HotView Pro Version 10.15.0.0

Reference Manual

HotView Pro™ support for these hardware products:

- **HotPort™ 7010/7020 mesh nodes**
- **HotPort 5020-E/ER/LNK nodes**
- **HotPoint™ 5100/5200 access points**

Published January 2014

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, 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 10.10.0.0. The next table lists the chapter names and summaries.

Table 1. HotView Pro information

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

Table 1. HotView Pro information

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
	Edge node settings	Contains HotPort edge node 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

Table 1. HotView Pro information

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

You must also have administrator access to the mesh to be able to receive technical support.

The next table lists the contact information for customer support.

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

Firetide Mobility

HotPoint Access Points

Appendix

HotView Pro software

This section contains these chapters:

- HotView Pro introduction
- HotView Pro software installation
- Hot View Pro server configuration
- 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

Real-time monitoring and statistics. 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

You can install the client and server on the same computer. You can choose to move the server software to another computer at any time.

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

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 Standard R2 (64 Bit), • Fedora FC14 and FC16 (32 Bit) • Ubuntu 11.04 (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

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

Software requirements

HotView Pro is a Java-based software package. Make sure you have a 32-bit version of Java 7 installed on the server. For a copy of Java 7, visit www.java.com.

C**aution!** If you use another version of Java, you might experience unpredictable results.

The HotView Pro software package includes the following support software:

- JBOSS (required for the browser-based client)
- PostGreSQL version 9.1 (database)

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 detects the database.

Note: If you do not install the database software before you install the HotView Pro software, the system sends disruptive warning messages.

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 9.1 from http://www.postgresql.org/download/windows
- 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, you are finished.

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 8.4, 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 75.

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.

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 License To information, 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.
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, the systems sends a message. Select **No**.

If you accidentally select **Yes**, an error message appears. 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.
2. Go to **Server Administration > Configure HotView Server > Licensing > License Information** tab
3. Select the license that you want to make permanent, and then select **Import Permanent License**.
4. 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 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.

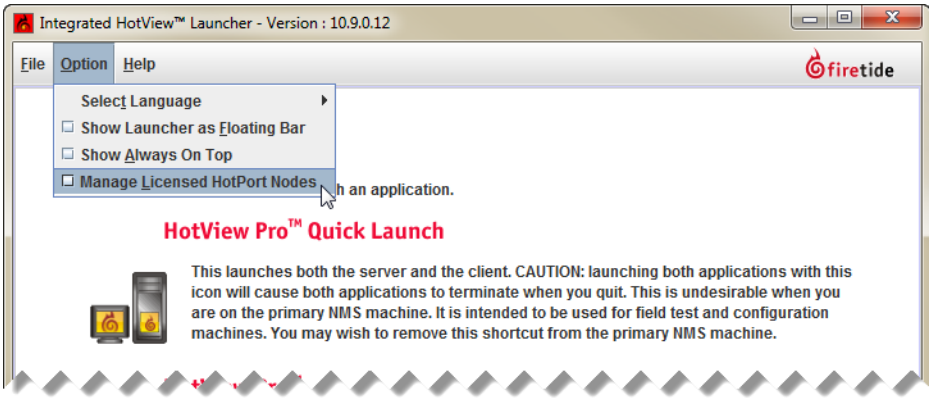
Using HotView Pro without a license key

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 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 10.15.0.0:

- Carefully evaluate the feature set for your needs.
- Make sure that you do not have any HotPort 6000 nodes in your mesh network. HotPort 6000 node interoperability is not supported in certain releases, and you will lose connectivity to them when you upgrade. Refer to the release notes for the firmware release that you want to use.
- 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.

Caution! Firetide strongly recommends that after an upgrade to HotView Pro 10.15.0.0, you do not downgrade to a previous version. A downgrade to a previous software version can cause network connectivity problems.

Hot View 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 RADIUS 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

Server management and firmware configuration options include:

- “Accessing HotView Pro server” on page 14
- “Starting HotView Pro server” on page 14
- “Stopping HotView Pro server” on page 14
- “Stopping the server manager” on page 15

- “Starting the server manager” on page 15
- “Configuring HotView Pro as a Windows Service” on page 15
- “Changing the chunk size and retry count for a firmware upgrade” on page 16
- “Enabling the overwrite firmware file option” on page 17

Other configuration options include:

- “SNMP and alarm configuration” on page 17
- “User account configuration” on page 25
- “Mesh account and membership configuration” on page 29

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-click 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**.

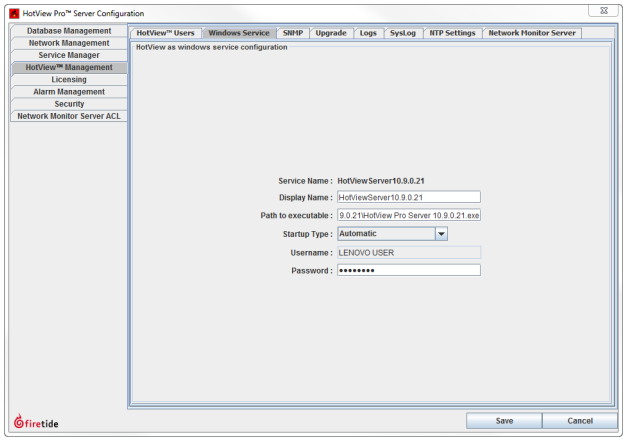
Configuring HotView Pro as a Windows Service

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.

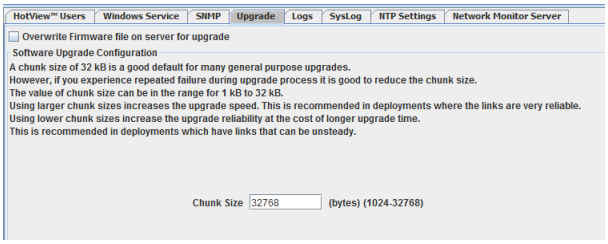
The default chunk size in bytes is 32768. The range of acceptable values is 1024 to 32768.

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

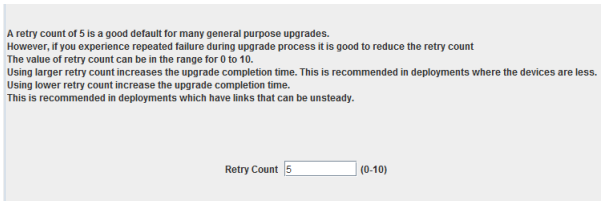
You can also enter the number of retry attempts during a firmware upgrade. The default number of retries is 5. If you experience upgrade failures, reduce the retry count. The range of acceptable values is 0 to 10.

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.

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-ER
- HotPort 5020-LNK

SNMP agent manager tasks include:

- “Starting the SNMP agent manager” on page 20
- “Stopping the SNMP agent manager” on page 20
- “Configuring the SNMP agent manager” on page 20

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 21.
2. Set up a HotView Pro SMTP server entry.
3. Configure the alarms in HotView Pro. See “Adding an alarm” on page 22.

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
Mesh alarm	Bridge link down
	Bridge link up
	Faults (Ethernet port) up
	Faults (Ethernet port) down
	Head node up
	Head node down
FMC alarm	FMC down
	FMC up
	Mesh down
	Mesh up
	Mobile node authentication success
	Mobile node authentication fail
	Mobile node down
	Mobile node up
	Mobile node roam
	Static node down
	Static node up

Alarm type	Event
Access point alarm	HotPoint down
	HotPoint up
	Station association
	Station disassociation
PTP alarm (point-to-point)	PTP node down
	PTP node up
	Head node down
	Head node up
	PTP link down
	PTP link up
	Faults (Ethernet port) up
	Faults (Ethernet port) down

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.

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:

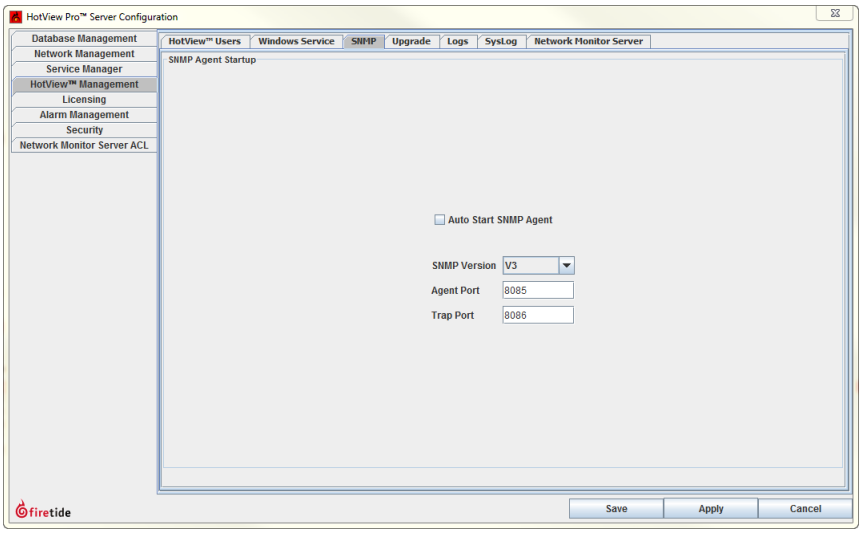
1. Go to **Server Administration > Configure HotView Server > Service Manager**
2. In the SNMP Agent Manager section, click **Stop SNMP Agent**.

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 not set by default. The agent port is from x to y.

Prerequisite: You must enable the SNMP agent manager.

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

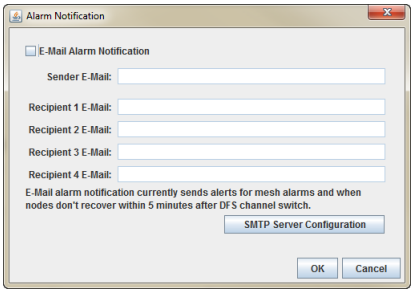


Configuring an SMTP server in HotView Pro

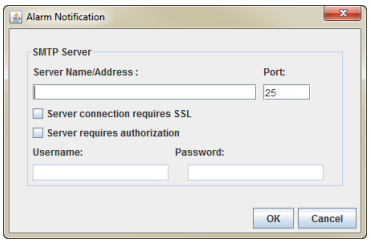
To use the alarm management features, you have to configure the SMTP server within HotView Pro.

To configure an SMTP server:

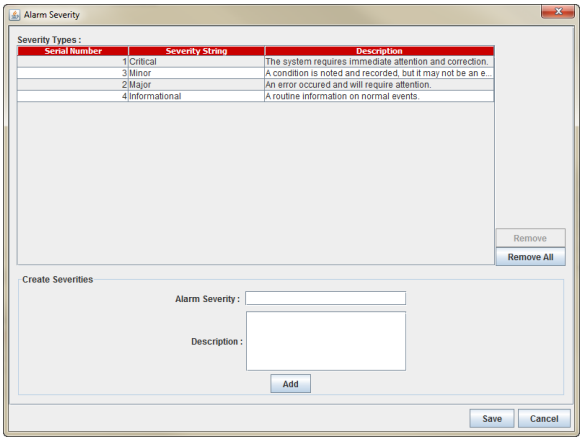
1. Go to **Server Administration > Configure HotView Server > Alarm Management**
2. Click **Configure SMTP Server**.
   a. (Optional) Click email notification box, and then enter the email for the sender and up to four recipients.



   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.



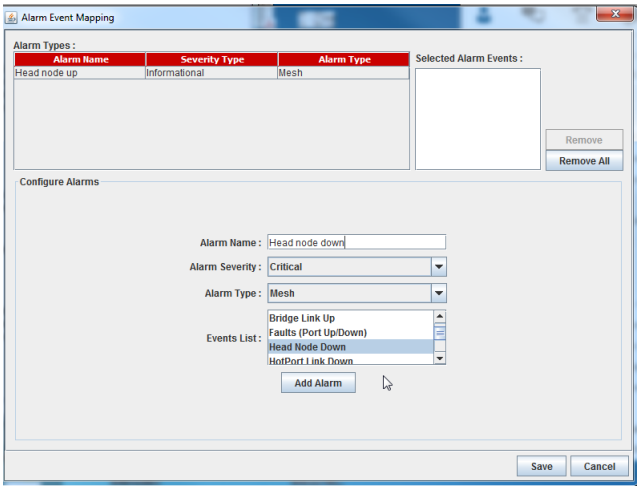
4. Click **Save**.

Adding an alarm

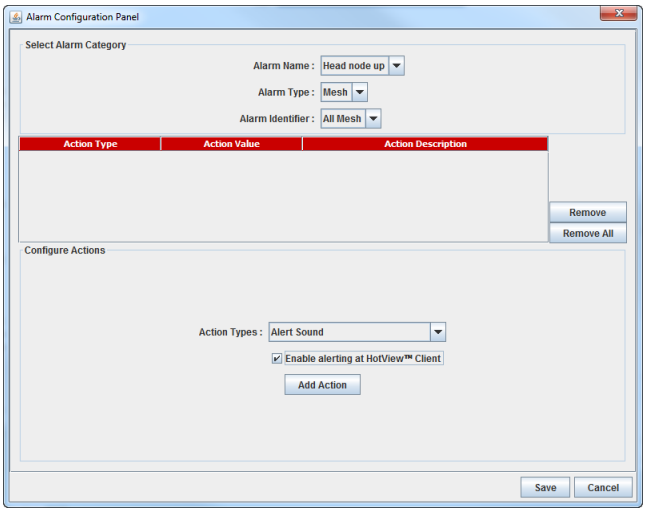
To configure an alarm:

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:

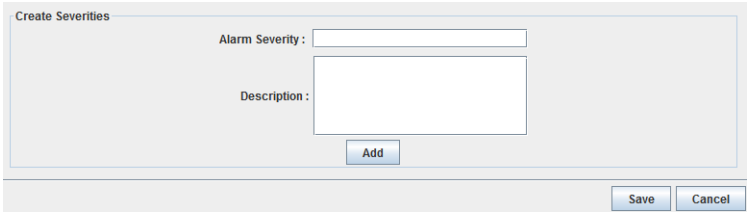
1. Go to **Server Administration > Configure HotView Server > Alarm Management > View Alarms/Configure Actions**

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**



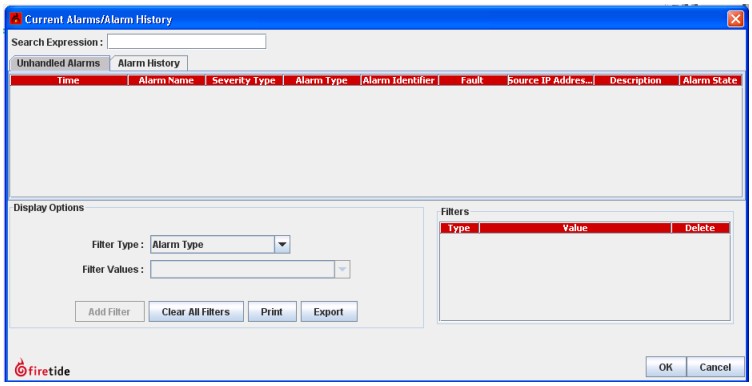
2. Enter a name (up to 30 characters long) for the severity level.
3. Add a description.
4. Click **Add**.

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 26

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

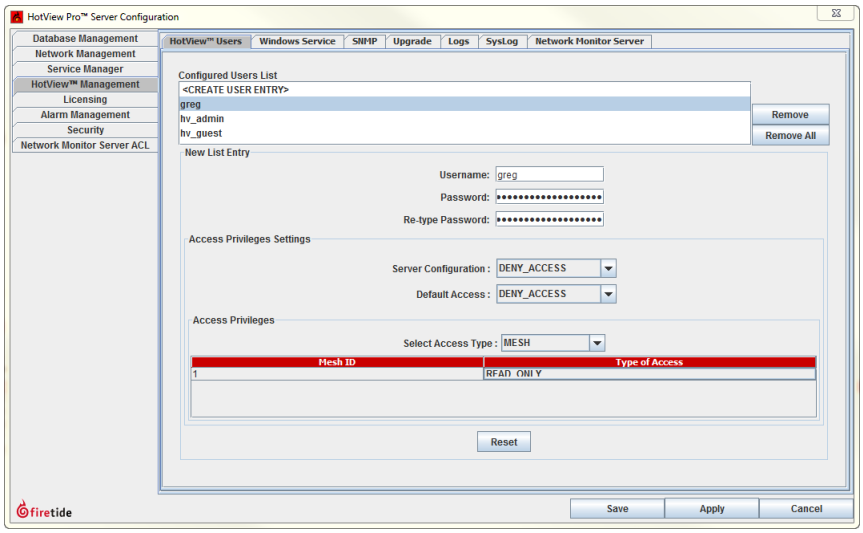
When you make a new user account, you have these options:

- 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

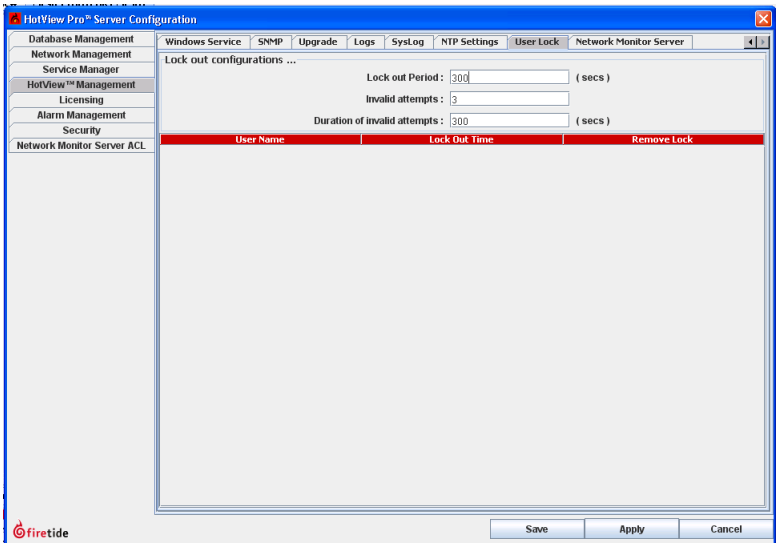
A user lockout entry lets you configure how many tries a user has to enter the correct login credentials. This feature is available for networks that use high security.

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:

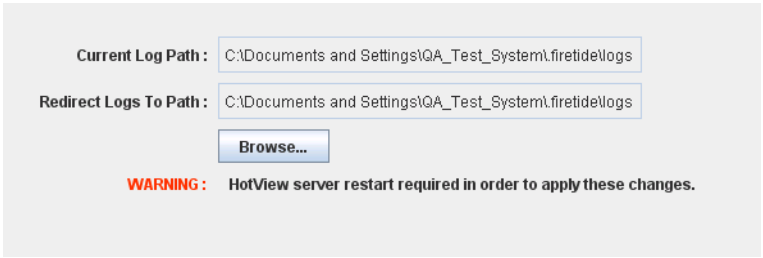
1. Go to **Server Administration > HotView Management > User Lock** tab
2. Enter the lock out period, number of invalid login attempts, and duration of invalid attempts.
3. Click **Save**.



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.

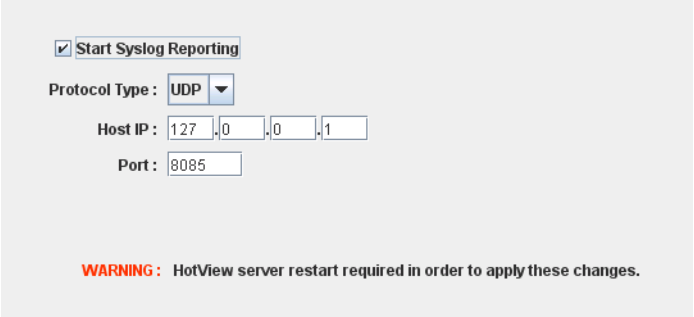


3. Click **Save**.
4. Restart the HotView server.

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 30

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

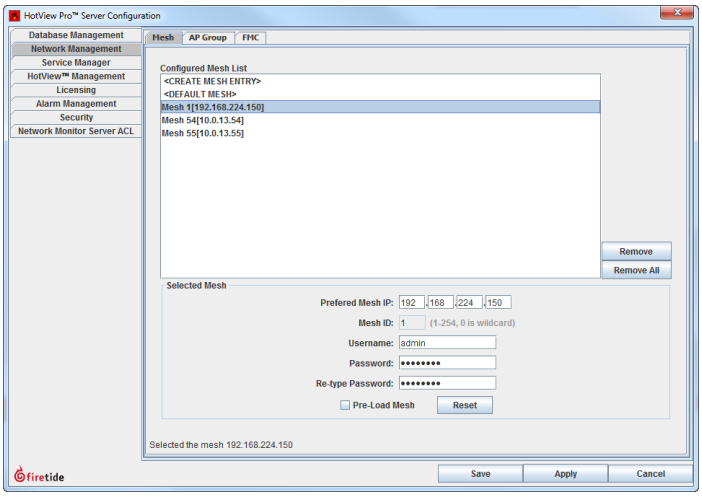
Note: You can also make password changes from **Server Administration > Configure HotView Server > Network Management** tab.

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.

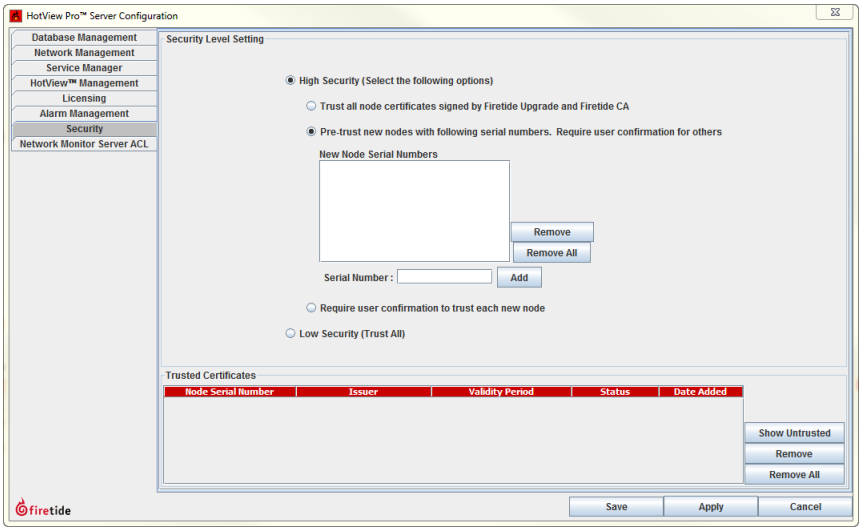
If the mesh has high security enabled, when you do future firmware upgrades you must use the digitally signed (.bin2) file.

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™ Server Configuration
Database Management
Network Management
Service Manager
HotView™ Management
Licensing
Alarm Management
Security
Network Monitor Server ACL
Security Level Setting
High Security (Select the following options)
Trust all node certificates signed by Firetide Upgrade and Firetide CA
Pre-trust new nodes with following serial numbers. Require user confirmation for others
New Node Serial Numbers
Remove
Remove All
Serial Number :
Add
Require user confirmation to trust each new node
Low Security (Trust All)
Trusted Certificates
Node Serial Number
Issuer
Validity Period
Status
Date Added
Show Untrusted
Remove
Remove All
firetide
Save
Apply
Cancel

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.

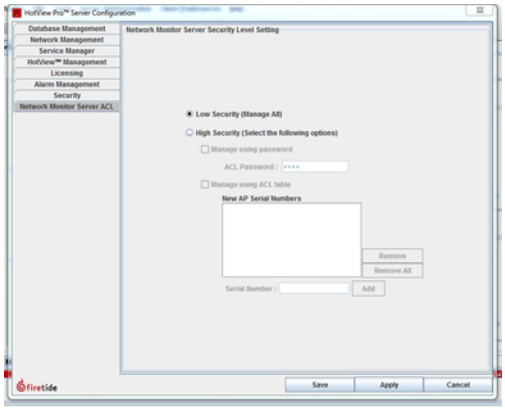
1. Click the HotView Pro shortcut > **Server Configuration > Configure HotView Server > Service Manager**
2. Click the button to stop or start the monitoring server.
3. Click **Save**.

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**.

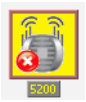
Viewing access points using HotView

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)

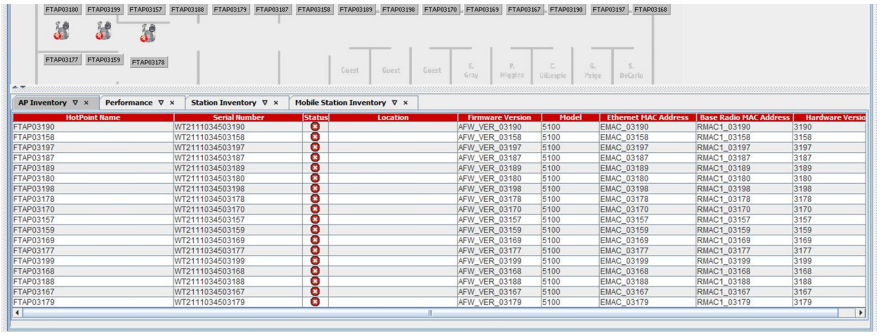


Managed AP (DOWN)

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:

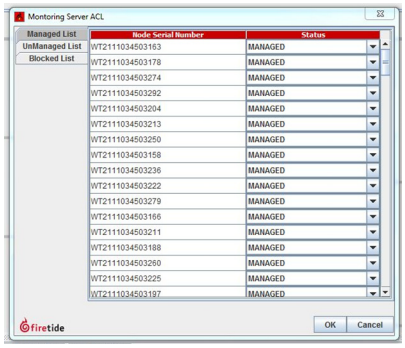
- HotPoint name
- Serial number
- Status
- Location
- Firmware version
- Model
- Ethernet MAC address
- Base radio MAC address
- Hardware version

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 21.

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 107.

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 107.

MAC address filtering

MAC address filtering can be used to block specific MAC addresses. For more information, see “Configuring MAC filters” on page 103.

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.

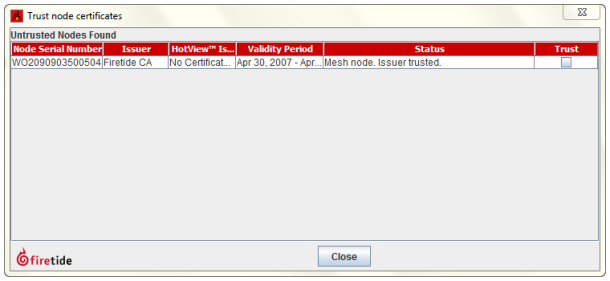
High security options include:

- 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.

Interference from other RF sources and incorrectly configured meshes affect RF signal quality, and from incorrectly-configured meshes. These problems appear as dropped packets and retries in the statistics panel.

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	

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.

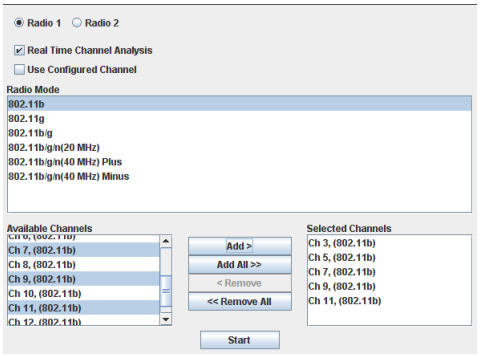
Spectrum analysis works by using one radio in the node to sequentially scan through the list of selected channels, recording the duration and power of any RF signals it finds. The other radio in the node sends the result back to HotView Pro,

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.

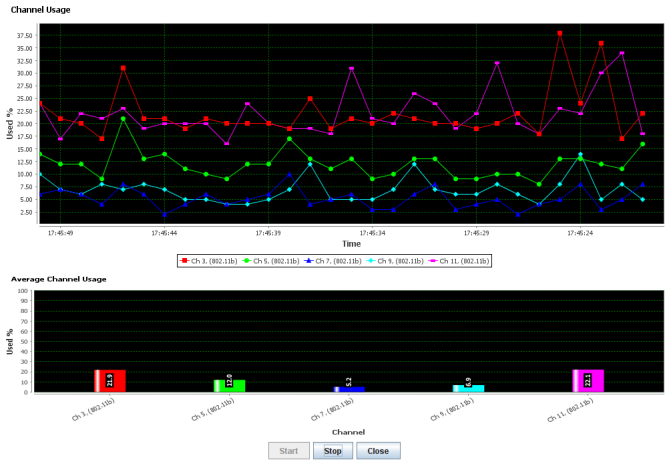
To access the spectrum analysis feature:

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.

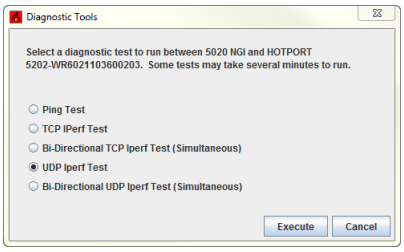
The Iperf test is a deployment diagnostic tool and is not a performance benchmark test. The results are indicative of baseline performance, but actual throughput performance can be higher.

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.

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 112.

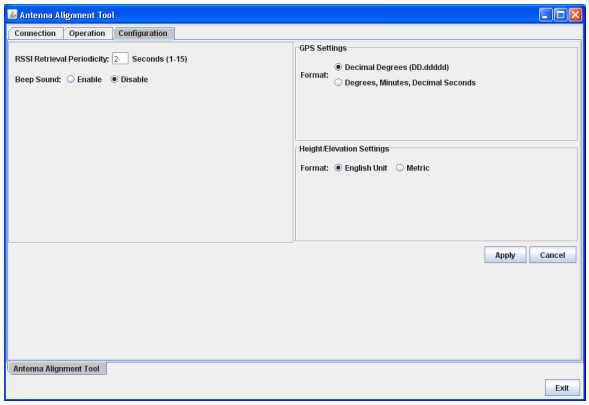
To configure the antenna alignment tool:

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**.



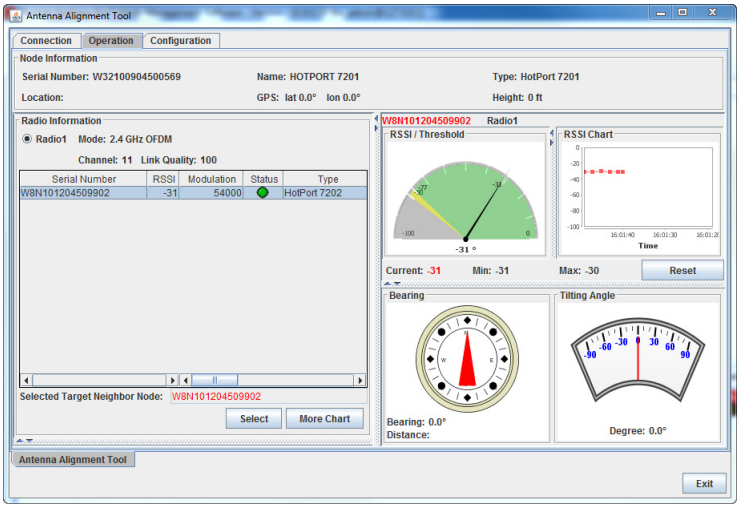
Using the antenna alignment tool

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 112.

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:

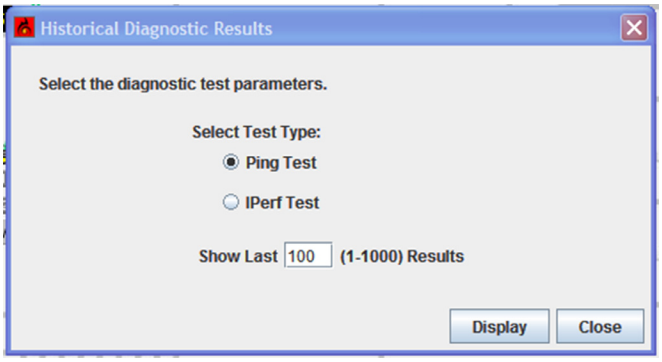
- TCP Iperf Test
- Bi-Directional TCP Iperf Test (simultaneous)
- UDP Iperf Test
- Bi-Directional UDP Iperf Test (simultaneous)

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

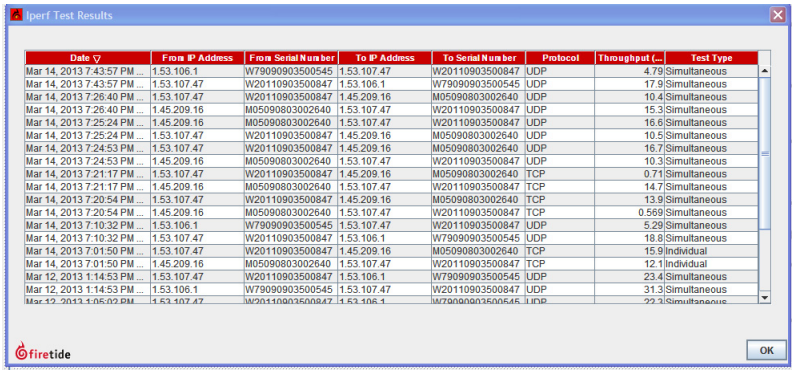
Prerequisite: You must install and enable the database functions.

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

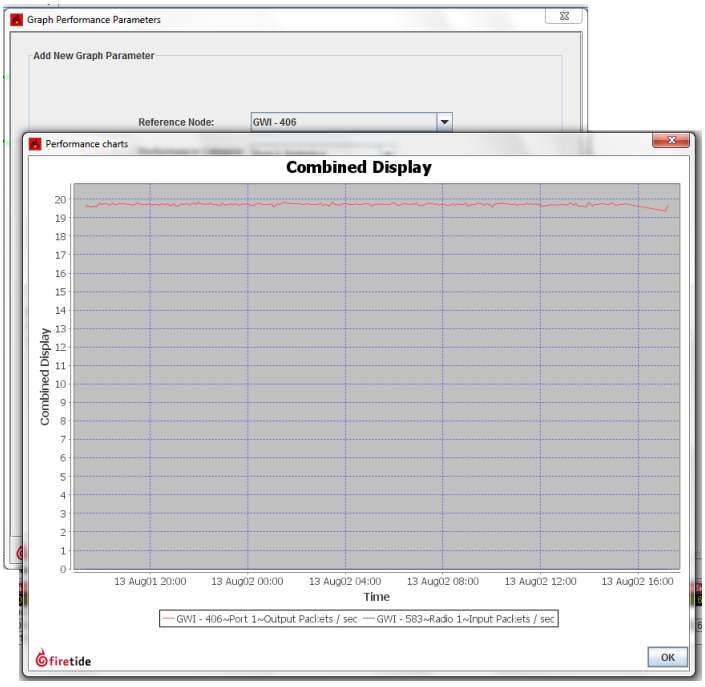
Graph Statistics lets you graph statistics for up to four parameters.

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

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, edge nodes, 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 upgrade” on page 16.

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, edge nodes, 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.

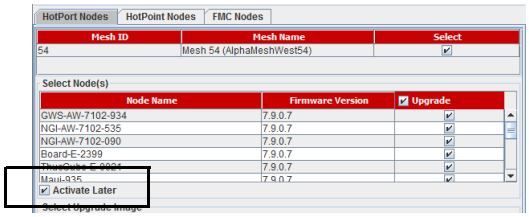
By default, the system uses the configuration in cache for multiple upgrades.

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.

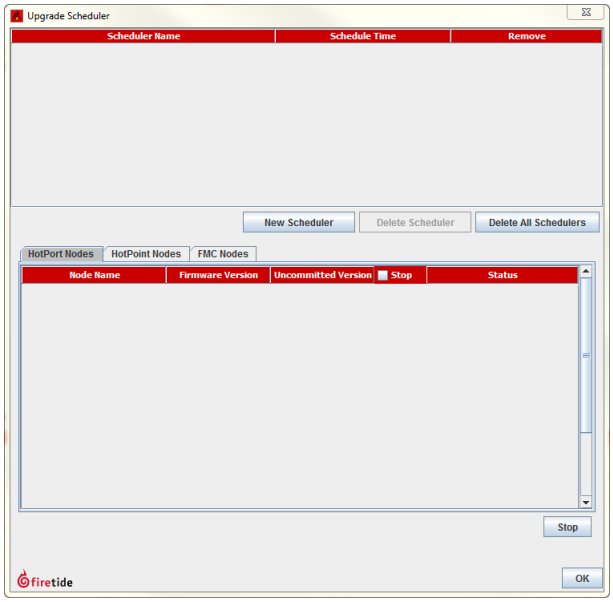


When you schedule an upgrade time (Scheduler Operation: Later), the HotView server, if it is running, starts the job at the scheduled time. If the HotView server is not running at the time scheduled, the scheduled jobs start immediately after you start the HotView server.

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:

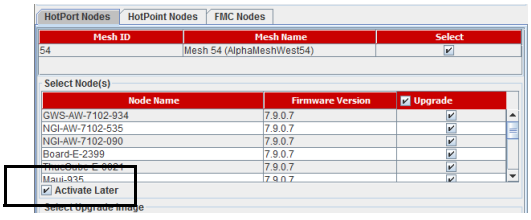
1. Go to **Network > Upgrade Firmware**
   The upgrade scheduler appears.



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 41.

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

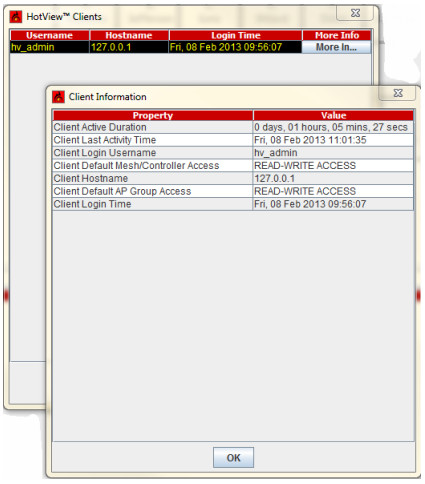
You can retrieve information about these HotView client properties:

- 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.

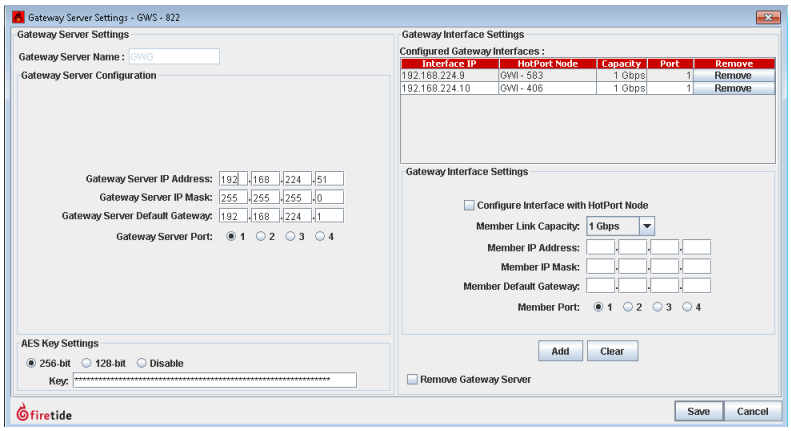
6. Log out of the mesh.

   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.

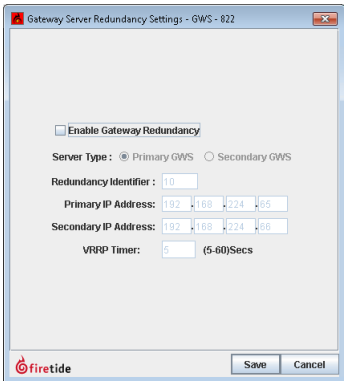
The redundant gateway server should have the same IP address, and the same values for the gateway interfaces.

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.

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.

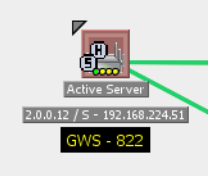
Prerequisite: Permanent management license for each server

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.

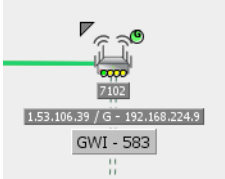
Mesh views and icons

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

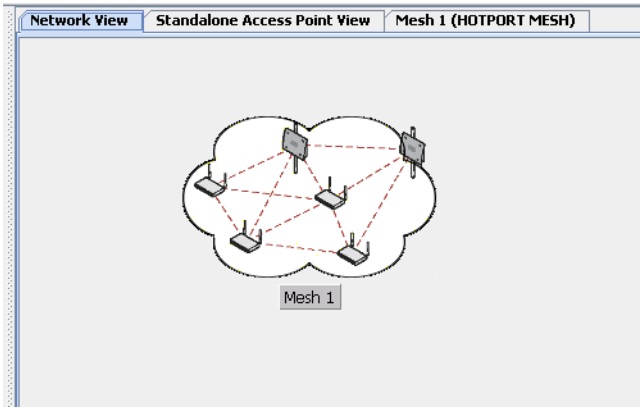
Gateway server icon. The next image shows a gateway server icon. It is a head node (H) because it has an Ethernet connection. It is marked S because it is a server. The one active port is green, and the three other ports are yellow. A gateway server only has one active Ethernet port. The two solid green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



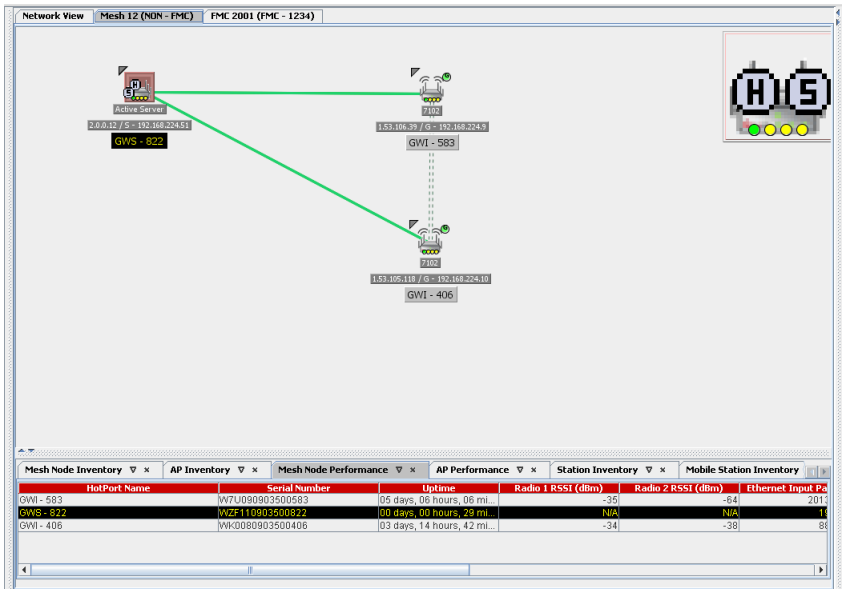
Gateway interface. A gateway interface mode has one connection to a gateway server and connections to other mesh or edge nodes. The next image shows a gateway interface.



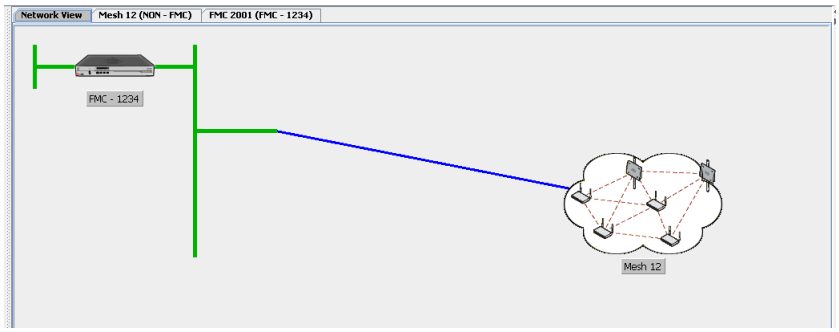
Network view. The next image shows a view of the network. You see this tab after you log in.



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 port on a node can support up to eight Ethernet Directs connections. The system puts ports with Ethernet Direct connections in a separate VLAN.

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.

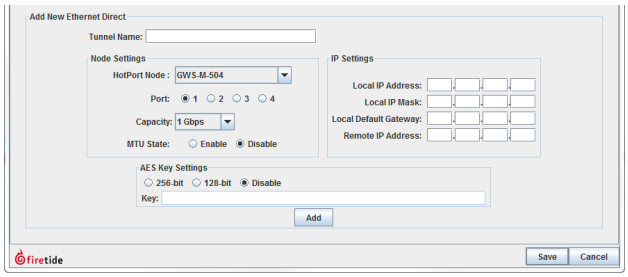
You cannot modify an Ethernet Direct configuration entry. You must delete it and make a new entry.

When you remove the Ethernet Direct configuration, the system disables the Ethernet ports that were used on the nodes.

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. Select the tunnel entry in the Ethernet Direct Tunnel list at the top of the window.
8. Click **Mirror**.
   a. Enter the IP address of the gateway server and its subnet mask.
   b. Click **Add**.
9. At the bottom of the window, click **Save**.
10. 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 63.

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

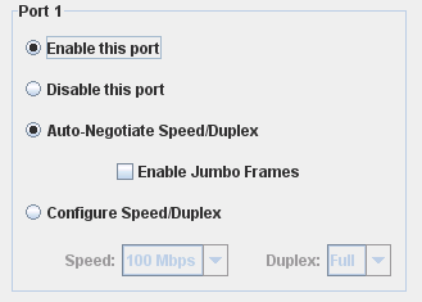
If you want to make a change to an already configured Ethernet Direct connection, you must delete the tunnel entry and configure the entry again. When you delete the tunnel configuration, the system automatically disables the physical Ethernet ports used on each node.

To make changes to the security settings for an Ethernet Direct connection:

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**.

Note: When you delete an Ethernet Direct connection, the system automatically disables the Ethernet ports.

5. 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 far end node.
6. Enter the tunnel name, which can be a descriptive name for this connection.
7. 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)
8. Enter the IP settings:
    - Local IP address
    - Local IP subnet mask
    - Local default gateway
    - Remote IP address
9. Enter the security settings:
    - Select 256-bit AES or 128-bit AES key.
    - Enter a key.
10. Click **Add**.
11. Select the tunnel entry in the Ethernet Direct Tunnel list at the top of the window.
12. Click **Mirror**.
    a. Enter the IP address of the gateway server and its subnet mask.
    b. Click **Add**.
13. At the bottom of the window, click **Save**.