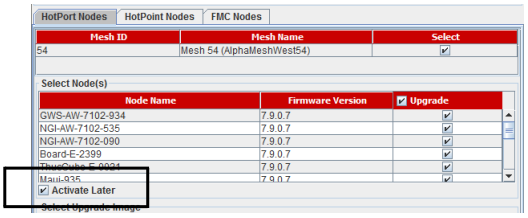
By default, the system uses the configuration in cache for multiple upgrades.

Best practice: Upgrade the image two times because you want the backup image and primary images to be the same. If a backup image is older than the primary image, the node might not support the same features.

With the upgrade scheduler you can:

- Upgrade and activate the firmware now.
- Upgrade the firmware now and activate it later.
- Upgrade the firmware on a specified day at a configured time and then activate it immediately or later.

By default, the scheduler activates the firmware immediately.
If you select the **Activate Later** check box, the scheduler copies the firmware image to the node but does not activate the firmware.

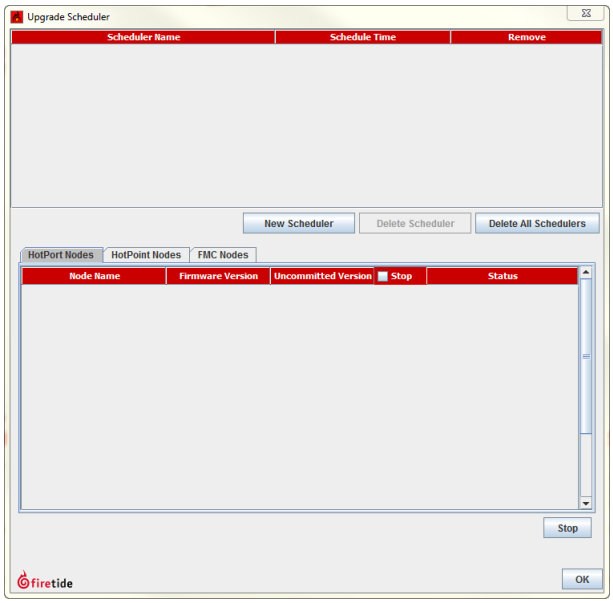


When you schedule an upgrade time (Scheduler Operation: Later), the HotView server, if it is running, starts the job at the scheduled time. If the HotView server is not running at the time scheduled, the scheduled jobs start immediately after you start the HotView server.

Best practice: If you choose to upgrade a production mesh, schedule the upgrade and activation for a convenient time. Firmware upgrades can consume considerable bandwidth. The mesh is not available for two minutes when you activate new firmware.

To schedule a firmware upgrade for a later date and for later activation:

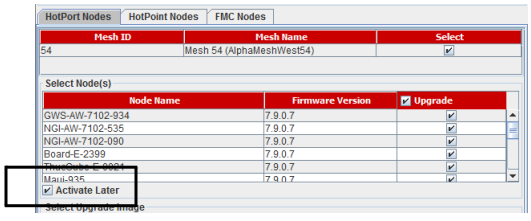
1. Go to **Network > Upgrade Firmware**
   The upgrade scheduler appears.



2. Click **New Scheduler**.
   a. Select Upgrade.
   b. Select the time: Later. Use the calendar to a future date and time.
   c. Click the tab to select a device type (HotPort Nodes for a mesh network, HotPoint Nodes for access points, or FMC for mobility controllers), and then select the mesh or device by ID or name.

Note: The system selects all nodes within a mesh for simultaneous upgrade because all of the nodes have to run the same firmware. If a node should not receive the upgrade image, you can remove the mark from the upgrade check box.

   d. Select **Activate Later**.



   e. Select the upgrade image.

3. Click **OK**.

The "upgrade complete" message means that the image file is on the node and is valid. You can then activate a few nodes at a time until all of the nodes are running the same firmware version.

Generating self-signed certificates

When you use high security settings, you can generate certificates for your Firetide products. First, configure the high security settings, and then generate self-signed certificates. To enable high security, see "Blocking Unauthorized Nodes" on page 56.

To generate a self-signed certificate:

1. Go to **Network > Self Sign Certificate**
2. Enter your certificate signing authority information.
3. Click **Save**.

Viewing HotView clients

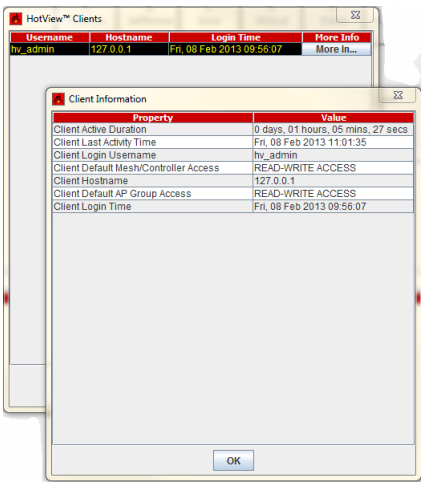
You can retrieve information about these HotView client properties:

- Duration of activity
- Last login time
- Client login user name
- Mesh ID
- Default mesh and controller access
- Client host name which is the IP address
- Default access point group access level
- Client login time

To view information about HotView clients:

Go to **Network > View HotView Clients**

Click **More Info**.



Exiting the HotView Pro application

Go to **Network > Exit** to close HotView Pro.

Gateway group configuration

If a node that is the only connection from a wired to a wireless domain fails, the mesh is cut off from the wired domain. A gateway group is a method to keep the two domains connected even if a node fails.

Gateway groups provide redundant, load-balanced connections between a wireless mesh and wired infrastructure.

A gateway group is the combination of one or more network gateway interface (NGI) nodes and a gateway server (GWS).

NGI nodes are gateways between the wireless world and wired networks. A network can have from two to 30.

The GWS manages the NGI nodes. The GWS does load balancing and routes broadcast and multicast traffic.

A gateway group consists of tunnels between the NGI nodes and the GWS. You can have up to 30 gateway interfaces in a gateway group.

Caution! A gateway server is a single point of failure in a network. You should install the server in a protected area and use UPS. It is possible to configure a redundant backup gateway server.

Configuring a gateway group

To make a gateway group:

1. Use the Import Mesh Configuration command to make a current copy of the mesh configuration for the mesh to which you are adding the gateway group.

   Import the current mesh configuration from the current mesh, and save the file where you can find it later. Log out of the mesh and physically disconnect from it.
2. Connect an Ethernet cable from a laptop to a new (or unused) node.
3. Apply power. After one minute when the node boots, ping it at 192.168.224.150.
4. Using HotView Pro, go to **Mesh > Add Mesh**.
   a. Enter 192.168.224.150.
      Ignore the country code warning if it appears.
   b. Enter the password.
   c. Click **Login**.
5. Right-click the node **> Re-Configure this Node to > Configure This Node as a Gateway Server**.

   A warning message appears, and then the node reboots.

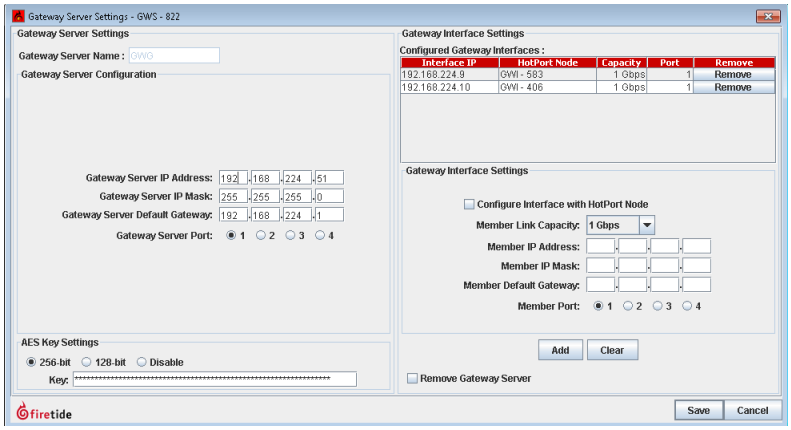
6. Log out of the mesh.

   The node IP address is 192.168.224.150.

7. When the node reboots, go to **Mesh > Add Mesh** to re-connect to the node.
8. Click **Apply Saved Mesh Configuration**.

   Note: The gateway group is not active until you apply the saved mesh configuration. When you apply the configuration, the system changes the IP address of the mesh.

9. Log out of the mesh.
10. Add the mesh at the new address.
11. Configure the tunnel IP addresses and other information in the Gateway Server:
    a. Right-click the Gateway Server node **> Gateway Server Settings**.



    b. Enter the IP addresses for endpoints of the gateway server tunnel.
    c. From the Member Link Capacity drop-down, select the data rate of the connection between the gateway interface node and the wired backbone. T

    Note: The nodes can operate at 1 Gbps, but the back-haul link can be slower. Setting the link capacity helps the gateway server do load balancing.

12. Manually configure one node, already on the mesh, to be a gateway interface node.
13. Log out of the gateway server mesh.
14. Physically disconnect from it, and then physically connect to the original mesh again.
15. Go to **Mesh > Add Mesh** to connect to the original mesh.
16. Right-click one of the nodes that will be a gateway interface node (not the current head node).
17. Disconnect the existing mesh connection.
18. Connect the new gateway interface node and the gateway server node with a switch.

19. Log out of the mesh.
20. Disconnect the cable from the head node to the switch.
21. Connect the Gateway Server node to the switch, then connect the Gateway Interface node you just configured to the switch.
22. From HotView Pro, go to **Mesh > Add Mesh** to connect to the mesh.
    If the configuration is correct, a solid green line appears between the gateway server node and the gateway interface node.

Redundant gateway server nodes

A second node can be a backup for the primary gateway server node. This is recommended for mission-critical networks.

Connect the backup gateway server node to a different power supply system, so that a power failure or UPS failure does not affect the device.

Also, do not use the same Ethernet switch as the primary gateway server.

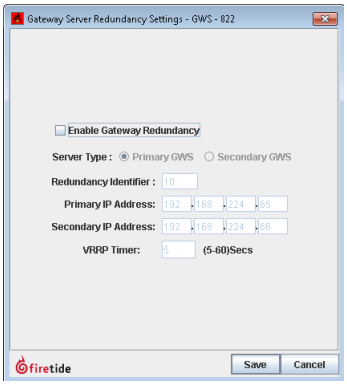
The redundant gateway server should have the same IP address, and the same values for the gateway interfaces.

Prerequisites: You configured a gateway group, and you confirmed that the gateway group is working correctly.

Note: You can only use an indoor node as a gateway server.

To configure a redundant gateway server:

1. Right-click the gateway server node **> Gateway Configuration > Redundancy Settings**
2. Select **Enable Gateway Redundancy**.
3. Select Primary GWS or Secondary GWS.
4. Enter these settings:
   a. Redundancy identifier, a number from 1 to 254. You must enter the same number for both gateway server nodes.
   b. Primary IP address
   c. Secondary IP address
   d. VRRP timer (The default value is 5. The range is 5 to 60.)
5. Click **Save**.



6. Verify that the mesh is still operating correctly.
7. Log out of the mesh.
8. Physically disconnect from the mesh.
9. To log into the mesh, go to **Mesh > Add Mesh**.
10. Click **OK**.

Fault tolerance and graceful network recovery

Firetide technology features detection and recovery from packet-delivery problems. This self-healing can be used to protect a wired connection with a wireless one.

A series of Firetide nodes are placed along a path that connects the two endpoints of the wired connection. The two endpoint nodes, and (optionally) nodes along the path, are connected and configured as a gateway group.

In normal operation, the gateway group algorithm uses the faster, wired path. However, if a part of the wired link goes down, the gateway group algorithm uses the wireless link to bridge the traffic.

Gateway server settings

1. Select the Gateway Interface that is not configured, and click the box below it that says **Configure Interface**.
2. Select the node from the drop-down that appears. Click **Apply**.
3. Repeat if necessary.
4. Click **Save**.

Gateway server redundancy settings

1. Right-click the gateway server node **> Gateway Configuration**
2. Specify the tunnel IP addresses for the connection between the redundant Gateway Servers.
3. To successfully bring up redundancy on a Gateway Server, the VLAN configuration should be identical.

A system-generated message appears when one gateway server configuration is different from the other.

Configuring a HotView Pro backup server

You can configure a backup HotView Pro server for mesh management.

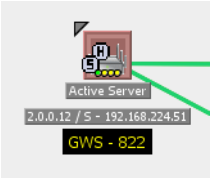
Prerequisite: Permanent management license for each server

Note: You cannot mix two systems. If you decide to transfer management licenses to the nodes in a mesh, you must do so to all nodes in the mesh.

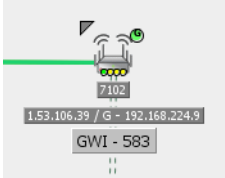
Mesh views and icons

HotView Pro has icons and different views to help system administration a visual task.

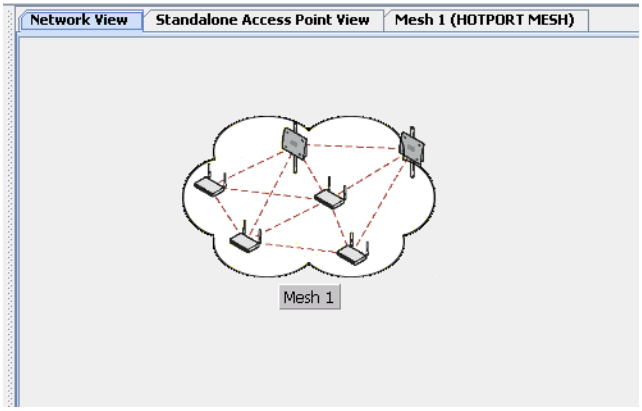
Gateway server icon. The next image shows a gateway server icon. It is a head node (H) because it has an Ethernet connection. It is marked S because it is a server. The one active port is green, and the three other ports are yellow. A gateway server only has one active Ethernet port. The two solid green lines that come from the node are active core wired links that terminate on a port of a gateway interface.



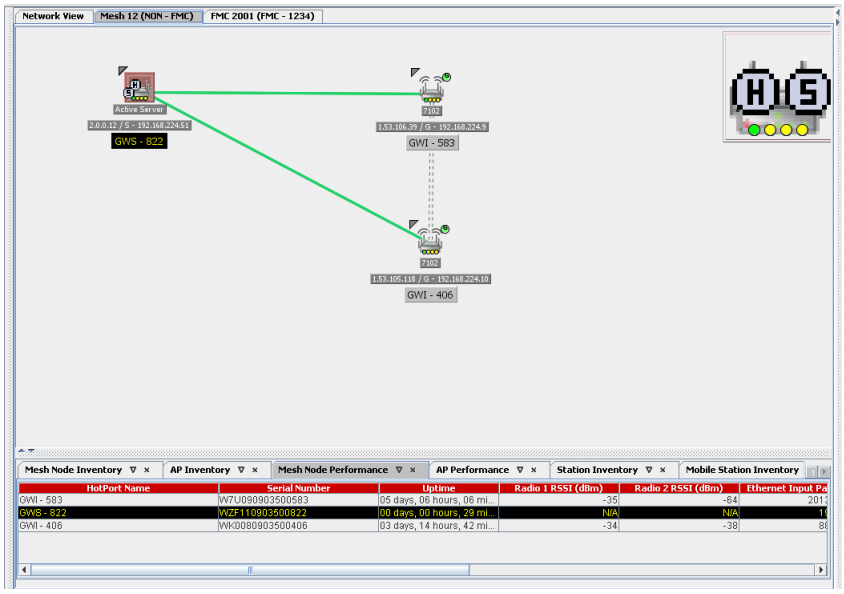
Gateway interface. A gateway interface mode has one connection to a gateway server and connections to other mesh or 5020-Es. The next image shows a gateway interface.



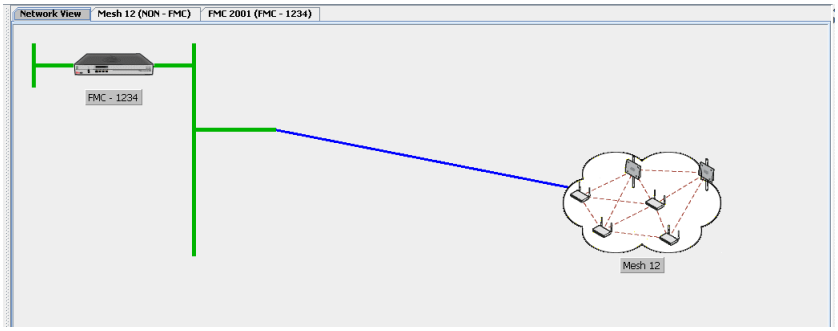
Network view. The next image shows a view of the network. You see this tab after you log in.



Mesh view. The next image shows the devices in a mesh network.



FMC view. The next image shows the network view for a mobility application that has an FMC device.



Ethernet Direct

Ethernet Direct is a software configuration and a wired Ethernet connection from a port on one node to the port of another node. Ethernet Direct connections can be used to make a mesh network. This helps enhance the throughput of the mesh network when nodes can be connected over Ethernet.

Each Ethernet Direct connection creates a separate Ethernet tunnel. Maximum number of tunnels is eight per port or per node.

You can enable the system to send the maximum packet size with the maximum transmission unit (MTU) setting. The MTU setting is disabled by default. Use of the MTU setting can make the connection more efficient.

You cannot modify an Ethernet Direct configuration entry. You must delete it and make a new entry.

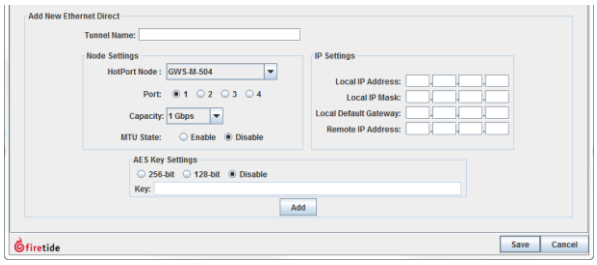
When you remove the Ethernet Direct configuration, the system disables the Ethernet ports that were used on the nodes. However, HotView Pro will not disable a port if more than one Ethernet tunnel exists.

Note that Ethernet Direct cannot be setup on a Hybrid Trunk Port or on a node used as a Gateway Server or a Network Gateway Interface.

Configuring an Ethernet Direct connection

To configure an Ethernet Direct connection:

1. Go to **Mesh > Ethernet Direct Connections**
2. Enter the tunnel name, which can be a descriptive name for this connection.
3. Enter the node settings:
   - Select the node on the near end of the tunnel from the drop-down list of discovered nodes
   - Port (1 to 4) from which you will install a wired connection
   - Capacity of the link (128 Mbps to 1 Gbps)
   - MTU state (enable or disable)
4. Enter the IP settings:
   - Local IP address
   - Local IP subnet mask
   - Local default gateway
   - Remote IP address
5. (Optional) Enter the security settings:
   - Select the key type: 256-bit AES or 128-bit AES.
   - Enter a key.
6. Click **Add**.



7. In a situation where a wireless connection between two nodes does not exist, click on **Save**.
8. Use HotView Pro and connect to the intended node for Ethernet Direct and follow steps 1 to 7.
9. In a situation where a wireless connection between two nodes intended for Ethernet Direct does exist, the next step is a continuation from step 6.
10. Select the tunnel entry in the Ethernet Direct Tunnel list at the top of the window.
11. Click **Mirror**.
    a. Enter the IP address of the gateway server and its subnet mask.
    b. Click **Add**.
12. At the bottom of the window, click **Save**.
13. Use an Ethernet cable to physically connect the ports that you logically configured.

Security on Ethernet Direct tunnels

Ethernet Direct tunnel connections support Advanced Encryption Standard (AES) 256-bit and 128-bit keys. By default encryption is disabled.

To enable AES key use on an Ethernet Direct connection, see "Configuring an Ethernet Direct connection" on page 78.

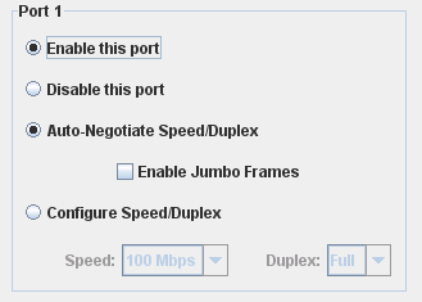
If you want to enable security on an already configured Ethernet Direct connection, you must delete the tunnel entry and configure the entry again.

Changing an Ethernet Direct connection

If you want to make a change to an already configured Ethernet Direct connection, you must delete the tunnel entry and configure the entry again. Saving your changes will not be possible if down nodes exist in a mesh. Delete all down nodes, if HotView Pro will not save your changes.

1. Go to **Mesh > Ethernet Direct Connections**
2. From the Ethernet Direct Tunnels list at the top of the window, select the tunnel entry.
3. Manually copy the information from the settings that you want to keep.
4. Click **Remove**.
5. A save is required before a new tunnel can be created.

6. Enable the Ethernet ports.
   a. Right-click the node in the mesh view **> Configure Node Port > Port Configuration**



   b. Select **Enable this port**.
   c. Click **Save**.
   d. Repeat steps a to c for the remote Ethernet Direct node.
7. After the ports have been enabled, refer to configuring an Ethernet Direct connection for steps on setting up a single tunnel entry or multiple tunnel entries.

Transfer of licenses

You always need to have a license for all devices that you manage. You might also need to move a license from one node to a replacement node. License transfer must be done with the Firetide online license server.

Before beginning, make sure your HotView Pro server system has Internet access or plan to make a copy of the license change file that the system generates to send to the Firetide online license server.

Types of Firetide product licenses

The next table shows types of product licenses and the device type for which they are available.

License type	HotPort mesh nodes	HotPort 5020-Es	Gateway server
Management	Yes.	Yes.	Yes.
Mobility	Yes for HotPort 7010/7020.	No. Mobility is not supported on 5020-Es.	Required for mobility.
Dual-radio	Yes. To be able to use RADIO 2, you must purchase and install a dual-radio license.	Yes. For the dual-radio model, the dual-radio license is pre-installed.	Required for mobility.
MIMO	Yes. To be able to use MIMO, you must purchase and install a MIMO license.	Yes. The MIMO license comes pre-installed.	Required for mobility.

Table 10

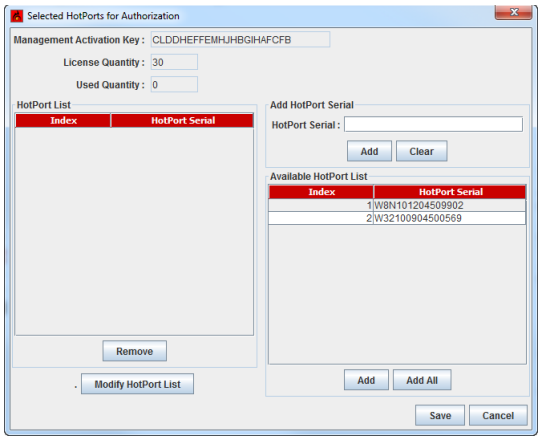
Note: Each HotPoint access point requires a management license whether or not they are integrated with a HotPort mesh node.

Applying a management license to a mesh node

Applying a management license to all mesh nodes in a mesh means that this mesh can be managed from a HotView Pro Server that does not have a management license. For this option to work, every node in a mesh must have an applied management license.

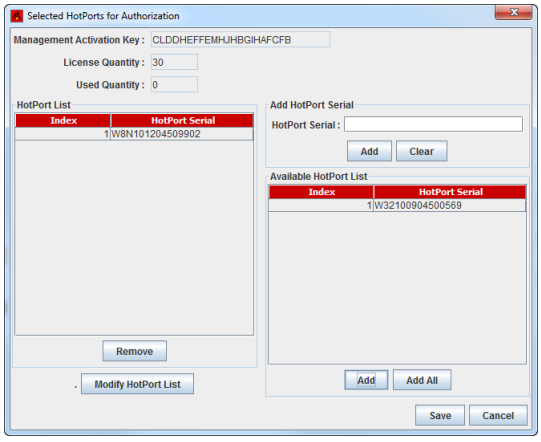
To apply a management license to a node:

1. Go to **Server Administration > Configure HotView Server > Licensing**
2. Select the management license table row.
3. Click **HotPort List**.
   A new window appears.



4. Select the node that needs a license.
5. Click **Add**.

6. Click **Yes** to confirm the license application.



The license is applied to the node, without a node reboot. From the mesh view, you can confirm that the license was pushed to the node by doing a right-click on the node, select HotPort License... and check License State for Enabled or Disabled for Management.

Installing license keys on an existing mesh

When you install new keys on an existing mesh:

1. Install keys to the farthest node.
2. Install the nodes closer to the node from which you are working.
3. Install the keys to the node from which you are working.

Modifying the HotPort List

If you have to replace a node, you can transfer licenses to a new or replacement node.

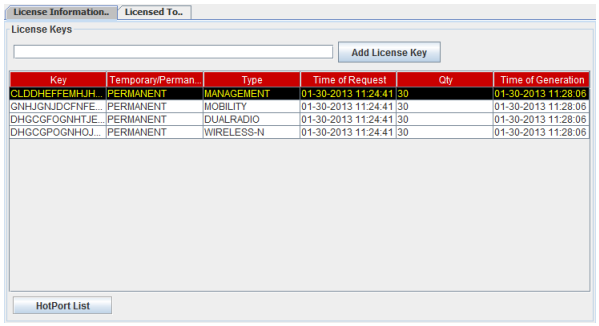
License transfer is a three-step process:

1. Transfer the license to the replacement node.
2. Send the change file to licensing@firetide.com. Firetide will process your request within 48 hours.
3. Import the file from Firetide Licensing.

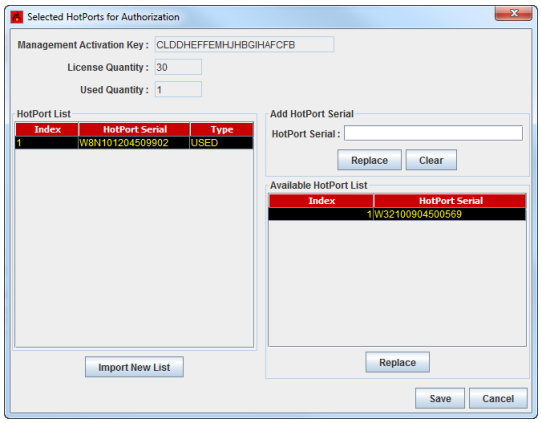
Best practice: Load the mesh into HotView, and then apply licenses.

To transfer a license to a replacement node:

1. Load the mesh into HotView Pro.
2. Go to **Server Administration > Configure HotView Server > Licensing**
3. Select the table row to show the type of license you want to transfer.



4. Click **HotPort List**.
5. Select the node which is being replaced, and then click **Add**.
6. Click **Yes** to confirm the selection.
7. Select the node that is going to receive the license. You have two options:
   - If it is an existing node, select the node from the Available HotPort List.
   - If it is a new node and is not powered up in the mesh, enter its serial number in the **Add HotPort Serial** field.

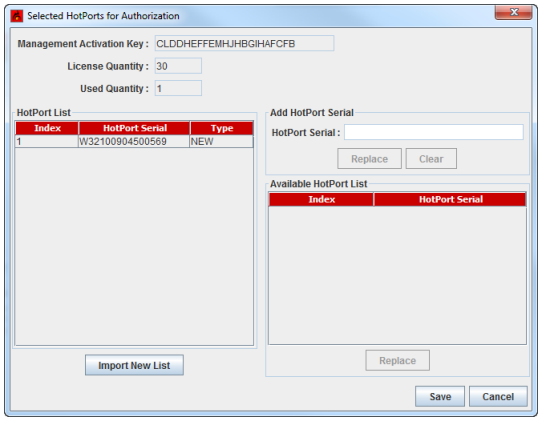


8. Click **Replace**.

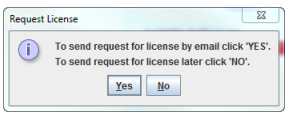
   When you click Replace, the system checks for available unassigned licenses. If you have at least one available license, the system replaces the serial number of the selected node in the HotPort List with the serial number of the selected node from the Available HotPort List. If you have no available licenses, you need to contact Firetide customer support for assistance.

9. Click **Yes** to confirm the addition of the node to the HotPort list.

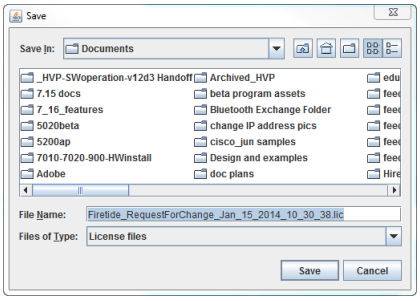
   The system replaces the old entry with the replacement node. The next image shows the replaced HotPort serial number with the Type "New".



10. Click **Save**.
11. Request a license change from Firetide Licensing.
    If you have Internet access, click **Yes**. If you do not have Internet access, click **No**.

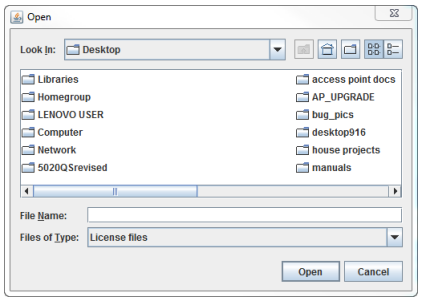


12. Do one of these steps:
    - Send the change file to licensing@firetide.com.
    - Save the change file locally, copy it to a machine that has Internet access, and then send the file to licensing@firetide.com.

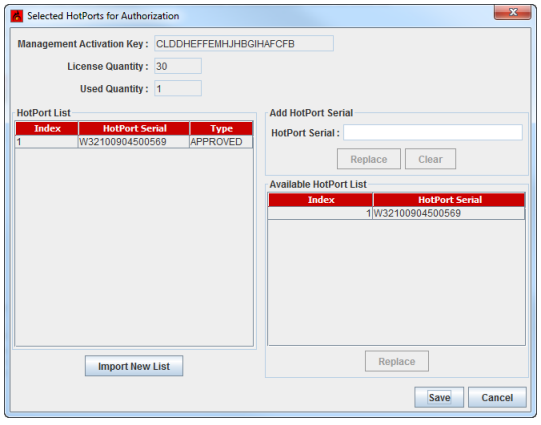


Within 48 hours, you will receive a change file with the updated licensing information.

13. After you receive the change file, save it locally.
14. In HotView Pro, go to **Server Administration > Configure HotView Server > Licensing**
15. Click **HotPort List**.
16. Click **Import New List**.



17. Browse to the change file, and then click **Open**.
    The system updates the type to "Approved".



18. Refresh the node configuration.
    After the node reboots, the license transfer process is finished.

Client preferences

HotView Pro lets you set a custom workspace for your network administrators:

Viewing all RF links in a mesh

Select **Show All Links** to see all of the active RF links in the mesh. This feature is enabled by default.

For larger meshes, too many RF links is difficult to interpret. To see fewer links, select **Show Links Only** or **Hide All Links**.

Finding a particular HotPort mesh node

Select **Find HotPort** lets you search for a node on the screen. The system highlights the node.

Selecting a new background image

You can select a different background image, such as a floor plan or site map. The background image must be:

- 1280 pixels wide x 1024 pixels high
- 4:3 aspect ratio. The system changes any other ratio to be 4:3.
- JPG or GIF

The inventory view covers the bottom part of the image.

Note: Firetide recommends that you use an image-editing program, such as Photoshop, to create a file of the correct aspect ratio. Make the bottom 25% of image empty or a solid color.

Note: To remove the background image, remove the check mark on the Show Background Image button.

To select a default background image:

1. Go to **Client Preferences > Default Background Image**
2. Select an image:
   - Indoor
   - Outdoor
   - Custom, and then **Browse** to the file

   A reboot HotView Pro server message appears.
3. Click **OK**.

   The system changes the background image.

Changing the select method to mouse-over

To change the node select method, select **Select HotPorts automatically on mouse-over**.

Viewing particular types of information

You can select to view these items:

- **Show All Inventory**
- **Show Background Image**
- **Show Information Bar** opens a large section on the right side of the display. This panel can be used to examine mesh settings and node settings.
- **Show Explorer Bar** opens a pane on the left side of the screen. This provides a hierarchical view of all meshes, nodes, and other equipment.
- **Show Status Bar** shows a status bar at the bottom of the display window.
- **Show Model Number** shows the model number under each node's icon.
- **Show HotPort mesh node IP Address** reveals the hidden internal addresses nodes use among themselves. These are not visible or accessible from outside the mesh, and they cannot be routed. They are used for internal tests only.
- **Show Node Status** adds additional information to the node icon, such as whether it is a Gateway Interface node. You should turn this option on.
- **Show Selected HotPort Radio Info** shows the Radio 1 and Radio 2 settings for each node when you click on the node. This is useful in multi-channel mesh designs.
- **Shows Notes** shows notes.
- **Show APs**, **Hide Down APs**, and **Show Standalone APs**.
- **Show Mesh Configuration Conflicts** checks the settings on each node to make sure they are in agreement.
- **Show HotClient View Tab** opens a new tab which shows all CPE equipment.

Troubleshooting HotView Pro software and mesh issues

This section lists problems and potential solutions.

Problem	Possible solution
Cannot ping the HotView Pro server	Make sure that the required ports are open. Clear the ARP cache and ping again. To clear ARP cache: 1. Verify administrator privileges. 2. Open a command prompt. 3. Type: arp –d <mesh ip>
HotView client cannot connect to the HotView Pro server	Make sure you can ping the server. Check the firewall settings.
Installation does not finish	If installation takes longer than 5 minutes, or does not finish, check the version of Java. For stable performance, you must use Java 7 or Java 8 (32-bit). See table in this guide for specific versions of Java.
Cannot see Remove or Remove All buttons	When you view shortened windows, you cannot see the whole display. Expand the window to see the Remove or Remove All buttons.
You do not know the IP address of the mesh	If you do not know the mesh IP address, you can use a utility to discover it, such as Advanced IP Scanner at http://www.advanced-ip-scanner.com/ or Angry IP Scanner at http://www.angryip.org When you use these tools, make sure you turn off the wireless features of the laptop from which you run the utility.

Problem	Possible solution
Cannot log into HotView Pro server	• Make sure you can ping the server machine. If the server process is running on the same machine (such as your laptop) you may need to use 127.0.0.1, the loopback address, instead of your machine's actual IP address. Some systems do not recognize their own IP address if the network is not connected. • Verify that the server process is running. You should see two javaw.exe processes, one for the launcher program and one for HotView Pro itself. • If a firewall is between the client computer and the server, you need to open ports in the firewall. See "Ports that HotView Pro software uses" on page 7. • If your login credential is correct, but the program says it is not correct, the login file might be corrupt. Delete the NmsUsers.xml file to correct the problem.
Cannot shut down HotView server	Open the task manager, and then stop all Java processes.
Cannot apply license or fill out Licensed To form	• If you are on a multi-user PC and are not running HotView Pro as the administrator, you cannot add a license. • If you are on a multi-user PC and are not running HotView Pro as the administrator, you cannot use the Licensed To form. You must run the program as the administrator, and then fill out the form.
Cannot add a mesh to HotView Pro	• Make sure you can ping the mesh. The ping must be from the server machine and not from the client. • Make sure that the ports required by Firetide products are open. See "Ports that HotView Pro software uses" on page 7.
A port is not working	• Make sure that the port is enabled. Enable the port if necessary. • Check the cable.

Problem	Possible solution
Node missing from mesh (down nodes)	• Ping the node • See "Forcing node discovery" • If you cannot see one or more mesh nodes in HotView Pro, make sure that you set the extended range and multiple hop feature. The extended range feature is for applications where mesh nodes are 0.8 km (0.5 mile) or more apart. The multi-hop optimization feature decreases the possibility of packet collisions. If you can see the head node but not other nodes, then you also might have a configuration problem.
During staging tests the head node is visible in the network view but one or more nodes are not visible	• Make sure that all of the nodes are running the same active image. • Make sure that the radio channels are configured correctly. • Make sure that you have staging antennas on Radio 1/connector 1 and Radio 2/ connector 1 for each node. • If indoors and the nodes are close together, decrease the radio transmit power to 50%. • You might have another configuration problem.
After multiple reboots a mesh node is missing	If a mesh node reboots five times within 10 minutes, the mesh node loads the second saved firmware image. The previous firmware, if older or different from the firmware of the other mesh nodes in a mesh network, might not be recognized by the mesh and HotView Pro will not detect the mesh node. To prevent this behavior, always upgrade the firmware image on each mesh node two times, so both images are the same.

Problem	Possible solution
Poor mesh performance	• Check for RF problems with the Statistics panels and diagnostics tests (Iperf). • Make sure you enabled multi-hop optimization. • Make sure the extended range is longer than the longest link in your mesh. • Record the RSSI levels for each link. RSSI levels close to or below the absolute minimums cause performance issues. • Run a UDP Iperf test across each link, and record the throughput. If the throughput is low, the receiving end probably has a problem. • Check the number of dropped packets and number of retries. If either value is more than 1% of the total packets sent, interference exists.
Hardware in network is not working correctly.	• Use MAC address filtering to block traffic from the hardware that is not working as expected.
Installing license keys	When you install new keys on an existing mesh: 1. Install keys to the far node. 2. Install the keys to the node from which you are working.
Invalid license message	Save the License To information during the permanent license request process.
An access point does not change to use 5 GHz radio	In a wireless distribution system configuration if you remove and then install the Ethernet cable, the access point does not change to the 5 GHz radio. When you enter the serial number of a new access point: 1. Click on the relay station and compare the configuration to the new access point. 2. Edit the VAP group. 3. Add the new access point and click **Save**. Go to **Access Point > Configure VAP,** and click **Save**.
Online DFS authentication failed	Use the offline DFS authentication method.

Problem	Possible solution
Node configuration restoration failed	Node configuration restoration fails when the system detects mismatched: • Country codes • Model number • Firmware (version is later than that of the selected node)

Table 11

Forcing node discovery

If one or more nodes fail to join the mesh after five minutes, you can try to recover the node. When you recover a neighbor node, the system recalculates the whole mesh. The mesh loses the radio channel plan. To recover from a mesh recalculation, reboot each node individually.

To force discovery of a missing node:

1. Select a node that is geographically close to the missing node.
2. Right-click the node, and then select **Advanced Tools > Attempt to Recover Neighbor Node**.
3. Reboot each node individually.

If you recently changed a mesh setting, change it back to the original settings and see if the node joins the mesh. If it does, try the change again.

When changing radio settings, it is often best to change just one setting at a time. For example, when changing the bonded-mode mesh-wide radio settings, change Radio 1, and then make sure all nodes joins the mesh before changing Radio 2.

If you cannot recover the node, follow these steps:

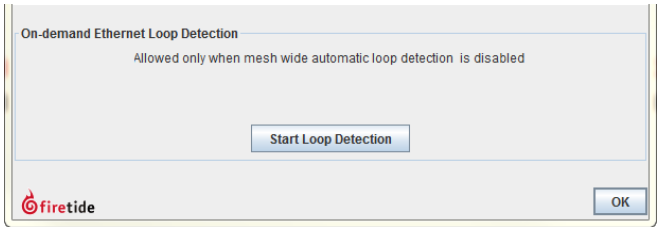
1. Connect to it directly through an Ethernet connection.
2. Change its settings to match those of the rest of the mesh.
3. Import the mesh settings from the head node, and then log out of the mesh.
4. Connect directly to the down node. Use the ping command to check the IP address. If you do not know the IP address of the node, press the reset button with a paper clip for about 15 seconds.

Detecting an Ethernet loop

The system detects Ethernet loops automatically. If you disable loop detection, you can use the manual loop detection feature.

To use on-demand Ethernet loop detection:

1. Go to **Tools > Ethernet Loop Detection**.
2. Click **Start Loop Detection**.
3. Click **OK** when finished.



Link throughput tests

HotPort mesh nodes have a built-in link throughput tool.

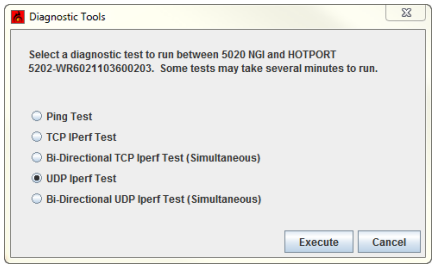
The Iperf test is a deployment diagnostic tool and is not a performance benchmark test. The results are indicative of baseline performance, but actual throughput performance can be higher.

To measure link throughput performance:

1. Right-click on one of the two nodes between which you want to measure performance.
2. Select **Run Diagnostics Tools**, and select the second node from the menu.

   A window appears from which to select a test:

   - Ping. A ping test checks for a link between the nodes. It does not generate enough traffic to affect mesh operation. The ideal result is a low, consistent, ping response time. Highly inconsistent times indicate RF signal problems.
   - TCP Iperf and bi-directional TCP Iperf. Both tests send a large amount of TCP traffic between the nodes on one link. The bi-directional test runs the test traffic in both directions simultaneously.
   - UDP Iperf and bi-directional UDP. Both tests run a large amount of UDP traffic between the nodes on one link. The bi-directional test runs traffic in both directions simultaneously.
3. Select the type of test.
4. Click **Execute**.



Note: Iperf tests flood a link with as much traffic as it can carry. This can disrupt other traffic on the mesh. Iperf sends a large, fixed amount of traffic. If iperf cannot complete the transfer in a fixed period of time, it stops. If you receive a failure message, run the test again. If the test fails consistently, substantial interference exists on the RF link.

Resolving interference issues

Ensure that the source of the interference is not the other radio in the node or from poor antenna orientation.

Use the Spectrum Analyzer feature and a directional antenna to locate the source of the interference. When you find the direction of maximum signal strength, rotate the antenna to change its polarization from vertical to horizontal or horizontal to vertical as necessary. Alternately, you can use other spectrum analysis equipment to look for sources of interference.

After you locate the approximate direction and polarization of the interference, you can:

- Use more-directional antennas to minimize interference, or aim the antennas you have to minimize pickup.
- Change antenna polarization to the opposite of the interference source.
- Change operating bands. Changing channels within the band can help, but inter-channel rejection within one band is not good.
- Add a single-channel bandpass filter to the antenna lead. These devices are selective and can eliminate interference. Contact Firetide for options and resellers.
- Move the equipment out of the path or range of the source of the interference.

Powerful microwave transmitters, such as those used by television satellite uplink equipment, emit a strong enough nearby field that it is difficult to get 802.11 equipment to operate reliably if it is near such transmitters.

Using Telnet and SSH

You can use telnet or SSH to connect to the head node of a mesh. The account name is ftusr, and the password is ftu5r. After you connect to the head node, you can then telnet to other nodes in the mesh as necessary for testing.

Quadritarium:~ admin$ ssh 192.168.224.20 -l ftusr

ftusr@192.168.224.20's password:

Welcome to Firetide Command shell

ftsh >> help

Firetide Command Shell Usage

show :This command tells ftsh to get some information

conf :This command tells ftsh to set some information

perf :This command takes to Performance menu

table :See the various tables in the node

stats :This command takes to Statistics menu

telnet:telnet to a node. telnet <Node IP addr>

ssh:Set up SSH session to a node. ssh <Node IP addr>

help:This command prints this help

exit:Quit/Exit Firetide Command Shell

The perf command lets you run Iperf from the command line. You can write scripts on your computer to connect and run various types of tests across multiple links simultaneously.

Troubleshooting multicast issues

These tables show the reserved addresses used for various multicast functions and Ethernet MAC addresses. Ensure that your network does not use reserved addresses for anything but the intended purpose.

IPv4 address	Purpose
224.0.0.0	Base multicast address
224.0.0.1	All hosts multicast group
224.0.0.2	All routers
224.0.0.4	Distance vector multicast routing protocol (DVMRP)
224.0.0.5	All OSPF routers
224.0.0.6	All D routers
224.0.0.9	RIP version 2 group address
224.0.0.10	EIGRP group address
224.0.0.13	Protocol independent multicast (PIM)
224.0.0.18	Virtual router redundancy protocol (VRRP)
224.0.0.19to .21	IS-IS over IP
224.0.0.22	IGMP version 3
224.0.0.102	Hot standby router protocol version 2 (HSRPv2) and gateway load balancing protocol (GLBP)
224.0.0.107	Precision time protocol version 2 peer delay measurement messaging
224.0.0.251	Multicast DNS (mDNS) address
224.0.1.1	NTP clients
224.0.1.39	AUTO-RP-ANNOUNCE address
224.0.1.40	AUTO-RP-DISCOVERY address

IPv4 address	Purpose
224.0.1.41	H.323. gatekeeper discovery address
224.0.1.129 to .132	Precision time protocol version 1 time announcements
224.0.1.129	Precision time protocol version 2 time announcements
224.0.1.133 to 239.255.255.255	Available for multicast groups

Table 12

Ethernet MAC address	Type field	Purpose
01-00-0C-CC-CC-CC	0x0802	Cisco discovery protocol (CDP), VLAN trunking protocol (VTP)
01-00-0C-CC-CC-CD	0x0802	Cisco shared spanning tree protocol address
01-80-C2-00-00-00	0x0802	Spanning tree protocol (for bridges) IEEE 802.1d
01-80-C2-00-00-08	0x0802	Spanning tree protocol (for provider bridges) IEEE 802.1ad
01-80-C2-00-00-02	0x8809	Ethernet OAM protocol IEEE 802.1ah
01-00-5E-xx-xx-xx	0x0800	IPv4 multicast (RFC 1112)
33-33-xx-xx-xx-xx	0x86DD	IPv6 multicast (RFC 2464)

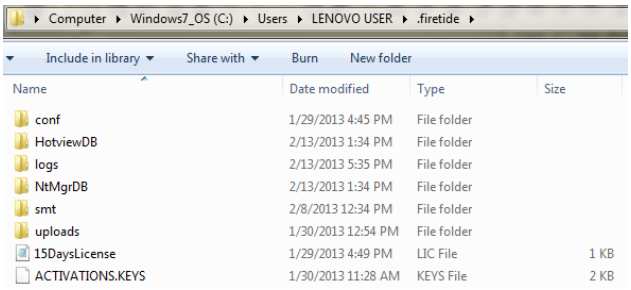
Table 13

User accounts and server directory structures

This section explains the server and user directory systems.

Best practice: When you install HotView Pro to the production server, create a user account for HotView Pro. Do not run HotView Pro under your ordinary personal user account. To create a new user account, refer to Microsoft help.

The HotView Pro software creates a .firetide directory in the home folder of the account under which it is installed. If you are running Windows 7, the path to the is C: > Users > *HotView Pro* > .firetide



This directory contains:

- License files and keys
- Log files
- Other installation-specific data

If you log in as another user on the server machine and launch HotView Pro, it creates a new .firetide directory in that account's home folder.

User account directory structure

HotView creates a subdirectory called .firetide in the user's home directory. This contains:

- User IDs
- Passwords
- License keys
- Installation-specific data

When you delete HotView Pro from a computer, the uninstaller does not delete this directory. If you need a clean installation, you have to manually delete this directory.

Best practice: To save the directory and have a clean installation, put the directory within another directory to keep the data.

Moving licenses from one system to another

A management license has to be installed on the computer from which you run HotView Pro.

To clear the license information from an old computer and submit a request to license a new system:

1. From the computer that contains the license information, go to the C: drive or the main drive where HotView Pro is installed:
   - If using XP, go to the Documents and Settings folder.
   - If using Vista, Windows 7 or 8, go to the Users folder.

2. Open the profile that contains the HotView software, and locate the .firetide folder.
3. If you do not have a copy of the key:
    a. Open the Licensing tab in HotView.
    b. Copy the line that contains your key or keys (use Ctrl + C) and paste it into a text editor, such as Notepad.
    c. Save the key file.
4. Shut-down HotView Pro software and all processes that use Java and javaw.exe.
5. Delete the .firetide folder.
6. From the new computer, install HotView Pro software.
7. Enter the management license key that you copied from the old computer.
8. Activate the license key.
9. Enter the License To information, and submit a new request for a permanent license.

HotPort mesh node configuration

This section contains these chapters:

- Mesh-wide node configuration
- Mesh node-specific settings
- HotPort 5020-M Mesh node-specific settings
- 5020-Esettings

Mesh-wide node configuration

This section contains the network-wide mesh configuration settings.

Adding a mesh

HotView Pro starts to manage a mesh after you add it. The system records device and network performance data and events until you explicitly remove the mesh from management control.

If you want to load a mesh individually, remove the check from the Pre-Load Mesh feature.

Note: When the Pre-Load Mesh feature enabled, HotView Pro can keep the configuration information for many meshes. It can save you time if you want to monitor or make small changes. If you want to load a new mesh or make many changes to only one mesh, the Pre-Load Mesh feature can cause you to wait while the information for all meshes loads.

The default or factory new management IP address is 192.168.224.150.

The login information for the two default administrator accounts is:

- Read-write access: admin/firetide
- Read only access: guest/guest

To add a mesh:

1. Go to **Mesh > Add Mesh**
2. (Optional) Check the **Pre-Load Mesh** feature.
3. Enter this information:
   - Management IP address
   - User name
   - Password
4. Click **Login**.

Setting the country code

If you have a new mesh, the first thing to do is set the country code.

Note: If you set the country to USA and then you set the node to factory default settings, the country code will stay set to USA.

You want to set the country code to change the devices in a mesh from low-power, low range device mode to a correct full-power operational mode.

Caution! Make sure you configure the device for the correct country. If you do not configure the country correctly, the device might operate in a manner that is not legal or create problems with other wireless devices.

For information about default radio settings by country, see "Worldwide default radio assignments" on page 4-21.

To set the country code for a factory new device:

1. Log into the mesh network.

   The first time you log into a new mesh and until you set the country code, periodically the system prompts you to set the country code.
2. From the drop-down list, select the country in which you intend to operate the device.
3. Click **Save**.

Mesh configuration

Mesh configuration includes the following types of settings:

- Network
- Wireless
- Security
- User accounts
- Advanced

Bonded mode

By default each radio of a node is in bonded mode. Bonded mode settings apply to the entire mesh network. Bonded mode ensures:

- Automatic link formation between two or more nodes
- Correct radio channel assignment with neighbor nodes
- Higher throughput on the link

Configuring mesh and mobility settings

Mesh settings include:

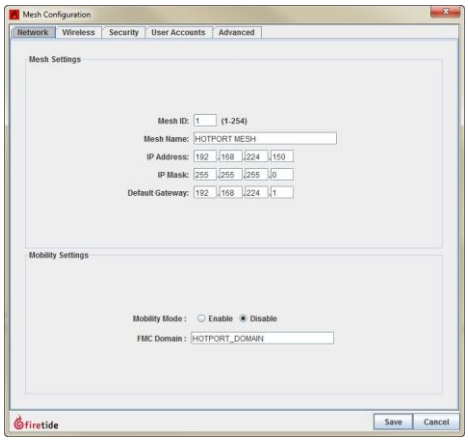
- Mesh ID, a unique number for this mesh. Values can be 1 to 254.
- Mesh name, a string of up to 32 alphanumeric characters. You can use names meaningful to your environment. The system does not use this name to identify the mesh.
- IP address is an IPv4 address.
- Subnet mask is an IPv4 mask.
- Default gateway is the IPv4 address of the gateway.

Mobility settings include:

- Mobility mode, which can be enable (for mobility) or disable. The default setting is disable.
- FMC domain, is the name of the domain from which the FMC manages this mesh.

To configure a mesh and mobility settings:

1. Go to **Mesh > Configure Mesh**
2. Enter the settings.
3. Click **Save.**



Wireless contention control

Wireless contention control reduces the overall number of collisions in the air and increases the cumulative throughput when multiple contending transmitters are present.

This is a mesh-wide configuration setting.

To configure wireless contention control on a mesh:

1. Right-click on the **Mesh** & select **Configure Mesh**
2. Select **Advanced** tab
3. “Enable Contention Control” by clicking the check box.

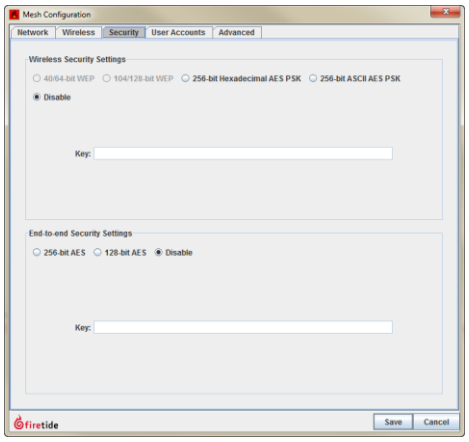
Configuring wireless security settings

Wireless security protocols to ensure security include:

- 256-bit hexadecimal AES PSK
- 256-bit ASCII AES PSK

To configure wireless security settings for a mesh:

1. Go to **Mesh > Configure Mesh**
2. Select the wireless security protocol that you want to use.
3. Enter the security key.
4. Click **Save**.



Configuring end-to-end security

End-to-end security is a mesh-wide setting. The system lets you configure a 128-bit or 256-bit AES key. End-to-end security works with or without wireless security or tunnel encryption enabled. End-to-end security is disabled by default.

Note: When this feature is enabled, some performance decrease might happen.

To configure end-to-end security for a mesh:

1. Go to **Mesh > Configure Mesh**
2. Select type of AES key to use: 128-bit or 256-bit.
3. Enter the security key.
4. Click **Save**.

Configuring a mesh user account

For each mesh, you have to assign a secure machine login for read-write access and a login for read only access.

To configure a user account:

1. Go to **Mesh > Configure Mesh >** Click the **User Account** tab

2. In the correct role, enter the user name and password two times.
3. Click **Save**.

Configuring wireless settings

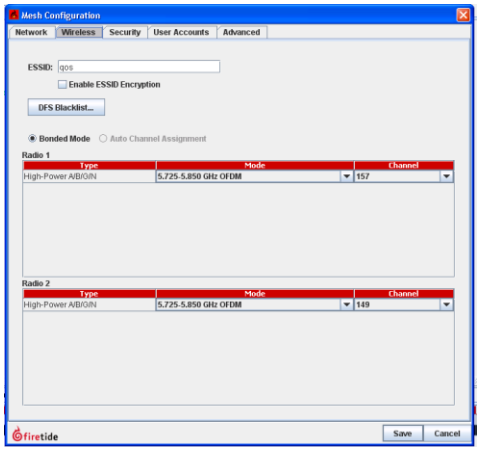
The wireless settings tab is where you configure the following items:

- ESSID is an identifier for a wireless station. The ESSID can be a descriptive name. To prevent others from learning the name of a specific station, you can check the ESSID encryption box. If someone eavesdrops the ESSID appears as a meaningless string.
- Bonded mode, which is a mixed mode for channel assignment.

Note: For some radios you need a license to be able to set them.

To configure wireless settings:

1. Go to **Mesh > Configure Mesh >** Click the **Wireless** tab
2. Enter the ESSID.
3. (Optional) Check **Enable ESSID encryption**.
4. Select the operational mode and channel for radio 1 and radio 2.
5. Click **Save**.



Configuring advanced mesh features

Advanced mesh features include:

- Multi-Hop Optimization

  Multi-Hop Optimization enables a Request-to-Send/Clear-to-Send handshake to avoid collisions in networks with more than two nodes.

- Wireless Class-of-Service

  By default, a mesh handles all packets with the same level of service. Packets that enter the mesh from the Ethernet side can have different priority settings. If a packet has no priority setting, you can use a combination of

wireless class-of-service and port-based priority tagging to assign a priority.

Enable Wireless Class-of-Service is a mesh-wide parameter that lets all nodes within a mesh use class-of-service rules, even if the node does not route priority traffic. If you want to honor packet priority levels, enable this feature.

- Enable Interoperability

  Enable Interoperability lets communication between 6000 Series and 7000 Series nodes occur (disabled by default).

- RSSI threshold value

  A link does not form between two nodes when the RSSI value is below the RSSI Threshold Value. Enforcing the threshold value avoids link fluctuations. The hysteresis value defines how far above the threshold the signal must be before a link between two nodes can form.

  For example, if the RSSI threshold value is -85 dBi and the hysteresis value is 3, when the link goes down (breaks), the system does not let the link become available until the value is -82 dBi or betterk.

- Noise Floor Threshold

  Noise Floor Threshold is a mesh-wide setting used to tune the network in noisy RF environments. The radios determine if a signal is noise or a real signal. They estimate the average in-band power of a number of samples taken during quiet periods. The threshold sets a floor for this value for better network stability and improved performance. The next table lists the settings, corresponding floor values, and the environments in which to use each setting.

Environment	Setting	Floor value
Quiet	Normal	-96 dbm (default setting)
Some noise	Medium	-91 dbm
Noisy	Aggressive	-87 dbm

- Enabling STP BPDU switching

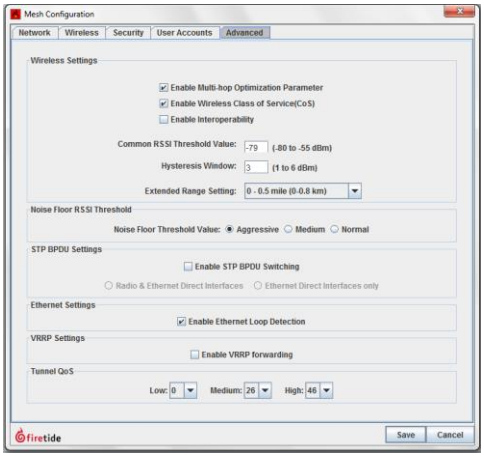
  By default a mesh does not transmit multicast traffic. If you need a mesh to transmit multicast traffic, you can enable the spanning tree protocol (STP) bridge protocol data unit switching (BPDU) feature. You can also control whether the multicast traffic stops at Ethernet Direct interfaces or goes to the wireless interfaces.

- Ethernet Loop Detection
- Virtual Router Redundancy Protocol (VRRP) frame forwarding
- Tunnel QoS

To configure advanced mesh features:

1. Go to **Mesh > Configure Mesh >** click the **Advanced** tab

2. Enter the settings.
3. Click **Save**.

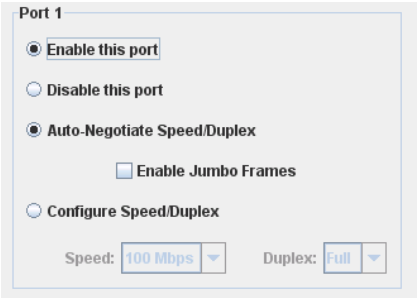


Sending jumbo frames

Ethernet jumbo frames are Ethernet frames with more than 1500 bytes of payload. HotPort 7000 mesh nodes support Jumbo Ethernet frames that contain up to 1840 bytes of payload.

To enable a HotPort 7000 node to send and receive jumbo frames:

1. Right-click the mesh node **Configure Node Port > Port Configuration**
2. Select a port (for example Port 1) and these features:
   - Enable this port
   - Auto-Negotiate Speed/Duplex
   - Enable Jumbo Frames
3. Click **Save**.



Multi-node radio settings tool

The Multi-Node Radio Settings Tool lets you apply radio-specific settings to multiple nodes at the same time. For example, you can set Radio 2 on several nodes to a new frequency or reduce the transmit power for several nodes.

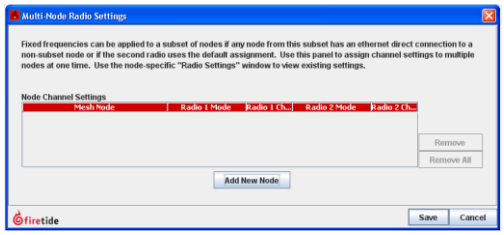
Best practice: Change one radio at a time. Changing the settings on both radios at the same time creates a risk of failure.

Note: It is common practice to set the radio data rate to a value slightly less than the maximum for that radio mode. You might set 802.11a to 36 Mbps instead of 54. This reduces jitter caused by the node shifting data rates.

To use the multi-node radio settings tool:

1. Go to **Tools > Multi-Node Radio Settings**.
2. Click on **Add New Node**.

   A node-specific radio settings window appears.
3. Select the node, and then make changes.
4. Repeat for as many nodes as you need.
5. Click **Save**.



VLANs

A virtual LAN is a software solution to provide network segmentation.

Firetide products support these types of VLAN port configurations:

- Access port (access mode)
- Trunk port
- Hybrid trunk port

You can use a mesh network with a VLAN configuration to replace a fiber connection. Depending on the networks that you want to connect the VLAN configuration might be a trunk or hybrid trunk VLAN configuration.

VLAN settings apply to ports. The settings apply to the ingress or egress traffic as it relates to the port. The settings apply to one mesh.

Note: For more information about VLAN standards, refer to IEEE 802.1Q and IEEE 802.1p.

Note: Some vendors use the term *bonded* for *trunk*.

Access port configuration

Some computer equipment, such as IP cameras, cannot generate VLAN-tagged traffic. In this case, you can configure an access port to add a tag. When traffic enters the access port with a primary VLAN, the system includes a tag with the VLAN ID in the Ethernet frame and forwards it.

If you configure more than one VLAN, you can select one VLAN to be the primary VLAN. When you select a primary VLAN, the system gives an ingress Ethernet frame that has no tag the primary VLAN tag. At egress two results are possible:

- The system removes the tag and forwards the Ethernet frame.
- If you selected the optional "Tag this port" feature, the system does not remove the tag and forwards the Ethernet frame with the tag.

The next table shows native VLAN behavior.

Frametype	Ingress port behavior	Egress port behavior
Tagged	Discards all tagged frames	—
Untagged	Adds the native VLAN tag and forwards the frame	Removes the tag and forwards the frame

Table 14

The next table shows the behavior for a VLAN configured with a VLAN ID of *x*, which can be 2 to 4094.

Frame type	Ingress port behavior	Egress port behavior
Tagged	· Tag = x: forwards the frame · Tag is not x: discards the frame	tag = x: forwards the frame · "Tag this port" is checked, the frame keeps the tag · "Tag this port" not checked, the system removes the tag before it forwards the frame
Untagged	Discards all untagged frames	Untagged frames: —

Table 15

The next table shows the behavior of two or more VLANs. This example is VLAN tags *x*, *y*, and *z* where each tag is a unique number between 2 and 4094. VLAN *x* is the primary VLAN.

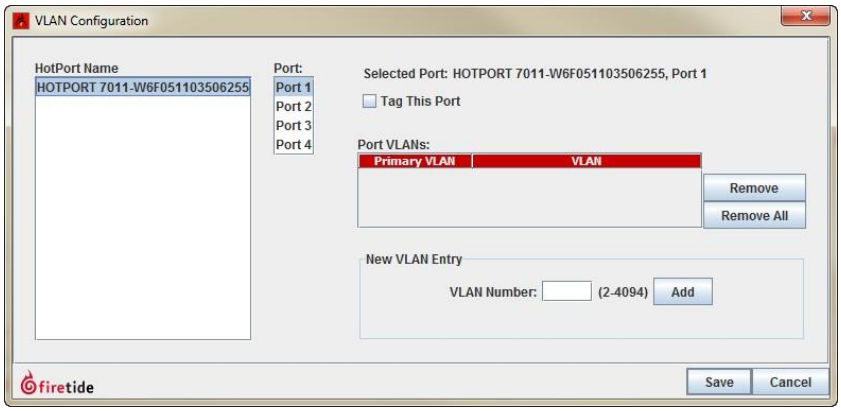
Frame type	Ingress port behavior	Egress port behavior
Tagged	· Tag = *x*, *y*, or *z*: forwards the frame · tag is not *x*, *y*, or *z*: discards the frame	· tag = *x*, *y*, or *z*: forwards the frame · tag is not *x*, *y*, or *z*: discards the frame
Untagged	Adds the primary VLAN tag and forwards the frame	Discards the frames

Table 16

Configuring an access port

To configure an access port:

1. Go to **Mesh > VLAN**
2. Click **Edit VLAN Interface**.



3. Select a node and a port on that node.
4. (Optional) Select **Tag This Port**.
5. Enter a VLAN number (VLAN ID), and then click **Add**.
6. Click **Save**.

Trunk port configuration

A VLAN trunk is a connection between two switches that carries traffic from multiple VLANs. The system does not drop frames in a trunk port configuration. These settings apply only to ingress frames.

You can configure a trunk port to be a native or management VLAN. If untagged traffic arrives on a trunk port, the system assigns the traffic default native tag or the management VLAN ID.

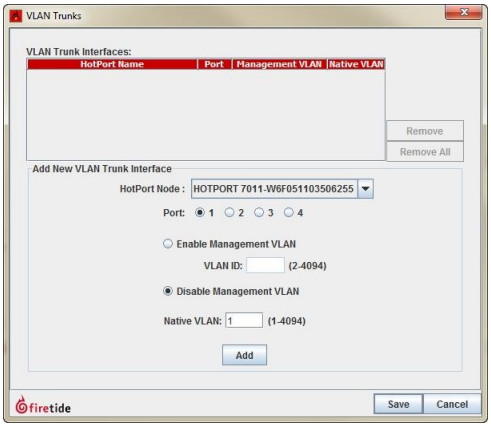
Management VLAN is for HotView Pro management data. A native VLAN is for client data. The next table lists VLAN trunk behavior.

Frame type	Ingress port behavior	Egress port behavior
Tagged	Forwards all frames	Forwards all frames with tags
Untagged	Adds native VLAN tag (1 by default, but the tag can be a custom number) and forwards the frame	Forwards all frames with the native VLAN tag

Configuring a VLAN trunk port

To configure a VLAN trunk port:

1. Go to **Mesh > VLAN**
2. Click **Edit VLAN Trunks**.



3. Select a node and node port.
4. Enable Management VLAN or Native VLAN.
5. Enter a VLAN number (VLAN ID):
   - Management VLAN can be 2 to 4094.
   - Native VLAN can be 1 to 4094. The default value is 1.
6. Click **Save**.

Hybrid trunk port configuration

If you want to send tagged and untagged frames, you have to use a hybrid trunk port. When you enable the port, tagged frames that come into the port keep the tag; and frames without tags forwarded without tags. By default, hybrid trunk ports are disabled.

A hybrid trunk is designed to have these settings, which cannot be changed:

- Management VLAN =1
- Native VLAN = 1

When a hybrid trunk is configured on a port, that port cannot be configured with management VLAN or native VLAN settings.

The next table lists the default hybrid trunk port behavior.

Frame type	Ingress port behavior	Egress port behavior
Tagged	Forwards all frames	Forwards all frames
Untagged	Forwards all frame	Forwards all frames

Table 17

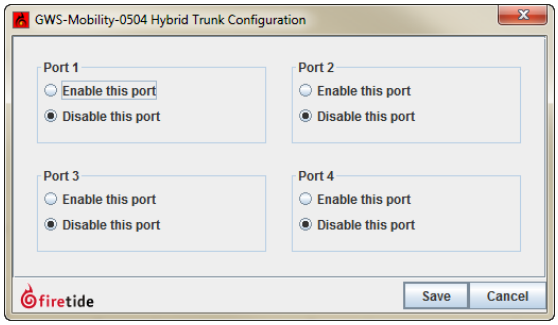
Enabling a hybrid trunk port

To enable a hybrid trunk port:

1. Right-click the mesh node, and then go to **Configure Node Port > Hybrid Trunk Configuration**

Note: If you want to change from one port to a different port, select "Disable this port" and then click **Save**.

2. Enable the correct port.



3. Click **Save**.

Configuring VLAN settings for multiple mesh nodes

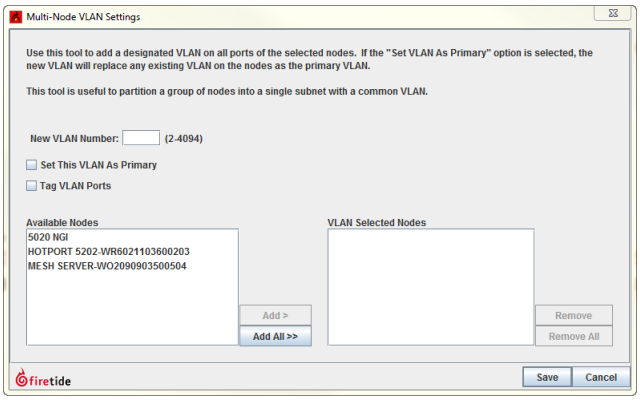
Multi-Node VLAN Settings lets you add a VLAN on all ports of the mesh nodes that you select. You can use this tool to make a group of mesh nodes into a single subnet with a common VLAN.

The optional features are:

- Tag VLAN Ports: If you select this feature, the egress frames keep the VLAN tags.
- Set This VLAN as Primary.

To use the multi-node VLAN settings tool:

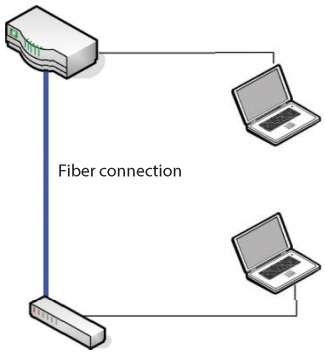
1. Go to **Tools > Multi-Node VLAN Settings**.
2. Enter a new VLAN number (VLAN ID).
3. (Optional) Select **Set this VLAN as Primary**.
4. (Optional) Select **Tag VLAN Ports**.
5. Select the node and click **Add**, or click **Add All** to select all of the nodes.
6. Click **Save**.



Example: VLAN and wireless connection to replace fiber

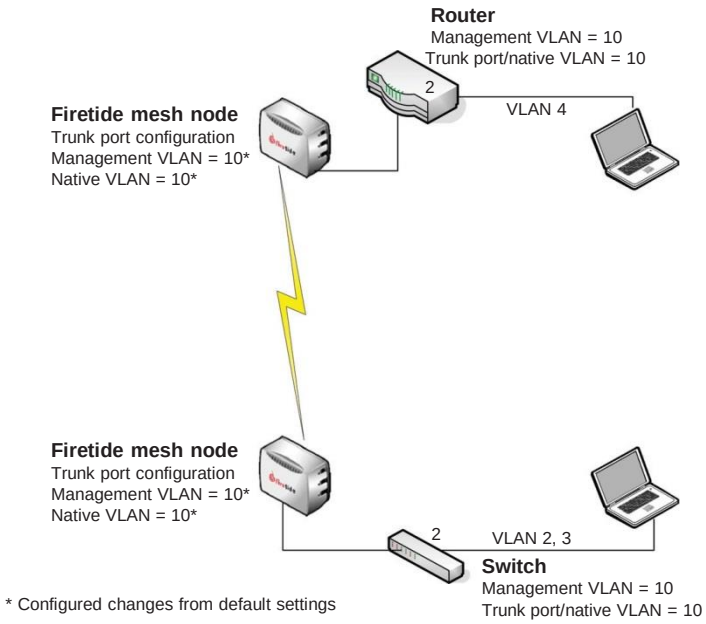
Note: This use case is for routers and switches that are 802.1-compliant.

The installation of a wireless mesh is a viable, cost-effective solution compared to fiber installation between a router and switch. The next figure shows the connection of a, 802.1-compliant router and switch with fiber between the two devices. In this case the router and switch use 802.1q trunk ports with a management VLAN, 10, and trunk port and native VLAN, also 10.



The next figure shows the fiber connection replaced by two Firetide mesh nodes.

The two Firetide mesh nodes use a trunk port to carry the traffic with the tags that the switch needs. You need to enable a trunk port on each mesh node that has a management VLAN of 10 (the default value is 1) and native VLAN of 10 (the default value is 1).



For traffic to pass correctly use this work flow:

1. Install two or more mesh nodes between the router and switch to form a wireless link.
2. Connect the router to one mesh node with Ethernet.
3. Connect the switch to a neighbor mesh node with Ethernet.
4. Use the next table to set the mesh node VLAN configuration.

Traffic from router	From each Firetide mesh node
Tagged and VLAN tag = Management VLAN tag	1. Disable Hybrid Trunk Port (if any). 2. Set the native VLAN to 1.
Untagged	1. Disable Hybrid Trunk Port (if any). 2. Set the management VLAN to 10 and the native VLAN to 10.

Table 18

Note: Do not enable any hybrid trunk ports.

5. Apply and save the configuration.

Multicast groups

Multicast is a layer-3 protocol widely used for audio and video distribution. Multicast packets have an IP address in the range of 224.0.0.0 to 239.255.255.255. These packets travel in Ethernet frames with MAC addresses in the range of 01:00:5E:00:00:00 to 01:00:5E:7F:FF:FF.

Multicast affects layer-2 because it uses a special range of Ethernet MAC addresses. Certain characteristics of the 802.11 family of wireless protocols are affected by these addresses.

Multicast is a challenge for a wireless device because the device does not know the intended recipient or how good the wireless connection is. The radio uses its lowest modulation rate and sends the Ethernet frame to all clients. This method is reliable but not efficient. A small amount of multicast traffic can slow down a mesh network.

Note: HotPort 7010/7020 and HotPort 5020-M nodes are limited to 256 kbps for multicast and broadcast traffic. You must create a multicast group to remove this limit.

HotView Pro lets you block all multicast traffic or configure multicast groups. A multicast group causes the system to encapsulate multicast traffic in unicast frames and send them to one or more receivers at full radio speed. The range of supported multicast group addresses is 224.0.1.133 to 239.255.255.255.

You can create a multicast group for each video feed.

Multicast and mobility

Reference the following two scenarios:
In a scenario where a multicast device, like a camera that is capable of sending multicast, is connected to a mobile node, then the multicast traffic can be viewed successfully from the network side. However, if a client device, like a laptop, is connected to a mobile node, then multicast traffic coming from the network side cannot be viewed successfully at its full rate.

Example: multicast groups

The next figure shows three multicast groups. Each multicast group uses a different multicast IP address:

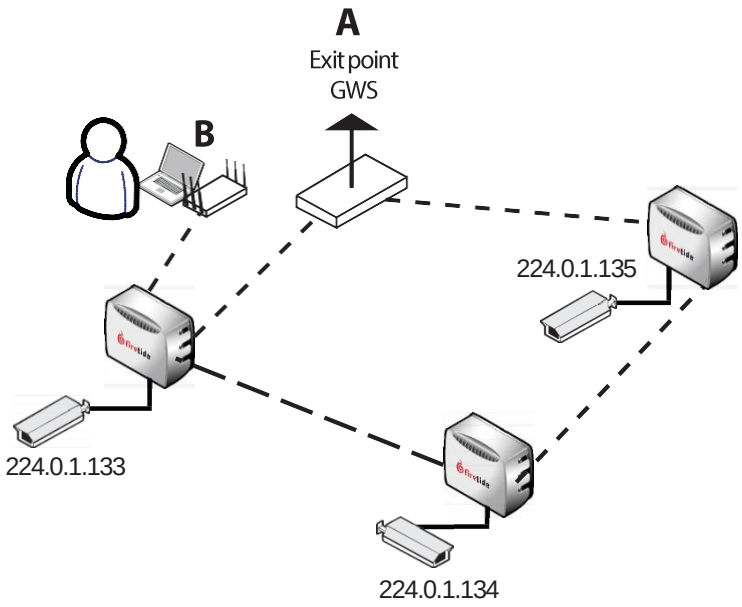
- 224.0.1.133
- 224.0.1.134
- 224.0.1.135

Gateway server (GWS) A is a receiver of multicast traffic and is the exit point for the video feeds. B is a another multicast traffic receiver for one group.

Multicast groups are organized by multicast IP address and include the multicast receivers (nodes that receive the traffic). The next table shows the groups and the receivers in each group.

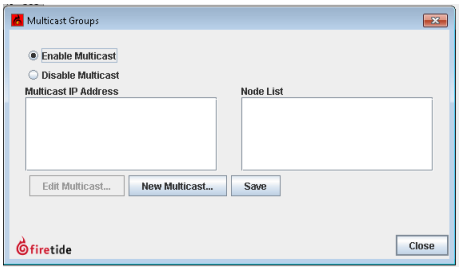
Multicast IP address	Multicast receiver
224.0.1.133	A, B
224.0.1.134	A
224.0.1.135	A

Table 19



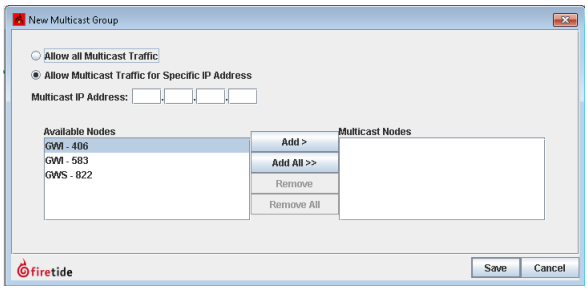
Creating a multicast group

You can permit all multicast traffic to or from all nodes or a subset of nodes. Allow multicast traffic to all nodes is used only if you do not know the multicast IP address groups.



1. Go to **Mesh > Multicast Groups**
2. Determine which multicast IP addresses to use on the mesh. IP addresses 224.0.1.133 to 239.255.255.255 are available for multicast groups.

   You should also identify the nodes which represent the source of the Multicast traffic (typically the camera nodes) and the destination (usually the head node or the network gateway interface nodes).
3. Click **New Multicast**.



a. Select **Allow all multicast traffic** or **Allow multicast traffic for specific IP address** and enter the multicast IP address.
b. Only add the node or nodes that will receive the multicast feed in the multicast group, and then click **Add**.
c. Click **Save**.

Add a multicast group for each multicast IP address you plan to use.

Removing a multicast group

To remove a multicast group:

1. Go to **Mesh > Multicast Groups**
2. Select **Edit Multicast**.
3. Remove all the nodes from the group.
4. Click **Save**.

Disabling multicast

If your network does not require multicast support, you should disable multicast. To disable multicast on a network-wide basis:

1. Go to **Mesh > Multicast Groups**
2. Select **Disable Multicast**.
3. Click **Save**.

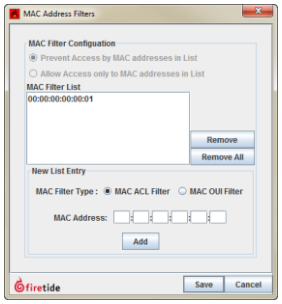
Configuring MAC filters

MAC filters let you permit or deny mesh access to a defined list of MAC addresses. This is a port configuration feature.

You can use this feature to stop traffic from entering a static mesh. You can block the data by MAC address or by MAC OUI (organizational unique identifier). For example, you can choose to deny traffic from a certain type of device with the MAC OUI.

Caution! If you make a mistake with this tool, you can lock yourself out of your mesh.

Note: HotPort 5020-M supports filters with a MAC OUI. It cannot block traffic from specific MAC addresses.



To add a MAC filter:

1. Go to **Mesh > MAC Filters**
2. Select the type of MAC filter.
3. Enter the MAC address.
4. Click **Add**.
5. Click **Save**.

To delete a MAC filter:

1. Go to **Mesh > MAC Filters**
2. Select the MAC filter entry from the list.
3. Click **Remove** the selected entry or **Remove All** to delete all of the entries.
4. Click **Save**.

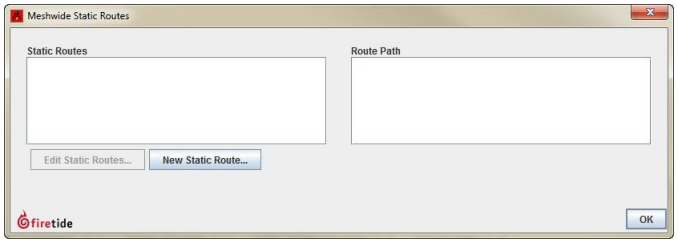
Static Routes

Automatic routing algorithms calculate the best paths from one node to another and between meshes.

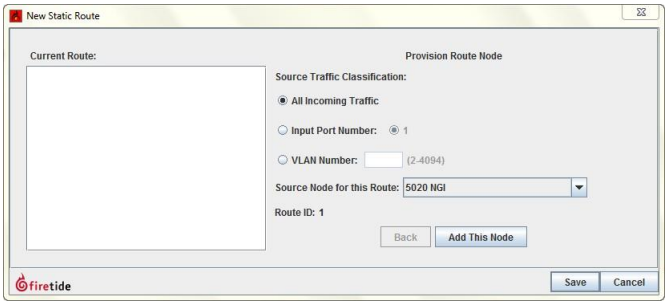
When most of the traffic goes to a particular node and the system calculates this route as a first choice path, the result is poor load sharing and can create traffic bottlenecks. In this case, you need to manually configure explicit routes to ensure load-balancing.

To add a new static route:

1. Go to **Mesh > Static Routes**



2. Click **New Static Route**.



3. Select the traffic classification: all incoming traffic, traffic from a specific port (one to four if available), or VLAN and enter the VLAN number.
4. From the drop-down list, select the source node for this route.
5. Click **Add This Node**.
6. Click **Save**.

Link Elimination

Link Elimination is used to force the mesh to delete weak, unplanned links that sometimes occur between mesh nodes.

Nodes can make links among themselves that are unplanned and not part of the mesh design. These extra links create overhead because the nodes update each other about the state of each link in the mesh.

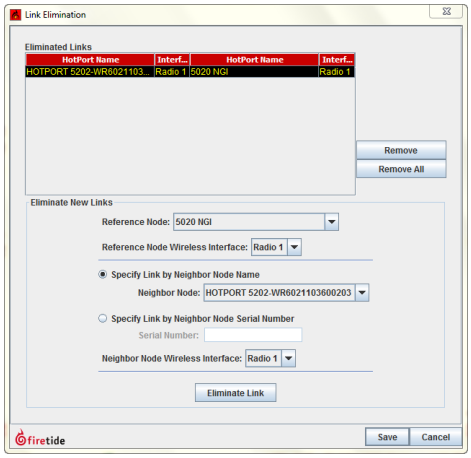
This feature is only for wireless links.

You might want to view all of the links that you eliminated or add some back. The eliminated link table at the top of the workspace is where you can permanently remove the links or restore them in the future.

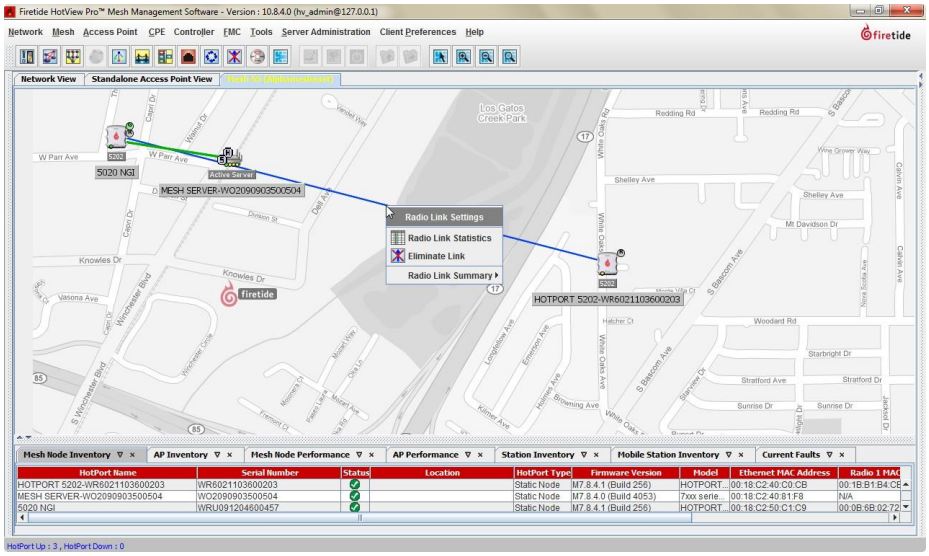
Removing an extra wireless link

To remove extra links in a mesh network:

1. Go to **Mesh > Link Elimination**
2. Select the node by name or enter its serial number
3. From the drop-down list of neighbor node wireless interfaces, select a wireless interface.
4. Click **Eliminate Link**.
5. Click **Save**.



Note: Optionally, you can click a link from the network view and right-click the link to eliminate it.



Restoring an eliminated link

HotView Pro keeps a table of eliminated links.

To restore a link that you have manually removed:

1. Go to **Mesh > Link elimination**
2. Select the link that you want to restore.
3. Click **Remove**.
4. Click **Save**.

Backup Node Configuration

Backup Node Configuration is the same as the node-menu version. It lets you make a backup file of a configured node.

Note: This command cannot be used to configure a node to replace a node that has failed in the field. A backed-up configuration file can only be applied to the node from which it was copied (and that has the same serial number).

The backup file is encrypted. You cannot read or make changes to the file.

Apply saved Mesh Configuration to the entire mesh

You can apply mesh-wide configuration settings to all nodes in a mesh.

Apply Saved Mesh Configuration to the Entire Mesh applies a previously-saved configuration file to an entire group of nodes. The configuration file is created from an individual node.

This function does not overwrite any node-specific configuration setting.

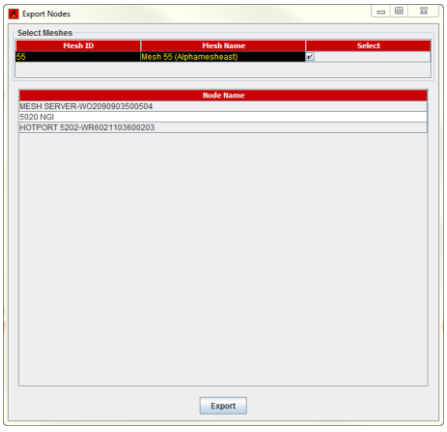
Export Mesh Data for Analytics

Export Mesh Data for Analytics exports the channel plan and certain mesh performance data in an XML. You can view the file in a browser.

You use this feature when collecting information when you receive customer support.

To export mesh data:

1. Go to **Mesh > Export Mesh Data for Analytics**
2. Select the mesh.
3. Click **Export**.



Reboot Mesh

Reboot Mesh causes all nodes on the mesh to reboot, but it does not affect any settings. This single action saves you the time of opening each node and rebooting it.

To reboot all nodes in a mesh:

1. Go to **Mesh > Reboot Mesh**
2. Click **Yes** to confirm that you want to reboot.

Delete Down Nodes

Delete Down Nodes, Delete Down Mobile Nodes, and Delete Down APs delete the hardware record of nodes or access points that are not used or do not exist from the HotView Pro database of known hardware. If you do not refresh the hardware record database, the system reports the devices as down.

HotPort Users Configuration

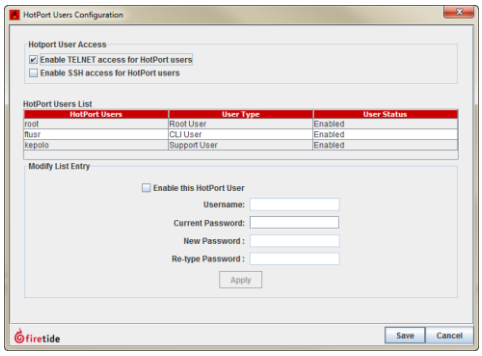
HotPort Users Configuration lets you define and limit telnet and SSH access to individual nodes.

The account *ftusr* can only access the internal CLI.

To permit telnet and SSH access, you must know the root user name and password.

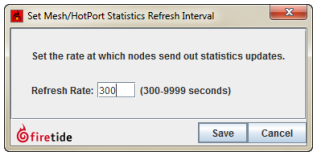
To block access to telnet or SSH:

1. Go to **Mesh > HotPort Users Configuration**
2. Remove the check from the check box for the correct service (telnet or SSH) to block all access to traffic from either service.
3. Click **Save**.



Set Mesh/HotPort Statistics Refresh Interval

Set Mesh/HotPort Statistics Refresh Interval lets you define how often the system collects statistics. The default value is 300 seconds. The maximum interval is 9999 seconds.



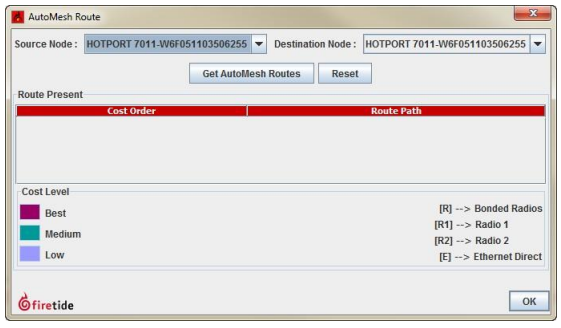
Viewing automatically generated routes

You can see the mesh's choices for traffic flows within the mesh. The AutoMesh feature shows this information:

- Source node, which you can change
- Destination node, which you can change
- Cost order
  - Best (first best path)
  - Medium (second best path)
  - Low (third best path)
- Route path

To view AutoMesh routes:

1. Go to **Mesh > Show AutoMesh Routes**
2. Select a source node from the drop-down list.
3. Select a destination node from the drop-down list.
4. Click **Get AutoMesh Routes.**



Verify Mesh Configuration

Verify Mesh Configuration compares the mesh-wide settings on all nodes and notifies you of differences.

View Mesh Log

View Mesh Log shows a log of mesh events. This information includes link up and down events on a per session basis.

The log filter is a dynamic real-time filter. When you close the window the sorted data is lost. The system does not keep the data.

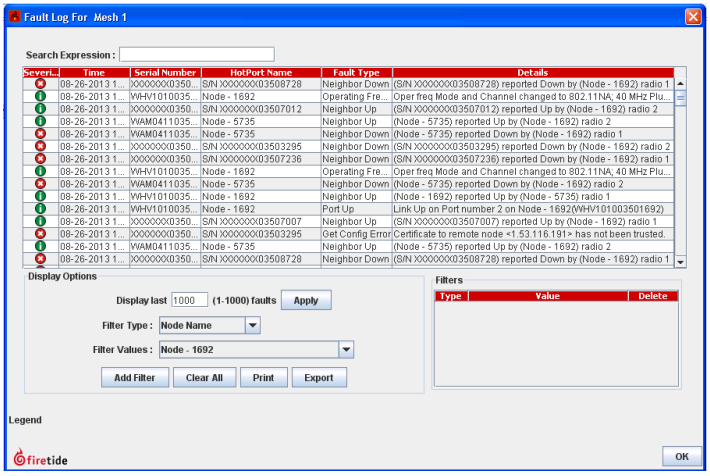
Note: If you want to keep the log events, you must install the database.

The system automatically populates the field values. Depending on the configuration, up to 1000 events or faults appear in the list.

You can create a custom value or sort by node type or by date.

The system sorts out of the limit you set.

You can search and filter the entries.



Mesh node-specific settings

The settings in this section are node-specific. The application of a mesh-wide configuration does not affect these settings.

To access node-specific commands:

1. Double-click a mesh on the Network View tab.
2. Right-click the mesh node to view your configuration options.

Setting the country code

If you have a new mesh node, the first thing to do is set the country code.

You want to set the country code to change the device from a low-power, low range setting to a correct full-power operational mode.

Caution! Make sure you configure the device for the correct country. If you do not configure the country correctly, the device might operate in a manner that is not legal or create problems with other wireless devices.

For information about default radio settings by country, "Worldwide default radio assignments" on page A-1.

To set the country code for a factory new device:

1. Log into the mesh network.
2. Right-click the node > **Country Code**
3. Select the country in which you intend to operate the device.
4. Click **Save**.

Changing the name of a mesh node

Rename HotPort lets you enter a unique, descriptive name for each node. This name can be up to 32 characters long. The name for the mesh node appears in the network view.

To change the name of a mesh node:

1. Log into the mesh network.
2. Right-click the mesh node you want to name **> Rename HotPort**
3. Enter a name for the mesh node.
4. Click **Save**.

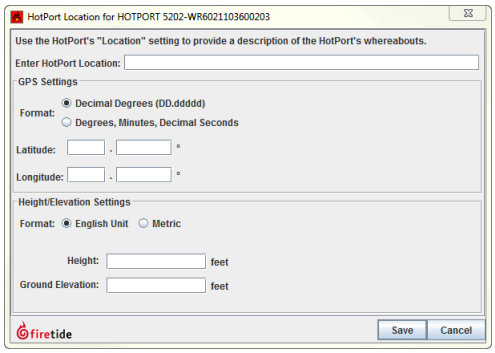
Entering a location for a mesh node

HotPort Location lets you enter a 256-character string to describe the location of the node.

Optionally, you can also enter the latitude, longitude, and elevation of the node. The antenna alignment tool uses this information to calculate antenna alignment. For more information about the antenna alignment tool, see "Antenna Alignment Tool" on page 63.

To enter information about the location of a mesh node:

1. Log into the mesh network.
2. Right-click the mesh node **> HotPort Location**
3. Enter a description.
4. Enter GPS settings:
   a. Select the format for the settings. The system accepts decimal degrees (DD.ddddd) and degrees, minutes, and decimal seconds.
   b. Enter the latitude and longitude of the mesh node.
5. Enter height and elevation settings:
   a. Select the format for the height and elevation settings. The system can accept imperial (USA) and metric values.
   b. Enter the height and elevation (from sea level).
6. Click **Save**.



Entering the node type

HotPort Type lets you configure a node to be static or mobile. Mobile nodes can be set to enable or disable scanning. Not all node models can be mobile nodes. Check the product specifications for which types are supported for your product.

HotPort Type is not available when a mesh node is a network gateway interface node.

About Dynamic Frequency Selection

Firetide mesh nodes support the use of dynamic frequency selection (DFS), which is an interference avoidance mechanism. If the system detects radar on the configured frequency, the radio stops data transmission within 200 ms to prevent interference. The mechanism changes to a different frequency within 10 seconds and monitors the new channel for 60 seconds:

- If the system detects no radar pulses, the radio starts data transmission.
- If the system detects radar on the new channel, the system changes the frequency again and starts the monitor period.

The next table lists DFS channels, frequencies, and the rules that apply to them.

DFS channel	**Frequency** (MHz)	**Rule**
52	5260	Can be used within 35 km radius of any Terminal Doppler Weather Radar (TDWR) station listed at http://transition.fcc.gov/eb/uniitdwr.pdf
56	5280	
60	5300	
64	5320	
100	5500	
104	5520	
108	5540	
112	5560	
116	5580	Can be used when these three conditions are met: - Not within line of sight (LOS) - More than 35 km from any TDWR station listed at http://transition.fcc.gov/eb/uniitdwr.pdf - Channel center frequency of the mesh node radio and the TDWR frequency are separated by 30 MHz
120	5600	Can be used by TDWR station only.
124	5620	
128	5640	

DFS channel	Frequency (MHz)	Rule
132	5660	Cannot be used within line of sight (LOS) or within a 35 km radius of any TDWR station listed at http://transition.fcc.gov/eb/uniitdwr.pdf Can be used if the channel center frequency of the mesh node radio and the TDWR frequency are separated by 30 MHz.
136	5580	Can be used within 35 km radius of any Terminal Doppler Weather Radar (TDWR) station listed at http://transition.fcc.gov/eb/uniitdwr.pdf
140	5700	

Table 20

Best practice: If your installation is within LOS or 35 km of a TDWR station, register with the Wireless Internet Service Providers Association (WISPA) database so that cases of interference can be identified quickly.

FCC radar detection threshold

The FCC defines a DFS radar detection threshold to be the signal level above which the presence of any radar signal requires a frequency change.

The next table lists the radar detection thresholds for the USA.

Radio power output	Radar detection threshold
Less than 200 mW	-62 dBm
200 mW or more	-64 dBm
*The detection threshold is based on an antenna gain of 0 dBi.	

Table 21

Note. Check with the agency that regulates radio frequency usage in the country in which you want to use Firetide products.

DFS certification

You must take an online certification course to become DFS-certified. After you pass the course, you can request DFS credentials to enter into HotView Pro when you configure the receive path gain setting. The credentials that you enter are a unique user name and password.

To sign up for the course, visit http://www.firetide.com/training-form/

DFS configuration

DFS credentials are required to use DFS channels in the USA.

Authentication of your DFS credential can happen with (online method) or without (offline method) Internet connectivity.

If you choose to authenticate your DFS credentials with the offline method, you need to send the serial numbers of all nodes that you plan to use or already use in your network to Firetide Customer Service. Firetide Customer Service will send you a DFS file.

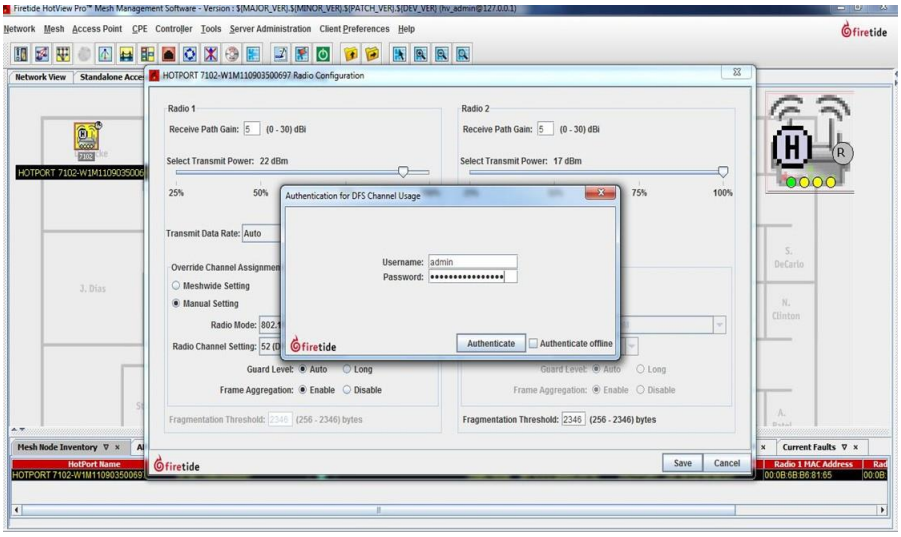
Configuring DFS with online authentication

To enable DFS channels with the online method:

1. Take and pass the online DFS training course.
2. Request DFS credentials from licensing@firetide.com

   Firetide Customer Service will send you a username and password. Use this information when the system prompts you.
3. Right-click the node > **Radio Settings**
4. In the Override Channel Assignment section of the radios, select a DFS channel.
5. Click **Save**.

   The Authentication for DFS Channel Usage window appears.
6. Enter your DFS credentials.
7. Click **Authenticate**.



If authentication fails, you need to use the offline authentication method.

Configuring DFS channel use with offline authentication

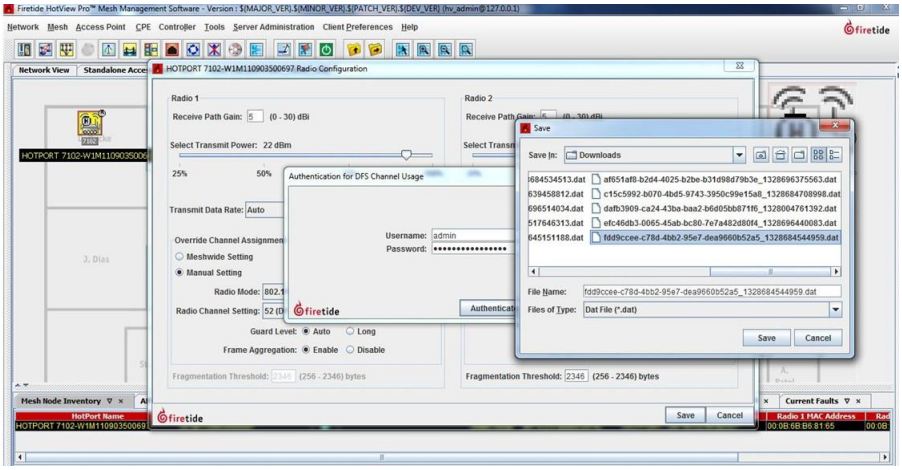
To enable DFS channels with the offline method:

1. Take and pass the online DFS training course.
2. Request DFS credentials from licensing@firetide.com

   Firetide Customer Service will send you a username and password. Use this information to authenticate DFS configuration privileges.
3. Right-click the node > **Radio Settings**
4. In the Override Channel Assignment section of the radios, select a DFS channel.
5. Click **Save**.

   The Authentication for DFS Channel Usage window appears.
6. Select **Authenticate offline**.

7. Enter your DFS username and password.
8. Click **Authenticate**.
9. Browse to the authentication file that Firetide Customer Service sent you.



10. Click **Save**.

Setting the receive path gain for DFS channels

The default receive path gain is 5 dBi, which is correct for the staging antennas. You can change the receive path gain to be a value from 0 dBi to 30 dBi. You must set the value to be the actual receive path gain for the antennas you need to use for the deployment.

The receive path gain is the gain of the antenna minus cable loss.

To set the receive path gain setting:

1. Right-click the node > **Radio Settings**
2. Enter the receive path gain setting for Radio 1 and Radio 2.
3. Click **Save**.

Configuring a DFS blacklist

HotView Pro lets you configure a blacklist. The DFS change mechanism will not use any of the channels in the blacklist. By default, no channels are configured.

To add a channel to the DFS blacklist:

1. Go to **Mesh > Configure Mesh**
2. Click the Wireless tab.
3. Click **DFS Blacklist**.
4. Select the channels you want to add to the blacklist.
5. Click **OK**.
6. Click **Save**.

Entering radio settings

Radio Settings lets you set radio settings on a node by node basis.

By default, 802.11 radios negotiate the best possible speed for the current RF conditions. If this is less than the maximum, the link negotiates the speed up and then down again when necessary.

In mesh applications this behavior can introduce some jitter in mesh transit times. It also creates more mesh overhead traffic because the nodes share link speed information for routing purposes.

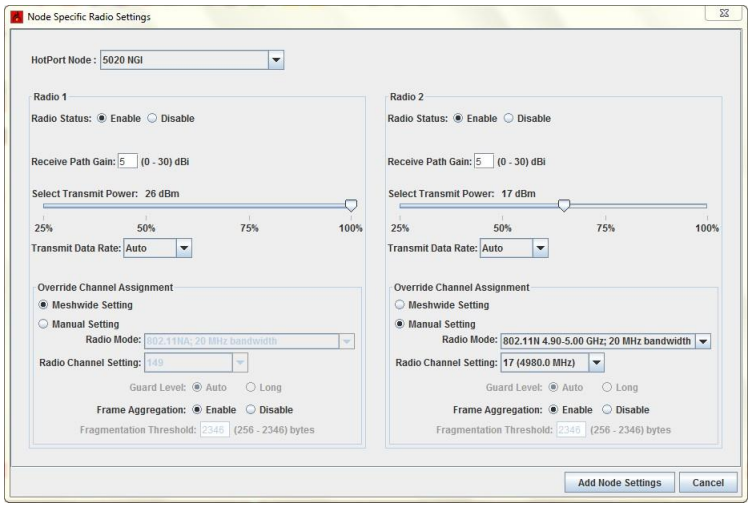
You can adjust the maximum possible speed at which an RF link can operate to a value less than the maximum. This action affects performance, but it can reduce overhead and jitter. It also increases link tolerance for marginal signal strength and interference. This is usually a beneficial trade-off in meshes, which carry video or voice traffic.

For information about default radio frequencies by country, see “ Worldwide default radio assignments” on page A-1.

To configure radio settings:

1. Right-click the node > **Radio Settings**
2. Enter radio 1 and 2 settings.

3. Click **Add Node Settings**.



Tunnel QoS settings for a node

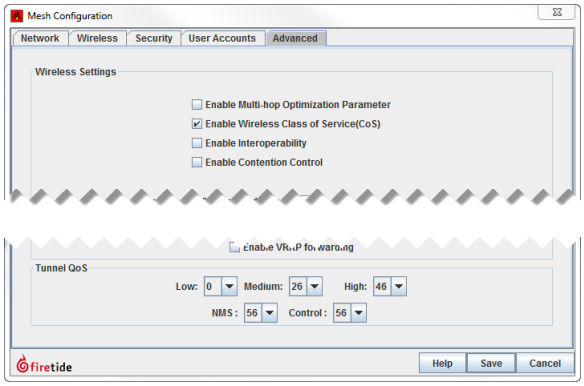
Node QoS lets you define 802.1p and port-based traffic priority.

The bandwidth of a tunnel link between two gateway servers or a gateway server and gateway interface is 1 Gbps. The traffic across those large links is not prioritized because all packets are forwarded without drops.

Node QoS is important when a mesh connects to other network devices that provide QoS. External routers and L3 switches provide classify and prioritize packets based on type of service (TOS)/DSCP value in the packet header.

HotView Pro lets you configure QoS parameters with differentiated services code point (DSCP) for control and for network management server (NMS) traffic. By default, higher priority is given to control and NMS traffic than to data traffic.

When the mesh configuration includes Node QoS settings, the TOS value of the outer IP header is set to the configured value when packets leave the tunnel device.



By default QoS settings are 0 (low priority), 26 (medium priority), and 46 (high priority). You should change the tunnel QoS settings for low, medium, and high priority traffic to have the same settings for the switch or router to which the node connects.

The work flow for QoS configuration is:

1. Go to **Mesh > Configure Mesh > Advanced** tab
2. Under Wireless Settings, select Enable Wireless Class of Service (CoS).
3. Under Tunnel QoS, set the QoS priority values to match your network needs:
   a. Set the low, medium, and high thresholds.
   b. Select the QoS value for control traffic.
   c. Select the QoS value level for the network management server.
4. Click **Save**.
5. Configure QoS (CoS) on the node:
   a. Right-click a static mesh node **> Node QoS**
   b. Select the correct type of QoS and settings.
6. Click **Save**.

Configuring a node port

Configure Node Port has a sub-menu:

- Port Configuration lets you disable unused wired-Ethernet ports, for security. It also lets you manually configure port speed and auto-sense.
- Hybrid Trunk Configuration is used as part of VLAN setup. See "VLANs" on page 111.
- VLAN ACL Configuration is used as part of VLAN setup. See "VLANs" on page 111.
- Reboot HotPort mesh node reboots the node.
- Backup and Restore Node Configuration lets you make a backup file of a configured node and then restore the node settings to the node.

Note: You cannot apply a backed-up node configuration to a different node. This feature cannot be used to configure a replacement node for a node that failed in the field. A backed-up configuration file can only be applied to the same serial-number node from which it was extracted.

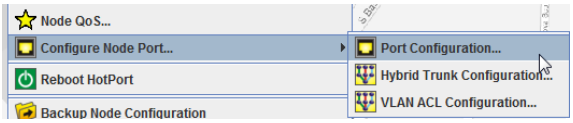
The file created by the Backup Node Configuration command is encrypted.

Disabling a mesh node port

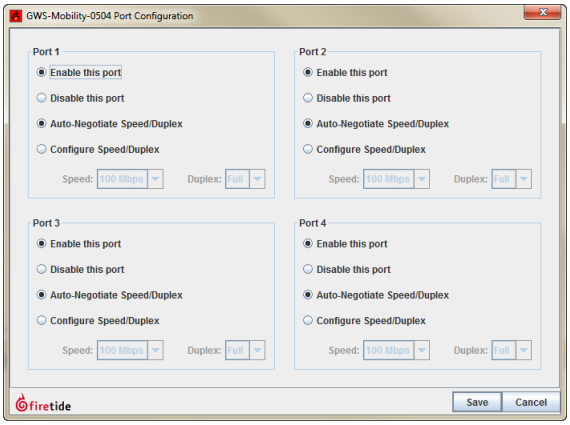
For security, Firetide recommends that you disable all Ethernet ports that you do not use.

To disable a port:

1. Right-click the mesh node, and then go to **Port Configuration**



2. Click **Disable this port**.



3. Click **Save**.

Disabling integrated access points

Disable Integrated Access Points deletes the association between a HotPort mesh node and its HotPoint access points.

Changing the node mode

Re-Configure Node To lets you change the operating mode of a node to be either a mesh node or a gateway server node.

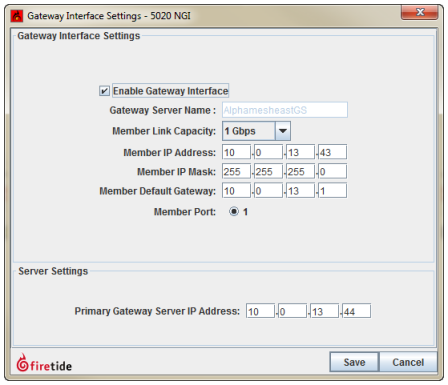
Configuring gateway interface settings

Gateway Interface Settings let you define the required parameters for nodes which are part of a gateway group.

Note: Not all product models let you configure gateway interface settings. Check product specifications to make sure if your product supports this feature.

For one node in the gateway group:

1. Right-click the node > **Gateway Interface Settings**
2. Enter the IP address of the primary gateway server.
3. Click **Save**.



Refreshing the display for a node

Refresh Configuration for this HotPort mesh node refreshes the display.

Configuring radio silence

Radio Silence lets you turn off the radios (disabled by default). A timer lets you configure the radios to come on at a later time. You can set the timer to enforce radio silence from 1 to 300 minutes.

This feature is not a radio scheduling tool. Radio silence is a feature to support public services during emergency situations. For example, if a wireless device is designed to trigger a nearby incendiary device.

To configure radio silence:

1. Right-click the node > **Enable Radio Silence**
2. Select **Enable**.
3. If you want to set the timer, select **Enable timer**.
4. Enter the number of minutes that you want the radio to wait.
5. Click **Apply**.

Caution! Radio silence is intended for specific wired deployments of gateway interfaces and a gateway server. If you enable radio silence in a wireless mesh, the mesh becomes inaccessible.

Deleting nodes from the database

Delete this HotPort Mesh Node lets you remove nodes individually from the software database. Use this action only on mesh nodes that are down (not working correctly) or do not exist.

Copying a mesh configuration from a node

Save Mesh Configuration from this HotPort lets you create a file on a local computer that contains all of the mesh-wide settings for a mesh node or gateway server.

When you save a configuration from an NGI node, the file contains the NGI-specific settings of that node.

When you save a configuration from a GWS node, the file contains the GWS settings and NGI interface list.

Note: Mesh configuration files contain only basic mesh parameters. They do not contain all aspects of system configuration. They contain no mesh node-specific information, such as node names, local radio settings, and so on.

Configuration files are written in XML. You can view them in a browser.

Applying a mesh configuration to a node

To apply a saved configuration to new nodes so that they can join the mesh, select **Apply Mesh Configuration**.

When you apply a configuration that contains the NGI-specific setting to a new node, the system prompts you to apply the NGI setting or not.

A configuration file copied from a GWS node can only be applied to a GWS node where the GWS server settings are not configured. When you apply a GWS mesh configuration file on a static mesh node, you can apply the mesh configuration and any NGI interface setting in its list.

Backup and restore node configurations

You can save a copy of the configuration file from one node (original node) and apply it to another node that has the same model number and that has the same firmware as that of the original node.

When you restore a configuration that has link elimination, static routes, or multicast groups configured, those features might not work as expected after the configuration file is applied to the node. Be prepared to check the configuration of those features and test that they are working as expected after a configuration restoration.

Node configuration restoration fails when the system detects mismatched:

- Country codes

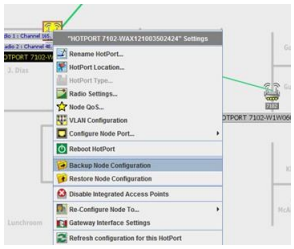
- Model number
- Firmware (version is later than that of the selected node)

Making a backup configuration file from a node and applying it to another node

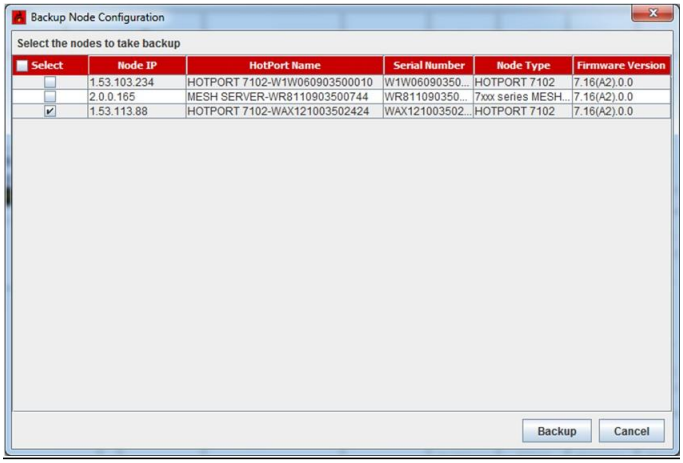
You can save a backup configuration file of several different nodes into a single file.

To make the backup of a node configuration and apply it to another node:

1. Right click the node, and then select **Backup Node Configuration**.

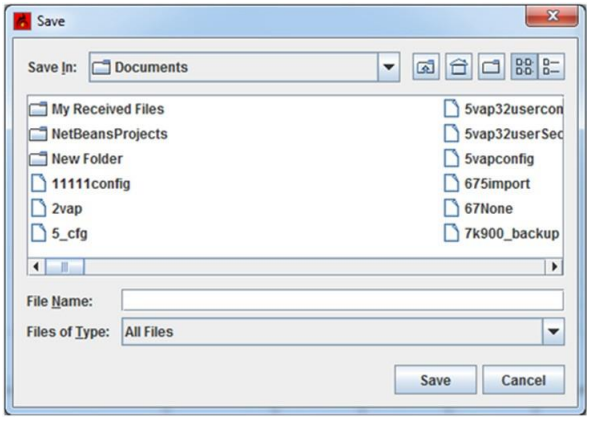


2. Select one or more nodes from which to copy the configuration.
3. Click **Backup**.



The file chooser appears.

4. Give the file a name, and then click **Save**.



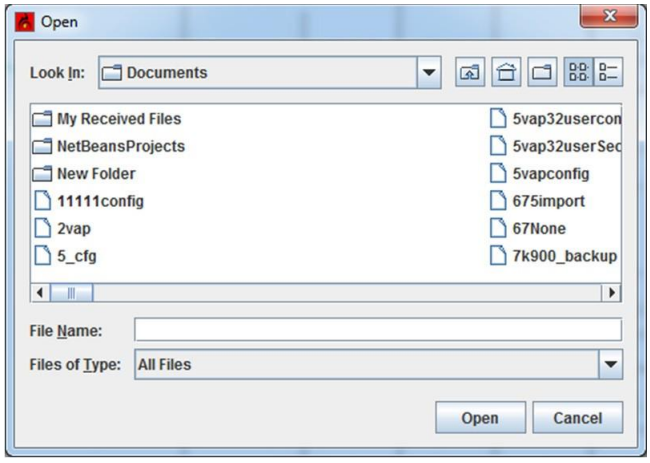
Restoring a node configuration

Prerequisites: The node from which a backup file is made and the node on which the backed up configuration is being applied must have the same model number and be running the same image version.

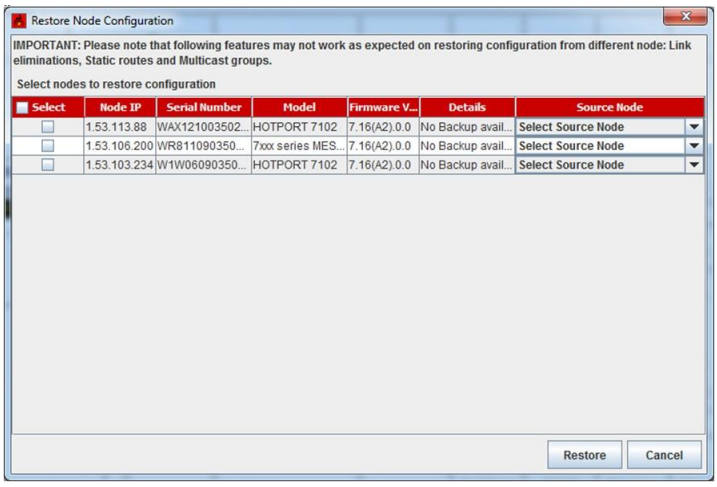
When you restore a configuration that has link elimination, static routes, or multicast groups configured, those features might not work as expected after the configuration file is applied to the node. Be prepared to check the configuration of those features and test that they are working as expected after a configuration restoration.

To restore the configuration of a node:

1. Right click on the node **> Restore Node Configuration**
   The file chooser window appears.



2. Browse to the configuration file, and then click **Open**.



The Restore Node Configuration window appears.

3. Select the nodes to which you want to apply or restore the configuration.
4. Click **Restore**.
5. Verify that the configuration settings and feature functionality are as expected.

MAC aging interval and time

You can control the MAC aging interval and aging period. When the aging period expires, the system removes the MAC entry from the table.

When a packet enters a node:

- Over Ethernet, the source MAC address of the packet is learned through the forwarding process and the system records the MAC address as a local entry in the MAC table.
- Through a radio, the source MAC address of the packet is learned, and the system records it in the MAC table as a dynamic entry.

When the packet stops entering the node, the system removes the stale MAC entries from the MAC table. The system checks for stale entries at the MAC interval you configure. Entries age until the MAC age timer is reached.

MAC age timer

The MAC aging time is the total time the node waits before it removes the MAC address from the table because packets with this source MAC stopped entering the node. By default the period is 300 seconds. The configurable range is 1 to 1800 seconds. The MAC age timer can be configured from HotView Pro and ftsh.

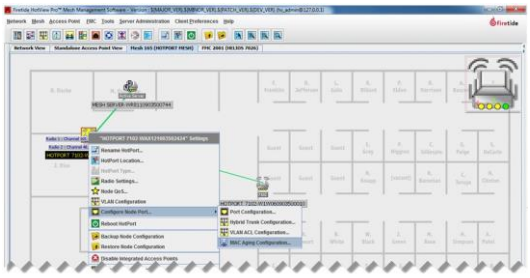
MAC aging interval

The MAC aging timer value is a multiple of MAC aging thread interval. If the MAC aging interval is 30 seconds, then MAC age timer can be set to a multiple of 30, from 30 to 1800 seconds.

Configuring the MAC aging interval and time settings

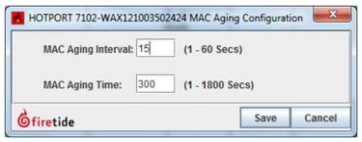
To configure MAC aging interval and time settings for one node:

1. Right-click the node **> Configure Node Port > MAC Aging Configuration**



The MAC Aging Configuration window appears.

2. Enter the MAC aging interval and time where MAC aging interval should be between 1 to 60 seconds and MAC aging time should be between 1 to 1800 seconds and should be in steps of MAC aging interval.

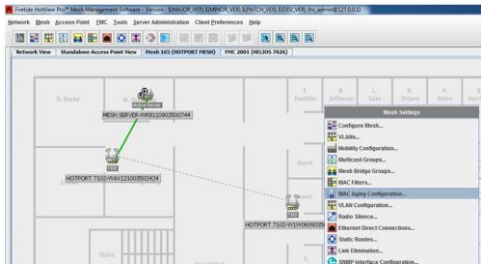


3. Click **Save**.

Setting a global MAC aging interval and time

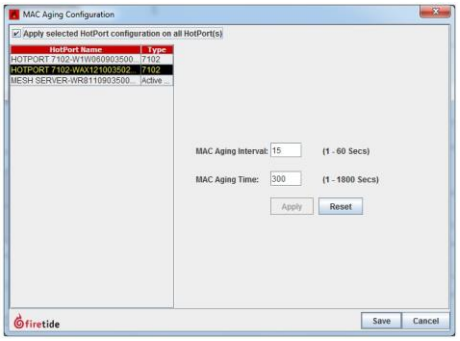
To set a global MAC aging interval and time for all mesh nodes:

1. Right-click the mesh in the Network View **> MAC Aging Configuration**



The MAC aging configuration window appears.

2. Select the “Apply selected HotPort configurations on all HotPort(s)” checkbox.



3. Enter the MAC aging interval and time, and then click **Apply**.

   When you click Apply, the system validates your configuration.

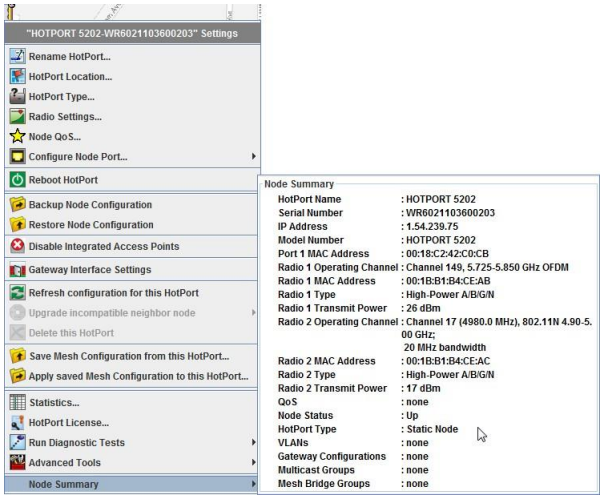
   Note: The Reset button sets the MAC aging interval and time values to their previously saved values.

4. Click **Save**.

Viewing a summary of a node configuration

Node Summary shows a summary of node settings. You can view:

- HotPort name
- Serial number
- IP address
- Model
- Port 1 MAC address
- Radio 1 settings (operating channel, MAC address, type, and transmit power)
- Radio 2 settings (operating channel, MAC address, type, and transmit power)
- QoS
- Node status
- HotPort type
- VLANs
- Gateway configurations
- Multicast groups



Individual radio settings

The two radios in each node can be individually configured. A mesh network can operate with uniform mesh-wide settings, but optimized radio settings can yield better performance.

The individual radio settings are:

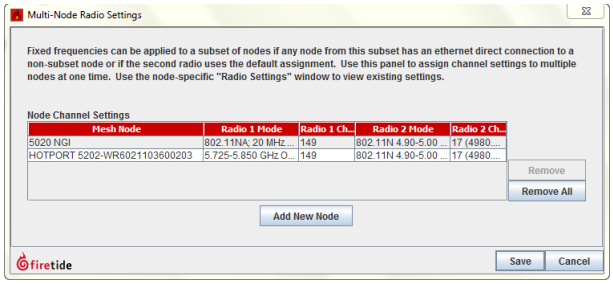
- Receive Path Gain: This setting calibrates the radar-detection function of the US FCC-mandated Dynamic Frequency Selection. Enter the net gain of that radio antenna (gain less cable loss).
- Select Transmit Power: This slide bar reduces transmit power when the receive strength (RSSI) at the far end of the link is too high. RSSI values stronger than -20 dBm can cause receiver overload, which increases the error rate and number of retransmissions. The exact level at which the receiver overloads depends on the total amount of background noise, and radio-to-radio variation.
- Transmit Data Rate: The transmit data rate is the maximum raw over-the-air rate at which the radio operates. For example, 802.11a radios operate at 54 Mbps. Radios always run at the highest possible speed. When a radio fails, it slows, and then it negotiates a higher speed after a period. This behavior adds jitter to a network. Limiting the maximum data rate to a lower value reduces jitter. Low data rate applications can be set to a lower speed, which reduces the RSSI requirement and permits longer links or smaller antennas.
- Override Channel Assignment: You can change the channel for the radio of one node.

- Fragmentation Threshold: Smaller packet sizes are better in noisy RF environments. If retransmissions are common and you eliminated other possible causes, set a smaller fragment size. This option is not available in 802.11n mode.

To make individual radio changes:

1. Right-click the mesh node **> Radio Settings**
2. Make the radio setting changes:
   - Enable or disable each radio
   - Enter the receive path gain (5 dBi by default)
   - Slide to select the transmit power (25 to 100% power in dBm)
   - Select the transmit data rate (auto by default)
   - Select any overrides:
     - Mesh-wide setting
     - Manual setting (radio mode and radio channel setting)
     - Enable or disable frame aggregation
3. Click **Save**.

To save time and make changes to multiple nodes at the same time, go to **Tools > Multi-Node Radio Settings Tool**

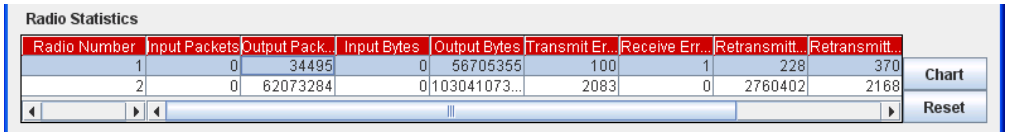


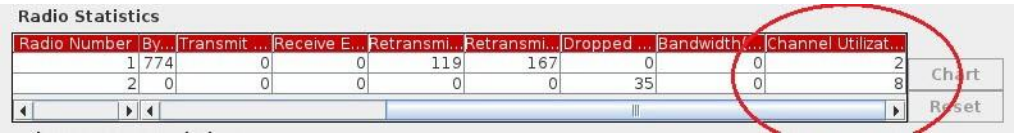
Viewing radio statistics

Radio statistics are in the middle of the window.

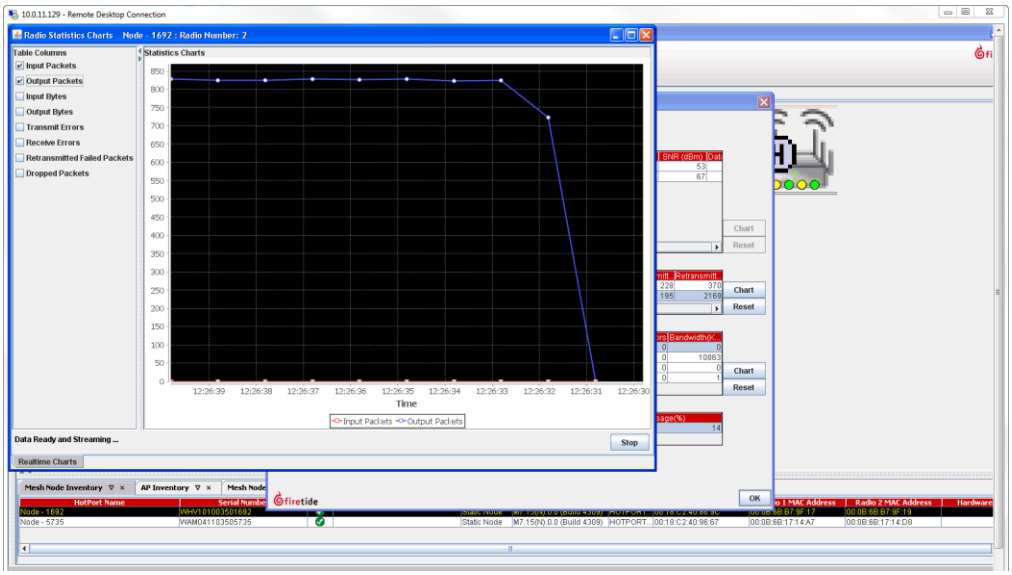
To view radio statistics:

1. Right-click the node **> Statistics**
2. Select the channel/radio row.





3. Click **Chart**.
4. Select types of data to view:
   - Input packets
   - Output packets
   - Input bytes
   - Output bytes
   - Transmit errors
   - Receive errors
   - Retransmitted failed packets
   - Dropped packets
   - Channel utilization (in %)



The system makes a graph with the real-time data for the options you selected.

5. Click **Stop** or close the window to exit.
6. Click **OK** to exit the statistics window.

Resetting statistics

To reset the statistics for a channel/radio or Ethernet port:

1. Right-click the node **> Statistics**
2. Select the channel/radio.

3. Click **Reset**.

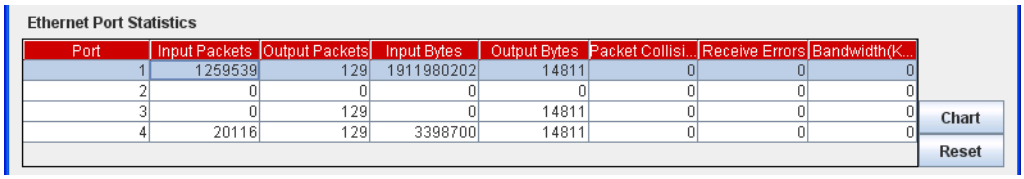
Note: Reset clears statistics and removes the row selection for radios and Ethernet ports of HotPort 7000 series and HotPort 5020 nodes.

Viewing Ethernet statistics

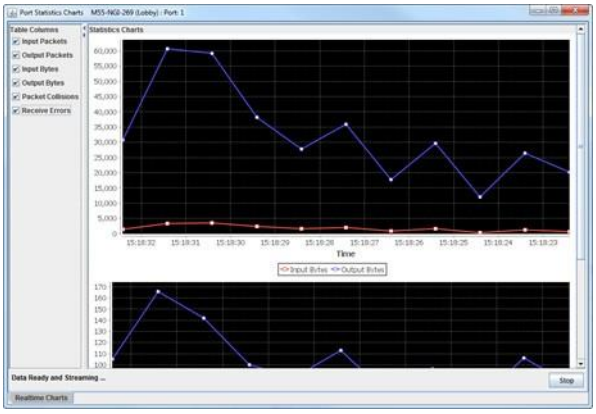
You can view detailed, real-time Ethernet link statistics.

To view Ethernet statistics:

1. Right-click the node **> Statistics**
2. Select the Ethernet port row.



3. Click **Chart**.
4. Select type of data to view:
   - Input packets
   - Output packets
   - Input bytes
   - Output bytes
   - Packet collisions
   - Receive errors



5. Click **Stop** or close the window to exit.
6. Click **OK** to exit the statistics window.

HotPort 5020-M Mesh node-specific settings

The settings in this section are node-specific. The application of a mesh-wide configuration does not affect these settings.

Note: HotPort 5020-M nodes can be used in these countries: Australia, Indonesia, Japan, Malaysia, Philippines, Singapore, South Korea, Taiwan, Thailand, and Vietnam.

The next table lists the mesh features by product model.

Feature	HotPort 7010/7020	HotPort 5020
Setting the country code	Supported	Limited support
Changing the name of a mesh node	Supported	Supported
Entering a location for a mesh node	Supported	Supported
Entering radio settings	Supported	Supported
QoS settings for a mesh node	Supported	Supported
Disabling integrated access points	Supported	Supported
Changing the node mode	Supported	Not supported
Configuring gateway interface settings	Supported	Not supported
Refreshing the display for a node	Supported	Supported
Upgrading a neighbor node	Supported	Supported
Deleting nodes from the database	Supported	Supported
Copying a mesh configuration from a node	Supported	Supported

Feature	HotPort 7010/7020	HotPort 5020
Applying a mesh configuration to a node	Supported	Supported
Viewing a summary of a node configuration	Supported	Supported
Individual radio settings	Supported	Supported

Table 22

To access node-specific commands:

1. Start HotView Pro.
2. Load the mesh.
3. Double-click a mesh on the Network View tab.
4. Right-click the mesh node to view configuration options.

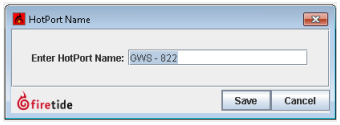
If you do not see the configuration option or setting you need, make sure that the mesh node model and mode supports the option or setting.

Changing the name of a mesh node

Rename HotPort lets you enter a unique, descriptive name for each node. This name can be up to 32 characters long. The name for the mesh node appears in the network view.

To change the name of a mesh node:

1. Log into the mesh network.
2. Right-click the mesh node you want to name **> Rename HotPort**
3. Enter a name for the mesh node.
4. Click **Save**.



Entering a location for a mesh node

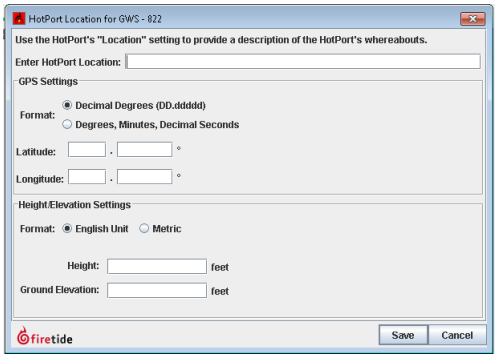
HotPort Location lets you enter a 256-character string to describe the location of the node.

Optionally, you can also enter the latitude, longitude, and elevation of the node. The antenna alignment tool uses this information to calculate antenna alignment. For more information about the antenna alignment tool, see “Antenna Alignment Tool” on page 23.

To enter information about the location of a mesh node:

1. Log into the mesh network.

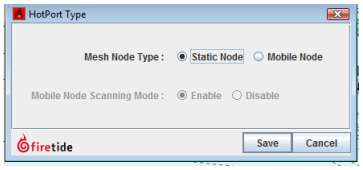
2. Right-click the mesh node **> HotPort Location**
3. Enter a description.
4. Enter GPS settings:
   a. Select the format for the settings. The system accepts decimal degrees (DD.ddddd) and degrees, minutes, and decimal seconds.
   b. Enter the latitude and longitude of the mesh node.
5. Enter height and elevation settings:
   a. Select the format for the height and elevation settings. The system can accept imperial (USA) and metric values.
   b. Enter the height and elevation (from sea level).
6. Click **Save**.



Entering the node type

HotPort Type lets you configure a node to be static or mobile. Mobile nodes can be set to enable or disable scanning.

HotPort Type is not available when a mesh node is a network gateway interface node.



If you want to change the node to be a gateway server, see “Changing the node mode” on page 155.

Entering radio settings

Radio Settings lets you set radio settings on a node by node basis.

By default, 802.11 radios negotiate the best possible speed for the current RF conditions. If this is less than the maximum, the link negotiates the speed up and then down again when necessary.

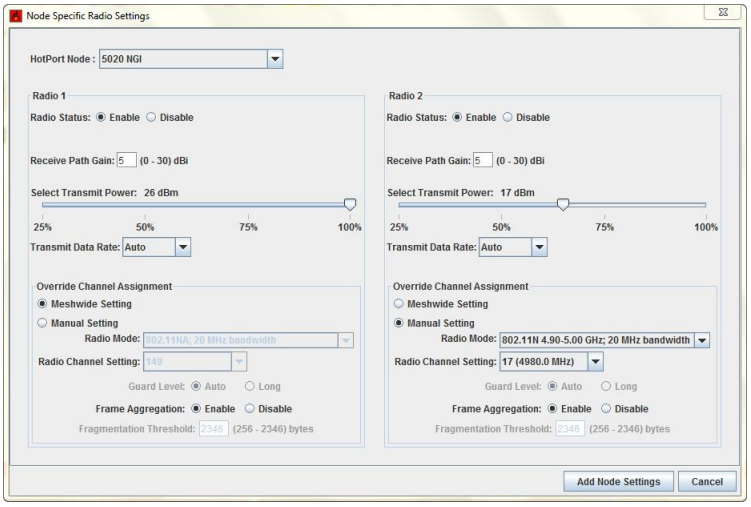
In mesh applications this behavior can introduce some jitter in mesh transit times. It also creates more mesh overhead traffic because the nodes share link speed information for routing purposes.

You can adjust the maximum possible speed at which an RF link can operate to a value less than the maximum. This action affects performance, but it can reduce overhead and jitter. It also increases link tolerance for marginal signal strength and interference. This is usually a beneficial trade-off in meshes, which carry video or voice traffic.

For information about default radio frequencies by country, see "Worldwide default radio assignments" on page 4-21.

To configure radio settings:

1. Right-click the node **> Radio Settings**
2. Enter radio 1 and 2 settings.
3. Click **Add Node Settings**.



QoS settings for a mesh node

Node QoS lets you define 802.1p and port-based traffic priority.

Note: HotPort 5020-M nodes do not support port-based traffic priority.

Configuring a node port

Configure Node Port has a sub-menu:

- Port Configuration lets you disable unused wired-Ethernet ports, for security. It also lets you manually configure port speed and auto-sense.
- Hybrid Trunk Configuration is used as part of VLAN setup. See "VLANs" on page 111.
- VLAN ACL Configuration is used as part of VLAN setup. See "VLANs" on page 111.

- Reboot HotPort mesh node reboots the node.
- Backup and Restore Node Configuration lets you make a backup file of a configured node and then restore the node settings to the node.

Note: You cannot apply a backed-up node configuration to a different node. This feature cannot be used to configure a replacement node for a node that failed in the field. A backed-up configuration file can only be applied to the same serial-number node from which it was extracted.

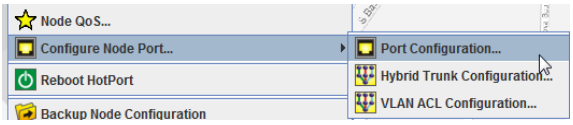
The file created by the Backup Node Configuration command is encrypted.

Disabling a mesh node port

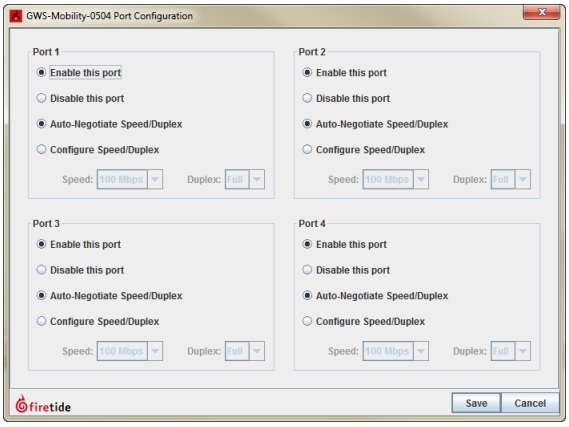
For security, Firetide recommends that you disable all Ethernet ports that you do not use.

To disable a port:

1. Right-click the mesh node, and then go to **Port Configuration...**



2. Click **Disable this port**.



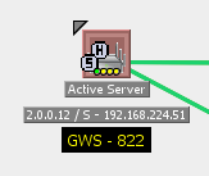
3. Click **Save**.

Disabling integrated access points

Disable Integrated Access Points deletes the association between a HotPort mesh node and its HotPoint access points.

Changing the node mode

Re-Configure Node To... lets you change the operating mode of a node to be a mesh node or a gateway server node.

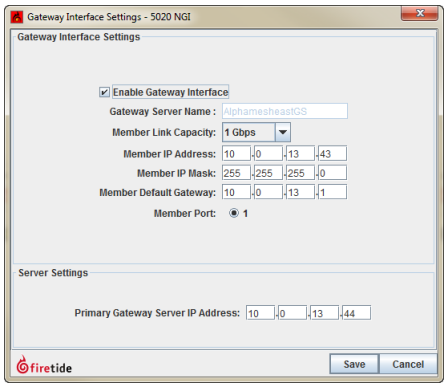


Configuring gateway interface settings

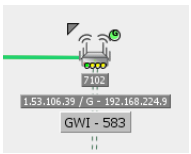
Gateway Interface Settings let you define the required parameters for nodes which are part of a gateway group.

For one node in the gateway group:

1. Right-click the node > **Gateway Interface Settings**
2. Select **Enable Gateway Interface**.
3. Enter the Gateway Interface Settings:
   - Member link capacity
   - Member IP address
   - Member IP mask
   - Member default gateway
   - Select the port if the device model has more than one available port
4. Enter the IP address of the primary gateway server.
5. Click **Save**.



Gateway interface nodes look like this in the mesh view.



Refreshing the display for a node

Refresh Configuration for this HotPort mesh node refreshes the display.

Upgrading a neighbor node

Upgrade Incompatible Neighbor Node lets you force a node that has incompatible firmware to receive new firmware.

Deleting nodes from the database

Delete this HotPort Mesh Node lets you remove nodes individually from the software database. Use this action only on mesh nodes that are down (not working correctly) or do not exist.

Copying a mesh configuration from a node

Save Mesh Configuration from this HotPort... lets you create a file on a local computer that contains all of the mesh-wide settings for a mesh node or gateway server.

When you save a configuration from an NGI node, the file contains the NGI-specific settings of that node.

When you save a configuration from a GWS node, the file contains the GWS settings and NGI interface list.

Note: Mesh configuration files contain only basic mesh parameters. They do not contain all aspects of system configuration. They contain no mesh node-specific information, such as node names, local radio settings, and so on.

Configuration files are written in XML. You can view them in a browser.

Applying a mesh configuration to a node

To apply a saved configuration to new nodes so that they can join the mesh, select **Apply Mesh Configuration**.

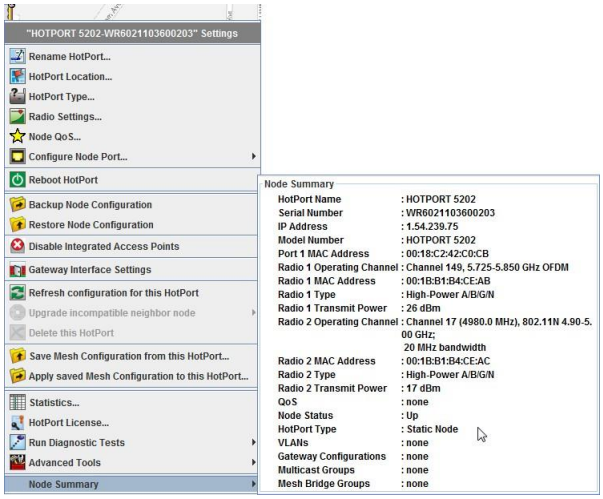
When you apply a configuration that contains the NGI-specific setting to a new node, the system prompts you to apply the NGI setting or not.

A configuration file copied from a GWS node can only be applied to a GWS node where the GWS server settings are not configured. When you apply a GWS mesh configuration file on a static mesh node, you can apply the mesh configuration and any NGI interface setting in its list.

Viewing a summary of a node configuration

Node Summary shows a summary of node settings. You can view:

- HotPort name
- Serial number
- IP address
- Model
- Port 1 MAC address
- Radio 1 settings (operating channel, MAC address, type, and transmit power)
- Radio 2 settings (operating channel, MAC address, type, and transmit power)
- QoS
- Node status
- HotPort type
- VLANs
- Gateway configurations
- Multicast groups



Individual radio settings

The two radios in each node can be individually configured. A mesh network can operate with uniform mesh-wide settings, but optimized radio settings can yield better performance.

The individual radio settings are:

- Receive Path Gain: This setting calibrates the radar-detection function of the US FCC-mandated Dynamic Frequency Selection. Enter the net gain of that radio antenna (gain less cable loss).
- Select Transmit Power: This slide bar reduces transmit power when the receive strength (RSSI) at the far end of the link is too high. RSSI values stronger than -20 dBm can cause receiver overload, which increases the

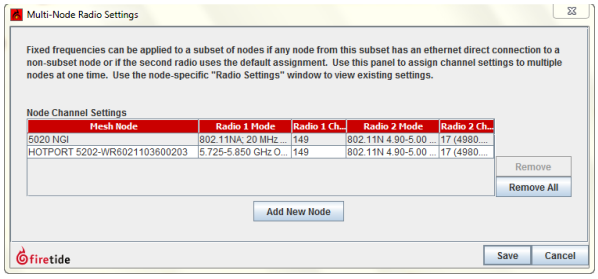
error rate and number of retransmissions. The exact level at which the receiver overloads depends on the total amount of background noise, and radio-to-radio variation.

- Transmit Data Rate: The transmit data rate is the maximum raw over-the-air rate at which the radio operates. For example, 802.11a radios operate at 54 Mbps. Radios always run at the highest possible speed. When a radio fails, it slows, and then it negotiates a higher speed after a period. This behavior adds jitter to a network. Limiting the maximum data rate to a lower value reduces jitter. Low data rate applications can be set to a lower speed, which reduces the RSSI requirement and permits longer links or smaller antennas.
- Override Channel Assignment: You can change the channel for the radio of one node.
- Fragmentation Threshold: Smaller packet sizes are better in noisy RF environments. If retransmissions are common and you eliminated other possible causes, set a smaller fragment size. This option is not available in 802.11n mode.

To make individual radio changes:

1. Right-click the mesh node **> Radio Settings...**
2. Make the radio setting changes:
   - Enable or disable each radio
   - Enter the receive path gain (5 dBi by default)
   - Slide to select the transmit power (25 to 100% power in dBm)
   - Select the transmit data rate (auto by default)
   - Select any overrides:
     - Meshwide setting
     - Manual setting (radio mode and radio channel setting)
     - Enable or disable frame aggregation
3. Click **Save**.

To save time and make changes to multiple nodes at the same time, go to: **Tools > Multi-Node Radio Settings Tool**



5020-E settings

The settings in this section are specific to 5020-E configuration. The application of a mesh-wide configuration does not affect these settings.

5020-Es in HotView Pro

5020-Es can only have one active link to a mesh node at any time. HotView Pro shows this information when it loads a mesh network:

- Active radio links are broken green lines between nodes
- Product icon
- Model, IP address, and descriptive names are under the product icon
- Port information

Note: If you cannot see the information you want to see, go to **Client Preferences**.

The next image shows the HotView Pro icon for an 5020-E that is working correctly.

The next image shows the HotView Pro icon for a 5020-E with a broken (down) radio link. The link line color is red. A red circle with an "X" is on the device, and a yellow circle with a red exclamation symbol is next to the device icon.

Setting the country code

If you have a new HotPort 5020-E, the first thing to do is set the country code. You want to set the country code to change the device from a low-power, low range setting to a correct full-power operational mode.

Caution! Make sure you configure the device for the correct country. If you do not configure the country code correctly, the device might operate in a manner that is not legal or create problems with other wireless devices.

For information about default radio settings by country, see "Worldwide default radio assignments" on page A-1.

To set the country code for a factory new device:

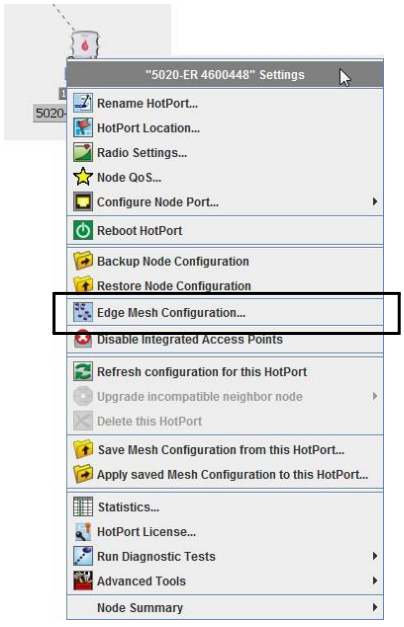
1. Go to **Mesh > Add Mesh**
2. Enter the IP address of the mesh and password.
3. Click **Log in**.

   The system detects new nodes that do not have a country code setting and prompts you to set the country code.
4. Select the country in which you intend to operate the device.
5. Click **Save**.

Accessing 5020-E configuration settings

To access 5020-E settings:

1. Double-click a mesh on the Network View tab.
2. Right-click the 5020-E to view your configuration options.
3. Select the setting to view the configuration window.



Adding a radio link to an 5020-E

5020-Es have one radio link (Radio 1).

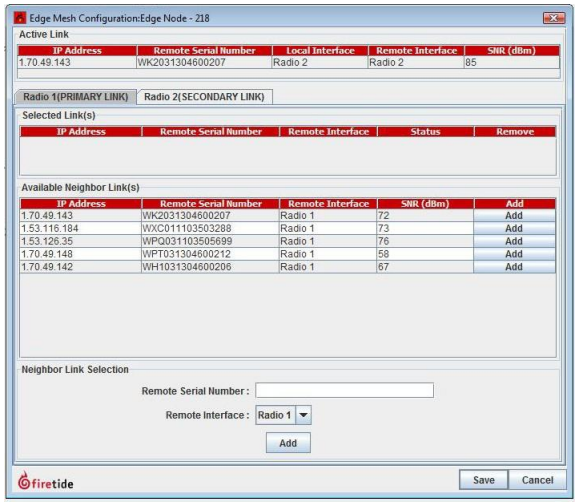
Before you add a radio link you need to do these tasks:

- Set the country code so the node works at full radio strength
- Apply a configuration file from a mesh node in the network so the 5020-E can connect to the correct mesh

After you configure the basic network information and give the 5020-E power, it finds neighbors to which it can connect.

To add a radio link on an 5020-E:

1. Right-click the 5020-E **> Edge Mesh Configuration**
2. From the Radio 1 tab, click **Add** to select the neighbor to which you want the 5020-E to connect.
3. Click **Save**.
   After you save the configuration settings, the 5020-E makes an active link to the neighbor configured for Radio 1.



Removing a radio link

To remove a radio link:

1. Right-click the 5020-E **> Edge Mesh Configuration**
2. From the Radio 1 or Radio 2 selected links section, click the box in the Remove column to select the link that you want to delete.
3. Click **Save**.

Configuring a radio link to a 5020-E not in the network

When you receive a new 5020-E and configure it to be in an active network, the node to which you want it to attach might not be in the area for the node to find. You can configure a radio link to a particular mesh node with this procedure.

Before you begin, you need the serial number and name of the remote interface to which you want the 5020-E to attach.

To configure a 5020-E to connect to a particular neighbor node that is not in the staging or current network:

1. Right-click the 5020-E **> Edge Mesh Configuration**
2. In the Neighbor Link Selection section (bottom of the window), enter the serial number of the neighbor mesh node.
3. Select the remote interface: Radio 1 or Radio 2.
4. Click **Add**.
5. Click **Save**.

   The 5020-E will connect to the correct mesh node when it is installed in the network.

Changing the name of a HotPort node

Rename HotPort lets you enter a unique, descriptive name for each HotPort node. This name can be up to 32 characters long. The name for the node appears in the network view.

To change the name of a HotPort node:

1. Log into the mesh network.
2. Right-click the node you want to name **> Rename HotPort**
3. Enter a name.
4. Click **Save**.

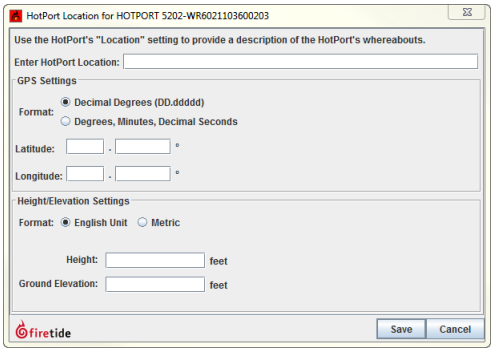
Entering a location for a HotPort node

HotPort Location lets you enter a 256-character string to describe the location of the node.

Optionally, you can also enter the latitude, longitude, and elevation of the node. The antenna alignment tool uses this information to calculate antenna alignment. For more information about the antenna alignment tool, see “Antenna Alignment Tool” on page 63.

To enter information about the location of a HotPort node:

1. Log into the mesh network.
2. Right-click the node **> HotPort Location**
3. Enter a description.
4. Enter GPS settings:
   a. Select the format for the settings. The system accepts decimal degrees (DD.ddddd) and degrees, minutes, and decimal seconds.
   b. Enter the latitude and longitude of the node.
5. Enter height and elevation settings:
   a. Select the format for the height and elevation settings. The system can accept imperial (USA) and metric values.
   b. Enter the height and elevation (from sea level).
6. Click **Save**.



Entering radio settings

Radio Settings lets you set radio settings on a node by node basis.

By default, 802.11 radios negotiate the best possible speed for the current RF conditions. If this is less than the maximum, the link negotiates the speed up and then down again when necessary.

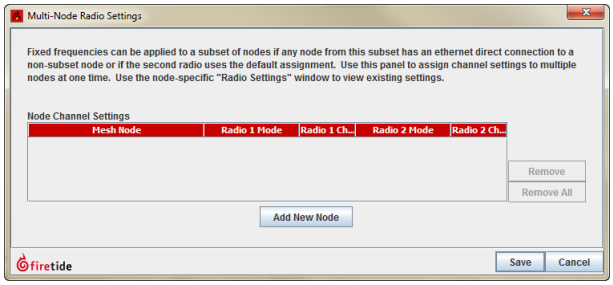
In mesh applications this behavior can introduce some jitter in mesh transit times. It also creates more mesh overhead traffic because the nodes share link speed information for routing purposes.

You can adjust the maximum possible speed at which an RF link can operate to a value less than the maximum. This action affects performance, but it can reduce overhead and jitter. It also increases link tolerance for marginal signal strength and interference. This is usually a beneficial trade-off in meshes, which carry video or voice traffic.

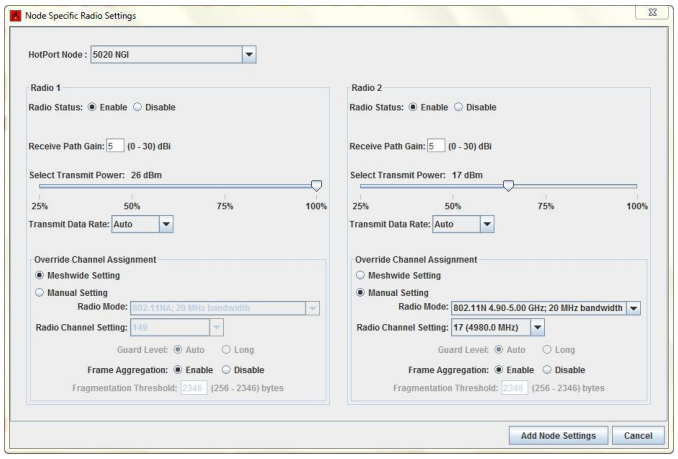
For information about default radio frequencies by country, see "Worldwide default radio assignments" on page A-1.

To configure radio settings:

1. Go to **Tools > Multi-Node Radio Settings Tool**
2. Click **Add New Node**.



3. Select a node from the drop-down list.
4. Enter the radio settings: transmit power, transmit data rate, and manual settings.
5. Click **Add Node Settings**.
6. Click **Save**.



QoS settings for a node

Node QoS lets you define 802.1p. See "Tunnel QoS settings for a node" on page 135.

Configuring a node port

Configure Node Port has a sub-menu:

- Port Configuration lets you disable unused wired-Ethernet ports, for security. It also lets you manually configure port speed and auto-sense.
- Hybrid Trunk Configuration is used as part of VLAN setup. See "VLANs" on page 111.
- VLAN ACL Configuration is used as part of VLAN setup. See "VLANs" on page 111.
- Reboot HotPort node reboots the node.
- Backup and Restore Node Configuration lets you make a backup file of a configured node and then restore the node settings to the node.

Note: You cannot apply a backed-up node configuration to a different node. This feature cannot be used to configure a replacement node for a node that failed in the field. A backed-up configuration file can only be applied to the same serial-number node from which it was extracted.

The file created by the Backup Node Configuration command is encrypted.

Disabling a HotPort port

For security, Firetide recommends that you disable all Ethernet ports that you do not use.

To disable a port:

1. Right-click the node **> Port Configuration**

2. Click **Disable this port**.
3. Click **Save**.

Disabling integrated access points

Disable Integrated Access Points deletes the association between a HotPort node and its HotPoint access points.

Refreshing the display for a node

Refresh Configuration for this HotPort node refreshes the display.

Copying a mesh configuration from a node

Save Mesh Configuration from this HotPort lets you create a file on a local computer that contains all of the mesh-wide settings for a node or gateway server.

Note: Mesh configuration files contain only basic mesh parameters. They do not contain all aspects of system configuration. They contain no node-specific information, such as node names, local radio settings, and so on.

Configuration files are written in XML. You can view them in a browser.

Applying a mesh configuration to a node

To apply a saved configuration to new nodes so that they can join the mesh, select **Apply saved Mesh Configuration to this HotPort**.

Viewing a summary of a node configuration

Node Summary shows a summary of node settings.

To view the node configuration: right-click the 5020-E **> Node Summary**

Individual radio settings

The two radios in each node can be individually configured. A mesh network can operate with uniform mesh-wide settings, but optimized radio settings can yield better performance.

The individual radio settings are:

- Receive Path Gain: This setting calibrates the radar-detection function of the US FCC-mandated Dynamic Frequency Selection. Enter the net gain of that radio antenna (gain less cable loss).
- Select Transmit Power: This slide bar reduces transmit power when the receive strength (RSSI) at the far end of the link is too high. RSSI values stronger than -20 dBm can cause receiver overload, which increases the error rate and number of retransmissions. The exact level at which the receiver overloads depends on the total amount of background noise, and radio-to-radio variation.
- Transmit Data Rate: The transmit data rate is the maximum raw over-the-air rate at which the radio operates. For example, 802.11a radios operate at 54 Mbps. Radios always run at the highest possible speed. When a radio fails, it slows, and then it negotiates a higher speed after a period. This behavior adds jitter to a network. Limiting the maximum data rate to a lower value reduces jitter. Low data rate applications can be set to a lower speed, which reduces the RSSI requirement and permits longer links or smaller antennas.
- Override Channel Assignment: You can change the channel for the radio of one node.

- Fragmentation Threshold: Smaller packet sizes are better in noisy RF environments. If retransmissions are common and you eliminated other possible causes, set a smaller fragment size. This option is not available in 802.11n mode.

When you manually select a radio mode, the guard level, frame aggregation feature, and fragmentation threshold become available or not.

If you select a "plus" radio mode, the channel assignment occupies the same air space but uses the next adjacent channel up. If you select a "minus" radio mode, the channel assignment occupies the same air space but uses the next adjacent channel down.

To make individual radio changes:

1. Right-click the node **> Radio Settings**
2. Make the radio setting changes:
   - Enable or disable each radio
   - Enter the receive path gain (5 dBi by default)
   - Slide to select the transmit power (25 to 100% power in dBm)
   - Select the transmit data rate (auto by default)
   - Select any overrides:
     - Mesh-wide setting
     - Manual setting (radio mode and radio channel setting)
     - Enable or disable frame aggregation
3. Click **Save**.

Firetide Mobility

This section contains information about these topics:

- Linear mobility
- Non-linear mobility
- Firetide Mobility Controller (FMC) configuration
- Mobility views in HotView Pro
- Telnet to FMC and Mobile Nodes

Mobile network solutions

A Firetide Mobility Controller (FMC) device lets you enable real-time roaming.

Note: HotPort 5020-E and HotPort 5020-M nodes do not support mobility and cannot be static nodes in networks that have mobility enabled.

A mobile LAN, such as a network on a train or bus, is a special application for which Firetide product are designed.

Mobile LANs can be designed to achieve up to 100 Mbps at high speeds with less than 1 ms per hop latency and seamless (as low as 5 ms) hand-off action. This level of performance enables the delivery of real-time video surveillance, digital signs, and Wi-Fi connectivity.

Note: Static nodes in linear mode can use the same channel to have shorter hand-off times.

Requirements to roam across meshes

Requirements for seamless roaming include:

- Active scanning is required for mobility solutions. Refer to the release notes to make sure that active scanning is legal in the location of intended use.
- One Firetide Mobility Controller (FMC) device
- Static and mobile nodes with licenses for mobility, dual radios, and correct firmware version for each node (static and mobile) in the meshes

Note: See the data sheets of the products you want to use in your deployment for firmware compatibility information.

- One gateway server in each mesh
- (Optional) backup FMC device and one backup gateway server for each installed gateway server

Note: Firetide recommends redundant FMC devices and gateway servers for fault tolerance.

Components of a mobile network

The components of a mobile network include:

- Firetide Mobility Controller device
- Mesh nodes

Firetide Mobility Controller device

The *Firetide Mobility Controller (FMC)* device does the following tasks:

- Keeps all configuration information for the mobile nodes.
- Communicates exclusively with the gateway servers in each mesh and the mobile nodes
- Pushes upgrades and changes to the mobile nodes

The FMC is used to schedule upgrades and perform the following changes to a mobile node:

ACL

- link state
- Auto Negotiation
- VLAN / Trunk configuration

Features

- QoS
- MAC filter
- Enable Mobile node redundancy
- Enable Multicast
- Scanning frequency and Radio1/2 Transmit power

The FMC device only works with a gateway server, which is the single point of contact to the mesh.

Best practice: Have redundant FMC devices within the same LAN for fault tolerance.

HotView Pro can manage multiple FMC devices. One FMC device manages a group of meshed networks. Mesh nodes cannot be members of more than one group at a time.

Mesh nodes

A mobility application requires mesh nodes configured and licensed to operate by purpose:

- Mobile node

  The nodes that move across the mesh networks are *mobile nodes*. You can change a static node into a mobile node through software configuration. After a node becomes a mobile node, then all configuration changes and upgrades come from the FMC device. All nodes in a mobility application require these licenses: management, mobility, dual-radio, and MIMO.

  The dual radios make reliable, quick performance possible. One radio exclusively scans and other radio makes the attachment. The radio that scans finds the closest, best signals for the link.

Mobile nodes have a scan interval, and they update the mobile scan list which lists the available channels.

- Static node

  Static nodes form the infrastructure of the network and can be along a track and other permanent positions throughout a city. Static nodes in a mobility application require these licenses: management, mobility, dual-radio, and MIMO.

- Gateway servers

  The gateway server is a mesh node that you configure to be the single point of contact for an FMC device. Gateway servers in a mobility application require these licenses: management, mobility, dual-radio, and MIMO.

Best practice: Have redundant gateway servers and redundant gateway interfaces within the same LAN for fault tolerance.

Mobile network configuration process

To set up a Firetide mobility enabled solution, do the following:

1. Set up one or more static meshes.
2. Configure one node in each mesh to be a gateway server.
3. Configure the gateway interface.
4. Install a mobility license to all nodes in each mesh.
5. Enable the Mobility Node setting and enter the FMC domain name.

Note: Make sure the domain name is the same across all meshes.

6. Configure the management IP address of the FMC on the gateway servers.
7. Select a static node for conversion:
   a. Factory reset this node prior to conversion.
   b. Make this node a "head node," apply the mesh-wide configuration settings, and convert the node from static to mobile.
8. From the FMC, add the serial number of the static node that you just converted to a mobile node, and enter it in the FMC (ACL list).
9. Configure the FMC mobility view.
10. From the FMC, configure the mobile node.

    The mobile node scans for information about the configured domain name. After authentication finishes, the FMC sends the configuration to the mobile node.

Note: The mobile node does not have to be in the mesh when you make configuration changes. The FMC keeps the change information, and then it sends the changes when the mobile node comes into the mesh domain.

Mobility and encryption

If you have end-to-end encryption enabled on a mesh, save a configuration file without end-to-end encryption to use with mobile nodes. Mobile nodes receive their encryption keys from the FMC. The system does not allow mismatched encryption keys.

Converting a mesh node to be a mobile node

For the nodes that you want to put in a vehicle, you need to change the operation mode from normal to mobile.

Prerequisites: A dual radio license must be installed on each mobile node. Make sure that scanning is enabled on the node.

Dual radios makes reliable, fast performance possible. One radio only scans and other radio makes the attachment. The radio that scans finds the closest, best signals for the link.

To convert a node to a mobile node:

1. Right-click the node **> HotPort Type > Mobile Node > Save**
2. Click **Yes**.

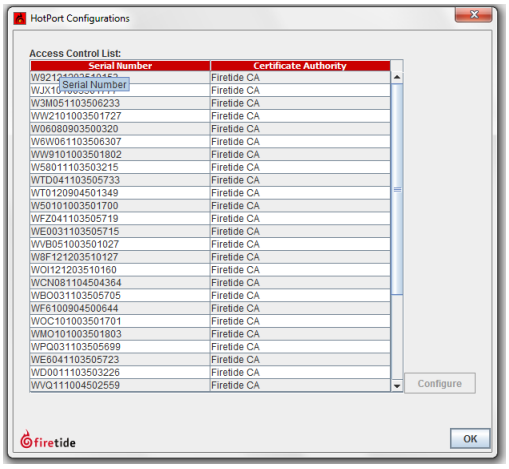
Configuring a mobile HotPort mesh node

Prerequisite: the radios must be configured before you convert a static node to be a mobile node.

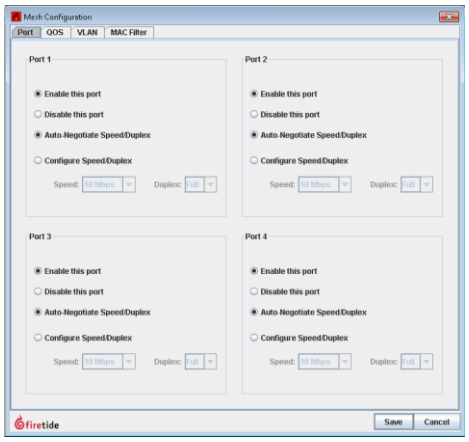
After conversion, mobile node configurations are modified from a right-click on the node or from the FMC device.

To configure a mobile HotPort mesh node:

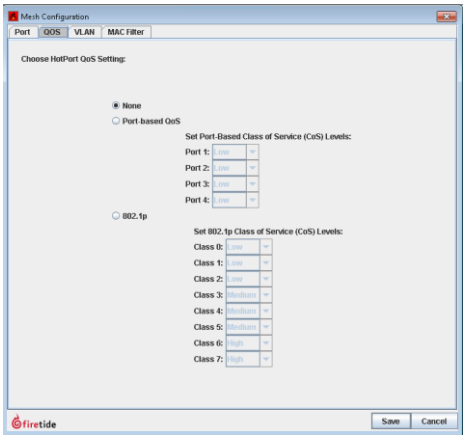
1. Right-click the **FMC > HotPort Configuration**
2. Right-click the mobile node in the ACL list.



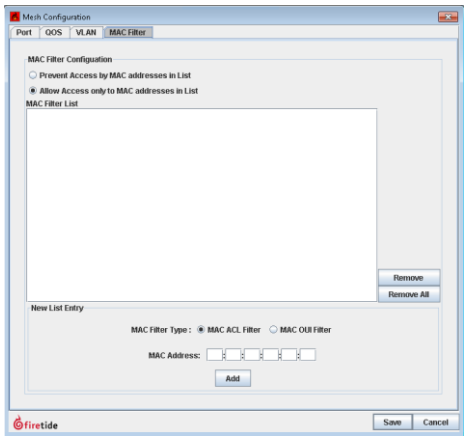
3. Configure the port settings as needed.



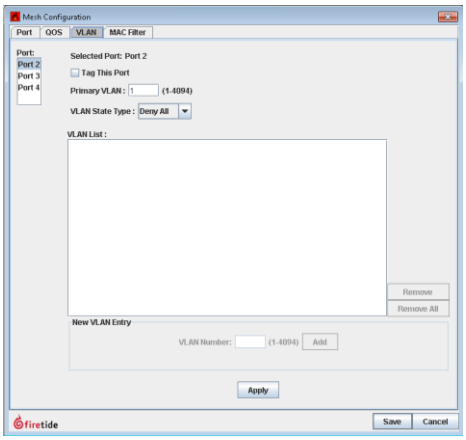
4. Configure the QoS settings as needed.



5. Configure the MAC filter as needed.



6. Configure the VLAN settings as needed.



7. When you are finished, click **Save**.

Configuring linear mobility

A mobile node downloads the mobility state when it first boots up and attaches to an attachment point or when it roams from one mesh to another. After the mobile node attaches to the static mesh network, it will not automatically know about any changes made to the mobility state, unless it is rebooted or if it leaves the static mesh and comes back later.

Direction of movement

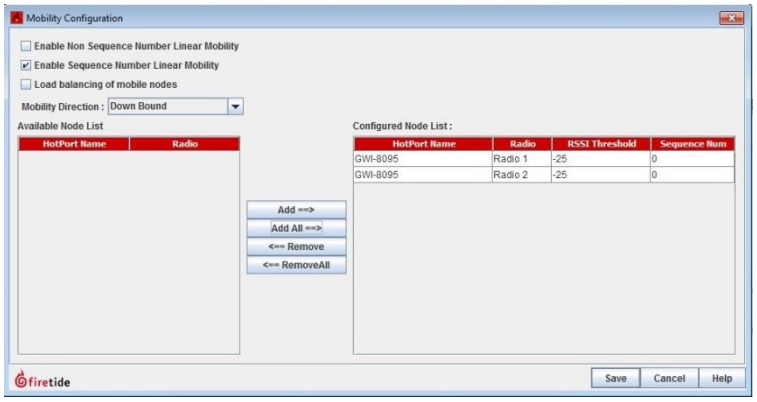
The direction of a radio on a static node defines the direction of movement of the mobile node in which this radio will serve as an attachment point for the mobile node. A mobile node moving in an upbound direction only attaches to radios that are configured to be upbound.

Mobile nodes automatically learn the direction of movement:

- When a mobile node changes attachment from one static node to another static node (not from one radio to another radio on the same static node), the direction of the mobile node is set to that of the second static node's radio.

To enable linear mobility:

1. Go to **Mesh > Mobility Configuration**
2. Select the type of linear mobility: non-sequential or sequential.
   - Non-sequential: add nodes to the list.
   - Sequential: add the sequence number of each node.
3. Select the direction of travel: upbound or downbound.
4. Select the node and radio that you want to be in the path in the order you want them to be used from the available nodes list.
5. Click **Save**.



Detachment threshold

The detachment threshold is the maximum RSSI value at which a mobile node stops a connection to the radio of the current static node and attaches to the radio of another static node.

Whenever the RSSI of a radio on a static node in a mobility application exceeds five, the mobile node looks for alternative attachment points and if found, it detaches from that static node and forms a link with a radio on another static node. You need to configure the detachment threshold for each radio of every static node in a mobility application.

To set the detachment threshold, see "Entering radio settings" on page 134.

Load balancing with mobile nodes

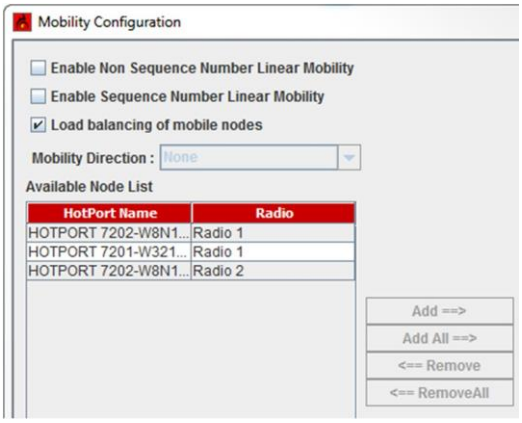
By default, when a mobile node looks for a static node attachment, the mobile node only uses the strongest RSSI value as the selection criteria. To ensure fair distribution of attachments and to decrease a potential for traffic bottlenecks and over-utilization, you can enable the load balancing feature. The load balancing feature increases the static node attachment selection criterion to include:

- CPU load and available bandwidth
- RSSI value
- Current channel utilization
- Channel congestion in the channel of the mobile node
- Number of neighbors attached to a particular static node

Enabling load balancing in a mobility application

To enable load balancing in a mesh:

1. Go to **Mesh > Mobility Configuration**
2. Select **Load balancing of mobile nodes.**



3. Click **Save.**

Firetide Mobility Controller device tasks

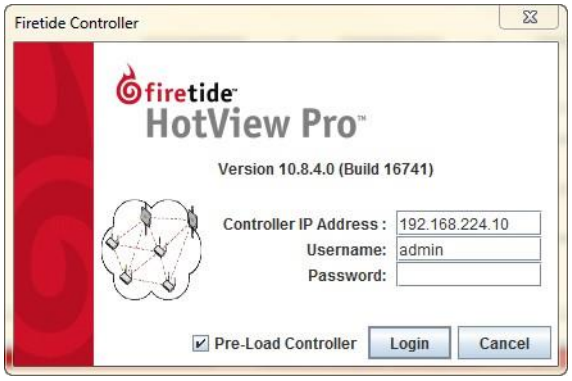
This section contains tasks that you do with an FMC. The default IP address for a new device is *192.168.224.170*. The default username is *admin,* and the default password is *firetide*.

Adding a Firetide Mobility Controller device

To add a controller:

1. Go to **FMC > Add FMC**
2. (Optional) Check **Pre-Load Controller**.

3. Click **Log in**.



Viewing Firetide Mobility Controller logs

You can view the controller log. The log contains this information:

- Severity
- Date
- Serial number
- Controller Name
- Fault type
- Details

The log filter is a dynamic real-time filter. When you close the window the sorted data is lost. The system does not keep the data.

Note: If you want to keep the log events, you must install the database.

The system automatically populates the field values. Depending on the configuration, up to 1000 events or faults appear in the list.

You can create a custom value or sort by node type or by date.

The system sorts out of the limit you set.

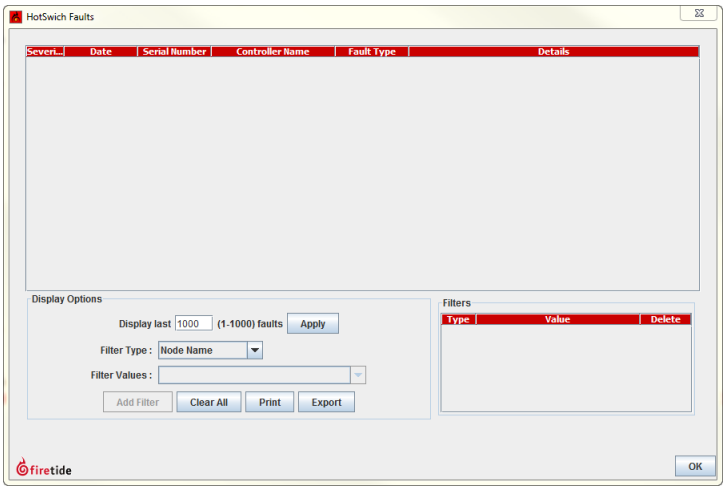
To filter the log:

- Enter a number between 1 and 1000 to see fewer entries, and then click **Apply**.
- Select the type of data to filter. You can choose to filter by date or node name.
- Add a filter.

To print the log, click **Print**.

To export the log, click **Export**.

To release the filter, click **Clear All**.



Deleting down controllers

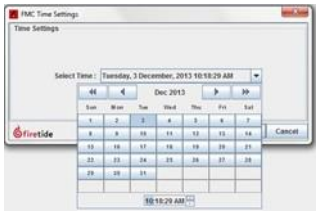
To delete a down controller from the management window, go to **FMC > Delete Down FMCs**.

Setting the time on an FMC

You can set the time on the primary and redundant FMC devices.

1. Start and then log into HotView Pro.
2. Go to **FMC > Add FMC**
3. Log into the FMC.
4. Right-click the primary **FMC > FMC Time Settings**

5. Select the date from the calendar drop-down arrow.



To change the time, double-click the hours, minutes, and then the seconds and use the up or down arrow to increment or decrement the time.

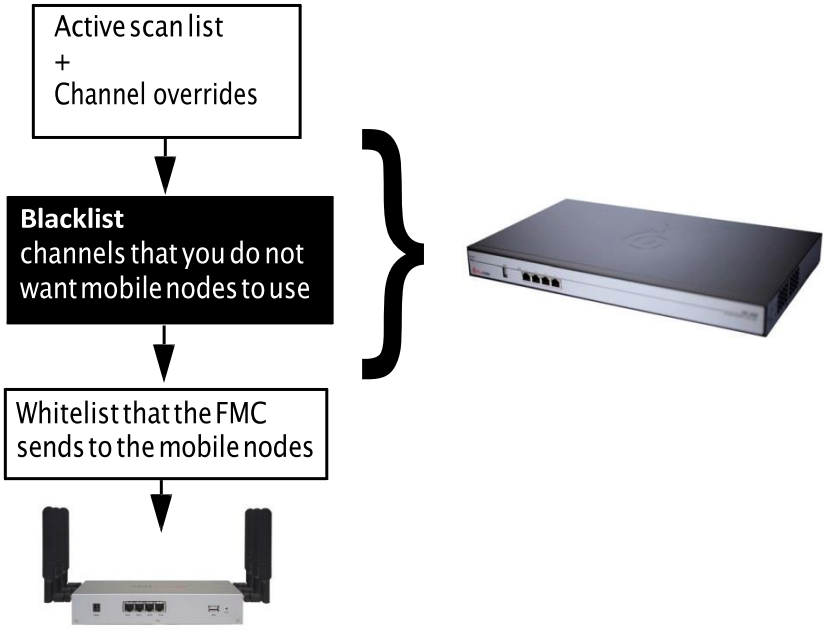
6. Click **Set Time**.

The FMC device reboots and then appears in the Mobility view. If the network has a redundant FMC, both FMC devices reboot and sync.

Mobile Node Scan List

The active scan list contains the available mesh-wide radio channels and mode pairs and override channels of all meshes connected to an FMC device. If an attached mesh experiences channel failure, the system does not report the channels and mode of that mesh in the list.

If you add one or more channels to the blacklist, the FMC device removes these channels from the active scan list to make a whitelist, a list of approved channels. The FMC system sends the whitelist to the mobile nodes.



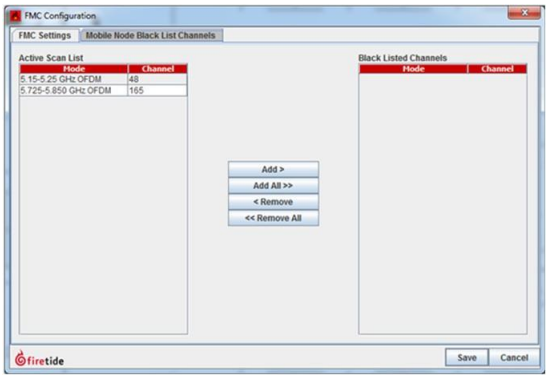
Denying channel access to mobile nodes

The active scan-list in each FMC device contains the radio channels and radio modes of the meshes connected to the FMC. By default mobile nodes have access to all of the channels in the active scan list. If no meshes are connected to FMC, however, the list is empty.

You can deny access to one or more channels by configuring a blacklist, which is stored in a database in the FMC device. If you select all available channels for the blacklist, however, the mobile nodes cannot connect to the network.

To add a channel to the blacklist:

1. Right-click the FMC device **> FMC Configuration > Mobile Node Black List Channels**
2. Select the channel that you do not want the mobile nodes to use from the active scan list (table on the left side of the window).



3. Click **Add** to move the Active Scan List channel to the Mobile Node Black List Channels list.

   Caution! If you move all channels to the blacklist, mobile nodes will disconnect from the network.

4. Click **Save**.

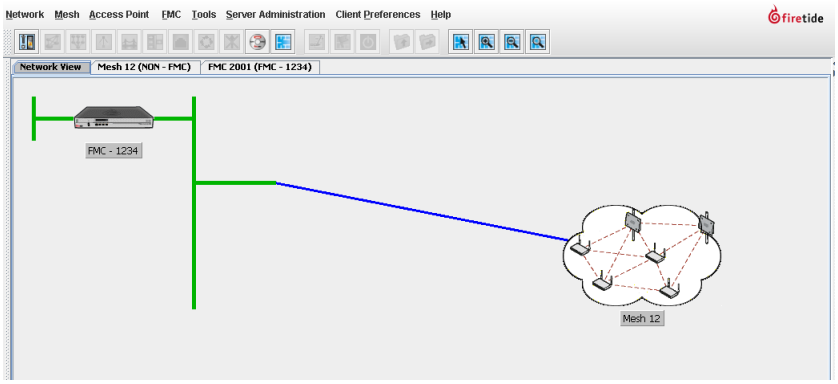
Node-specific FMC tasks

To administer mobile node configuration with an FMC device present in the network, you select the FMC for that group of mobile nodes and then right-click to view the options.

Changing the FMC ID

You should change the FMC ID value to a number from 2001 (default value) to 2100. This number can be helpful when you use the FMC mesh view.

The next image shows an FMC mesh view.



To change the FMC ID:

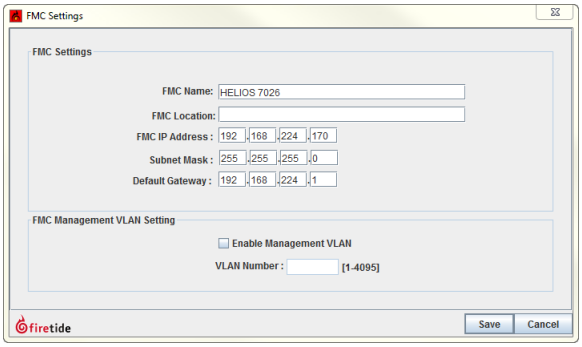
1. Right-click the FMC > **FMC ID**
2. Enter a number to identify the FMC.
3. Click **Save**.

Configuring the FMC

You can enter a descriptive name, location, and VLAN settings for the FMC device.

To configure or change FMC settings:

1. Right-click the FMC > **FMC Configurations**
2. Enter or modify the IP:
   - FMC name, which can be up to 32 alphanumeric characters long
   - FMC location, which can be an address or description of where to find the FMC device
   - FMC IP address, which is an IPv4 address
   - Subnet mask
   - Default gateway, which is the IPv4 address of a gateway server
3. (Optional) Enable the management VLAN feature and then enter the VLAN number.
4. Click **Save**.



Configuring FMC redundancy

If an FMC device breaks or experiences a power outage, mobile nodes become unable to roam. To provide graceful failover, we recommend that you have a backup FMC device.

Note1: When an FMC failover happens, the gateway server does not failover. It cycles at the next reboot.
Note2: To successfully bring up redundancy on an FMC and mobility, the VLAN configuration should be identical; otherwise, redundancy will not come up.

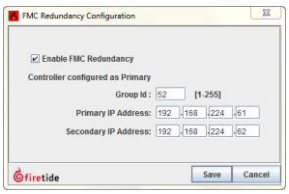
When you configure redundancy, you need to configure redundancy for both FMC devices. FMC redundancy uses Virtual Router Redundancy Protocol (VRRP). The Group ID or VRID determines the last byte of a virtual MAC address that the system maps to a virtual IP address for the primary and secondary FMC devices.

For example, 192.168.224.170 is the virtual IP address for a primary FMC device with IP address 192.168.224.171 and a secondary FMC device with IP address 192.168.224.172. If the primary device is active, it is reachable at 192.168.224.170 and 192.168.224.171.

The group ID is a number between 1 and 255.

To configure a redundant FMC:

1. Right-click the FMC **> FMC Redundancy Configuration**.
2. Check **Enable FMC Redundancy**.
3. Enter the relationship of the FMC device: primary or secondary.
4. Enter this information:
   - Group ID
   - Primary IP address
   - Secondary IP address
5. Click **Save**.



Upgrading firmware on an FMC device

You can view the current firmware version from the Upgrade tab.

Download different firmware files from the Firetide Partner Portal.

Caution! If the mesh has high security enabled, you must upload the .bin2 file. If you try to load the .bin file, the upgrade will fail.

To upgrade firmware on an FMC device:

1. Right-click the FMC **> Upgrade FMC**
   A window that shows the FMC devices available for upgrade appears.
2. From the Select Upgrade Image section of the Image Upgrade tab, click **Browse** and navigate to where you saved the firmware file.
3. Click **Open**.
4. Click **Start**.
   HotView Pro loads and activates the image file.

Upgrading firmware on a mobile node

To upgrade firmware on a mobile node that is controlled with an FMC device, you have to make the upgrade through the FMC interface (right-click on the FMC).

The mobile node does not have to be present in the mesh when you make firmware changes. The FMC keeps the change information, and then it pushes the firmware when the mobile node is present within the mesh domain. You cannot schedule mobile node upgrades.

Caution! If the mesh has high security enabled, you must upload the .bin2 file. If you try to load the .bin file, the upgrade will fail.

Note: To upgrade firmware on a static node, go to **Network > Upgrade Firmware**

To upgrade firmware on a mobile node:

1. Right-click the FMC **> Upgrade HotPort Mobile Nodes**
   A window that shows the nodes available for upgrade appears.
2. Select the node or nodes to upgrade.
3. Click **Save**.

The "upgrade complete" message means that the image file is on the node and is valid.

The job scheduler lets you activate the previously-uploaded image at a convenient time.

When you activate a firmware image, the affected node reboots. The affected node is not available for two minutes.

Upgrade messages

During a firmware upgrade procedure, the messages sent will reflect the following conditions:

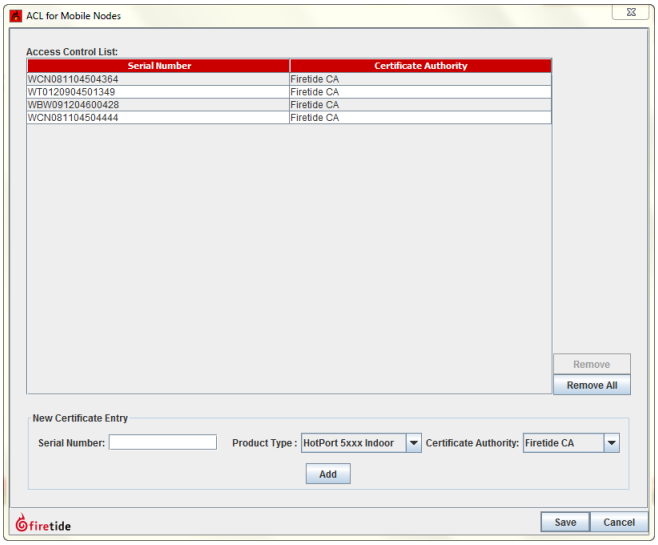
- success
- failure
- details if aborted

Adding mobile nodes to the FMC management group

You load mobile nodes into the FMC management group with access control list (ACL) entries. After the nodes are in the ACL, you can make node-specific changes.

To add a mobile node to the management group:

1. Right-click the FMC > **Mobile Node ACL Configuration**
2. In the New Certificate Entry section, enter this information:
   - Product serial number
   - Product type (indoor or outdoor node)
   - Certificate authority (Firetide CA, Firetide upgrade, or your custom CA if you configured self-signed certificates)
3. Click **Add**.
4. Reboot the FMC.



Making configuration changes on a mobile node

The mobile node does not have to be present in the mesh when you make configuration changes. The FMC keeps the change information, and then transfers the changes when the mobile node is present within the mesh domain.

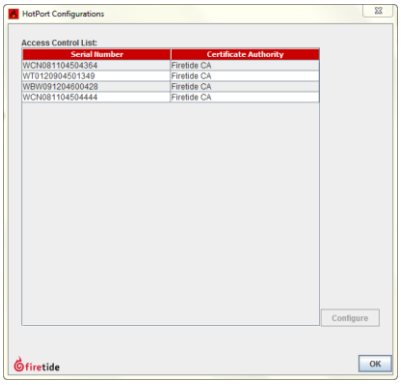
You have to add the mobile node to the ACL before you can make node-specific configuration changes.

Mobile node configuration includes settings for:

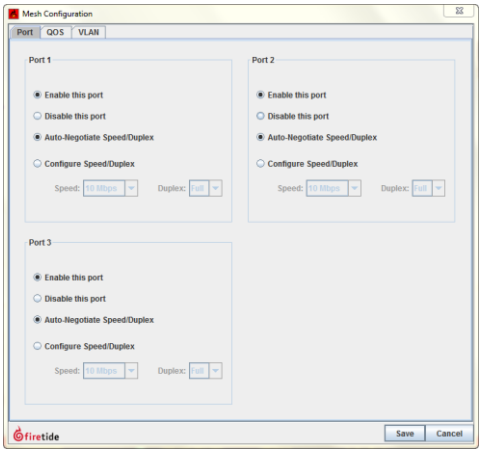
- MAC ACL
- Ports
- QoS and class of service
- VLAN
- Profile Switching (New in 10.17.0.0)
- Advanced (New in 10.17.0.0)

To make mobile node configuration changes:

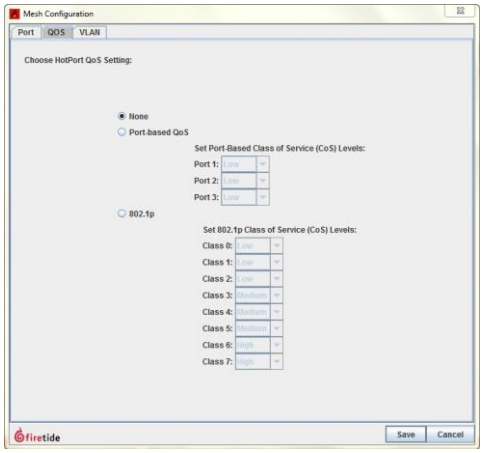
1. Right-click the FMC **> HotPort Configurations**
2. Select the mobile node by its serial number.
3. Click **Configure**.



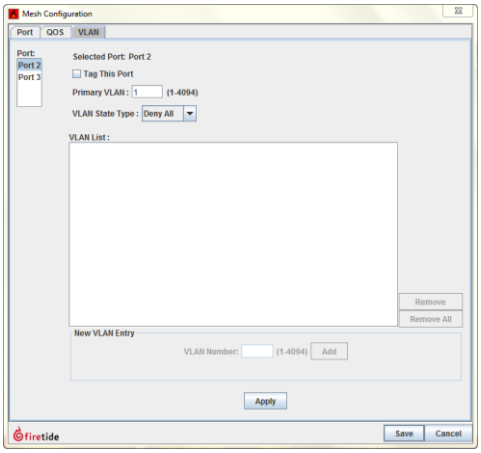
4. In the Mesh Configuration area (Port tab) enter these settings:
   - Enable or disable the ports
   - Auto-negotiate or explicitly configure the speed and duplex mode


Mesh Configuration
Port
QOS
VLAN
Port 1
Enable this port
Disable this port
Auto-Negotiate Speed/Duplex
Configure Speed/Duplex
Speed: 10 Mbps
Duplex: Full
Port 2
Enable this port
Disable this port
Auto-Negotiate Speed/Duplex
Configure Speed/Duplex
Speed: 10 Mbps
Duplex: Full
Port 3
Enable this port
Disable this port
Auto-Negotiate Speed/Duplex
Configure Speed/Duplex
Speed: 10 Mbps
Duplex: Full
firetide
Save
Cancel

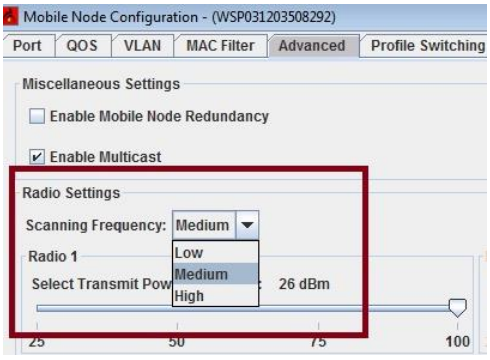
5. On the QoS tab enter these settings:
   - Disable QoS (default value)
   - If you enable QoS, select the class of service type: port-based or 802.1p



6. Enter the VLAN settings, and then click **Apply**.



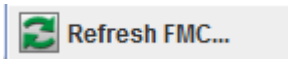
7. Advanced tab is used for setting Scanning Frequency (Low, Medium, High)



8. Click **Save**.
9. Click **OK** to exit the screen.

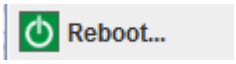
Refreshing the FMC configuration

In order to view the latest configuration settings after making multiple changes, doing a refresh of the FMC is recommended. A refresh of the display settings is performed by: Right-click the FMC **> Refresh FMC**.



Rebooting the FMC device

To reboot an FMC device, right-click the FMC **> Reboot**



Resetting the FMC device to the factory default settings

To reset the FMC device to the factory defaults with software, right-click an FMC device **> Factory Reset**

Saving a backup configuration from this FMC device

To save a copy of this FMC configuration, right-click the FMC device **> Import configuration from this FMC**

Applying a configuration to this FMC device

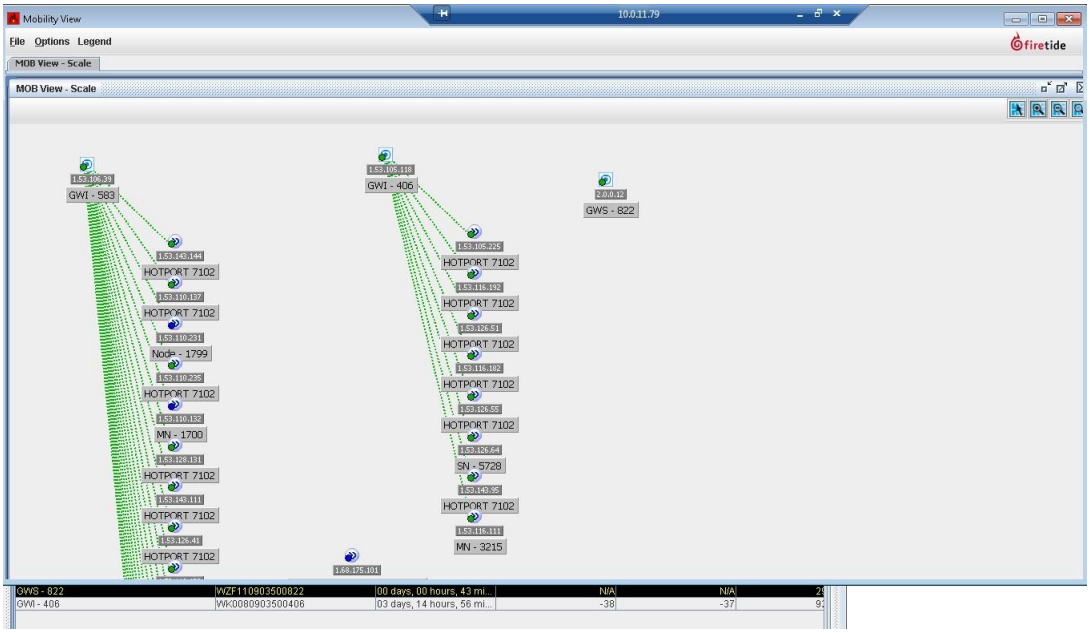
To apply a previously saved configuration for this FMC, right-click the FMC **> Apply saved configuration to this FMC**

Viewing a configuration summary from an FMC

To view a configuration summary of an FMC device, right-click the FMC **> FMC Summary**

Viewing a complex mobility application

You can view complex and mobility application with the mobility view.



Mobility Calibration Tool

The Mobility Calibration Tool is a planning tool to be used before you install a new mobility network. You can also use it as a diagnostic tool.

Use the Mobility Calibration Tool to make a map of radio conditions while a mobile node (set up to be a head node) roams from one mesh to another mesh. It scans for coverage along the path of the mobile node.

After you align the radio, add more nodes, and use these condition maps to design a better user experience.

Prerequisites:

- Ethernet cable
- One mobile node with mobile power source
- An administrator computer with sufficient battery power
  - HotView Pro must be installed
  - PostSQL must be installed

Note: You must run this tool locally. The Mobility Calibration Tool does not work remotely.

To use the Mobility Calibration Tool:

1. Connect the Ethernet cable from the administrator computer to the mobile node. This step makes the mobile node become a head node, and you can collect data from it.

2. Change the IP address of the administrator computer to an IP address on the same subnet as the mobile node.
3. Start HotView Pro.
4. Log into HotView Pro.
5. Go to **Mesh > Add Mesh**
6. Log into the mobile node with its IP address and password.
7. Go to **Tools > Mobility Calibration Tool**
8. Click **View Mobility Calibration Tool Log**.
9. Move the mobile node along the path.

Example: VLAN with mobility

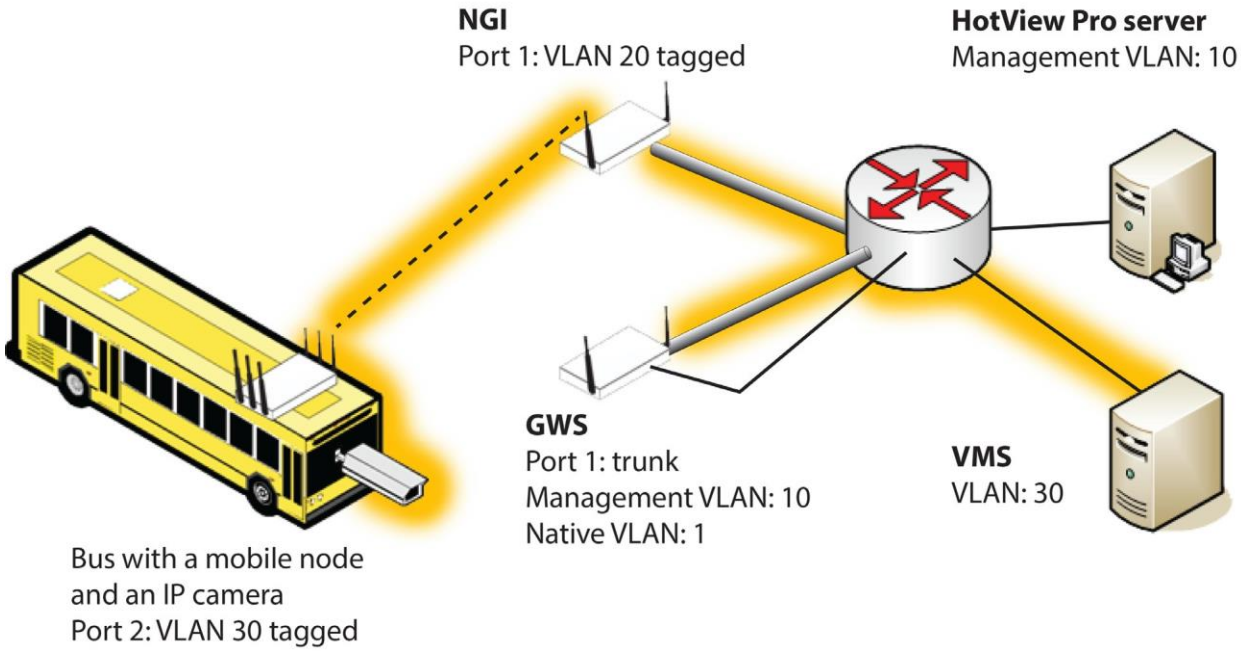
The next figure shows an example of VLAN configuration with mobility.

End-to-end VLAN. The video feed from the bus, which has a mobile node and an IP camera, has VLAN tags for VLAN 30 on port 2. The video traffic goes through the NGI and enters the trunk to the GWS and then goes to the video management server (VMS).

Management VLAN. The HotView Pro server and GWS send management traffic over VLAN 10.

Trunk VLAN. A trunk VLAN is between the NGI and the GWS over VLAN 20.

In this particular example, the NGI port to trunk setting could be the same as the GWS port setting. However, if you put the GRE tunnels (NGI to GWS) on a separate VLAN, you can then configure QoS on the tunnel traffic and lessen broadcast traffic.



For the steps to configure a VLAN with mobility, see "Configuring a mobile HotPort mesh node" on page 175.

For general information about VLAN concepts, see, "VLANs" on page 111.

Mobility views in HotView Pro

HotView Pro gives you a graphical and tabular view of static and mobile nodes and statistics for a mobility application. HotView Pro also lets you configure two different kinds of views:

- Linear view
- Aggregative (or depot) view

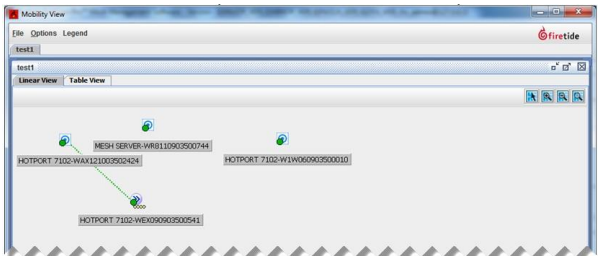
The aggregative view is specifically for video-offload deployments. From each view you can configure mobile nodes.

Filters options are available in an aggregative view, but not in a linear view.

Information in mobility views

The next image shows a linear mobility view:

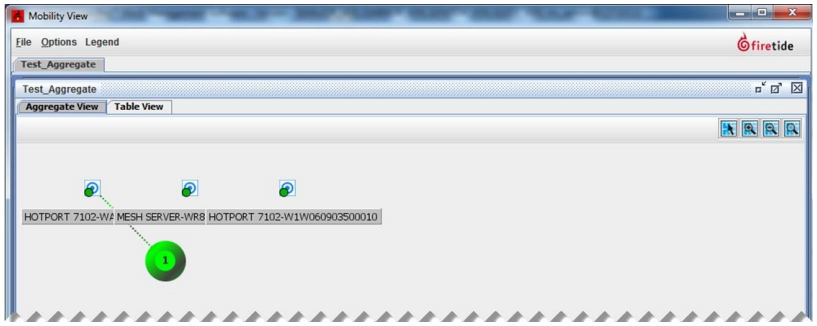
- Static nodes: Two HotPort 7102 nodes and one HotView Pro mesh server
- Mobile node: One HotPort 7102 with a double arrow icon to separate it from the symbol used with the static nodes



In a linear view, each device is represented by one icon.

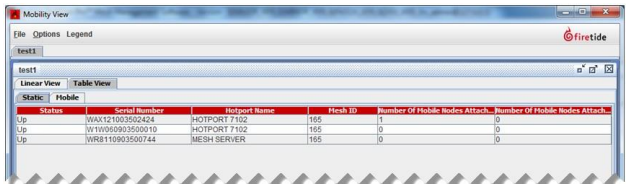
The next image shows an aggregate view:

- Static nodes: Two HotPort 7102 nodes and one HotView Pro mesh server
- Mobile node: One HotPort 7102, which is displayed as a solid green circle



In an aggregate view, groups of similar devices appear in a cloud with a number that represents the number of devices. For example, if you have 10 mobile nodes all attached to the same HotPort static mesh node and all 10 are up and running, a green cloud with the number 10 appears with a dotted line to represent the link. Reducing the number of icons on the monitor makes it easier to analyze the state of the network during video or data offload tasks.

The Table View tab lists information for static (Static tab) and mobile nodes (Mobile tab). The next image shows the table view.



Static node information includes:

- Node status (up or down)
- Serial number
- HotPort Name
- Mesh ID
- Number of mobile node attached to radio 1 and radio 2

Mobile node information includes:

- HotPort location
- Node status (up or down)
- Serial Number
- HotPort Name
- Mesh ID
- Static attachment serial number
- Local radio interface
- Remote radio interface

Mobility view icons

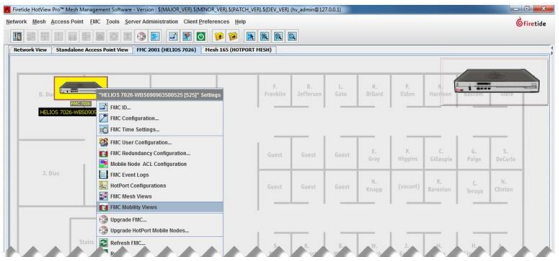
The next table shows the icons that appear in the FMC mobility views and their meanings.

Mobility view icon	View type	Meaning
	Linear	One static node that is up and running.
		One mobile node that is up and running. It has an attachment to a static node (green dotted line).
		One mesh server icon that is up and running.
	Aggregate	A green circle indicates a mobile node that is booted, running, and attached to the mesh. Any dotted green line to another node represents an attachment to a static node. The number is the number of mobile nodes.
		A blue circle indicates a mobile node that is booted, running and attached to any of the static nodes that are not displayed in the current view. The number is the number of mobile nodes the system detects in this condition.
		A red circle indicates a mobile node that is not connecting to the mesh and might not be running or might be running with failures. The number is the number of mobile nodes the system detects in this condition.

Creating a linear mobility view

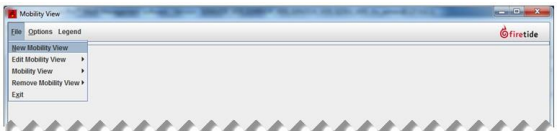
To create a linear mobility view:

1. Right-click the FMC device **> FMC Mobility Views**.

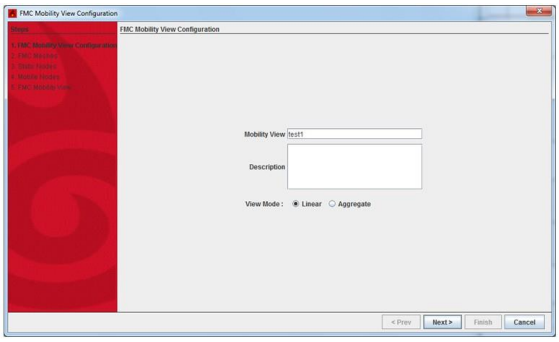


The Mobility View opens.

2. Go to **File > New Mobility View**.

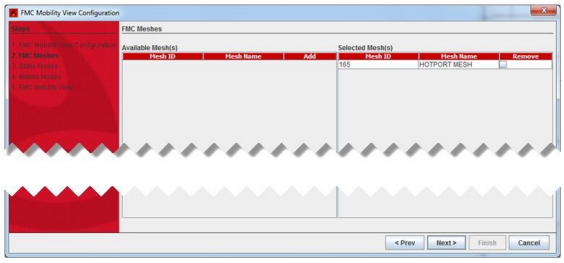


The FMC Mobility View Configuration wizard appears. The next image shows the wizard.



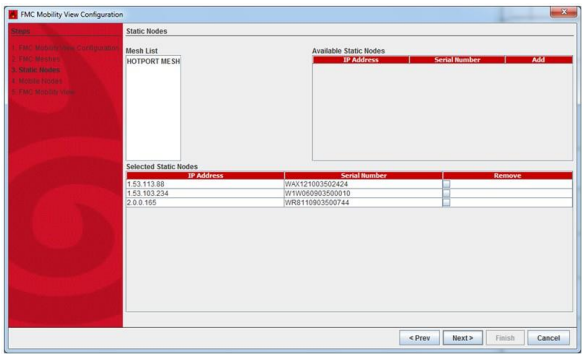
3. In the FMC Mobility View Configuration dialog, enter the configuration information:
   - Enter the mobility view name.
   - (Optional) Add a description in the text box.
   - Select **Linear**.
4. Click **Next**.

   The wizard takes you to the FMC meshes panel.

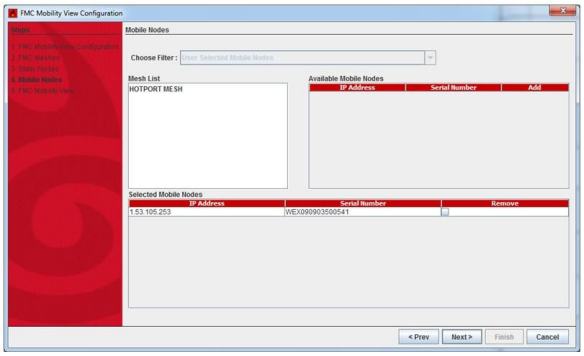


5. Select the FMC meshes to add to the view:
   a. Click **Add** in the Available Mesh table.
   b. Click **Next**.

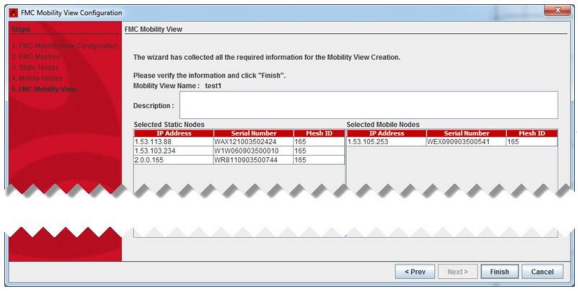
   The wizard takes you to the static nodes panel.



6. In the Available Static Nodes table, click **Add** to add the available static nodes in the mesh.
7. Click **Next** to add mobile nodes to the configuration.



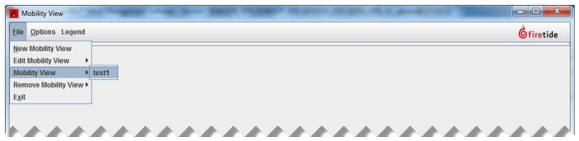
8. Click **Add** in the Available Mobile Nodes table.
   The system adds the selected nodes to the Selected Mobile Nodes table.
9. Click **Next**.
10. Make sure that you have the information you want in the view, click **Next** and then **Finish**.



Viewing a linear view file

To view a linear view file that you previously created:

1. Right-click the FMC device **> FMC Mobility Views**
2. Go to **File > Mobility View** and then select the name of the view you configured. The next image shows "test1" to be the available view file.



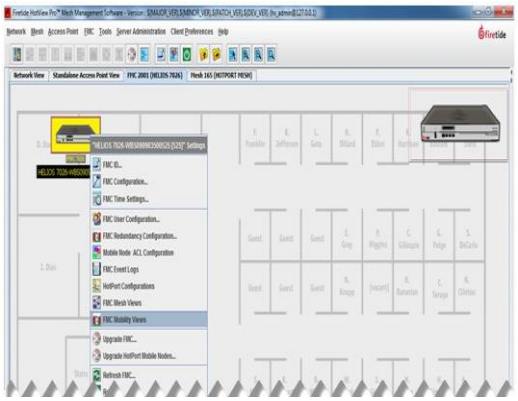
Two tabs appear: one with the name you configured, such as "test1," and one with a table.

Creating an aggregate mode mobility view

An aggregate view is a view where the system detects and shows you a graphical grouping of information. For example, the system shows a number of nodes in a cloud (circle) of a specific color. If you have 10 nodes that are working well, the number 10 appears in a solid green circle. If two nodes are not working, the number 2 appears in a solid red circle. For information about icon meaning, see "Mobility view icons" on page 198.

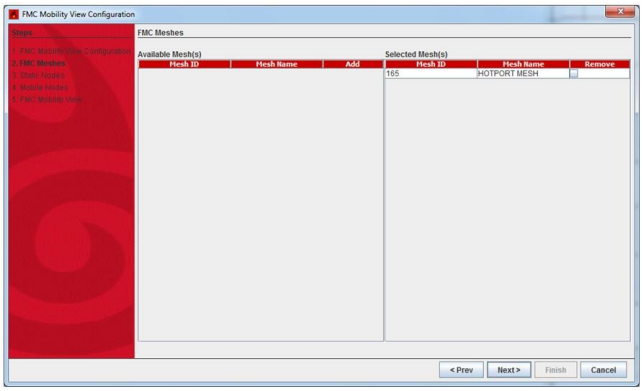
To create an aggregate mobility view:

1. Right-click the FMC device **> FMC Mobility Views**

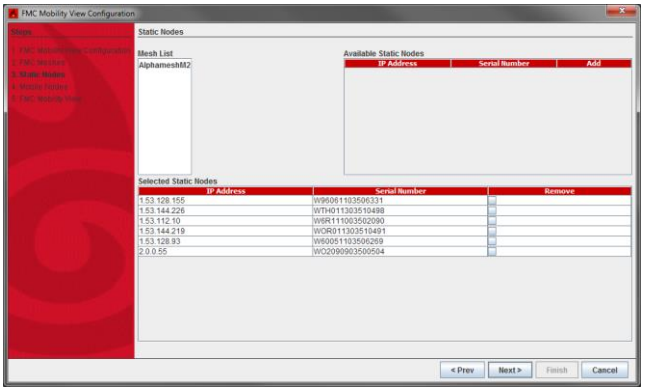


2. Go to **File > New Mobility View**
   The Mobility View wizard opens.

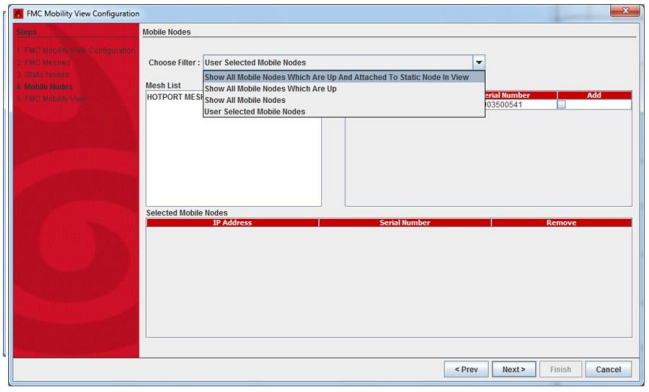
3. Enter the configuration information:
   - Enter a name for this view.
   - (Optional) Add a description in the text box.
   - Select **Aggregate**.
4. Click **Next**.
5. In the FMC meshes window, click **Add** to select the mesh or meshes that you want to add to the view.
6. Click **Next**.



7. Select the static nodes to add to the **Available Static Nodes** list, click **Next**.



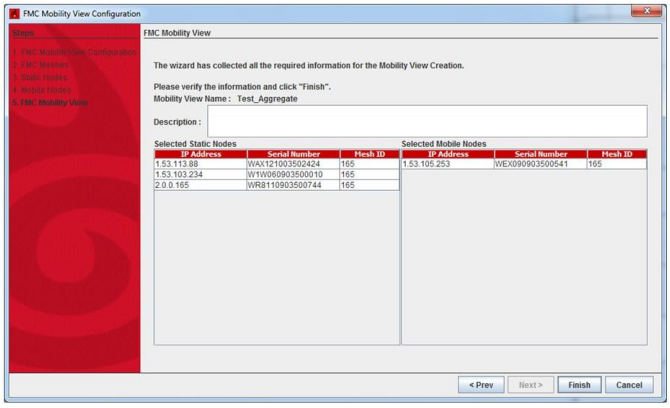
8. Add the mobile nodes from the Available Mobile Nodes table to the Selected Mobile Nodes table.



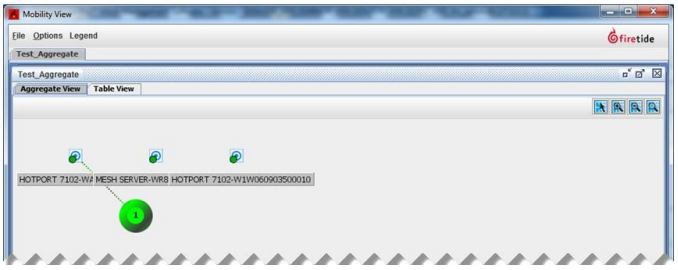
9. Select a filter. Filter options include:
   - Show all mobile nodes which are up and attached to the static nodes in the view.
   - Show all mobile nodes which are up.
   - Show all mobile nodes.
   - Show user-selected mobile nodes only.

   a. If you select User selected mobile nodes, select the mobile nodes from the available mobile nodes in the Available Mobile Nodes table.

   b. Click **Next**.



10. Click **Finish**.



Viewing expanded information in aggregate views

You can view more information about an aggregate cloud's contents with the expand feature.

To view details about the cloud:

1. With an aggregate view open, right-click a red, blue, or green cloud.
2. Select **Expand**.

A window containing the device serial numbers and status appears.

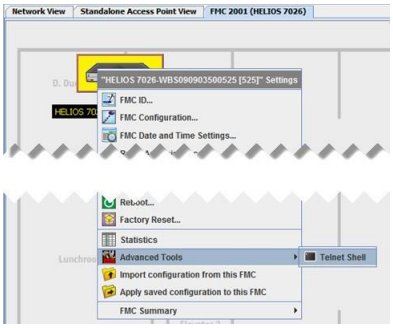
Telnet to FMC and Mobile Nodes

From HotView Pro you use telnet to communicate with FMC devices and mobile nodes. Even though the mobile nodes are not directly reachable you can seamlessly open and close telnet sessions and make configuration changes.

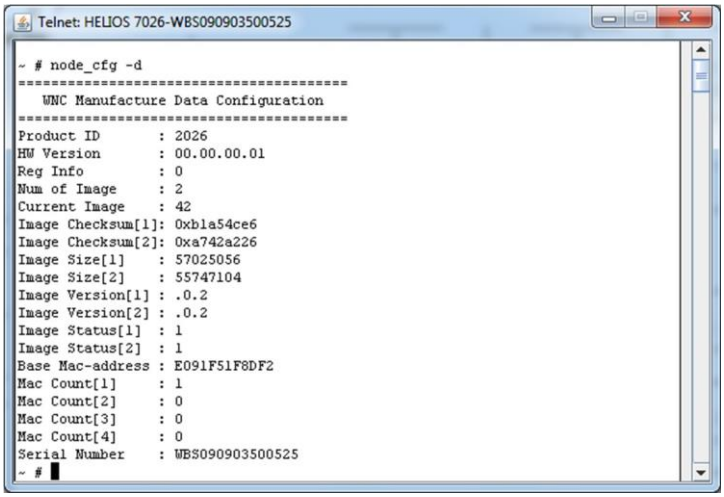
Starting a telnet session to an FMC device

To telnet to an FMC device:

1. Right click the FMC device icon **> Advanced Tools > Telnet Shell**
   The telnet login window appears.



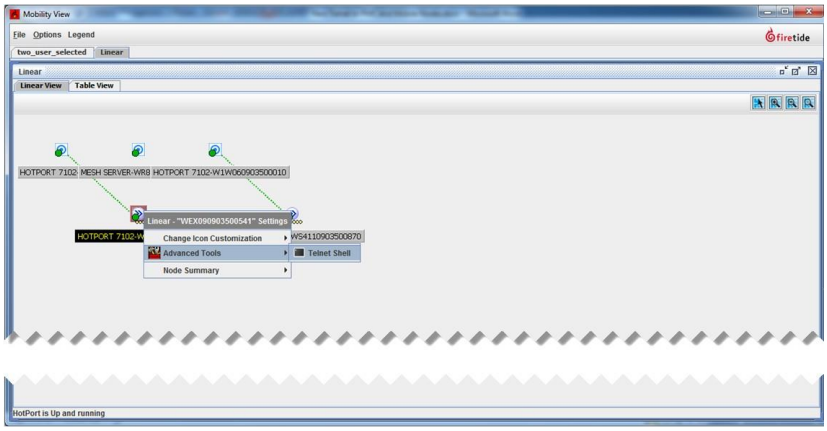
2. Enter the username and password for the FMC device.
3. Click **Log In**.
   The telnet window appears.



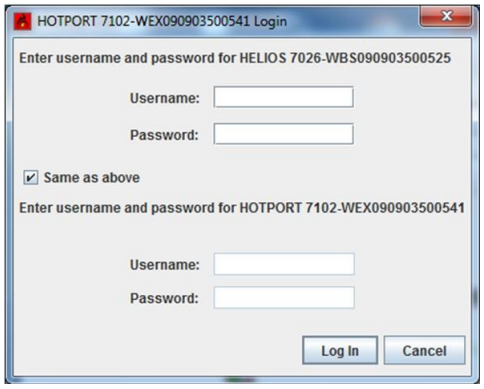
Starting a telnet session to a mobile node from a mobility view

To start a telnet session to a mobile node from a mobility mesh view:

1. Right-click the FMC device icon > **FMC Mobility Views**
2. Create a linear mobility view from the FMC device. "Creating a linear mobility view" on page 198.
3. Open the view you created in the previous step.

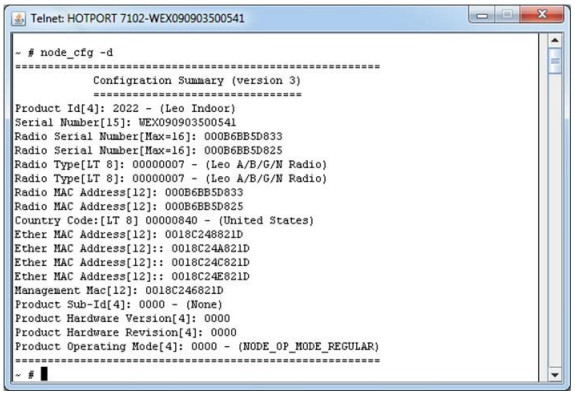


4. Right-click the mobile node > **Advanced Tools** > **Telnet Shell**
   The telnet login window appears.



5. Enter the login credential of the FMC device.
6. Enter the username and password for the mobile node.
7. Click **Log In**.
   The telnet session window appears.

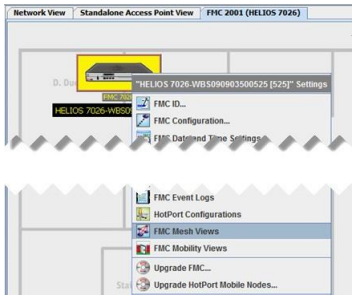
Telnet to FMC and Mobile Nodes



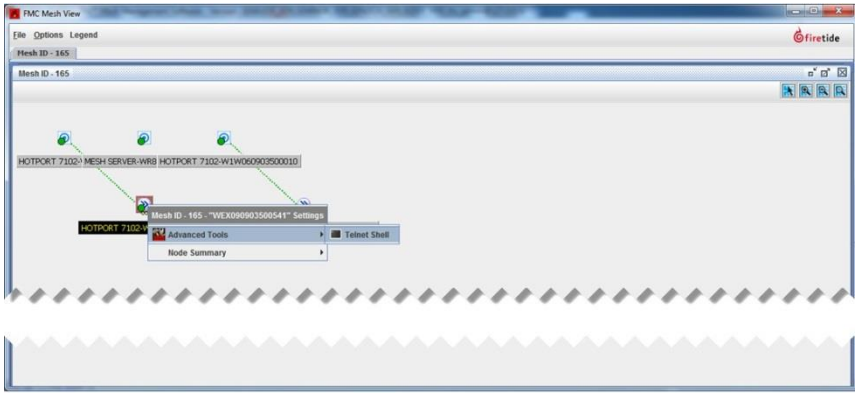
Starting a telnet session to a mobile node from the mesh view

To start a telnet session to a mobile node from the mesh view:

1. Right click on FMC **> FMC Mesh Views**

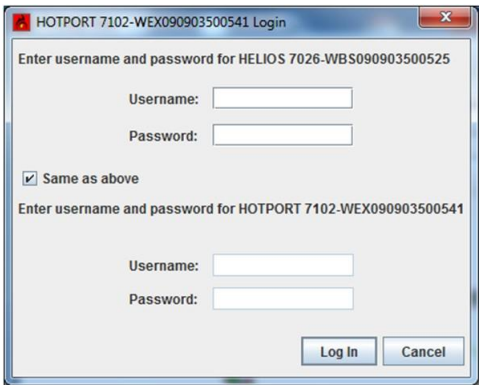


2. Open the mesh view.
3. Right click the mobile node **> Advanced Tools > Telnet Shell**



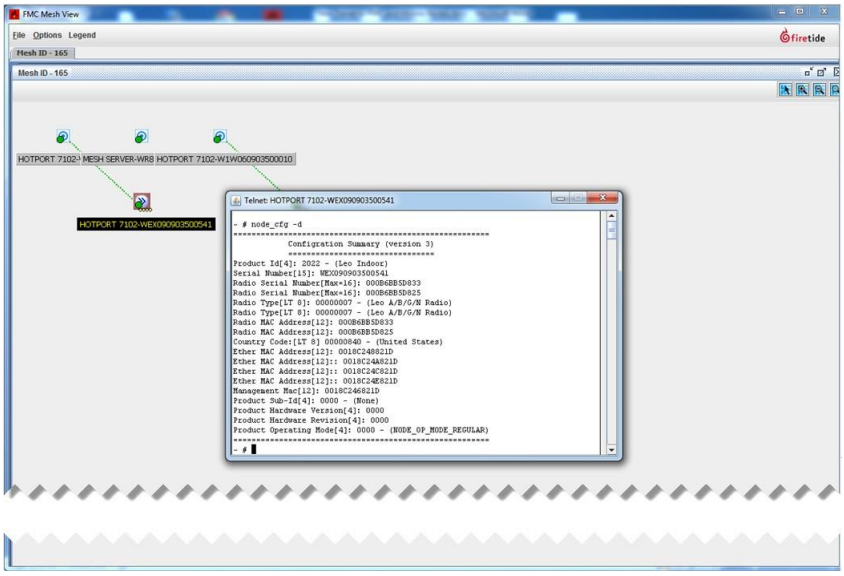
The telnet login window appears.

4. Enter the username and password of the FMC device and the username and password for the mobile node.



5. Click **Log In**.

   The telnet session window appears.



HotPoint Access Points

This section contains these chapters:

- Initial access point configuration
- Wireless LAN configuration
- Authentication and captive portal configuration
- Access point management
- Wireless distribution stations
- Wireless feature configuration
- Monitoring and reporting with HotView Pro
- Performance and diagnostic tools
- SNMP with HotPoint access points
- HotPoint access point MIB list
- Licenses for access points
- HotPoint access point messages
- HotPoint access point upgrade script

Initial access point configuration

HotPoint access points are DHCP clients. When you attach a HotPoint to a network that uses a DHCP server, it automatically uses an appropriate IP address.

Caution! If you don't have a DHCP server, then all of the default settings are the same for all access points. Do not give more than one HotPoint device power at a time. If you give power to two or more devices, address conflicts occur.

To do the initial configuration of a HotPoint access point:

1. Log into the access point.
    a. Go to **HotView Pro > Access Point > Standalone AP Configuration**
    b. Enter the default IP address of an access point: 192.168.224.160
    A standalone access point appears in the Standalone AP tab of HotView Pro.
2. Assign a management IP address to the access points. The IP address must be reachable. It does not need to be on the same subnet as the management address of the Firetide mesh.

Note: Firetide recommends that you not use DHCP to assign the management IP address to HotPoint access points. If you are using DHCP for standalone access points, you must capture the IP address assigned by the DHCP server to each HotPoint.

3. Log into the access point again.
    a. Right-click the access point **> Log in**
    b. Enter the new management address.
    c. Click **Log in**.
4. Set the Country Code. See "Setting the country code" on page 214.
    a. Go to
    b. Select the country in which you intend to operate the device.
    c. Click **Save**.
5. Change the default password. See "Changing the default password for an access point group" on page 215.
6. Add a descriptive name for the access point.
    a. Right-click the access point **> HotPoint Location**.
    b. Enter a description.
    c. Click **Save**.
7. Set the radio settings (channel and so on) for each access point:
    a. Right-click the access point **> Radio Settings**

b. Enter the settings.
c. Click **Save**.

Repeat steps 1 through 7 for all access points.

To manage the access points:

1. Create one or more VAP Groups. You must have at least one group, even if you only have one AP.
2. Configure those VAP features that are controlled by each access point, such as DHCP, DNS, and NAT.
3. (Optional) Assign the SSID, security, and other features for the entire VAP group. Make an access point group that contains all of the access points. You can make more than one group if you need multiple management domains.

Loading a standalone access point group

After you log in for the first time and do initial configuration, do these steps the next time you log in.

Prerequisites:

- HotView Pro is installed and running.
- One VAP or more is configured.
- One VAP group is configured.

To load a standalone access point group:

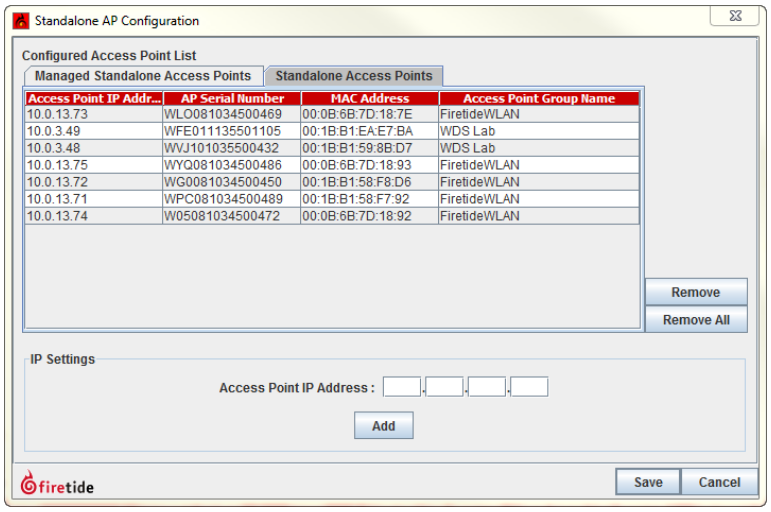
1. Go to **Access Point > Load Standalone AP Group**
2. (Optional) Check the Login to Standalone AP feature.
3. Enter the password.
4. Click **Log in**.

Adding a standalone access point

To add a new standalone access point:

1. Go to **Access Point > Standalone AP Configuration**
2. Click the Standalone Access Points tab.
3. In the IP settings section, enter the IPv4 address.

4. Click **Add**.
5. Click **Save**.



Removing a standalone access point

To remove a standalone access point from management:

1. Go to **Access Point > Standalone AP Configuration**
2. Select an access point.
3. Click **Remove** to delete only the selected access point, or click **Remove All** to delete all of the access points from the list.

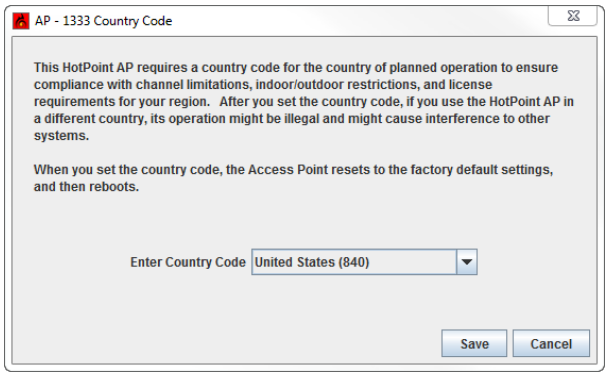
Setting the country code

You want to set the country code to change the device from a low-power, low range setting to a correct full-power operational mode.

Caution! Make sure you configure the device for the correct country. If you do not configure the country correctly, the device might operate in a manner that is not legal or create problems with other wireless devices.

To set the country code:

1. Right-click the access point > **Country Code**
2. Select the country in which you intend to operate the device.
3. Click **Save**.

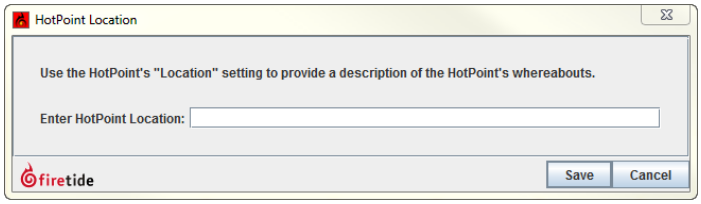


Adding a description to the access point

You can add a description to the access point, such as a meaningful location.

Prerequisite: None

1. Right-click the access point > **HotPoint Location**.
2. Enter a description.
3. Click **Save**.



Changing the default password for an access point group

An access point group can have one or more access points. When you modify an access point group login (user name or password), you change the login for all group members.

To change the machine login for an access point group:

1. Go to **Server Administration > Configure HotView Server**
2. Click the Network Management tab to view the machine accounts.
3. Click the AP Group tab to view access points.
4. From the list at the top of the workspace, select the name of access point group that you want to modify.
5. Edit the entry details that appear in the bottom half of the workspace.
6. Click **Reset**.
7. Click **Apply**.

Configuring port forwarding

When you set up port forwarding, you should follow this task sequence:

1. (Optional) Configure DHCP. DHCP lets the system auto-populate partial IP addresses in the port forwarding table.
2. Enable and configure NAT.
3. Configure port forwarding.

   Ensure that applications that use the same protocol, such as TCP, UDP, or both, do not have overlapping ports assigned to them.

To configure port forwarding for specific applications:

1. (Optional) Configure DHCP.
   a. From the Configuration tab, click **VAP > Basic > IP/DHCP**
   b. Select **Enable**.
   c. Enter the IP range, default router IP address, primary and secondary DNS server IP addresses.
   d. Click **Apply**.
2. From the Configuration tab, click **VAP > Advanced > Network**
   a. Select NAT state and optionally gateway feature.
   b. Enter the NAT IP address, which is the IP address of the access point.
   c. Click **Apply**.
3. From the Configuration tab, click **VAP > Advanced > Port Range**
   a. Select an empty entry.
   b. Select **Enable**.
   c. Enter a meaningful name for the entry, the start port, the end port, protocol.
   d. Enter the IP address (if DHCP is not enabled) or add the missing part of the IP address.
   e. Click **Apply**.

Wireless LAN configuration

HotView Pro lets you create a wireless LAN with access point (AP) groups and virtual access points (VAPs). An AP group is one or more physical access points. A VAP is a virtual access point. In an enterprise, you might have dozens or hundreds of VAPs. To simplify management, you can organize VAPs into VAP groups. A VAP Group is two or more VAPs.

The system requires one VAP group with at least one VAP in the group.

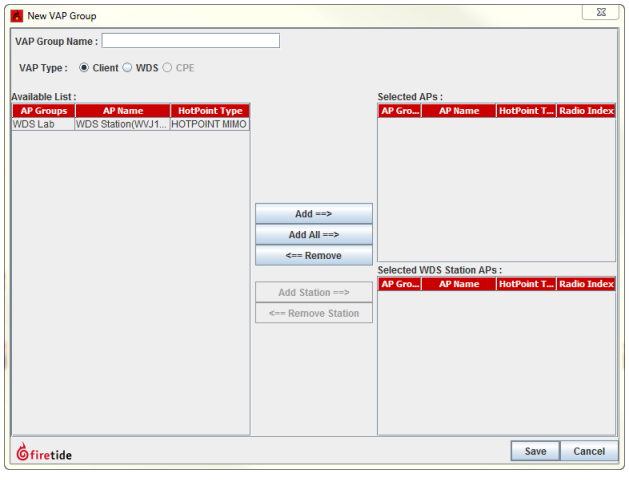
Creating a new virtual access point group

You can create virtual access point groups for clients or for wireless distribution stations (WDS). For more information and procedures specifically for WDS configuration, see "Wireless distribution stations" on page 246.

To create a VAP group:

1. Go to **Access Point > VAP Group Configuration**
2. Click **New VAP Group**.
3. Select the VAP type: client or WDS.
4. Select the access points that you want in the group one by one, and then click **Add**.
5. Click **Save**.

   After you create the VAP Groups, you can configure the group. Each radio can be assigned to a different VAP Group.

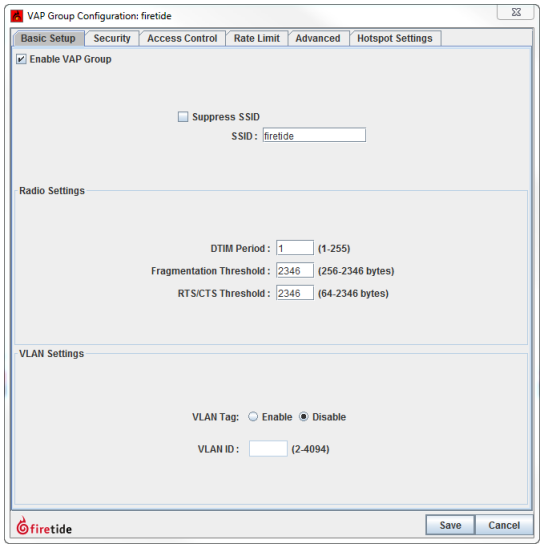


Configuring a virtual access point group

Note: Optionally, you can access the configuration screens from a right-click on an access point > VAP Group Configuration > <name of VAP Group>.

To configure a group of virtual access points:

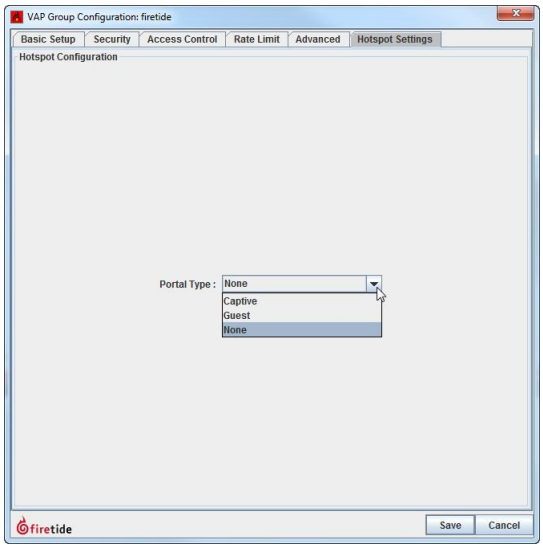
1. Go to **Access Point > VAP Group Configuration**
2. Click **Configure Group**.
3. On the Basic Setup tab, enter these settings:
   - Check Enable VAP Group.
   - (Optional) Check suppress SSID.
   - Enter the SSID.
   - Enter the radio settings:
     DTIM period (1 to 225; default value is 1)
     Fragmentation threshold in bytes (256 to 2346; default value is 2346)
     RTS/CTS threshold in bytes (64 to 2346; default value is 2346)
   - Enter the VLAN settings: disable (default value), or enable and enter a VLAN ID (2 to 4094).



4. On the Security tab, enter these settings:
   - Enable or disable the wireless security state.
   - Select an authentication type. Depending on which type you select you might have to enter encryption keys, RADIUS, or other settings.
5. On the Access Control tab, enter these settings:
   - Select to prevent or permit the MAC addresses in the list.
   - In the new list entry section, enter a MAC address, and then click **Add**. The system shows the MAC address in the list.

6. On the Rate Limit tab, enter these settings:
   - Enable or disable the user rate limit feature. When you enable this feature, you must also enter the rate limit from 64 Kbps to 5 Mbps.
   - Enable or disable the VAP rate limit feature. When you enable this feature, you must also enter the rate limit from 64 Kbps to 5 Mbps.
7. On the Advanced tab, enter these settings, enable or disable (default value) intra-cell blocking.
8. On the Hotspot Settings tab, select the portal type: captive, guest or none.

   For more information about HotSpot configuration, see "Authentication and captive portal configuration" on page 222.



9. Click **Save**.

Editing a virtual access point group

When you add a new access point, you need to ensure that the VAP group configuration is consistent with the configuration of the other group members. Inconsistencies can cause unexpected behavior. Security settings must be saved and updated even if no explicit configuration change is made.

To ensure consistent access point configuration, see "Comparing virtual access groups" on page 261.

To edit a virtual access point group:

1. Go to **Access Point > VAP Group Configuration**
2. Click **Edit VAP Group**.

3. Make your changes. You can change the radio index or remove one or all of the access points from the VAP group.
4. Click **Save**.

Intra-cell blocking

You can use intra-cell blocking to block clients from contacting each other. For example, if you disable intra-cell blocking and multiple wireless clients (such as W1 and W2) are associated with an access point and the clients get the DHCP IP address from the DHCP server on the VAP or from an external DHCP server, client W1 can ping W2 each other.

If you enable intra-cell blocking, a client cannot ping any other client.

To set the intra-cell blocking feature, see "Configuring a virtual access point group" on page 219.

Authentication and captive portal configuration

Part of the virtual access point (VAP) group configuration is a group of settings that let you configure authentication locally or with a RADIUS server and captive or guest portal services. These features let you design the wireless client's user experience:

- User logs in with a user name and password
- User logs in with email address only
- User does something and is required to watch something before continuing onto where the user wants to go

By default these features are disabled (none).

Authentication process

For user authentication, the system supports:

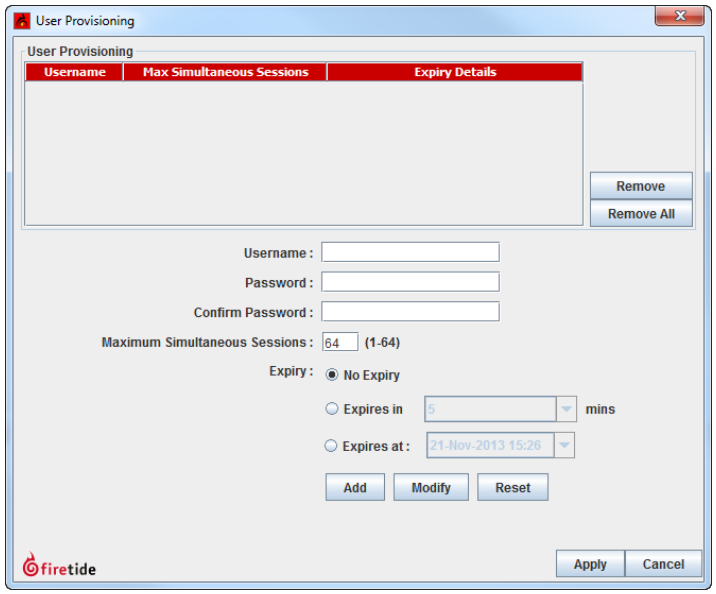
- Internal authentication with user provisioning
- External authentication with RADIUS

When a client enters their user name and password combination in the redirect web page:

1. The system sends the credentials to the captive application.
2. The captive application checks the internal user database that is stored in the access point.
3. If the credentials are not authenticated in the internal database, the user is denied access. If external authentication is configured, however, the system sends an access request to an external database, a RADIUS server.
4. If the credentials cannot be authenticated in the primary RADIUS server, the user is denied access. If a back up RADIUS server is configured, the system sends an access request to the backup RADIUS server.

HotPoint user management

An administrator can provision up to 32 users for each virtual access point (VAP).



Supported expiration options

For each user you can set one of these expiration options:

- No expiry. Users with this option never expire. Clients can use these user credentials forever.
- Expiry In [1 to 59 minutes] after First Login. With this option you can create users whose access expires after a specified period from the first login.
- Expiry At [Absolute Time and Date]. This option creates user accounts that expire at an absolute time. This kind of account expires even if no one logs in at the predefined time.

Tips for successful user provisioning

When the provisioned user expiry is reached, the connected clients become unauthenticated. The system redirects the clients to the redirect page and will not be able to access the Internet. If the configuration is not for single-time access, they can enter their credentials again.

If you modify or delete a user, all clients authenticated with those credentials become unauthenticated.

Expiry In [1 to 59 minutes] after First Login is not recommended for VAP groups that have more than one access point. Access points cannot communicate between each other, so the first login information is not propagated. Clients end up accessing the Internet separately from multiple access points.

For clients authenticated using internal authentication (user provisioning), no accounting information is sent to external RADIUS servers.

User names must be unique alphanumeric strings and from 6 to 32 characters in length.

A password is a string from 1 to 32 characters in length. Special characters are supported.

You can configure a maximum number of simultaneous sessions for each user. The maximum simultaneous session limit can be from 1 to 64.

For a guest portal each email ID must be unique for each client. An email ID cannot be used by more than one client at the same time.

When an authenticated user logs out, their usage summary appears:

- Data uploaded in kilobytes (KB)
- Data downloaded in KB
- Time used
- Time remaining

External Authentication (RADIUS server) and backup

If the credentials fail in the internal authentication then an access request is sent to the external database, a RADIUS server. You can configure a backup RADIUS server, too.

Supported authentication types

As part of the WLAN configuration, HotView Pro supports several kinds of authentication. The next table lists the available authentication types and the required information.

Authentication type	Settings
WPA-AUTO-Enterprise	Cipher option is TKIP. You must enter these RADIUS settings: - RADIUS server IPv4 address - RADIUS server port number - RADIUS server accounting port number - RADIUS server secret key
WPA2-Enterprise	Cipher option is AES-CCM. You must enter these RADIUS settings: - RADIUS server IPv4 address - RADIUS server port number - RADIUS server accounting port number - RADIUS server secret key
Open	Enable or disable this security state. Cipher options are none or WEP.

Authentication type	Settings
Shared key	Cipher option is WEP. Encryption key settings are: - Select a default key ID. - Enter up to four encryption keys. - Select a key length of 5 or 13 (default value).
WPA-AUTO-PSK	Cipher option is TKIP. Enter a pass phrase. Enter a group key update interval, which is a number between 1 and 3600 seconds; 600 is the default value).
WPA-PSK	Cipher option is TKIP. Enter a pass phrase. Enter a group key update interval, which is a number between 1 and 3600 seconds; 600 is the default value).
WPA2-PSK	Cipher option is AES-CCM. Enter a pass phrase. Enter a group key update interval, which is a number between 1 and 3600 seconds; 600 is the default value).

Table 23

Prerequisites to use RADIUS authentication

To do internal authentication you must install freeRADIUS, which is included in the HotView Pro software installation package. When you install HotView Pro to the HotView Pro server, select the optional freeRADIUS module.

The primary and backup RADIUS servers must be in sync.

After successful authentication, the access point sends an accounting START request to the RADIUS server. An accounting ALIVE request is sent at 15-minute intervals. When the client disassociates or logs out, the access point sends an accounting STOP request to the RADIUS server. Accounting ALIVE and STOP requests carry the data, such as ingoing and outgoing bytes and frames, and so on.

Captive portal

A captive portal requires user authentication.

Wireless clients that come to a captive portal enter credentials, a user name and password, before the access point allows access to a wireless network. The allowed list of users can be managed either from a local database and, optionally, a RADIUS database.

Walled garden domains

Walled garden domains are areas that clients can access without authentication. While browsing these domains, clients are redirected to a specific URL, such as the URL entered in the redirect URL field.

You can configure up to 32 walled garden domains by IP address or domain name.

Guest portal

A guest portal requires no user authentication. Email IDs are required for administrative purposes.

Wireless clients that come to a guest portal enter their email address to access a wireless network or the Internet.

How custom web pages work

The captive portal configuration workspace lets you browse to and upload a custom redirect web page with the extension .html or .htm. This web page appears when a client goes to the home URL instead of the default redirect page. To use a custom web page, you have to modify the web page so that it can pass the user's credentials (user name and password) to the access point for authentication. For more information, see "Script: redirecting a client to a different login page" on page 229.

After authentication, the client's browser opens to the homepage URL.

Access points keep the custom web pages in memory until change of Redirect URL type.

Custom web page guidelines include:

- Keep the file sizes small. The maximum file size is 32 KB for each VAP.
- Make sure you do not exceed the device cumulative total memory. The access point cumulative maximum size is 128 KB.
- Custom web pages cannot have references to external web pages or images.

Terms for the configuration page include:

- Home page URL is the URL that you want the client's browser to automatically load after user authentication happens.
- Customized URL is a custom web page that you create and add scripts and functions to so that it can pass login credentials to the access point for authentication.
- Redirect URL is the type of client redirection and can be remote, custom, or default.

Accessing the HotSpot features in HotView Pro

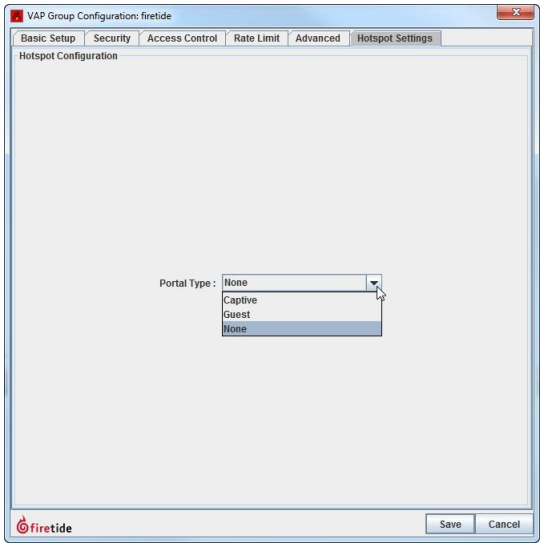
HotSpot features are disabled by default (none).

Note: Optionally, you can access the configuration screens from a right-click on an access point > VAP Group Configuration > <name of VAP Group>.

To access the HotSpot features:

1. Go to **Access Point > VAP Group Configuration**
2. Click **Configure Group**.
3. On the Hotspot Settings tab, select the portal type: captive, guest or none.

   For more information about HotSpot configuration, see "Authentication and captive portal configuration" on page 222.



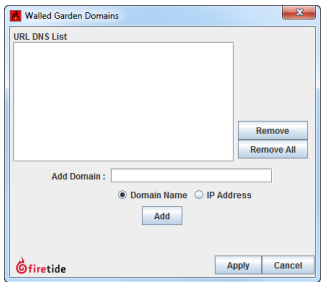
Different workspaces appear depending on your selection.

You are now ready to configure the guest or captive portal.

Configuring a custom captive portal

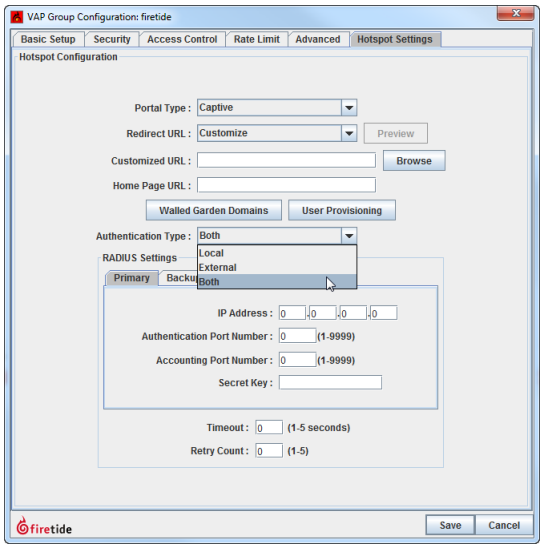
To configure a captive portal:

1. Go to **Access Point > VAP Group Configuration**
2. Click **Configure Group**.
3. On the Hotspot Settings tab, select the portal type: captive.
4. For the type of redirect URL, select **Customize**.
5. Enter the customized URL.
6. Enter the home page URL. For example, *www.firetide.net*.
7. Click **Walled Garden Domains**.



a. Enter one or more domains or IP addresses.
b. Select the input type: Domain Name or IP Address.
c. Click **Add**.
d. Click **Apply**.

8. (Optional task) Provision users.
9. Select the authentication type: Local, External, or Both.
10. If you selected Local, click **Save**. If you selected External or Both, enter the RADIUS information for the primary RADIUS server.
    a. Enter these settings:
        - IP address
        - Authentication Port Number, which is a value from 1 to 9999
        - Accounting Port Number, which is a value from 1 to 9999 but is not the same as the authentication port number
    b. Enter a secret key.
    c. Enter the RADIUS timeout, which is a period of 1 to 5 seconds.
    d. Enter the retry count, which is 1 to 5 times.
11. (Optional) Click **Preview** to view the custom page before you save it.
12. Click **Save**.



Configuring a simple guest portal

To configure a guest portal:

1. Go to **Access Point > VAP Group Configuration**
2. Click **Configure Group**.
3. On the Hotspot Settings tab, select the portal type: guest.
4. For the type of redirect URL, select **Default**.
5. Enter the home page URL. For example, *www.firetide.net*.
6. Enter the session length in hours and minutes. You can enter periods of 1 minute to 24 hours.
7. Click **Save**.

Configuring a guest portal that goes to a remote or custom web page

To configure the user to be sent to a remote web page for portal login:

1. Go to **Access Point > VAP Group Configuration**
2. Click **Configure Group**.
3. On the Hotspot Settings tab, select the portal type: captive, guest.
4. For the type of redirect URL, select Remote or Custom.
5. Enter the URL for the remote or custom page.
6. Enter the home page URL.
7. Enter the session length in hours and minutes. You can enter periods of 1 minute to 24 hours.
8. Click **Save**.

Configuring logout support

To get the logout page client has to type the 1.254.254.254 IP address in their browser. Logout is valid both for RADIUS-authenticated clients and local database-authenticated clients.

Script: redirecting a client to a different login page

In the following code snippet *nasip* is the IP address of the HotPoint access point. The access point appends the *nasip* in the redirect URL.

Paste this script in the head of the index.html page.

```
<script language="JavaScript">
function gup( name )
{
    name = name.replace(/[\[]/,"\\\[").replace(/[\]]/,"\\\]");
    var regexS = "[\\?&]"+name+"=([^&#]*)";
    var regex = new RegExp( regexS );
    var results = regex.exec( window.location.href );
```

```
    if( results == null )
        return "";
    else
        return results[1];
}

function doLogin() {
var uname =document.getElementById('username').value;
var passwd =document.getElementById('password').value;

if ( !uname.length || !uname.replace(/\s/g, '').length
||(uname.length > 63) ||
     !uname.match
     (/(^[a-zA-Z0-9]+(?:[._+-][a-zA-Z0-9]+)*)([@][a-zA-Z0-
9]+(?:[.-][a-zA-Z0-9]+)*[.][a-zA-Z]{2,})*$/) ){
    alert("Please enter a valid user name. A user name can be up
to 63 characters in length.");
    return false;
}

if ( !passwd.length || !passwd.replace(/\s/g, '').length
||(passwd.length > 63)){
    alert("The password field cannot be blank. Please enter your
password.");
     return false;
}

window.open("http://"+gup('nasip')+"/cgi-bin/
rdr.cgi?username="+uname+"&password="+passwd, "_self");
return false;
}
```

Script: logging into and out of a remote or custom web page

When you set up log in and log out with credentials, you have to add scripts to do log in and log out actions. In the next code snippet *nasip* is the IP address of the HotPoint access point. The access point appends the *nasip* in the redirect URL.

To login or authenticate a client, paste this function in the head of the target page:

```
function doLogin() {
window.open("http://"+gup('nasip')+"/cgi-bin/
rdr.cgi?username="+uname+"&password="+passwd, "_self");
}
```

For logout or stop access (de-authenticate), add this function in the head of the target page:

```
function doLogout() {
window.open("http://"+gup('nasip')+"/cgi-bin/
captive_logout.cgi"_self");
}
```

Script: collecting user data

To record user information and statistics, paste this code snippet into your remote or custom web page with the other scripts:

```
function getStats() {
window.open("http://"+gup('nasip')+"/cgi-bin/
captive_logout.cgi?stats_flag=1"_self");
}
```

Note. One URL request goes to the external web server for the login and logout pages. The auth_type is 1 for login and 1 for logout.

Disabling a captive portal or guest portal

To disable a captive or guest portal:

1. Save a backup copy of any custom portal web pages that are saved on the access point. When you change the portal type to “none” the access point deletes the custom web pages that were kept.
2. Go to **Access Point > VAP Group Configuration**
3. Click **Configure Group**.
4. On the Hotspot Settings tab, select **None**.
5. Click **Save**.

Access point management

The configuration of access point groups is one way to organize and simplify configuration of large numbers of access points.

For example, a hospital that has 100 access points in four different buildings could organize the access points into four access point groups. Chances are that many of the access point will have the same configurations. Instead of 100 individual access point configuration files, the administrator can configure the four groups of access points.

When using with network monitor server and access point groups, you can log into all access points in a group at the same time.

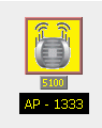
When you log into HotView Pro several different views are available for access points. The main tab is Standalone Access Point View from which you can see:

- Access Point Group View where you can go to the group tab, log in or out of the access point group, or view a group summary (AP group name and number of access points)

- Tabs by access group view name

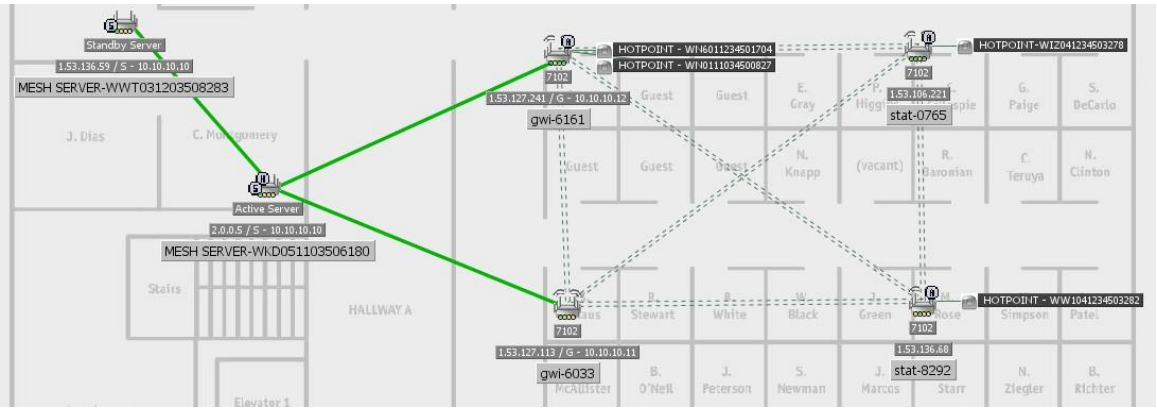
Terms related to access point management

Standalone access point is a HotPoint access point that does not need any other device to work and be configured or managed. Access points do not communicate with each other, so by definition, are all standalone. The next figure shows a standalone access point icon.



Integrated access point is a special configuration made from a nearby HotPort 7020 mesh node. By default the integration feature is enabled, so that when you log into HotView Pro you will be able to see nearby access points.

The next figure shows integrated access points in the mesh view. The access points are to the right side of the mesh nodes.



Managed access point is a HotPoint access point that the network monitor server tracks. For procedures to set up this feature, see "Setting the network monitor server settings" on page 236.

Configuring an access point group

By default when you load a standalone access point, it goes into a default access point group. From there you can create a new access point group, name it with a meaningful label, add access points to it and then configure them as a group.

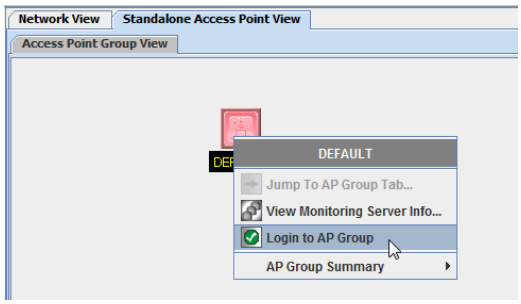
The next table lists the default usernames and passwords for new access point groups.

Privilege	Username	Password
Read-write	admin	firetide
Read-only	guest	firetide

Table 24

To configure an access point group:

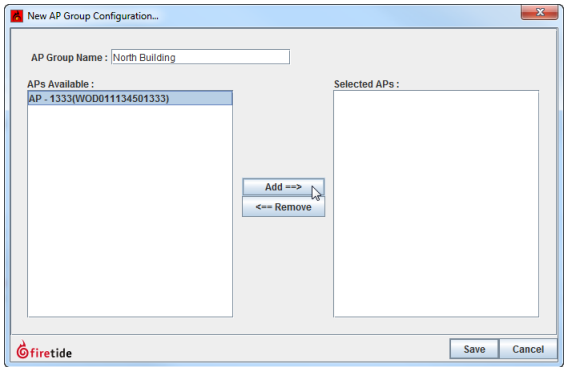
1. Log into the default access point group.
   a. Right-click the default access point group icon **> Log into AP Group**



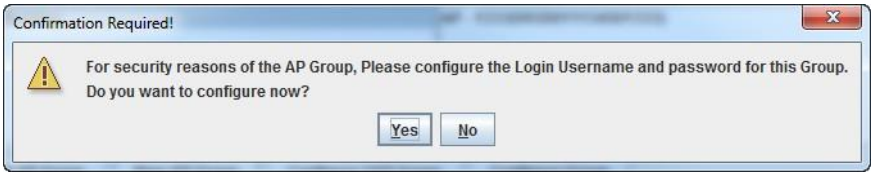
b. Enter the password for the default group.

c. Click **Log In**.

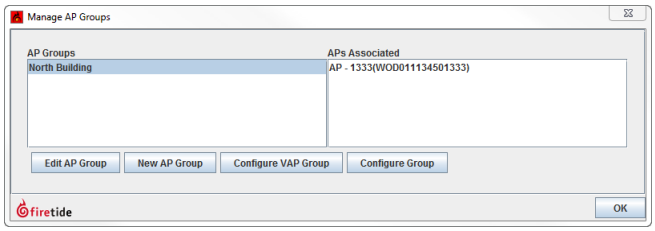
2. Go to **Access Point > AP Group Configuration**
3. Select **New AP Group**.
4. Enter the AP group name, for example, North Building.
5. Select the access point that you want to add to the group, and then click **Add**.



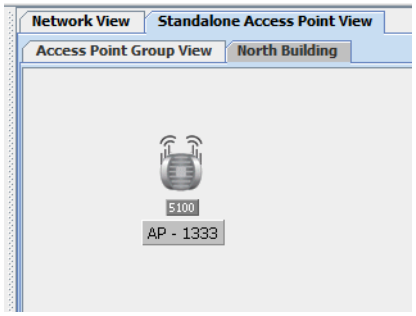
6. Click **Save**.



7. When the system prompts you to change the usernames and passwords for this AP group, click **Yes**.
8. Enter new user names and passwords for the read-write and read-only user accounts for this group.
9. Click **Save**.



10. Click **OK** to exit the Manage AP Groups workspace.



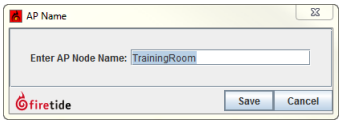
The system creates a tab with the AP group named *North Building*.

Naming an access point

Prerequisite: None

To name an access point:

1. Right-click the access point **> Rename AP**.
2. Enter a name.
3. Click **Save**.



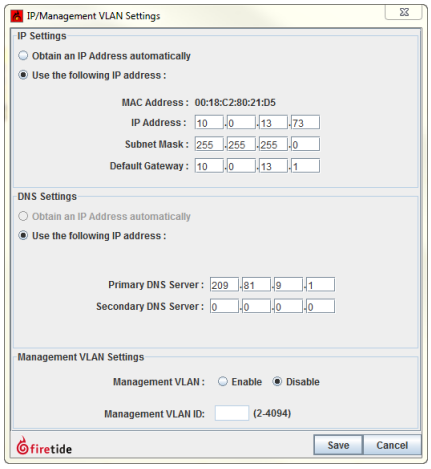
Configuring network settings

To configure the network settings of an access point:

1. Right-click the access point **> IP/Management VLAN Settings**
2. Enter these settings:
   - In the IP section: enter the IPv4 address, subnet mask, and default gateway address.
   - In the DNS section: select whether or not to use a DNS server. If DNS is enabled, enter the primary and secondary DNS IPv4 addresses.

- In the VLAN section: select whether or not a management VLAN is used. If VLAN management is enabled, enter the management VLAN ID.

3. Click **Save**.



Setting the network monitor server settings

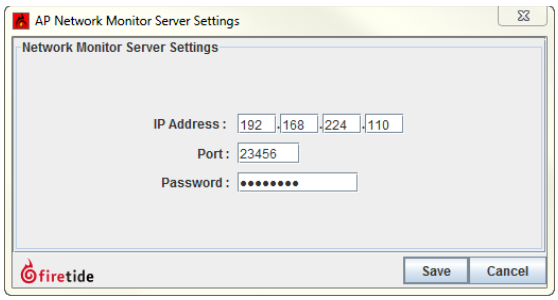
If you want to manage HotPoint access points from HotView Pro without logging into the access points:

1. Set up the network monitor server. For the network monitor server procedures, see the *HotView Pro Reference Manual*.
2. Log out of HotView Pro and then log in again.
3. Follow the steps in this section to point the access points to the network monitor server.

After the configuration is complete, you can see statistics from the access points without having to log in. The access points managed through the network monitor server appear in a table on the Managed Access Points tab in the Standalone AP Configuration window.

To set the network monitor settings on the HotPoint access point:

1. Right-click the access point > **AP Network Monitor Server Settings**
2. Enter the IPv4 address, port number, and password.
3. Click **Save**.



Changing read/write access

To prevent write access to all members in an access point group:

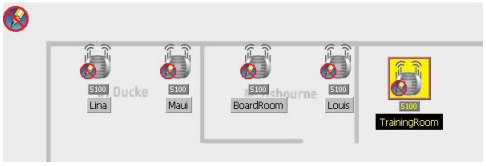
1. Right-click an access point.
2. Go to **Release Write Access**.

The system locks all write access for the selected group until you unlock this setting.

To restore write access:

1. Right-click an access point.
2. Go to **Acquire Write Access**.

The next figure shows no write access.



Logging into an access point

To log into an access point:

1. Right-click the access point > **Login**
2. Enter the administrative password.
3. (Optional) Check **Apply to all AP(s) in the Group**.
4. Click **Login**.

Upgrading firmware with HotView Pro

This procedure is for upgrading the firmware of mesh nodes, 5020-Es, access points, and FMC devices.

Caution! If the mesh has high security enabled, you must upload the .bin2 file. If you try to load the .bin file, the upgrade will fail.

By default, the system uses the configuration in cache for multiple upgrades.

Best practice: Upgrade the image two times because you want the backup image and primary images to be the same. If a backup image is older than the primary image, the node might not support the same features.

With the upgrade scheduler you can:

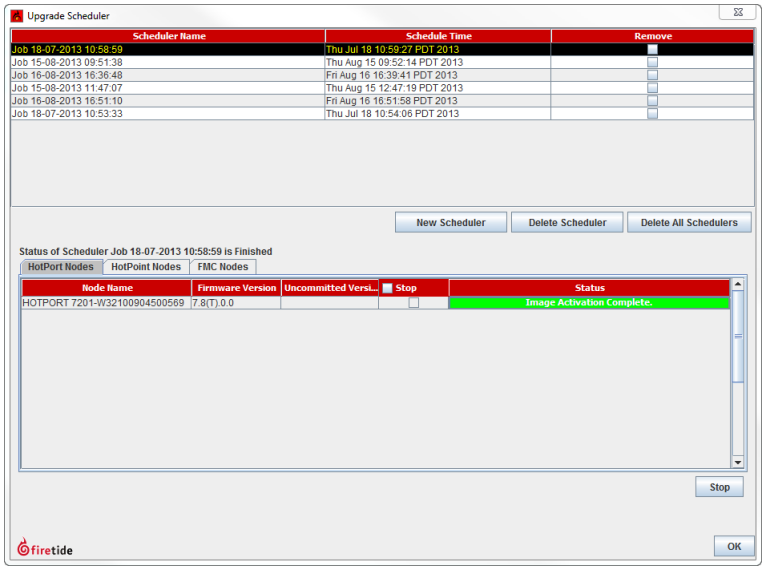
- Upgrade and activate the firmware now.
- Upgrade the firmware now and activate it later.

When you schedule an upgrade time (Scheduler Operation: Later), the HotView server, if it is running, starts the job at the scheduled time. If the HotView server is not running at the time scheduled, the scheduled jobs start immediately after you start the HotView server.

Best practice: If you choose to upgrade a production mesh, schedule the upgrade and activation for a convenient time. Firmware upgrades can consume considerable bandwidth. The mesh is not available for two minutes when you activate new firmware.

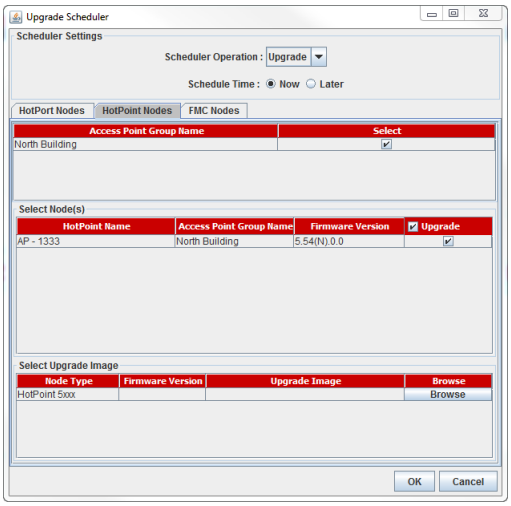
To schedule a firmware upgrade for a later date:

1. Go to **Network > Upgrade Firmware**
   The upgrade scheduler appears.



2. Click **New Scheduler**.

a. Select Upgrade.
b. Select the time: Later. Use the calendar to set the date and time.
c. Click the tab to select a device type, such as HotPoint Nodes, and then select the mesh or device by ID or name.



3. Select the upgrade image.
4. Click **OK**.

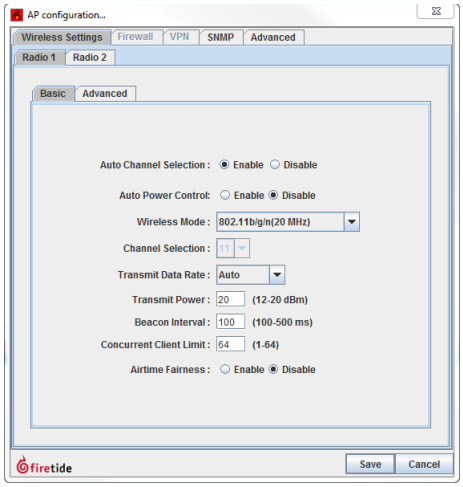
   The "upgrade complete" message means that the image file is on the node and is valid.

Configuring an access point

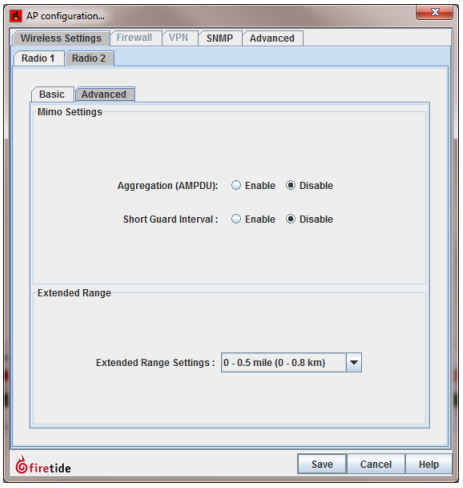
To configure an access point:

1. Right-click the access point **> AP Configuration**
2. From the Wireless Settings tab, select the radio that you want to configure: Radio 1 or Radio 2.
   a. Select the Basic tab and configure these wireless settings:
      - Auto Channel Selection (enabled by default)
      - Auto Power Control (disabled by default)
      - Select the channel. The available channels are different depending on the country and mode of operation.
      - Set the transmit data rate (Auto by default)
      - Set the transmit power (The range can be from 12 to 20 dBm. The default value is 20. The transmit power is different depending on the country and mode of operation.)
      - Set the beacon interval (The range is 100 to 500 ms. The default value is 100ms.)

- Set the concurrent client limit (The range is 1 to 64. The default value is 64.)
- Airtime Fairness (disabled by default)

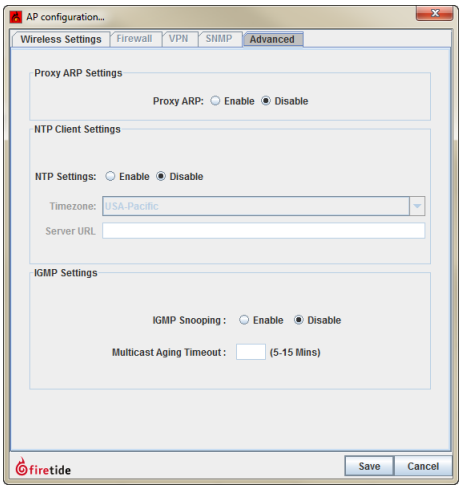


b. Select the Advanced tab and configure these wireless settings if needed:
- Set MIMO aggregation (AMPDU)



3. On the SNMP tab:
   - (Optional) Enable SNMP.
   - Select the version.
   - Set up to four SNMP traps. Enter the IP address and ports.

4. On the Advanced tab:
   - (Optional) Set the Proxy ARP settings. Proxy ARP is disabled by default.
   - (Optional) Set the time zone and enter the URL of a reference server. NTP is disabled by default.
   - (Optional) Set the IGMP settings. IGMP snooping is disabled by default. You can set the multicast aging timeout to be 5 to 15 minutes.



5. Click **Save**.

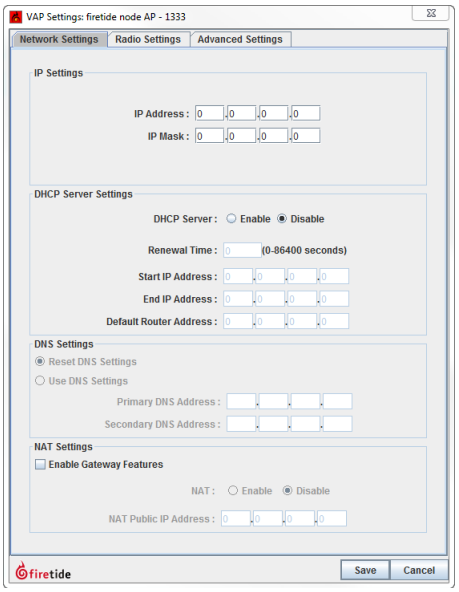
Configuring a virtual access point

The default virtual access point (VAP) for Radio 1 is *firetide*.

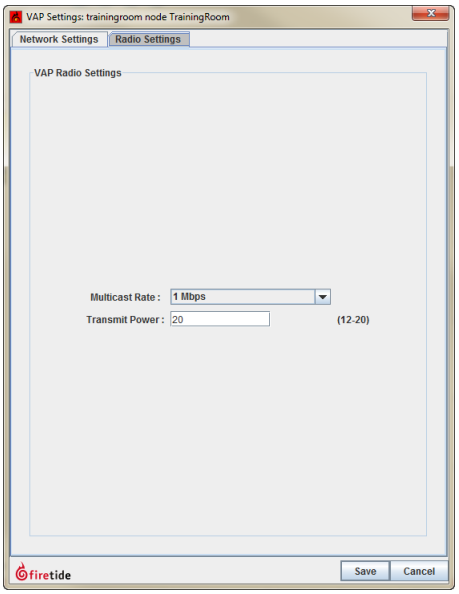
To configure a virtual access point:

1. On the Network Settings tab:
   - Enter the IPv4 address and subnet mask.
   - Enter the DHCP server settings. By default, DHCP is disabled.

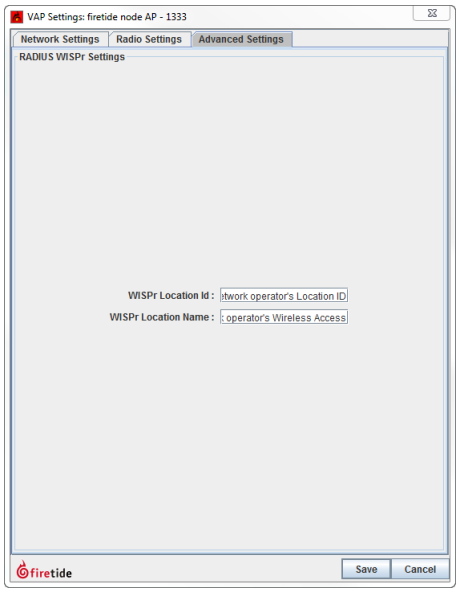
- Enter DNS settings.
- Enter NAT settings. By default, NAT is disabled.



2. Enter virtual access point radio settings:
   - Set the multicast rate
   - Set the transmit power



3. If you are using RADIUS for authentication (WISPr and WISPr location ID, set the setting on the Advanced tab.



4. Click **Save**.

Rebooting an access point

When you reboot an access point, the server also reboots.

To reboot an access point:

1. Right-click the access point **> Reboot This HotPoint**
2. When the confirmation message appears, click **Yes**.

Setting an access point to factory defaults

To return an access point to factory defaults with software:

1. Right-click the access point **> Factory reset this HotPoint**
2. When the confirmation message appears, click **Yes**.

Exporting a configuration file

You can export the configuration file of an access point to a network directory.

1. Right-click an access point **> Import Configuration from this HotPoint**
2. Browse to a directory where you want to save the file.
3. Click **Save**.

Applying a saved configuration file to an access point

To apply a saved configuration to an access point:

1. Right-click an access point **> Apply Configuration to This HotPoint**
2. Click **Apply**.

Refreshing the configuration of an access point

To refresh the configuration of an access point:

Right-click the access point **> Refresh Configuration for this HotPoint**

Wireless distribution stations

By default HotPoint 5100/5200 access points communicate with wireless clients only. If you want two or more access points to communicate with each other, you must enable the wireless distribution station (WDS) feature, which is part of the virtual access point (VAP) group configuration.

The WDS feature lets one access point be the server and one or more access points be stations.

For this group of procedures, you need:

- Two or more HotPort 5100/5200 access points
- HotPoint firmware version 5.54.0.0
- Computer with HotView Pro 10.15.0.0 or later
- Ethernet cables
- L2 switch

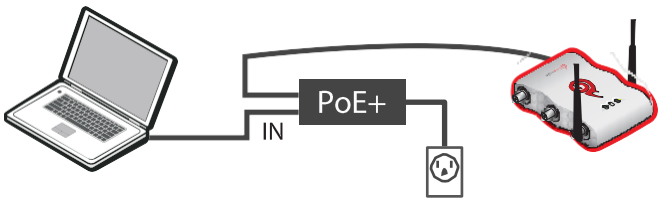
Note: If this is the first time you will log into the access point, you must use the default IP address 192.168.224.160 and make network setting changes that are correct for your network.

Note: Make sure you have unique IP addresses for all access points in the WDS network.

Connecting to a HotPoint access point for the first time

The first time you connect to the access point with an Ethernet cable, you need to connect your computer directly to the other port on the PoE injector and change the TCP/IP4 setting on the computer. 192.168.224.160 is the default IP address of the access point.

1. Attach the PoE injector and Ethernet cable as shown in the next figure.
    - Attach an Ethernet cable from the administrator's computer to the IN port of the PoE injector.
    - Attach an Ethernet cable from the OUT port of the PoE injector to the Ethernet port of the access point.
    - Attach the PoE injector power cable to a power outlet.



The access point boots in 1.5 to 2 minutes. The power LED glows steady and the 2.4G LED blinks.

2. From the computer connected to the access point, do one of the following:
   - Windows 7 users: go to **Start**, and then enter View Network Connections in the search box. Right-click on **Local Area Connection > Properties**. From the Networking tab, select TCP/IP4, and then click **Properties**.
   - Windows XP users: go to **Start > Connect To > Show all connections >** right-click Local Area Connection and select **Properties**. Select Internet Protocol, and then click **Properties**.
   - Windows 8 users: go to **Network and Internet > Network Connections >** right-click Wired Ethernet Connection **> Properties > Select Internet Protocol Version 4**, and then click **Properties**.
3. Enter an IP address/subnet mask for your computer of the format 192.168.224.*xxx* (where *xxx* is an address on the same subnet as the access point), and then click **Apply**.

Caution! Do not use 192.168.224.160. It is the default address of the access point.

4. From a command prompt window, ping the access point to verify connectivity.

```
ping 192.168.224.160
```

Downloading firmware from Firetide

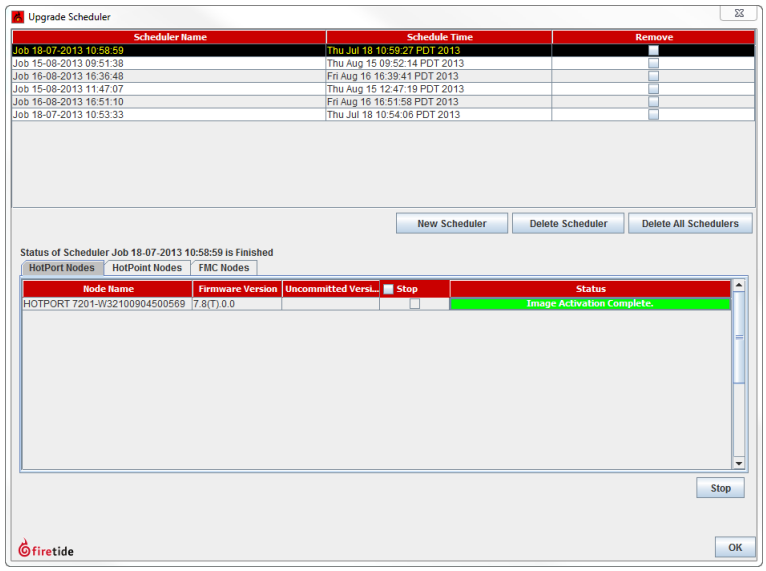
Check the firmware on the access points and make sure that it is HotPoint firmware version 5.54.0.0:

- If the firmware is earlier, do this procedure.
- If the firmware is correct, go to the next procedure.

To get the correct firmware that supports the WDS feature:

1. Go to: http://partners.firetide.com
2. Enter this information:
   - Email address: guest@firetide.com
   - Password: guest

3. Click **Continue**.
4. Go to: **Customer Service > Manuals & Software > Access > Access Points**
5. Download the correct file to a safe place that you can access later.
6. Go to **Network > Upgrade Firmware**
   The upgrade scheduler appears.



7. Click **New Scheduler**.
   a. Select **Upgrade**.
   b. Select the time.
   c. Click the HotPoint Nodes tab for access points, and then select the device by ID or name.
   d. Select the upgrade image.
8. Click **OK**.

Cabling the WDS network

Connect all of the access points to be used in the WDS network to the computer that is running HotView Pro through the L2 switch. Make sure that all access points are in the same subnet and have unique IP addresses.

Use this physical configuration to finish the software configuration.

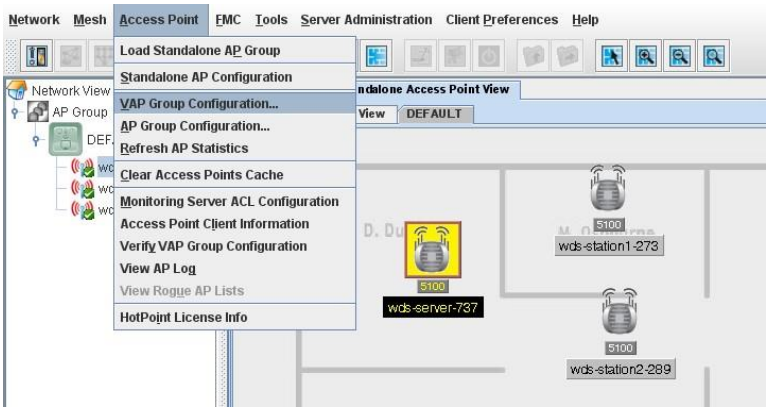
As you configure a WDS station, you will make a network loop between the new WDS station and WDS server. After the WDS configuration is saved, remove the Ethernet cable that causes the loop.

Configuring a WDS server

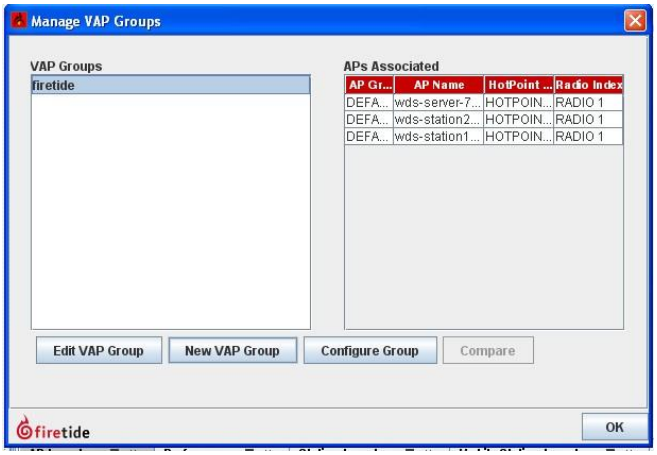
You must configure one WDS server for the configuration to work.

To configure a WDS server:

1. Go to: **Access Point > VAP Group Configuration**

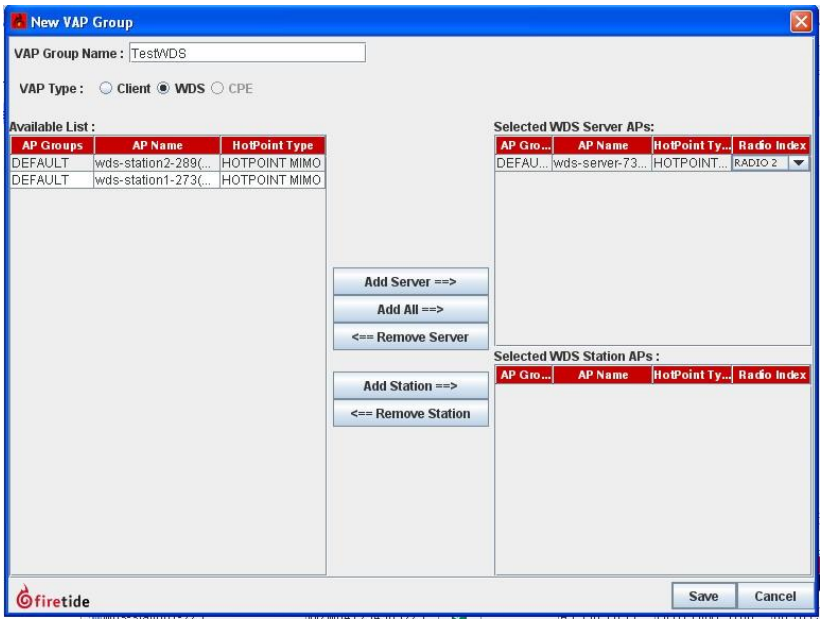


2. Click **New VAP Group**.

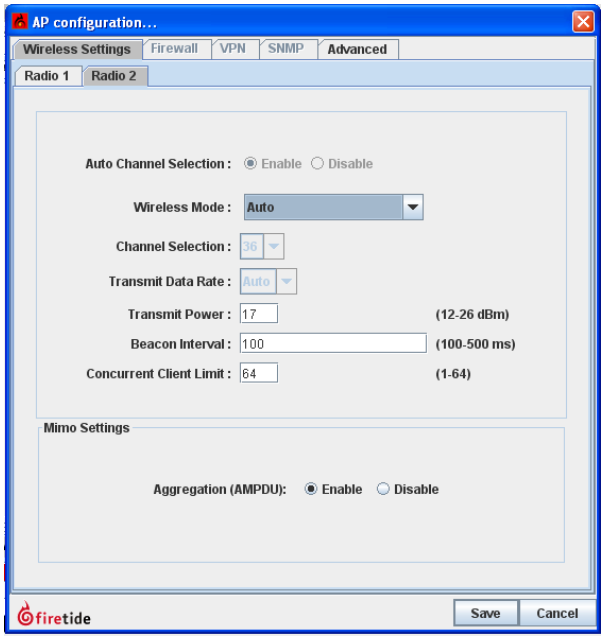


3. Enter a name for the VAP group, and then select WDS as the VAP type.

4. From the Available List, select the access point that you want to be the server, and then click **Add Server**.

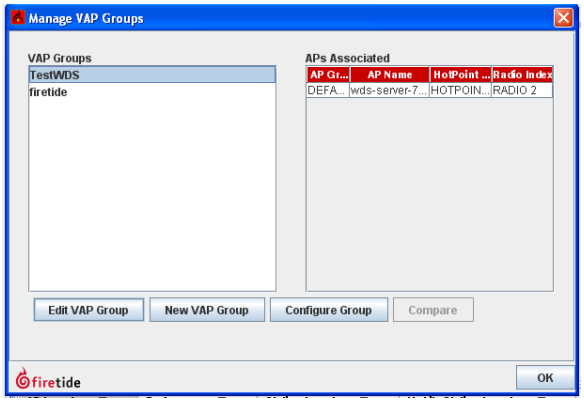


5. From the Radio Index drop-down list, select RADIO 1 (2.4 GHz) or RADIO 2 (5 GHz) to be the WDS radio.



6. Click **Save**.

   The system adds the server. Next, you need to add one or more stations o the VAP, and then you have to enable the WDS configuration to make a WDS link.

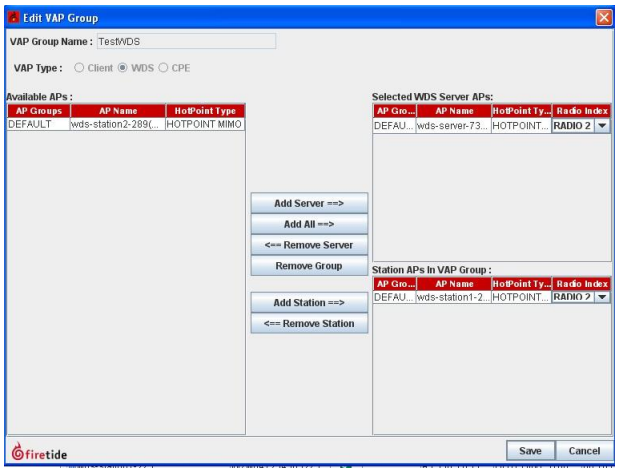


Configuring the first WDS station

A WDS configuration can have one or more stations.

To configure an access point to be a WDS station:

1. In HotView Pro, right-click the access point you want to use as a station **> AP Configuration**.
2. Set the Wireless Mode to Auto for the radio that you want to use for the WDS link. This is the same radio as the WDS server.
3. Go to **VAP Group Configuration > Edit the same VAP group**
4. From the Available access point list, select the access point that is to be a station, and then click **Add Station**.
5. Click **Save**.

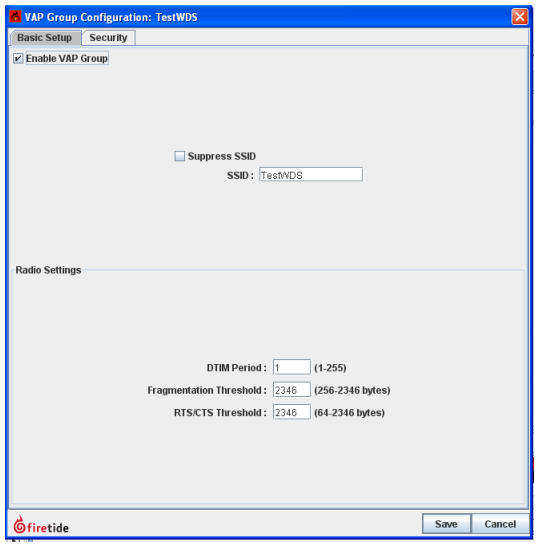


Next, you need to enable the WDS configuration.

Enabling a WDS configuration

To enable the WDS configuration:

1. From HotView Pro, go to **VAP Configuration > Configure Group**
2. Select **Enable VAP Group**, and then click **Save**.



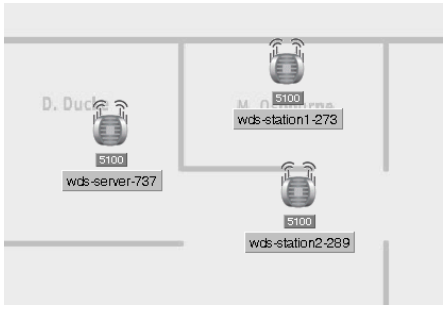
3. After the system enables the VAP, remove the Ethernet cable that connects the WDS server to the computer or the WDS station to the computer.

   Note: You must remove one of the cables to stop the network loop created and use the WDS link.

   Now the access point that is not connected to the administrator's computer can be managed through the wireless WDS link.

4. (Optional) Click the Security tab, and then set WEP as the security option.

   The Standalone Access Point View does not show a link (green line) between a WDS server and a station.



Note: You might have to reboot each access point before the WDS configuration works.

Adding more stations to a WDS configuration

If you want to add a new station to an enabled WDS VAP group, you must disable, save, and then enable and save the VAP configuration setting. A configuration conflict happens if you do not disable and then enable the WDS VAP group.

To add a new station to an existing WDS configuration:

1. In HotView Pro, right-click the access point you want to use as a station **> AP Configuration**.
2. Set the Wireless Mode to Auto for the radio that you want to use for the WDS link. This is the same radio as the WDS server.
3. Go to **VAP Group Configuration > Edit the same VAP group**
4. From the Available access point list, select the access point that is to be a station, and then click **Add Station**.
5. Go to **Access Group > Verify VAP group configuration**

   The system detects the configuration conflict.
6. Reconcile the VAP to the WDS server setting.
7. (Optional) Click the Security tab, and then set WEP as the security option.

   The Standalone Access Point View does not show a link (green line) between a WDS server and station.
8. After the VAP updates on the access point, remove the Ethernet cable connected to the access point to avoid a loop between the new WDS station and WDS server.

Note: You might have to reboot each access point before the WDS configuration works.

Wireless feature configuration

This section explains the steps to enable and configure various wireless features.

Dynamic Transmit Power Control

Dynamic Transmit Power Control (DTPC) is a radio resource management mechanism in a HotPoint access point. DTPC lets you dynamically control the transmit power with each transmitted packet to the clients. This feature ensures that the access point avoids unwanted interference among the co-channel networks for better communication and medium reuse. Correct resource management yields increased network capacity.

A HotPoint access point with DTPC sends packets with a power level sufficient to reach the clients. Because the power level is not the maximum for every data transmission, network contention is significantly reduced, which improves network throughput.

Enabling Dynamic Transmit Power Control

DTPC is configured on each radio. By default, this feature is disabled.

To enable DTPC on Radio 1:

1. Right-click the access point **> AP Configuration > Wireless setting > Basic**
   The settings for Radio 1 appear by default.
2. For the Transmit Power Control setting, select **Enable**.
3. Click **Save**.
4. (Optional) Select the Radio 2 tab and repeat steps 2 to 3.

Enabling airtime fairness

Airtime fairness improves the end user experience. This feature ensures that the total available bandwidth, or airtime, is fairly distributed among the clients which are connected to the HotPoint access point based on their usage.

Airtime fairness is configured for each radio. By default, this feature is disabled.

To enable airtime fairness on Radio 1:

1. Right-click the access point **> AP Configuration > Wireless setting > Basic**
   The settings for Radio 1 appear by default.
2. For the Airtime Fairness setting, select **Enable**.

3. Click **Save**.
4. (Optional) Select the Radio 2 tab and repeat steps 2 to 3.

Disabling auto channel selection

Auto channel selection ensures that each HotPoint access point radio finds and operates on the least congested channel in 11ng20 or 11na20 mode after boot up.

The auto channel selection feature is configured for each radio. By default, this feature is enabled for Radio 1 and Radio 2.

To disable auto channel selection on Radio 1:

1. Right-click the access point **> AP Configuration > Wireless setting > Basic**
2. For the Auto Channel Selection setting, select **Disable**.
3. Click **Save**.
4. (Optional) Select the Radio 2 tab and repeat steps 2 to 3.

Setting the transmit power manually

To make sure that a radio operates at the correct transmit power, you can set the transmit power setting. The settings for Radio 1 and Radio 2 are independent. The valid range of power settings is 12 to 20 dBm.

To set the transmit power value for Radio 1:

1. Right-click the access point **> AP Configuration > Wireless setting > Basic**
   The settings for Radio 1 appear by default.
2. Enter 12 to 20 in the Transmit Power field.
3. Click **Save**.
4. (Optional) Select the Radio 2 tab and repeat steps 2 to 3.

Setting the transmit data rate

You can limit the transmit data rate to clients with a fixed rate or an automatic data rate. The AUTO radio rate algorithm considers all data rates applicable for that mode. A fixed rate algorithm selects data transmit rates equal to or below the fixed rate.

The settings for Radio 1 and Radio 2 are independent. The default value is AUTO.

To set a fixed data rate for Radio 1:

1. Right-click the access point **> AP Configuration > Wireless setting > Basic**
   The settings for Radio 1 appear by default.
2. Select the max data rate from the drop-down list.
3. Click **Save**.
4. (Optional) Select the Radio 2 tab and repeat steps 2 to 3.

Setting the beacon frame interval

A beacon is a broadcast management frame that contains network information and capability information for the HotPoint access point. HotPoint access points send beacon frames at regular intervals (beacon interval) to synchronize all stations in a basic service set (BSS).

The settings for Radio 1 and Radio 2 are independent. The interval period can be 100 to 500 ms. The default period is 100 ms.

1. Right-click the access point **> AP Configuration > Wireless setting > Basic**
2. Enter 100 to 500 ms.
3. Click **Save**.
4. (Optional) Select the Radio 2 tab and repeat steps 2 to 3.

Setting a client limit

You can limit the number of simultaneous clients for a HotPoint access point.

The settings for Radio 1 and Radio 2 are independent. The valid range of concurrent clients is from 1 to 64. The default number of concurrent clients is 64.

To set the client limit for Radio 1:

1. Right-click the access point **> AP Configuration > Wireless setting > Basic**
2. Enter the value in specified range.
3. Click **Save**.
4. (Optional) Select the Radio 2 tab and repeat steps 2 to 3.

Disabling aggregated MPDU for 802.11n

Aggregated message protocol data unit (MPDU) is a feature for use with MIMO applications. When this feature is enabled, the HotPoint access point aggregates MPDUs as described in the 802.11n specification. MPDU aggregation increases throughput.

The settings for Radio 1 and Radio 2 are independent. By default the MDPU aggregation is enabled in MIMO mode.

To disable MDPU aggregation for Radio 1:

1. Right-click the access point **> AP Configuration > Wireless setting > Advanced**
2. For the Aggregation (AMPDU) setting, select **Disable**.
3. Click **Save**.
4. (Optional) Select the Radio 2 tab and repeat steps 2 to 3.

Disabling a short guard interval

The guard interval is the period between symbols or characters that a system transmits.

HotPoint access points let you set a short guard interval to give more throughput and a better end user experience. The standard guard interval is 800 ns, and the short guard interval is 400 ns.

The settings for Radio 1 and Radio 2 are independent. By default when a HotPoint access point is in 40 MHz mode, this feature is enabled for 40 MHz mode.

Note: This feature applies to 40 MHz mode only.

To disable the short guard interval on Radio 1:

1. Right-click the access point **> AP Configuration > Wireless setting > Advanced**
2. For the Short Guard Interval setting, select **Disable**.
3. Click **Save**.
4. (Optional) Select the Radio 2 tab and repeat steps 2 to 3.

Disabling proxy ARP

Proxy ARP stops ARP requests for client devices at the HotPoint access point to reduce traffic on your wireless LAN. Instead of forwarding ARP requests to client devices, the access point responds to requests for the associated client devices.

When Proxy ARP is disabled, the access point forwards all ARP requests through the radio port to associated clients, and the client responds. When Proxy ARP is enabled, the access point responds to ARP requests for associated clients and does not forward requests to clients. When the access point receives an ARP request for an IP address not in the cache, the access point forwards it to the client.

By default the proxy ARP feature is enabled.

To disable proxy ARP:

1. Go to **AP configuration > Advanced**
2. From the Proxy ARP settings, select **Disable**.
3. Click **Save**.

IGMP snooping

IGMP snooping prevents multicast flows from flooding all VAPs on a HotPoint access point. When IGMP snooping is enabled:

1. The HotPoint access point monitors Layer-3 IGMP packets and listens to the exchanges between the router and the host machines. From these exchanges, the access point learns which VAP is joining or leaving a multicast group.
2. The bridge module of the access point forwards these messages to the IGMP Snoop Module, where the VAP is added to or removed from the Layer 2 multicast forwarding group based on the IGMP message type.
3. Multicast streams are sent to VAPs that explicitly request the flow.

Wireless multicast traffic can be avoided on the VAPs, where no client is interested in a multicast flow, to improve network performance.

By default this feature is disabled on the access point.

To enable IGMP snooping:

1. Go to **AP configuration > Advanced**
2. Select Enable.
3. Enter the Multicast Aging Timeout. This is the aging timeout for inactive multicast group on the AP.
4. Click **Save**.

Enabling Network Time Protocol

If Network Time Protocol (NTP) is enabled, access point will get the correct time from the configured NTP server on the boot up. The access point syncs periodically with the NTP server to ensure the correct time. Using NTP with HotPoint access points helps maintain common time and time zone settings across all access points without any manual intervention.

By default NTP is disabled on HotPoint access points. When NTP is enabled, you can set these parameters:

- Time zone - a drop-down menu where user can select the intended time zone value.
- Server URL - the URL for the NTP server from which the HotPoint access point will sync the time periodically.

To enable NTP:

1. Go to **AP configuration > Advanced**
2. Enable NTP.
3. Set the time zone with the drop-down list.
4. Enter the URL of a reference server.
5. Click **Save**.

Monitoring and reporting with HotView Pro

HotView Pro lets you monitor statistics, compare configurations, and verify settings. You can also export and print access point inventory lists.

Viewing access point statistics

To view statistics for an access point:

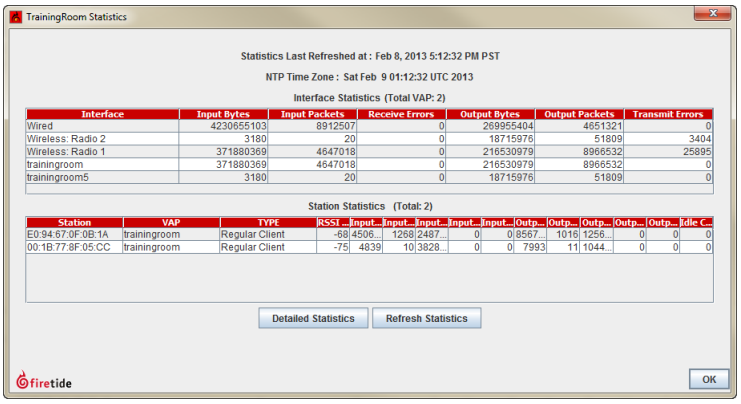
1. Right-click an access point.
   A statistics overview window appears.
2. Click **Refresh Statistics** to ensure that you see current data.

Viewing access point statistics

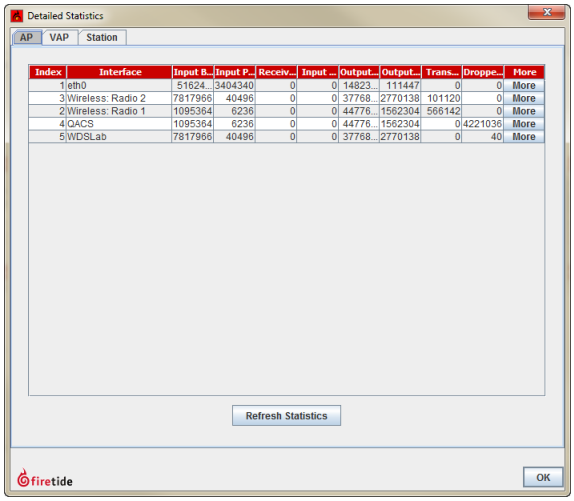
From the access point statistics window you can refresh the statistics and view detailed information about input and output traffic by bytes or packet.

To view access point statistics:

1. Right-click an access point **> Statistics**



2. Click **Detailed Statistics**.



3. Click **OK** to exit each screen.

Comparing virtual access groups

When you add a new access point to a wireless distribution system (WDS), if the access point does not use the expected settings, you might want to compare the configuration to that of a relay station.

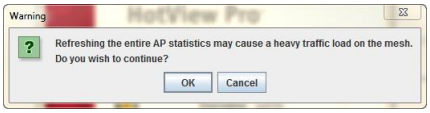
To compare two virtual access group configurations:

1. Go to **Access Point > VAP Group Configuration**
2. Click **Compare**.
3. Click **OK** to exit.

Refreshing access point statistics

When you refresh all access point statistics, the mesh can experience heavy traffic load.

1. Go to **Access Point > Refresh AP Statistics**
2. When the warning message appears, click **OK**.



Clearing access point cache

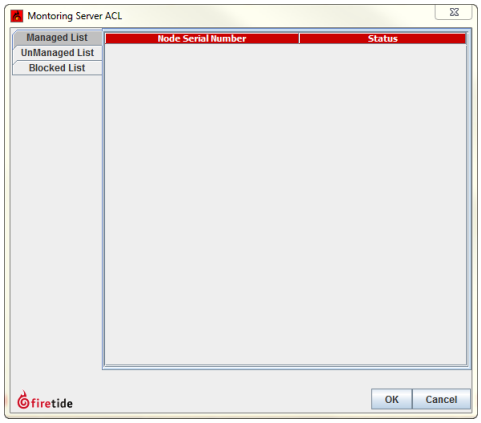
To clear the access points cache:

Go to **Access Point > Clear Access Point Cache**

Viewing the server access control list

To monitor the server access control list:

Go to **Access Point > Monitoring Server ACL Configuration**

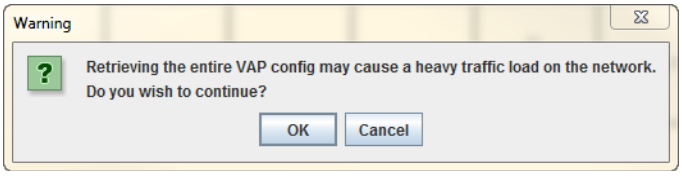


Verifying virtual access group configuration

When you verify the configuration of a VAP group, the network experiences heavy traffic load.

To verify the configuration of a VAP group:

1. Go to **Access Point > Verify VAP Group Configuration**
2. When the warning appears, click **OK**.



Viewing information about access points

You can view access point information several ways.

Viewing access point client information

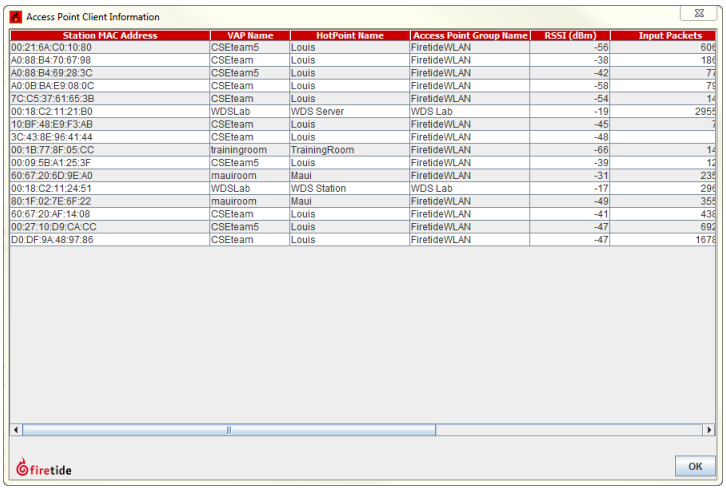
Client information that the system saves includes:

- MAC address of the station (Station MAC Address)
- VAP name
- HotPoint Name
- Access Point Group Name
- RSSI in dBm

- Input packets
- Input bytes
- Output packets
- Output bytes
- Idle count in seconds

To view the client information:

Go to **Access Point > Access Point Client Information**



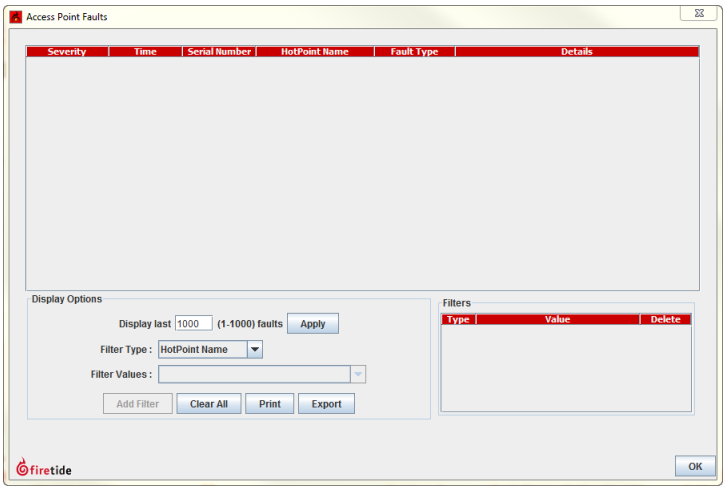
Viewing the AP log

The AP log contains:

- Severity of the fault
- Time the fault occurred
- Serial number of the device on which the fault occurred
- HotPoint name
- Fault type
- Details

To view the AP log:

Go to **Access Point > View AP Log**



Viewing HotPoint license information

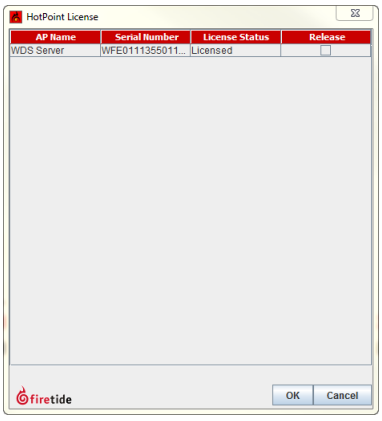
HotPoint license information includes:

- AP name
- Serial number
- License status
- Release

Prerequisite: None

To view HotPoint license information:

Go to **Access Point > HotPoint License Info**



Viewing write access

You can verify write access after you release write access.

To verify write access:

Right-click an access point **> View Write Access**

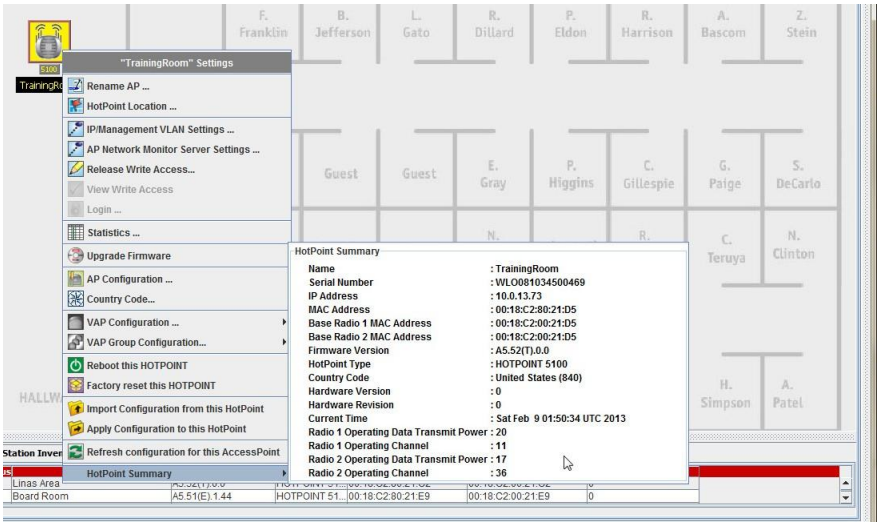
Viewing a summary of an access point

The HotPoint summary shows:

- Access point name
- Serial number
- IPv4 address
- MAC address
- Radio 1 MAC address, operating data transmit power, operating channel
- Radio 2 MAC address, operating data transmit power, operating channel
- Firmware version
- HotPort type
- Country code
- Hardware version and release
- Current time

To view a configuration summary for an access point:

Right-click the access point **> HotPoint Summary**

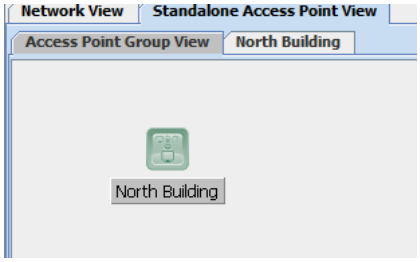


Viewing statistics from a managed access point

For access points that are configured to be managed from the network monitor server, you can view statistics without logging into any of the access points in the access point group.

To view the access point group statistics:

1. Go to **Standalone Access Point View** tab > <*name of access group*> tab and then right-click the access point group icon. See the next figure.



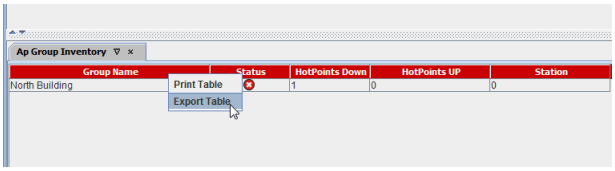
2. Right-click the icon **> Statistics**

Exporting an access point inventory

You can export a list of all access points that HotView Pro manages. This feature is for tracking company assets or device status.

To export a csv file from HotView Pro:

1. From the AP Group Inventory tab, right-click the red ribbon **> Export Table**



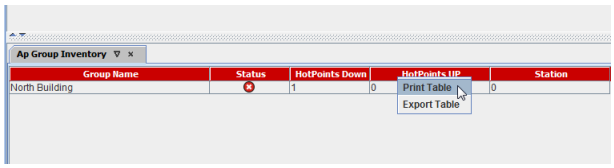
2. Enter a name for the file.
3. Click **Save.**

Printing an access point inventory

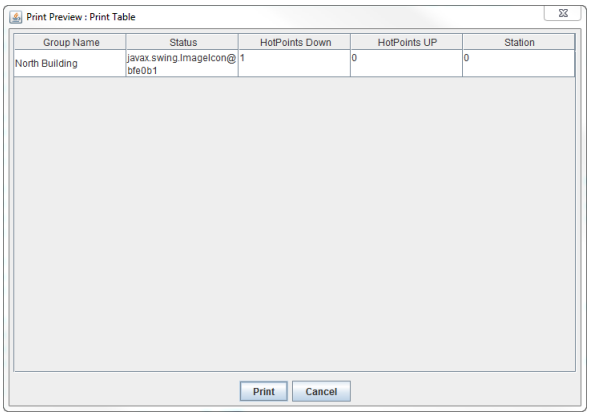
You can print a list of all access points that HotView Pro manages. This feature is for tracking company assets or device status.

To export a csv file from HotView Pro:

1. From the AP Group Inventory tab, right-click the red ribbon **> Print Table**



A print preview window appears.



2. Click **Print**.
3. Select a printer and set the printer properties.
4. Click **Save**.

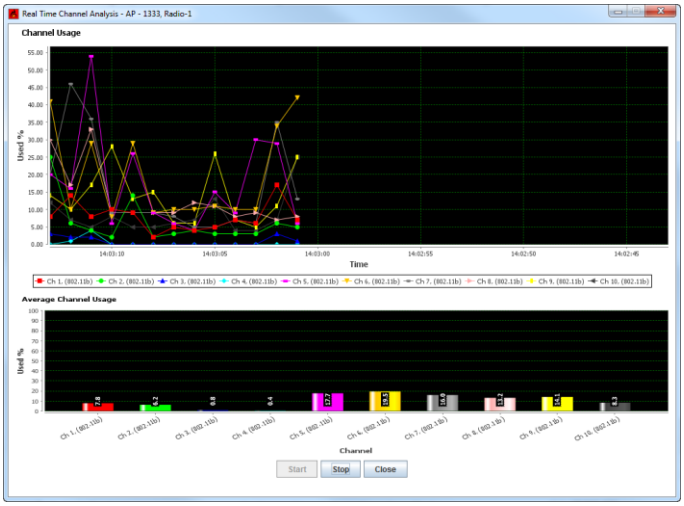
Performance and diagnostic tools

HotView Pro lets you use a spectrum analysis tool to evaluate the presence and strength of selected channels around an access point.

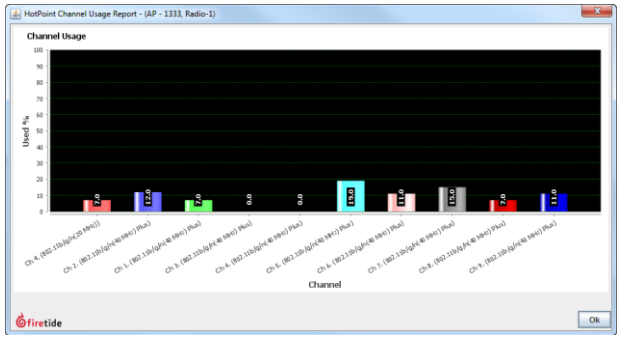
Using the spectrum analyzer

You can track up to 10 channels at one time.

The next figure shows the results of a real-time spectrum analysis of the first 10 channels for 802.11b. The top graph shows channel usage over time; the bottom graph shows the average channel use.

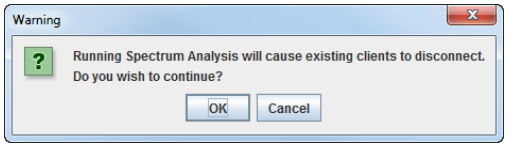


The next figure shows the results of spectrum analysis of different channels.

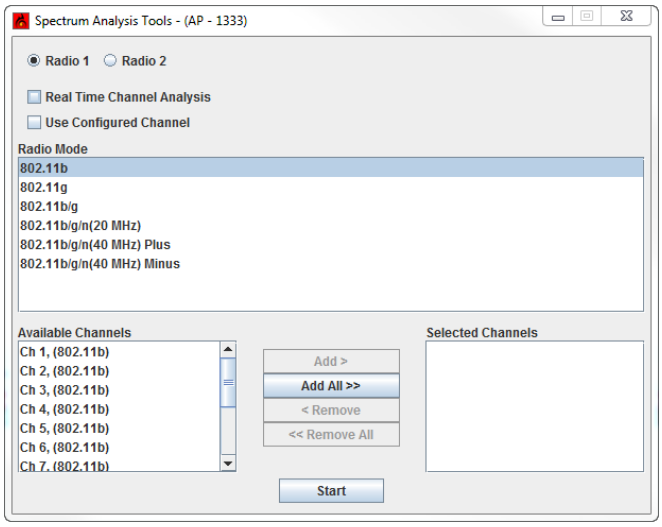


To configure a real-time spectrum data collection:

1. Right-click the access point > **Advanced Tools** > **Spectrum Analysis Tools**
   A message appears to warn you that existing client sessions will be disconnected if you run the spectrum analysis tool.



2. Select the radio (1 or 2). You can only analyze one radio at a time.



3. (Optional) Select "real-time channel analysis" and/or "use configured channel."

Note. If you select real-time channel analysis, the system can accept up to 10 channels at one time. If you use the regular non-real-time analysis method, the system can accept up to 32 channels.

4. Select the radio mode:
   - 802.11b
   - 802.11g
   - 802.11b/g
   - 802.11b/g/n(20MHz)
   - 802.11b/g/n(40MHz) Plus
   - 802.11b/g/n(40MHz) Minus
5. Select the channels you want to analyze, and then click **Add** or **Add All**.

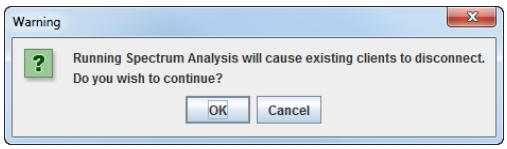
Note. To select more than one channel, press and hold **Ctrl**, click the channels, and then click **Add**.

6. Click **Start**.
7. Click **Stop** to stop data collection.

Viewing the average channel usage for a configured radio

To view the average channel usage as currently configured:

1. Right-click the access point > **Advanced Tools** > **Spectrum Analysis Tools**
   A message appears to warn you that existing client sessions will be disconnected if you run the spectrum analysis tool.



2. Select the radio (1 or 2). You can only analyze one radio at a time.
3. (Optional) Select "real-time channel analysis."
4. Select "use configured channel."
5. Click **Start**.
6. Click **Stop** to stop data collection.

Troubleshooting and access point

This section lists guidelines and tips to improve end user or wireless client experience.

Premature disconnects

If wireless clients experience premature disconnections from the access point or unexplained wireless service interruption, set the RTS value to 128 to improve connection persistence.

SNMP with HotPoint access points

Simple Network Management Protocol (SNMP) is used to monitor network-attached devices for conditions that need administrative attention. Native SNMP on HotPoint access points lets you:

- Monitor critical events, such as radar detection.
- Remotely manage and configure the device.
- Configure traps to collect specific important messages.

SNMP parameters

SNMP parameters for HotPoint access points include:

- SNMP Agent. You enable the SNMP Agent on a HotPoint access point to be able to collect SNMP data from this device.
- SNMP Version. SNMP V1, V2 and V3 are supported. For SNMP V3 you have to the users.
- Agent Port. The agent port is the UDP port on which the SNMP agent runs. The default SNMP port is 161, but the port can be changed.
- Trap IP Settings. You can set a maximum of four trap locations. A trap is an IPv4 address.

  The HotPoint access point will send periodical traps to these IP Addresses. Traps can be labels or messages such as, AP UP/DOWN, client association or disassociation, and so on.

SNMP V3 users

SNMP V3 supports three pre-configured default users and three custom additional users. The next table contains the default user information.

User name	Security level	Authentication		Privacy	
		Protocol	Password	Protocol	Password
noauthprivUser	No Authentication, No Privacy	—	—	—	—
authOnlyUser	Authentication, NoPrivacy	MD5/SHA	“password”	—	—
authPrivUser	Authentication, Privacy	MD5/SHA	“password”	DES/AES	“password”

Table 25

Enabling SNMP on a HotPoint access point

By default SNMP is disabled on the access point.

To configure SNMP:

1. Go to **AP configuration > Advanced**
2. Select the SNMP version from the drop-down list.
3. If you selected SNMP V3, click Users and enter the user's information.
4. Enter the UDP port for SNMP.
5. Enter up to four trap locations, which are IPv4 addresses.
6. Click **Save**.

Configuring an SNMP trap

You can set a maximum of four trap locations.

The HotPoint access point will send periodical traps to these IP Addresses. Traps can be labels or messages such as, AP UP/DOWN, client association or disassociation, and so on.

Prerequisites: SNMP agent is active and configured to be V3. You must install the MIB file named "FIRETIDE-APNODE-MIB.mib".

To configure an SNMP trap:

1. Go to **Server Administration > Configure HotView Server > HotView Management**
2. Click the SNMP tab.
3. Click **Add Target**.
4. Enter the target name (1 to 16 characters long), IP address, and target port.
5. Click **Save**.

HotPoint access point MIB list

The MIB (Management Information Base) file that installs with HotView Pro software lets you use the SNMP features. For more information about the SNMP hierarchical data structure, refer to RFC 1155.

You can use a third party MIB browser to get SNMP trap information through HotView Pro. Information from HotPoint access points goes to a MIB viewer through HotView Pro. SNMP data cannot be viewed directly from an access point.

MIB location

On a computer that runs Windows, the MIB folder is found along this path:

C://Program Files (x86)/Firetide/HotView/<software version>/mibs

MIB descriptions

The next sections list the MIB tables and variables.

firetideApNode

The next table lists the MIB name, description, and type.

Name	Description	Type
apTable	Summary of basic properties: • apSoftwareVer shows the current firmware version. • apSerialNo shows the serial number of the access point. • apMacAddr shows the Ethernet MAC address of the access point. • apRadioMacAddr shows the radio MAC address of the access point. • apNodeError is a string that shows when an access point-specific configuration apply fails. • apSoftwareUpgradeCompletion shows the percentage complete for during a software upgrade. • apTimeUp shows the time since the access node came up. • apNodeIndex indicates whether the node is up or down. • apDhcpState can be set to true(1) to enable a DHCP client or false(2) to disable a DHCP client. • apIpAddress is the IPv4 address of this access point. • apIpMask is the IPv4 mask of this access point.	read only

Name	Description	Type
	• apDefaultGateway is the IPv4 address of the default gateway. • apName is the name of the access point. • apGroupName is the name of the group to which this access point belongs. By default, all access points appear in the group DEFAULT. To remove an access point from a group, set this value to DEFAULT. • apMgmtVlanEnable can be true(1) when management VLAN is enabled, and VLAN ID is a valid VLAN tag other than 1. When this variable is false(2), the system disables the management VLAN. Setting this variable to true(1) does not have an effect. To enable a management VLAN, set apMgmtVlanId {apEntry 9 }to a valid VLAN. • apMgmtVlanId is the management VLAN tag for this access point. If management VLAN is disabled, this variable returns 1. • apNodeOperations -- When this variable is set to applyApConfig(6), any access point-specific manual login is needed only when login to this access point is incomplete. Incomplete login is when the system returns these states: apDownOrDisconnected(10), apConnectionFailed(11), or apLoginFailed(12). Successful login is when the system returns operationCompleted(1). If this variable is set to (13), the system refreshes the access point configuration and statistics. Other states include: • applyPending(3) when changes are not yet written to the access point. • applyInProgress(4) when configuration changes are being written to the access point. SETs during this state fail and configuration changes will be lost. • operationCompleted(1) when the system applies changes to the access point. • ErrorTryAgain(2) appears when the apply failed. The reason for failure is available in the variable apNodeErrorString. We recommend that you fix the error before retrying. • To roll back to the last applied configuration, use rollbackApConfig(5). • rebootAp(7) forces the access point to reboot. • factoryResetAp(8) forces the access point to revert to factory default values and a set to loginToAp(9) triggers a manual login, using the apLoginUserName and apLoginPasswd as user name and password.	read-write

Name	Description	Type
	• apSelectForUpgrade with includeInUpgrade(1) sets this access point for upgrade. To exclude an access point after selection, use excludeFromUpgrade(2). For doing the upgrade operation, see upgradeApSoftware {firetideApNode 3 }. • apProxyArpState sets the proxy ARP state: true(1) to enable and false(2) to disable. • apNTPSettings sets the time protocol state: true(1) to enable NTP and false(2) to disable NTP. • apNTPServerUrl is the URL for the reference NTP server. • apNTPTimeZone is the NTP time zone, which can be from 0 to 278. • apDnsMode sets the DNS mode: true(1) for static mode and false(2) for dynamic mode. • apDnsPrimaryIp is the primary DNS IP address for this access point. • apDnsSecondaryIp is the secondary DNS IP address for this access point. • apIgmpSnoopState sets the IGMP snoop state: true(1) to enable igmp snooping and false(2) to disable igmp snooping. • apMcastAgingTimeout sets the multicast aging timeout value. • apCountryCode sets the country of operation for this access point. This setting determines the available power levels, radio modes, and channels.	read-write
standaloneApTable	Summary of standalone access point configuration	read only
apSoftwareUpgradePath	Path to the upgrade software (.bin file). When the system starts an upgrade through the upgradeApSoftware variable, the bin file found in this path is uploaded to the access points.	read-write
apSoftwareUpgrade	Set this variable to: • upgradeAll(1) to do a software upgrade for all access points. • upgradeSelective(6) to do a software upgrade on certain access points. Select with apSelectForUpgrade {apEntry 19 }variable to includeInUpgrade(1). Specify the path to the new software (.bin or .bin2) with the variable upgradeApSoftwarePath. If an upgrade failure happens, view the reason with apNodeErrorString {apEntry 15 }. This variable takes the value upgradeFailed(3). To abort the upgrade operation set upgradeCancel(7). When an upgrade operation is in progress, the variable returns the value upgradeInProgress(4).	read-write

Name	Description	Type
apLoginUserName	Login user name for an access point	read-write
apLoginPasswd	Login password corresponding to apLoginUserName variable for an access point	read-write
apLoginErrorMessage	Error message from the last failed login attempt	read only
apGroupCreationTable	Access point group creation table	not accessible
apNetworkMonitorServer ConfigTable	Access point network monitor server configuration table	not accessible

Table 26

firetideApVap

The next table lists the MIB name, description, and type.

Name	Description	Type
vapGroupConfigTable	Common configuration for all access points that support a particular virtual access point (VAP)	not accessible
vapSpecificConfigTable	VAP configuration specific to an access point, which is supporting a particular VAP	not accessible
vapManageGroupConfigTable	Common configuration for all the access points that support a particular virtual access point	not accessible
vapGroupCreateConfigTable	VAP configuration specific to an access point, that supports a particular VAP	not accessible
vapNatPortForwardConfigTable	NAT Port Forwarding configuration specific to an access point that supports a particular VAP	not accessible
vapHotspotConfigTable	HotSpot configuration for a particular VAP	not accessible
vapHotspotWalledGardenTable	HotSpot walled garden configuration for a particular VAP	not accessible
vapHotspotUserProvisioningTable	HotSpot User Provisioning configuration for a particular VAP	not accessible

Table 27

firetideApRadio

The next table lists the MIB name, description, and type.

Name	Description	Type
apRadioTable	This table summarizes the radio configuration for an access point.	not accessible

Table 28

Name	Description	Type
apNodeRadioTable	This table summarizes the radio mode and channel configuration for an access point.	not accessible

Table 29

firetideApSecurity

The next table lists the MIB name, description, and type.

Name	Description	Type
vapSecurityTable	Security related parameters for a particular VAP	not accessible
apSecurityTable	Security related parameters for this access point	not accessible
vapAclTable	Access control list (ACL) for this VAP. The ACL denies all entries or allows only those in the list. vapAclPolicy {vapSecurityEntry 15 }variable controls this behavior.	not accessible
apFirewallTable	List of allowed ports (TCP or UDP) for clients connected to this access point. The firewall feature must be enabled for this access point to view this information.	not accessible
apGroupLoginPasswdConfigTable	List of access point groups for which you can configure Read-Write and Read-Only usernames and passwords.	not accessible

Table 30

firetideApStatistics

The next table lists the MIB name, description, and type.

Name	Description	Type
apStatisticsTable	Summarizes the access point-wide statistics (apStatisticsEntry): · apWirelessInBytes · apWirelessInPackets · apWirelessReceiveErrors · apWirelessOpBytes · apWirelessOpPackets · apWirelessTransmitErrors	read-only

Table 31

Name	Description	Type
apWiredStatisticsTable	Summarizes the access point-wide wired statistics (apWiredStatisticsEntry): · apWiredInBytes · apWiredInPackets · apWiredReceiveErrors · apWiredOpBytes · apWiredOpPackets · apWiredTransmitErrors	not accessible
apVapStatisticsTable	Summarizes the VAP-specific statistics (apVapStatisticsEntry): · apVapGroupName · apVapInBytes · apVapInPackets · apVapReceiveErrors · apVapOpBytes · apVapOpPackets · apVapTransmitErrors · apVapNumberofStations	not accessible
apStationStatisticsTable	This table summarizes the statistics of stations connected to VAPs.	not accessible

Table 32

firetideApTrapParams

The next table lists the MIB name, description, and type.

Name	Description	Type
policyName	Indicates the alarm type.	View
stationMacAddr	Indicates the MAC address of a WDS station.	View
alarmState	Indicates the alarm state.	View

Table 33

firetideApTrap

The next table lists the SNMP trap names and descriptions.

Name	Description
apDown	Indicates a lost connection with this access point.
apUp	Finished getting configuration from this access point. SNMP manager can get and set on this access point.
vapConfigInconsistent	The system sends this trap when you do a VAP configuration comparison and the VAP configuration is inconsistent.

Table 34

Name	Description
vapConfigConsistent	The system sends this trap when you do a VAP configuration comparison and the VAP configuration is consistent.
apLoginError	Login failed.
concurrentApModification	The system sends this trap when the system detects an attempt to modify the access point configuration from the HotView Client and SNMP agent simultaneously.
concurrentVapModification	The system sends this trap when the system detects an attempt to modify the VAP configuration from the HotView Client and SNMP agent simultaneously.
policyAlarm	When a PolicyAlarm is generated, the system sends this trap.
apAssoc	When an access point associates with a client, the system sends this trap.
apDisAssoc	When an access point stops associating with a client, the system sends this trap.
captiveUserLoggedOut	When a captive user logs out, the system sends this trap.
captiveUserLoggedIn	When a captive user logs in, the system sends this trap.

Table 35

Licenses for access points

All access point nodes, standalone and integrated with a mesh node, must have a management license.

Applying a management license to a node

Be sure to license all the nodes on your mesh. A *node* is any device that you manage from HotView Pro.

You do not have to transfer the licenses to all nodes at the same time, but you cannot have licensed and unlicensed nodes in the same mesh network.

Caution! After you apply the license, you cannot remove or recover it from the node. You can, however, transfer it to a replacement node.

To add a management license to a node:

1. Go to **Server Administration > Configure HotView Server > Licensing**
2. Select the management license.
3. Click **HotPort List**.

   A new window appears.
4. Select the node that needs a license.
5. Click **Add**.
6. Approve the license transfer.
7. Click **Yes**.

Field access without a management license

When you set up a new mesh network you purchase a bulk management license. and you apply that license to every mesh node. Each time you apply a management license to a mesh node, the management key count decrements by one.

This means that you do not need a license key to be able to manage a mesh network to access a node in the field.

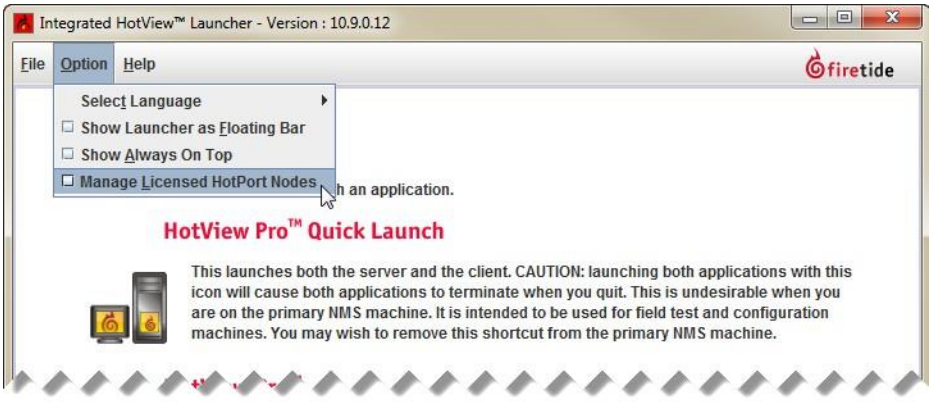
Using HotView Pro without a license key

Caution! You need to apply a management license to all nodes in a mesh. If one of the nodes in a mesh does not have a management license, then HotView sends an error message and prevents access to all nodes in the mesh.

To use HotView Pro without a license key after the management license key is assigned to the appropriate set of mesh nodes:

1. Install HotView Pro on a system that does or does not have a temporary or a permanent license.
2. Start the HotView Pro Launcher, and then select the Server Configuration icon.

3. Accept the prompts to access the Server Configuration, and remove the check from Use Database and Use Database for Radius.
4. Click **Save**.
5. From the HotView Pro Launcher, go to **Options > Manage Licensed HotPort Nodes**



You can now log into and manage the mesh from a different computer.

HotPoint access point messages

The next table lists the messages the system sends.

Type	Message	Action
Load Failure	Failed to load these HotPoint(s) of AP group [North Building] AP-1333 [secure connection to 192.168.224.160 not established.]	Make sure the access point is physically connected to the network and ping is successful.
Spectrum analysis tool	Running Spectrum Analysis will cause existing clients to disconnect. Do you wish to continue?	OK disconnects the existing client sessions. Cancel stops to system from action and returns you to the monitoring tab.

Table 36

HotPoint access point upgrade script

If you want to upgrade HotPoint access points from 5.51.0.0 to a later firmware, you must use the Firetide AP FW Upgrade Utility. For HotPoint access points that are running 5.52.0.0 or later you can use the script to save time because this utility lets you upgrade many access points at one time. The utility pings each device, and if the device is reachable, it starts the upgrade process. The upgrade_log.txt file records the IP address of each access point and when the upgrade process started.

Script folder contents

The script package includes:

- FT_AP folder with various files
- AP_FW_Upgrade.exe
- IP_LIST.cfg, which is the only file you have to edit.
- pass.txt
- pscp.exe
- Readme.txt
- upgrade_log.txt

Using the script to upgrade access points

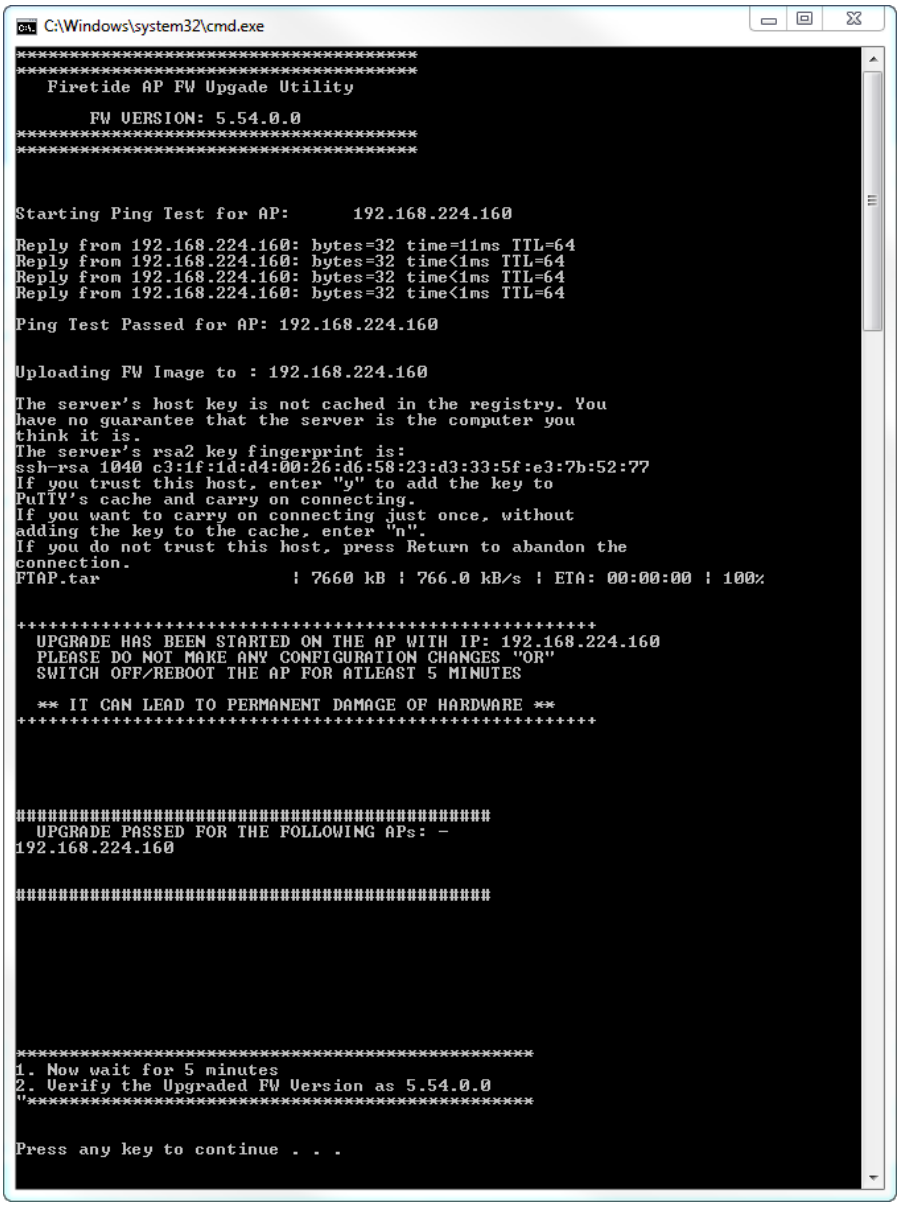
To upgrade one or more access points to run 5.54.0.0 firmware:

1. Download the ZIP file that contains the script and executables from the Firetide Partner Portal.
2. Double-click the ZIP file and drag the folder named AP_UPGRADE to the desktop.
3. From the AP_UPGRADE folder open the IP_LIST.cfg file in Notepad or other text editor.
    a. Delete the contents of the file.
    b. Enter the IP address or addresses of the access points you want to upgrade, one IP address on a new line.
    c. Save the file.
4. Make sure the administrator's computer has an IP address on the same subnet as the access points.
5. Make sure you can ping the access points.
6. Double-click AP_FW_Upgrade.exe.

    The script runs and the upgrade operation starts.

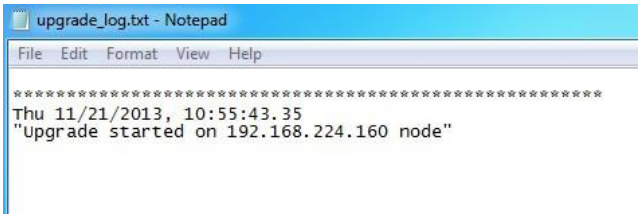
7. Wait five minutes before you log into an access point to ensure that the upgrade is complete and that the access point rebooted.

The next figure shows a screen capture of the script output during the upgrade of one access point with the IPv4 address set to the default value.



Viewing the access point upgrade utility log file

The upgrade_log.txt file records the IP address of each access point and when the upgrade process started. The next figure shows the screen capture of a log file.



Configuration with the web interface

To configure and manage a few HotPoint access points, you can use the web interface, an integrated HTTP-based application.

After you log in, set the country code, change the password, and then do the other configuration tasks.

Caution! Give power to one access point at a time. If you give power to two or more access points at the same time, IP address conflicts occur.

Logging into the web interface for the first time

Prerequisites:

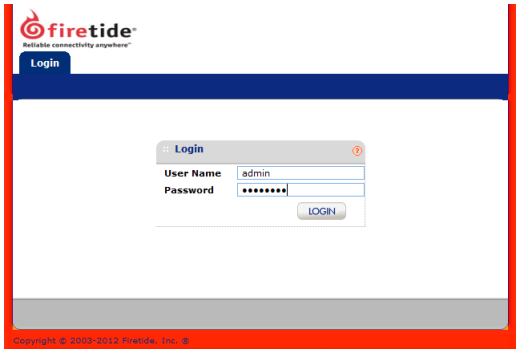
- Administrator's computer with a web browser
- Ethernet cable

To log into a new access point for the first time:

1. Supply power to the access point.
2. Attach an Ethernet cable to the access point and the administrator's computer.
3. Change the IP address of the administrator's computer to an IP address on the same subnet as the access point's default IP address.
4. In a browser, enter: 192.168.224.160.
5. When prompted, enter this information:

   User Name: admin

   Password:firetide
6. Click **Login**.



New access point configuration process

The sequence of tasks to configure an access point for the first time are:

1. Set the country code.
2. Change the password.
3. Verify that the access point acquired an IP address from your DHCP server.
   Note: If you do not use a DHCP server, then you have to manually set the IP address of the access point.
4. Configure wireless access features:
   - Virtual access points
   - Radios
5. Configure optional features as necessary, such as NTP (server time).

After you configure the access point, then you need to test it in a controlled environment with a wireless client.

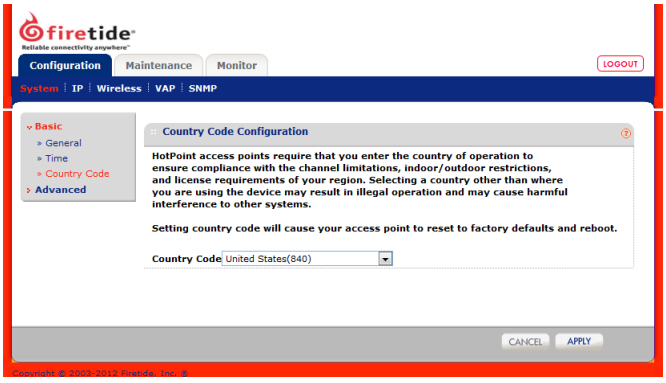
Setting the country code

You want to set the country code to change the device from a low-power, low range setting to a correct full-power operational mode.

You also want to set the country code to suppress prompts from the access point each time you change windows in the web interface.

Caution! Make sure you configure the access point for the correct country. If you do not select the correct country of operation, the device might operate in a manner that is not legal or create problems with other wireless devices.

1. Go to **Configuration > System > Basic > Country Code**



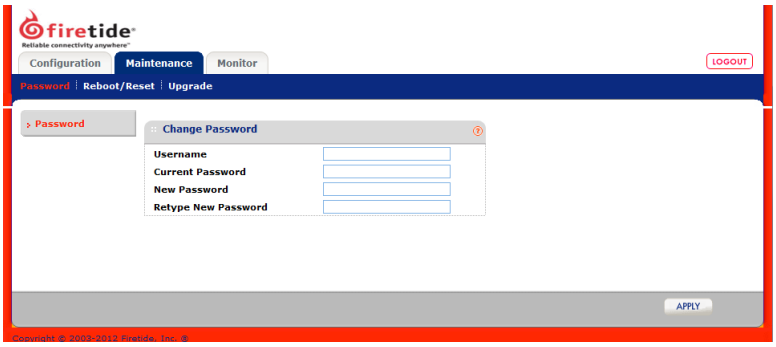
2. Select the correct country.
3. Click **Apply**.

Changing the default password

To prevent others from easily logging into this access point, change the password to something secure. You must have the current password to be able to change the password. The default password is *firetide*.

To set or change a password:

1. Go to the main window of the Maintenance tab.



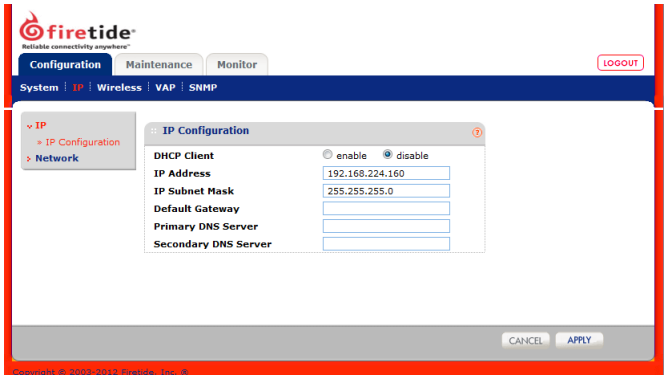
2. Enter your user name, current password, and the new password (twice).
3. Click **Apply**.
   The system logs you out.
4. Log in with the new password to verify that the new password works.

Setting the IP address of the access point manually

By default, DHCP client is enabled. The access point automatically gets an unused IP address from the network. If you disable DHCP, you have to set the IP address manually.

To set the IP address of an access point:

1. Go to **Configuration > IP**



2. Select disable DHCP client.

3. Click **Apply**.
4. Enter these settings:
   - IPv4 address and subnet mask
   - Default gateway address
   - Primary DNS server address
   - Secondary DNS server address
5. Click **Apply**.

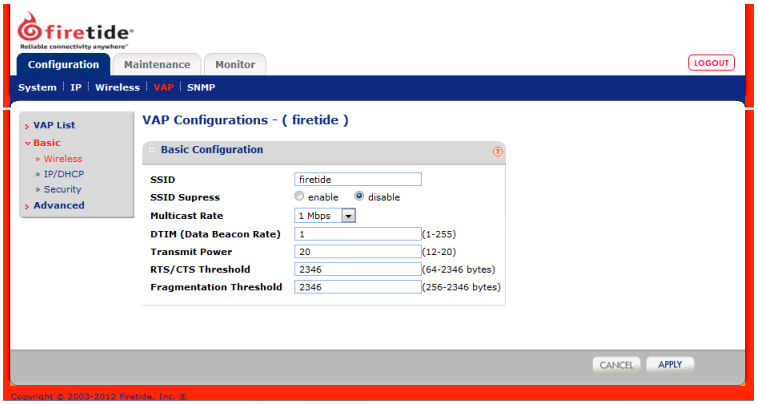
Configuring a wireless LAN

One access point can have one or more virtual access points (VAP). A VAP is a logical subgroup within an access point that lets you assign different permissions or quality settings to different wireless users, such as guest users and trusted users.

By default, no VAP configurations exist.

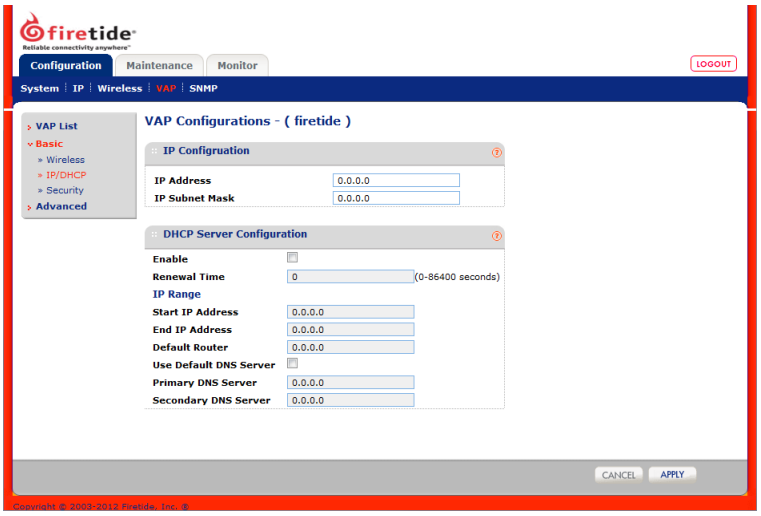
To configure a VAP:

1. Go to **Configuration > VAP > Basic**



2. Enter the settings:
   - SSID. Change the name “firetide” to a descriptive name.
   - SSID suppress
   - Multicast rate
   - DTIM (data beacon rate)
   - Transmit power
   - RTC/CTS threshold
   - Fragmentation threshold
3. Click **Apply**.

4. Click **IP/DHCP**.
   a. Enter the IP address and subnet mask.
   b. (Optional) Enable DHCP and enter the required information.



5. Click **Apply**.

Adding a VAP group

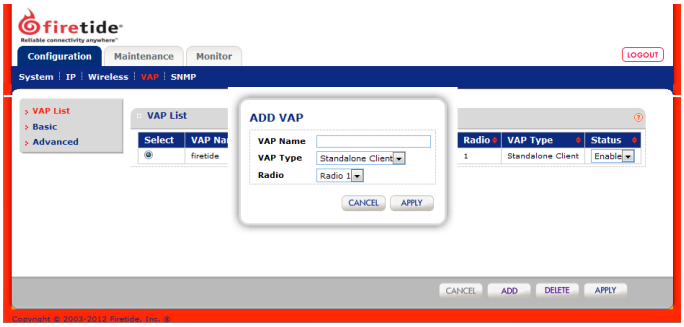
A VAP group is a logical group of users. You can assign a VAP group to a particular radio.

The system records the type of VAP:

- Standalone client
- Wireless Distribution (WDS) Client
- WDS Server

To add a VAP group:

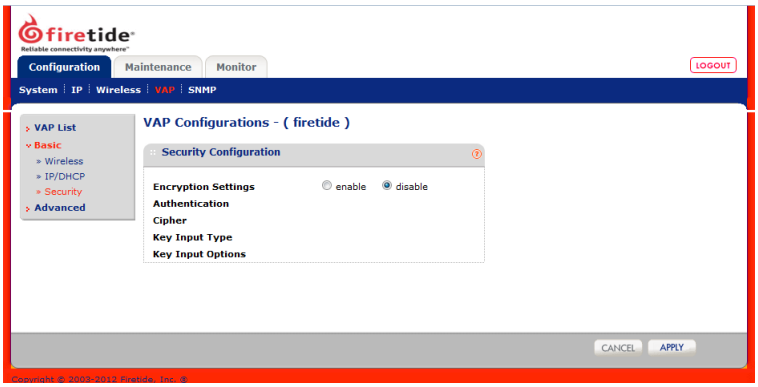
1. Go to **Configuration > VAP**
2. Click **Add** (in the bottom right corner of the window).
3. Enter a name for the VAP, select the VAP type (Standalone Client, WDS Client, or WDS Server), and select radio 1 or 2.
4. Click **Apply** in the Add VAP dialog box.



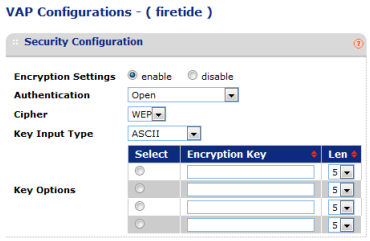
Configuring security for a wireless LAN

To configure security for a VAP:

1. From the Configuration tab, click **VAP > Basic > Security**
2. Enable encryption.



3. From the Authentication drop-down list, select the authentication type. Depending on your selection, the interface options change.
4. Enter or confirm the cipher, key input type, and key options.



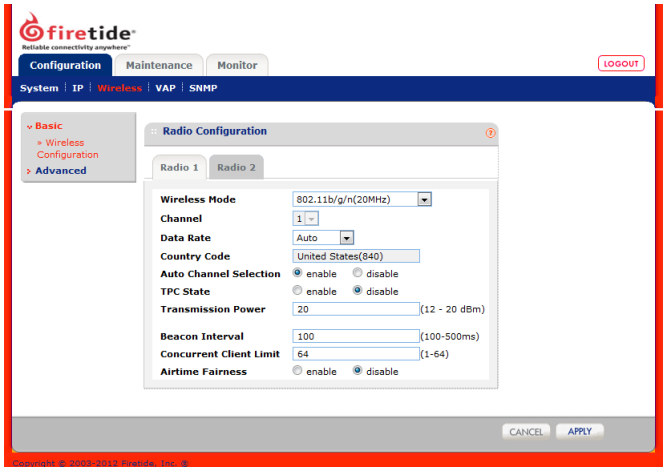
5. Click **Apply**.

Configuring the radios

By default, Radio 1 is 11ng, and Radio 2 is 11na.

To configure a radio:

1. Go to **Configuration > Wireless**



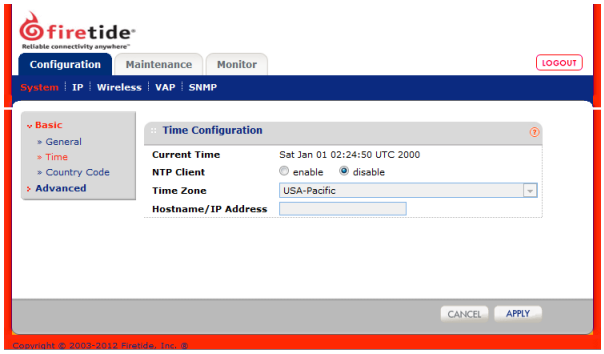
2. Change the radio settings for your application.

   Basic wireless settings include: wireless mode, channel, data rate, auto channel selection, TPC state, transmission power, beacon interval, concurrent client limit, and airtime fairness.

3. Click **Apply**.
4. For MIMO applications, click **Advanced**.

Setting the time

You can point to a time reference so that the access point keeps time. The access point can be an NTP client. By default this feature is disabled.

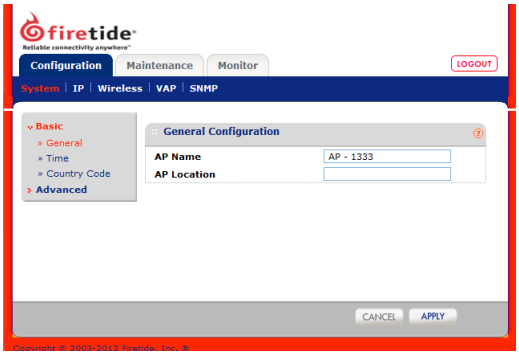


To set the time:

1. Go to **Configuration > System > Basic > Time**
2. Select enable NTP Client.
3. Select your time zone.
4. Enter a time reference server address:
   - time.windows.com
   - time.nist.org
   - Another valid time reference server
5. Click **Apply**.

Setting a name and location for the access point

You can set a meaningful, descriptive name and location for the access point.



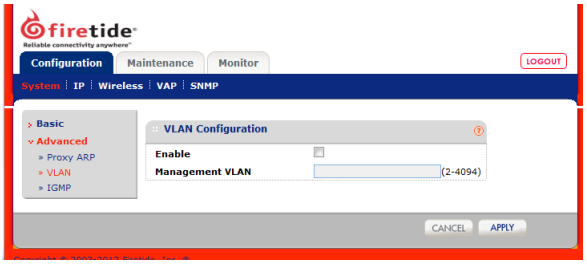
To set a name and location:

1. Open a browser.
2. Enter the IP address of the access point.

3. Log into the access point.
4. Enter a meaningful name for the access point.
5. Enter the location.
6. Click **Apply**.

Configuring VLAN tagging

By default, VLAN management is disabled. You can enter a value between 2 and 4094.

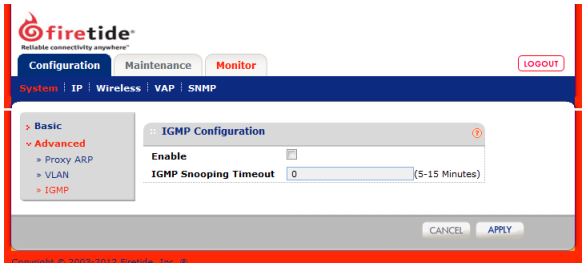


To configure a VLAN:

1. On the Configuration tab, click **Advanced > VLAN**.
2. Select Enable.
3. Enter the management VLAN tag value.
4. Click **Apply**.

Enabling IGMP

By default, IGMP snooping is disabled. You can configure IGMP snooping.

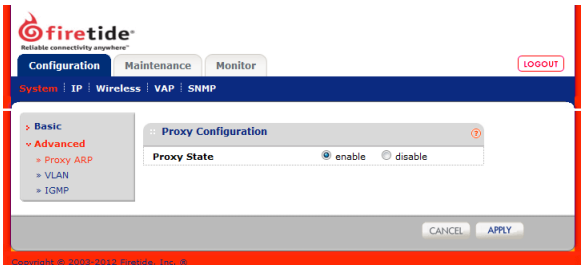


To enable IGMP snooping:

1. On the Configuration tab, click **Advanced > IGMP**
2. Check **Enable**.
3. Enter a timeout value (between 5 and 15 minutes).
4. Click **Apply**.

Enabling proxy ARP

By default, proxy ARP is disabled.



To enable proxy ARP:

1. On the Configuration tab, click **Advanced.**
2. Click **Enable**.
3. Click **Apply**.

Advanced settings

Advanced settings are those features that apply in special environments:

- Environments that use SNMP for monitoring.
- Web services, such as captive portal.
- Internal and/or external authentication
- Special security or network settings, such as port forwarding

SNMP

Simple Network Management Protocol (SNMP) is used to monitor network-attached devices for conditions that need administrative attention. Native SNMP on HotPoint access points lets you:

- Monitor critical events, such as radar detection.
- Remotely manage and configure the device.
- Configure traps to collect specific important messages.

By default SNMP is disabled.

SNMP parameters

SNMP parameters for HotPoint access points include:

- SNMP Agent. You enable the SNMP Agent on a HotPoint access point to be able to collect SNMP data from this device.
- SNMP Version. SNMP version cannot be configured from the web interface.
- Agent Port. The agent port is the UDP port on which the SNMP agent runs. The default SNMP port is 161, but the port can be changed.

- Trap IP Settings. You can set a maximum of four trap locations. A trap is an IPv4 address and port.

  The HotPoint access point will send periodical traps to these IP Addresses. Traps can be labels or messages such as, AP UP/DOWN, client association or disassociation, and so on.

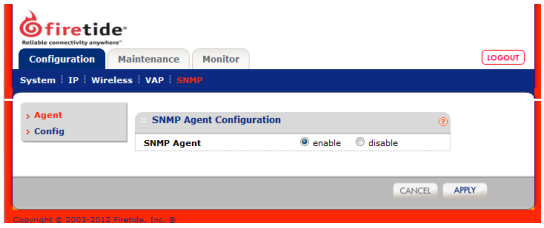
Configuring SNMP with the web interface

To configure the SNMP agent:

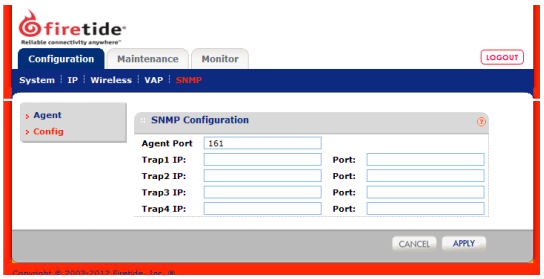
1. On the Configuration tab, click **SNMP**.

   By default the SNMP agent configuration appears.

2. Select **Enable**.



3. Click **Apply**.
4. Click **Config** to change the agent port and to set up to four trap locations. Enter IPv4 addresses and the port number.



5. Click **Apply**.

Configuring the network monitor server

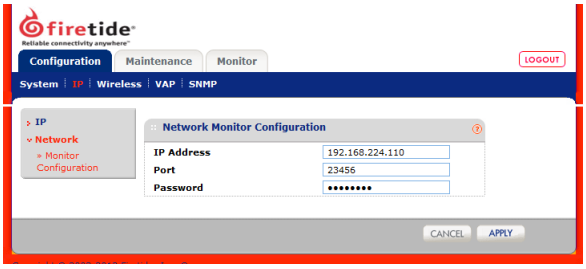
If you want to manage HotPoint access points from HotView Pro without logging into the access points:

1. Log into HotView Pro.
2. Set up the network monitor server. For the network monitor server procedures, see the *HotView Pro Reference Manual*.
3. Log out of HotView Pro.
4. Follow the steps in this section to point the access points to the network monitor server.

After the configuration is complete, in HotView Pro you can see statistics from the access points without having to log into them individually. The access points managed through the network monitor server appear in a table on the Managed Access Points tab in the Standalone AP Configuration window.

To set the network monitor settings on the HotPoint access point:

1. From the Configuration tab, click **IP > Network**
2. Enter the IP address, port, and password of the network monitor server.



3. Click **Apply**.

Captive portal and guest portal configuration

By default a portal is not enabled (none). You can configure a guest portal or captive portal.

A guest portal lets you configure a home page URL and a timeout. Guests can log in again after their session times out.

A captive portal lets you provision users for local authentication and walled gardens. The next table summarizes the HotSpot features of each portal type.

Feature	Guest	Captive
Redirect URL	—	remote or custom
URL Preview	Yes	Yes
Home page URL	Yes	Yes
Guest session timeout	Yes	No
Authentication type	—	Local, external, both
RADIUS IP address	—	Yes, IPv4 format
RADIUS port	—	Yes, 1 to 9999
RADIUS accounting port	—	Yes, 1 to 9999
RADIUS secret key	—	Yes

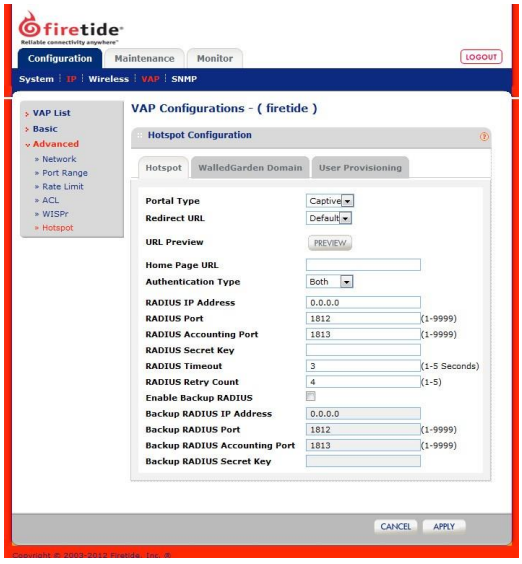
Feature	Guest	Captive
RADIUS timeout	—	1 to 5 seconds. The default value is 3 seconds.
RADIUS retry count	—	1 to 5 times. The default value is 4.
Backup RADIUS	—	Yes
Backup RADIUS IP address	—	Yes, IPv4 format
RADIUS port	—	Yes, 1 to 9999
RADIUS accounting port	—	Yes, 1 to 9999
RADIUS secret key	—	Yes

Table 37

To configure a captive portal:

1. From the Configuration tab, go to **VAP > Advanced > Hotspot**
2. From the Hotspot tab of the Hotspot Configuration workspace, select the portal type: captive.

   The configuration window changes.
3. Enter the configuration settings.
   - Redirect type: custom or remote
   - Home page URL
   - Authentication type
   - RADIUS information
   - Backup RADIUS information



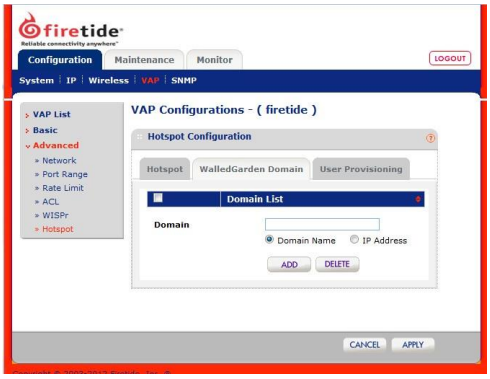
4. Click **Apply**.

5. Make sure that you set other RADIUS settings that might be required for your deployment, such as the WISPr ID and location. See “Configuring WISPr” on page 307.

Configuring a walled garden

To configure a walled garden:

1. From the Configuration tab, go to **VAP > Advanced > Hotspot**
2. Click **Walled Garden Domain**.

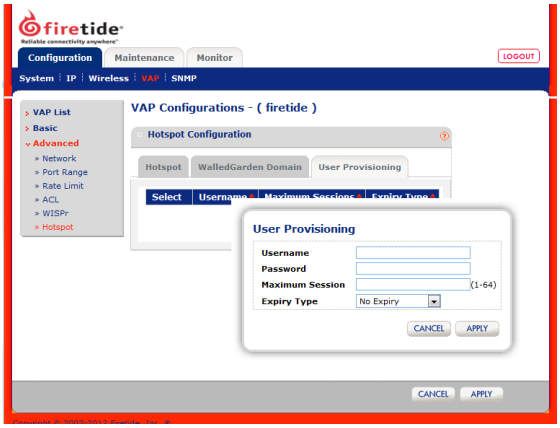


3. Enter the walled garden domain by IP address or by domain name.
4. Click **Apply**.

Provisioning users for authentication

To provision a user for authentication, which can be internal, external, or both:

1. From the Configuration tab, click **VAP > Advanced > Hotspot**
2. Click the User Provisioning tab and then **Add**.
3. Enter the user name, password, maximum number of sessions, and expiry type.



4. Click **Apply**.

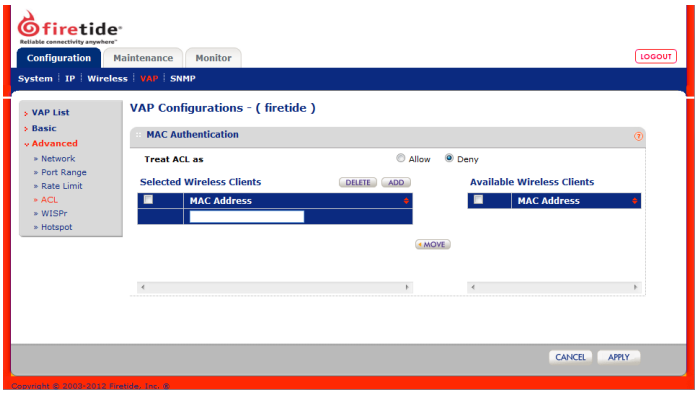
Configuring an access control list

You can move wireless clients that are already connected from the Available Wireless Clients list into a deny or allow ACL entry.

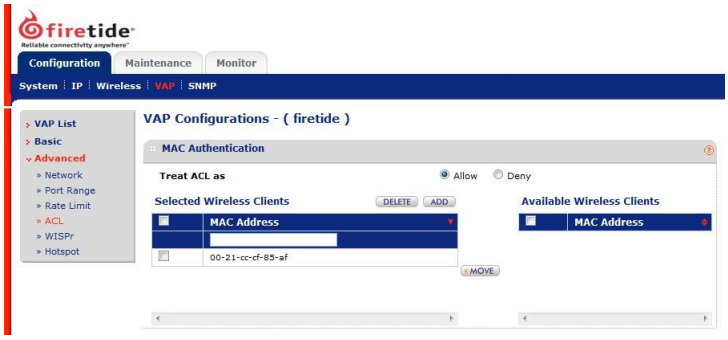
You can also configure an ACL while wireless clients are not connected to the system.

To configure an ACL:

1. On the Configuration tab, click **VAP > Advanced > ACL**
2. Select the list: allow or deny.



3. Enter the MAC address in the Selected Wireless Clients table, and then click **Add**.



The system adds the MAC entry to the end of the selected wireless clients list.

4. Click **Apply**.

Deleting an access control list entry

You can delete a MAC entry in an ACL.

To delete an ACL entry:

1. On the Configuration tab, click **VAP > Advanced > ACL**
2. Select the ACL entry that you want to delete.

3. Click **Delete**.
4. Click **Apply**.

Configuring port forwarding

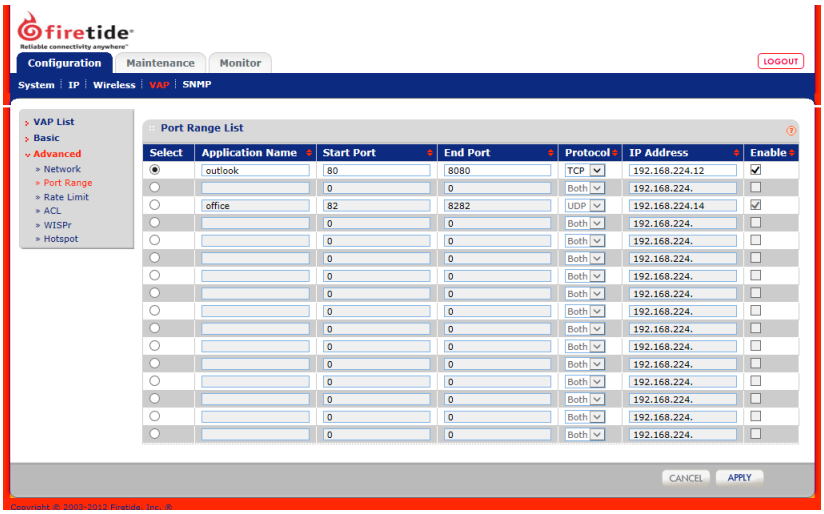
When you set up port forwarding, you should follow this task sequence:

1. (Optional) Configure DHCP. DHCP lets the system auto-populate partial IP addresses.
2. Enable and configure NAT.
3. Configure port forwarding.

   Ensure that applications that use the same protocol, such as TCP, UDP, or both, do not have overlapping ports assigned to them.

To configure port forwarding for specific applications:

1. (Optional) Configure DHCP.
   a. From the Configuration tab, click **VAP > Basic > IP/DHCP**
   b. Select **Enable**.
   c. Enter the IP range, default router IP address, primary and secondary DNS server IP addresses.
   d. Click **Apply**.
2. From the Configuration tab, click **VAP > Advanced > Network**
   a. Select gateway feature and then NAT state.
   b. Enter the NAT IP address, which is the IP address of the access point.
   c. Click **Apply**.
3. From the Configuration tab, click **VAP > Advanced > Port Range**
   a. Select an empty entry.
   b. Select **Enable**.
   c. Enter a meaningful name for the entry, the start port, the end port, protocol.
   d. Enter the IP address (if DHCP is not enabled) or add the missing part of the IP address.

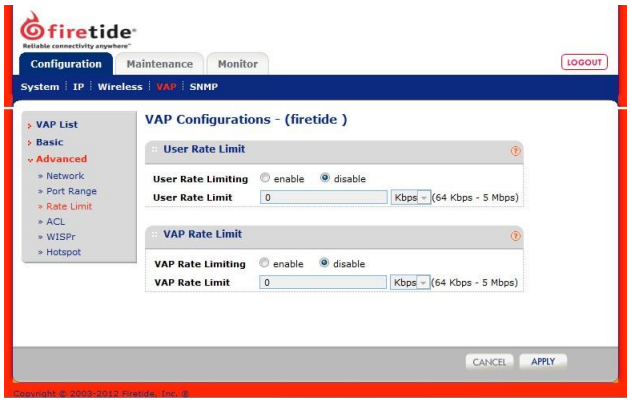


e. Click **Apply**.

Configuring a client rate limit

To configure a client rate limit:

1. From the Configuration tab, click **VAP > Advanced > Rate Limit**
2. Enter the settings for the type of limit you want to configure:
   - For a user rate limit, enable the limit, and then enter a rate with unit of measure (Kbps or Mbps). The valid range is from 64 Kbps to 5 Mbps.
   - For a VAP rate limit, enable the limit, and then enter a rate with unit of measure (Kbps or Mbps). The valid range is from 64 Kbps to 5 Mbps.

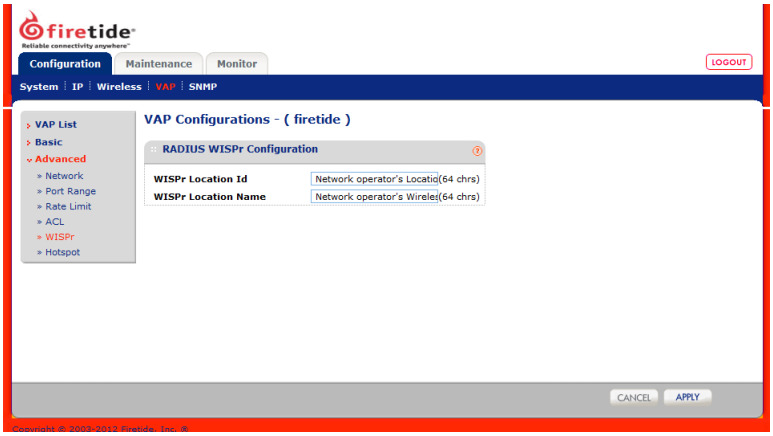


3. Click **Apply**.

Configuring WISPr

To configure the WISPr location and name for RADIUS authentication:

1. From the Configuration tab, click **VAP > Advanced > WISPr**
2. Enter the WISPr location ID and name. Each entry can be up to 64 characters in length.



3. Click **Apply**.

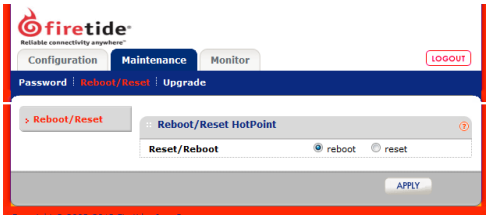
Maintenance tasks

The web interface is a way to do a firmware upgrade, reset or reboot the access point, and return a access point to a factory new state.

Resetting the access point to the factory default settings

Caution! When an access point is reset, all configuration information is erased except USA country code if set to 840 or 842.

You can reset the access point with the reset button or with software in the web interface.



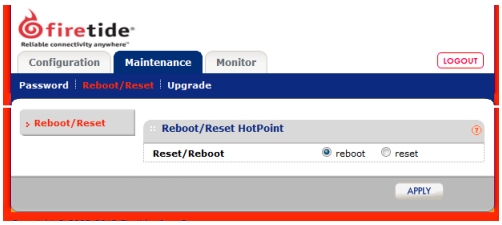
To reset the access point with the web interface:

1. Go to **Maintenance > Reboot/Reset**
2. Select **reset**.
3. Click **Apply**.

Rebooting the access point

To reboot an access point:

1. Go to **Maintenance > Reboot/Reset**



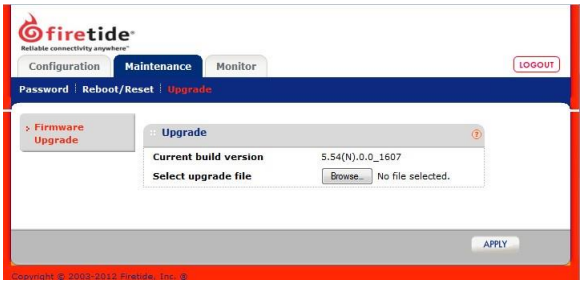
2. Select **reboot**.
3. Click **Apply**.

Upgrading firmware

You can view the firmware version from the Upgrade window. If necessary you can download different firmware from www.firetide.com.

To upgrade firmware:

1. Go to **Maintenance > Upgrade**



2. Download different firmware from www.firetide.com.
3. Click **Browse** and navigate to where you saved the firmware file.
4. Click **Apply**.

The access point automatically reboots.

Monitoring tasks

The web interface is a way to view virtual access point status, summaries, statistics, and provisioned users.

Viewing the virtual access point list

The VAP list has this information:

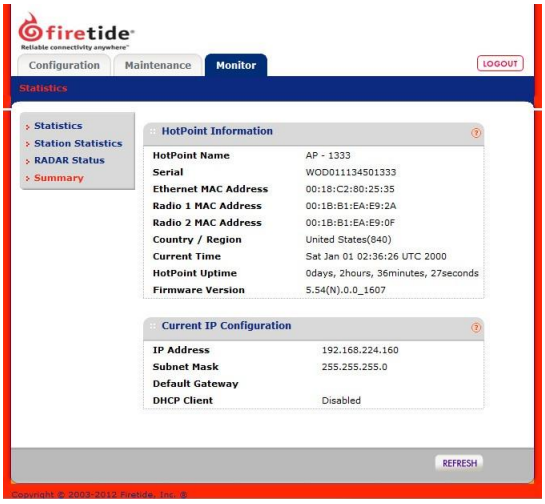
- Selection button, which lets you delete a VAP
- VAP Name
- IP address, which is an IPv4 address
- Net mask
- Radio number, which is Radio 1 or Radio 2
- VAP type, which is standalone client or WDS
- Status, which is Enable or Disable

On the Configuration tab, click **VAP**.

Viewing a summary

The configuration summary contains this information:

- Name
- Serial number
- Ethernet MAC address
- Radio 1 MAC address
- Radio 2 MAC address
- Country code
- Current time
- Uptime, how long the access point has run
- Firmware version
- IP configuration information
  - IP address (required)
  - Subnet mask (required)
  - Default gateway (if configured)
  - DHCP client status (enabled or disabled)

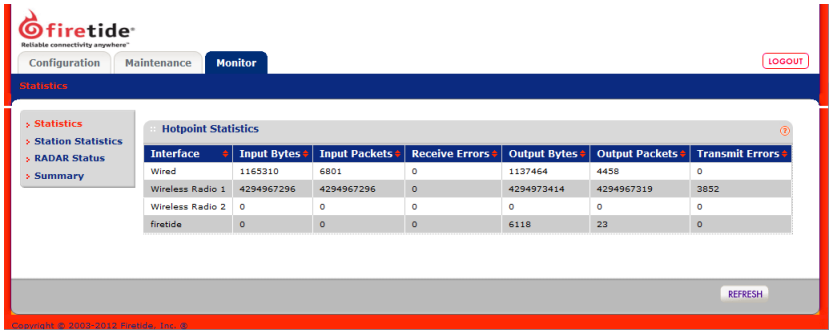


On the Monitor tab, click **Summary**.

Viewing traffic statistics

HotPoint traffic statistics include:

- Interface from which the traffic comes
- Input bytes
- Number of input packets
- Number of receive errors
- Output bytes
- Number of output packets
- Number of transmit errors

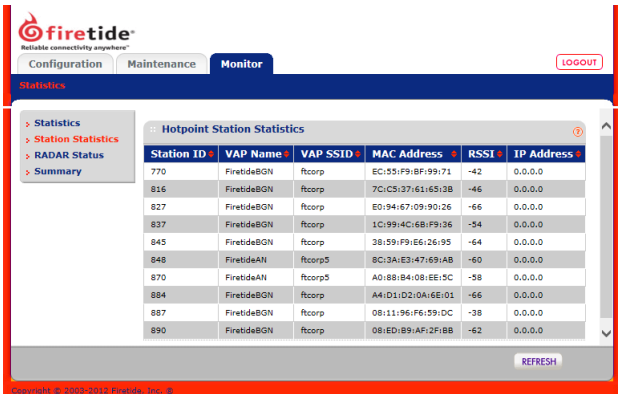


To access traffic statistics, go to the Monitor tab. HotPoint statistics are on the main page of the Monitor section.

Viewing station statistics for a WDS

Station statistics include:

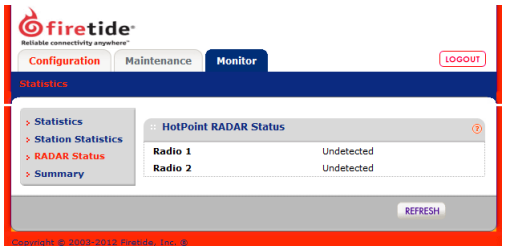
- Station ID
- VAP name
- VAP SSID
- MAC address
- RSSI
- IP address



To view station statistics from the Monitor tab, click **Station Statistics**.

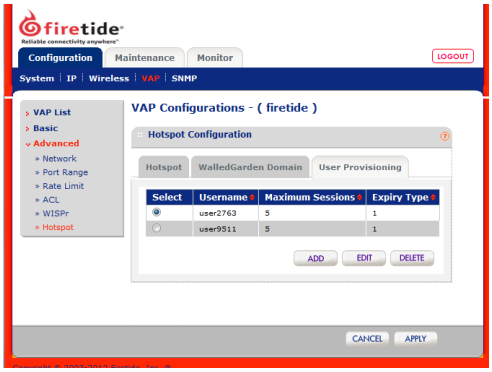
Viewing radar status

To view radar status, from the Monitor tab, click **Radar Status**.



Viewing provisioned users

Provisioned users are configured when you set up a captive portal with authentication services. You can view the entries in a table. From the table you can add, edit, or delete user entries.



To view the provisioned users table:

1. From the Configuration tab, click **VAP > Advanced > Hotspot**
2. Click **User Provisioning**.

Appendix

Worldwide default radio assignments

HotPort devices operate in low-power, short-range mode until you set the country code. When you set the country code, the device uses the correct default radio settings.

The next table lists by country, the country code, wireless mode, channel, and transmit power (in dBm).

Country	Code	Wireless mode	Channel	Transmit power (dBm)
Australia	36	A (5.25 to 5.35 GHz OFDM)	60	17
Austria	40	A (5.15 to 5.25 GHz OFDM)	40	15
Belgium	56	A (5.15 to 5.25 GHz OFDM)	40	17
Canada	124	A (5.25 to 5.35 GHz OFDM)	60	17
Denmark	208	A (5.15 to 5.25 GHz OFDM)	40	17
Finland	246	A (5.15 to 5.25 GHz OFDM)	40	17
France	250	A (5.15 to 5.25 GHz OFDM)	40	17
France2	255	A (5.15 to 5.25 GHz OFDM)	40	17
Germany	276	A (5.15 to 5.25 GHz OFDM)	40	17
Greece	300	G (2.4 GHz OFDM)	7	16
Hong Kong S.A.R.		A (5.25 to 5.35 GHz OFDM)	60	17
India	356	G (2.4 GHz OFDM)	7	16
Ireland	372	A (5.15 to 5.25 GHz OFDM)	40	17
Italy	380	A (5.15 to 5.25 GHz OFDM)	40	17
Japan	392	A (5.15 to 5.25 GHz OFDM)	42	17
Luxembourg	442	A (5.15 to 5.25 GHz OFDM)	40	17
Malaysia	458	G (2.4 GHz OFDM)	7	16
Netherlands	528	A (5.15 to 5.25 GHz OFDM)	40	17
New Zealand	554	A (5.25 to 5.35 GHz OFDM)	60	17
Norway	578	A (5.15 to 5.25 GHz OFDM)	40	17

Country	Code	Wireless mode	Channel	Transmit power (dBm)
People's Republic of China	156	A (5.725 to 5.850 GHz OFDM)	157	17
Portugal	620	A (5.15 to 5.25 GHz OFDM)	40	17
Singapore	702	A (5.725 to 5.850 GHz OFDM)	149	17
South Korea	410	A (5.725 to 5.850 GHz OFDM)	157	17
South Korea	411	A (5.725 to 5.850 GHz OFDM)	157	17
Spain	724	A (5.15 to 5.25 GHz OFDM)	40	17
Sweden	752	A (5.15 to 5.25 GHz OFDM)	40	17
Taiwan	158	A (5.725 to 5.850 GHz OFDM)	149	17
United Kingdom	826	A (5.15 to 5.25 GHz OFDM)	40	17
United States	840			
United States Public Safety	842			

Table 38