

FAAST Fire Alarm Aspiration Sensing Technology® Networking

USER GUIDE



Trademarks

PipeIQ, the PipeIQ icon, FAAST Fire Alarm Aspiration Sensing Technology, System Sensor, and the System Sensor logo are registered trademarks and/or trademarks of Honeywell International Inc. in the United States and/or other countries. Other parties' trademarks or service marks are the property of their respective owners and should be treated as such.

Microsoft, Windows, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Firefox is a registered trademark of the Mozilla Foundation.

Android and Chrome are trademarks of Google Inc.

The Trademark Blackberry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Honeywell is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited.

Copyright
©2012 System Sensor
www.systemsensor.com

Some screen shots are used with permission from Microsoft.

Table of Contents

Introduction.....	4
Features.....	4
TCP/IP Connectivity	4
Direct PC Connection	4
Network Adapter Configuration	5
Testing Connectivity.....	11
Configuration	12
LAN Connection.....	15
Remote Connection (VPN)	16
Notes on Operation.....	16
Troubleshooting	16
FAQ: TCP/IP Connectivity.....	17
PC Configuration and Monitoring	18
User Levels.....	18
Connection	18
Connection Status	19
Configuration	19
Monitoring	21
Live View	21
Live Trend Graph	22
Historical Trend Graph.....	23
Log View	24
FAQ: PC Configuration and Monitoring	25
Web Server.....	26
Requirements	26
Connection	26
Configuration Viewer	27
Live View	29
Events View	29
FAQ: Web Server	30
E-mail Client.....	31
Features	31
Network Requirements	31
Server Requirements.....	32
E-mail Client Requirements	32
E-mail Client Configuration.....	32
Testing and Verification	36
Notes on Operation.....	36
FAQ: E-mail Client.....	37
Appendix	38
Glossary.....	38
Specifications.....	39
Technical Support.....	39

Introduction

The FAAST 8100 series of aspiration smoke detectors are equipped with an onboard Ethernet port for network connectivity. This interface permits a number of intriguing remote monitoring possibilities, including the ability to receive alarm and fault notifications via e-mail. The detector has been designed to operate with common network technologies. However, it is important to recognize that network topologies can vary and network management can be rather complex. The networked operation of the FAAST detector requires third-party software and equipment that System Sensor is unable to support. It is recommended that professionals familiar with the local IT infrastructure be consulted when attempting to integrate the FAAST detector with a network. Their expertise and the information in this guide will help ensure a successful networked installation.

Features

The FAAST 8100 series of detectors are network capable devices and include the following:

- Integrated 10/100 wired Ethernet
- TCP/IP v4
- Configuration and monitoring using the PipelQ software
- Integral Web server for remote monitoring via a Web browser
- SMTP e-mail client for generating alarm and fault notifications

TCP/IP Connectivity

TCP/IP is a ubiquitous suite of protocols used for communication over the Internet and other networks. Traditionally, these protocols were employed primarily by servers and personal computers. Increasingly, TCP/IP can be found in a variety of devices from televisions and video game consoles to smartphones and sensors.

The FAAST detector supports connection to an IP network using version 4 of the Internet Protocol. The device comes pre-programmed with a default addressing configuration, which can be modified using the PipelQ software.

Default IP Configuration

Static/Dynamic IP Address	Static
IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Direct PC Connection



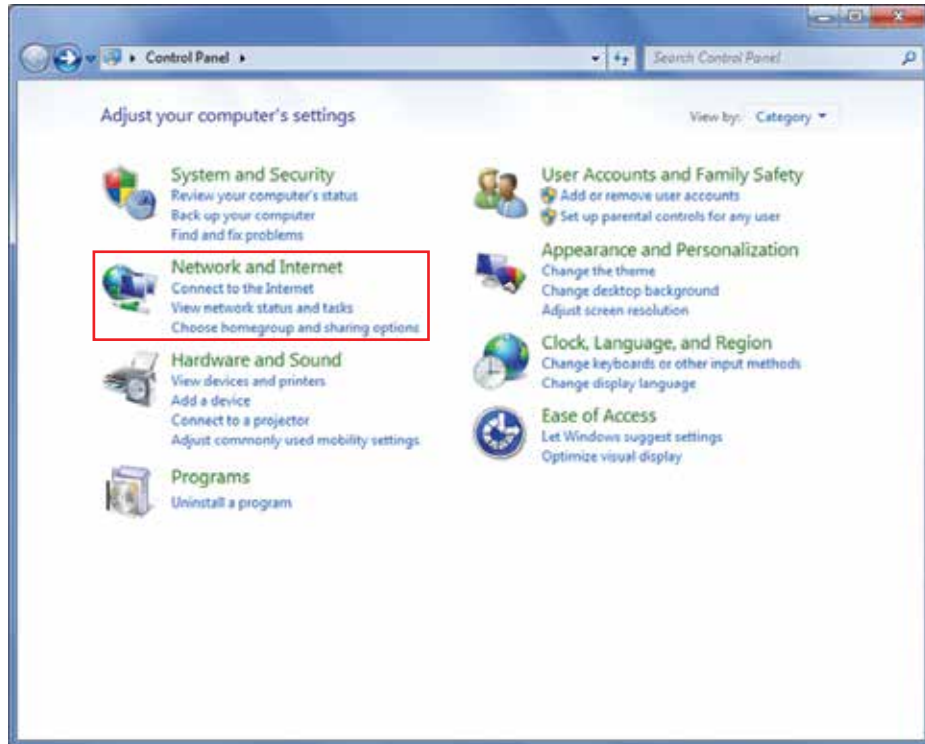
One of the benefits of the FAAST detector's Ethernet interface is that the unit can be configured without any special hardware. All that is required is a PC and a standard Ethernet cable. Instructions for directly connecting the FAAST detector to a PC are shown below.

1. Connect the PC and detector using a standard Ethernet cable (a crossover cable is not required).
2. Configure the PC network adapter according to the instructions for your operating system. See *Network Adapter Configuration*.
3. Verify the connection. See *Testing Connectivity* for details.
4. Connect to the detector using either the PipelQ software or a Web browser. See *PC Configuration and Monitoring or Web Server* for detailed instructions.

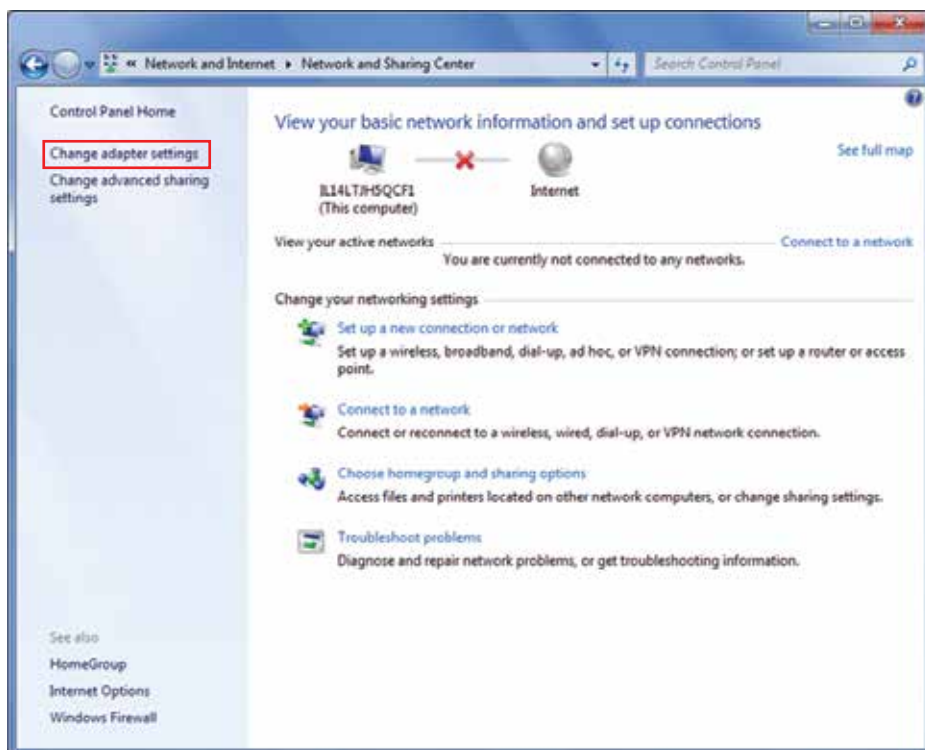
Network Adapter Configuration

Windows 7

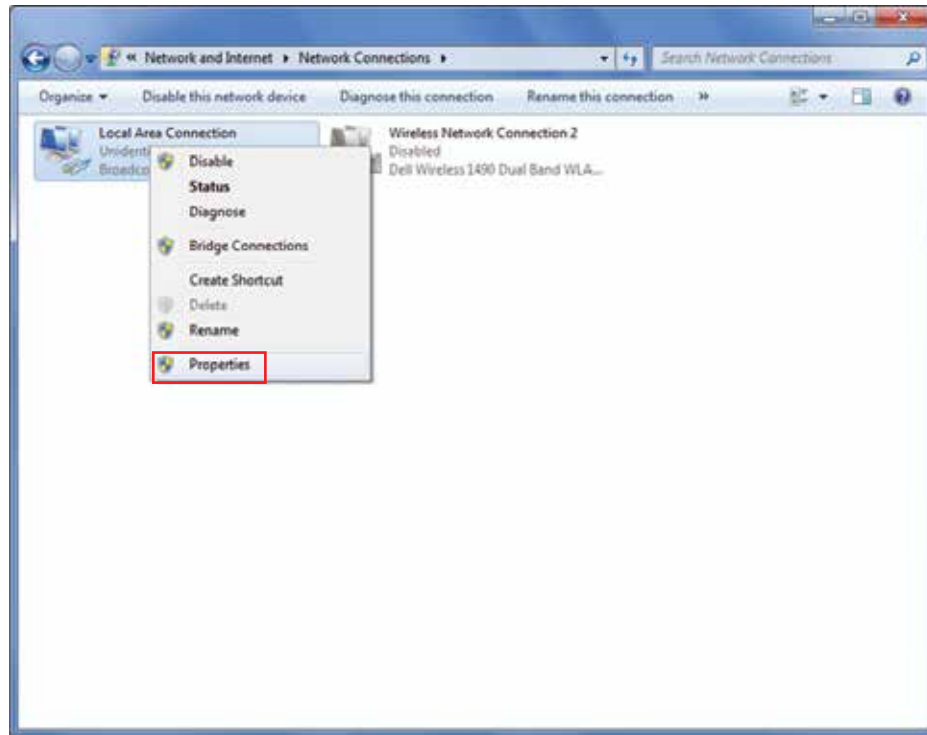
1. Open *Control Panel* and select *Network and Internet*.



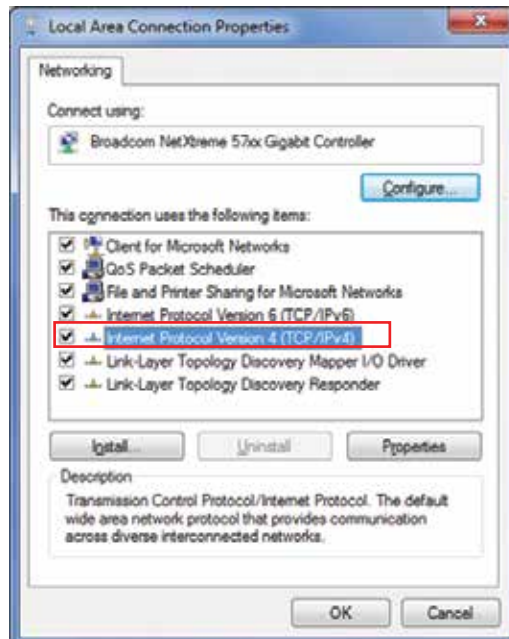
2. Select *Change adapter settings* from the menu on the left.



3. Locate the network adapter connected to the detector. In most cases this will be *Local Area Connection*. Right-click and select *Properties*.



4. Select *Internet Protocol Version 4 (TCP/IPv4)* and then click *Properties*.



- Examine the existing settings for your connection. If you use this adapter to connect to the networks, you *should* write down the settings so you can restore them later.



- Configure the network adapter to use a static IP address as shown below.



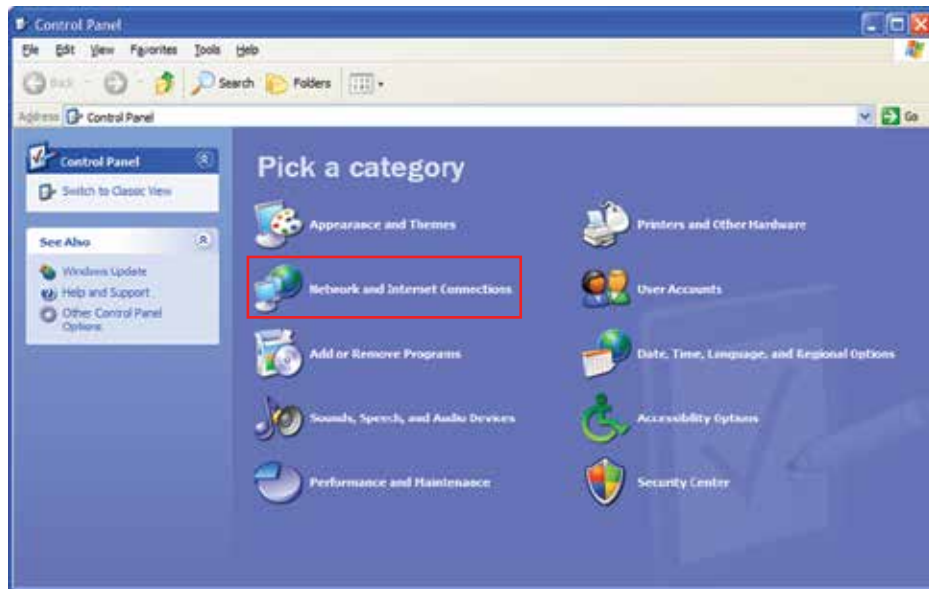
Note: The IP address you choose for the PC must be different than the IP address of the detector.

- Choose **OK** to save the settings. Then click **OK** to save and close the Local Area Connection properties.
- Network adapter configuration is complete. Test connectivity by pinging the detector. See **Testing Connectivity** for instructions.

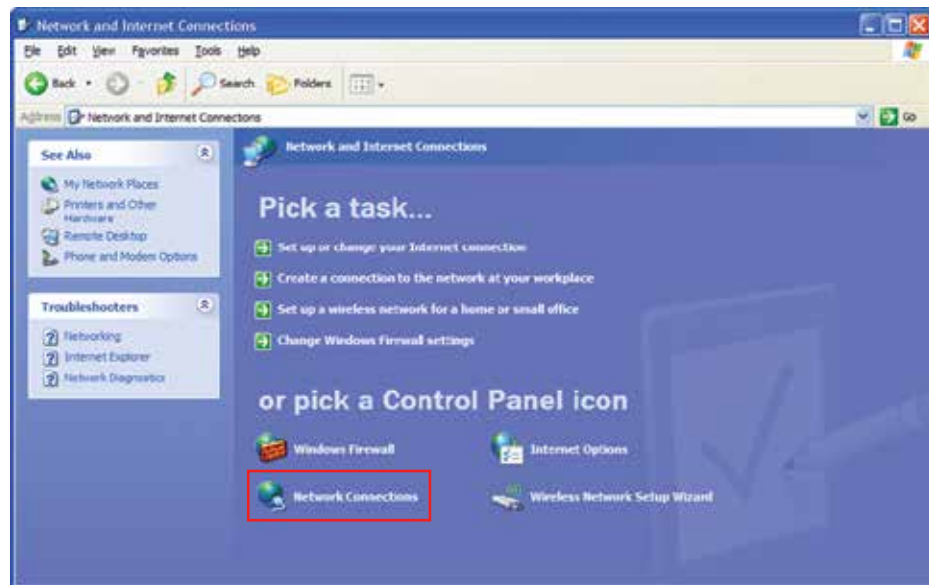
Note: Some PCs may require a restart for the settings to take effect.

Windows XP

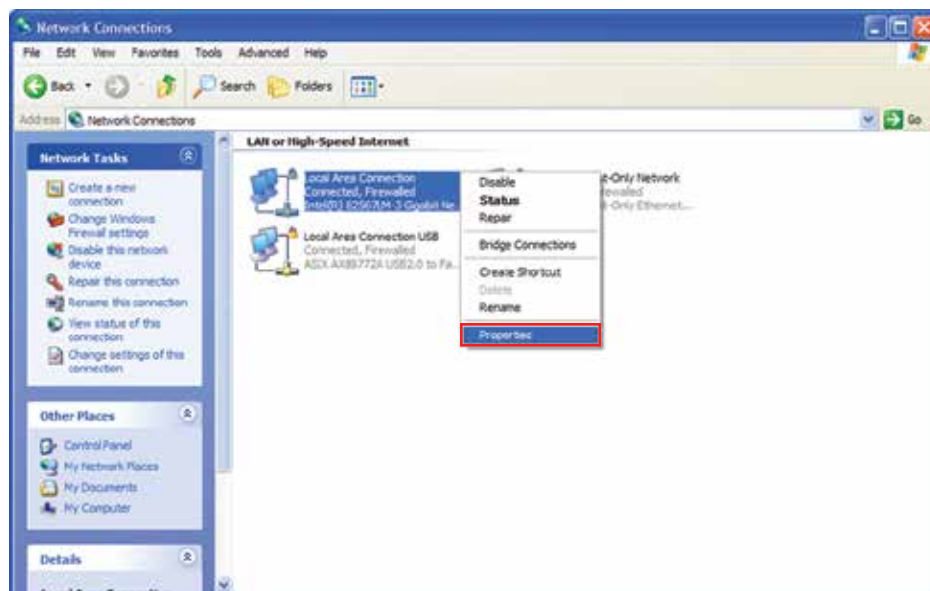
1. Open *Control Panel* and select *Network and Internet Connections*.



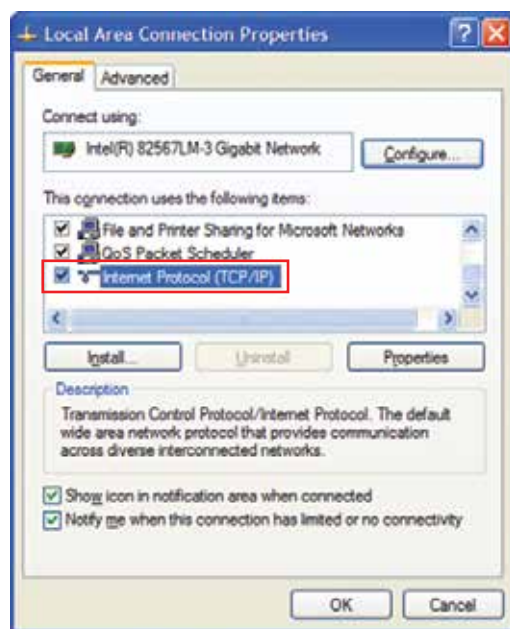
2. Select *Network Connections*.



3. Locate the network adapter connected to the detector. In most cases this will be *Local Area Connection*. Right-click and select *Properties*.



4. Select *Internet Protocol (TCP/IP)* and then click *Properties*.



- Examine the existing settings for your connection. If you use this adapter to connect to other networks, you *should* write down the settings so you can restore them later.



- Configure the network adapter to use a static IP address as shown below.



Note: The IP address you choose for the PC must be different than the IP address of the detector.

- Choose **OK** to save the settings. Then click **OK** to save and close the Local Area Connection properties.
- Network adapter configuration is complete. Test connectivity by pinging the detector. See **Testing Connectivity** for instructions.

Note: Some PCs may require a restart for the settings to take effect.

Testing Connectivity

Physical Link

Verify the physical connection on the Ethernet link by examining the green and yellow LEDs on the RJ-45 connector. They should be illuminated and/or blinking. If not, verify the cable is properly seated and all equipment is powered on.

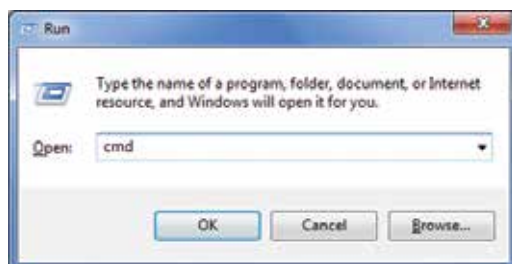


Note: The yellow LED will not illuminate when connected to 10 MBit equipment.

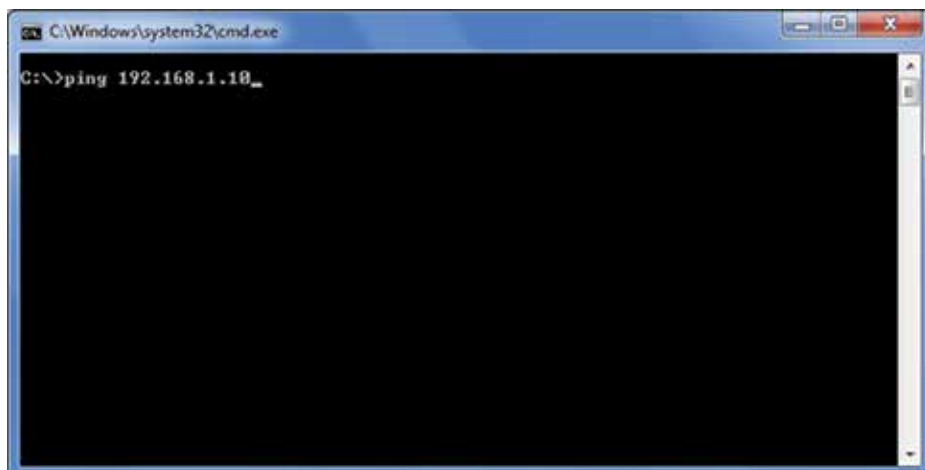
Ping Utility

Once the FAAST detector is connected to an Ethernet link, the next step is to verify IP connectivity between the device and your PC. This is accomplished using the ping utility.

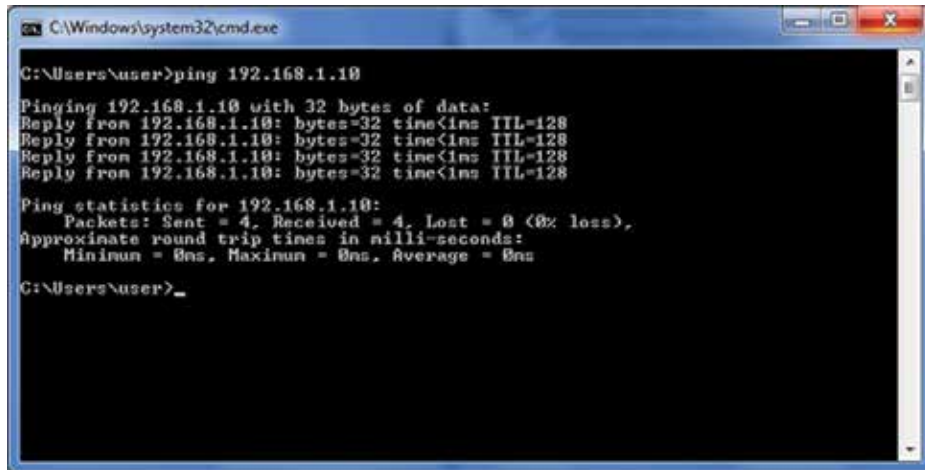
1. From the **Start** menu choose **Run...**
2. Type "cmd" in the text box and click **OK**.



3. In the command window type "ping 192.168.1.10" (the IP address of the FAAST detector) and press **Enter**. The utility on the PC will attempt to contact the detector at this IP address. If you have configured the detector to use a different IP address, substitute as appropriate.



4. Examine the results. By default, the ping program attempts to contact the detector four times. If at least one reply is received, the PC is able to contact the detector.

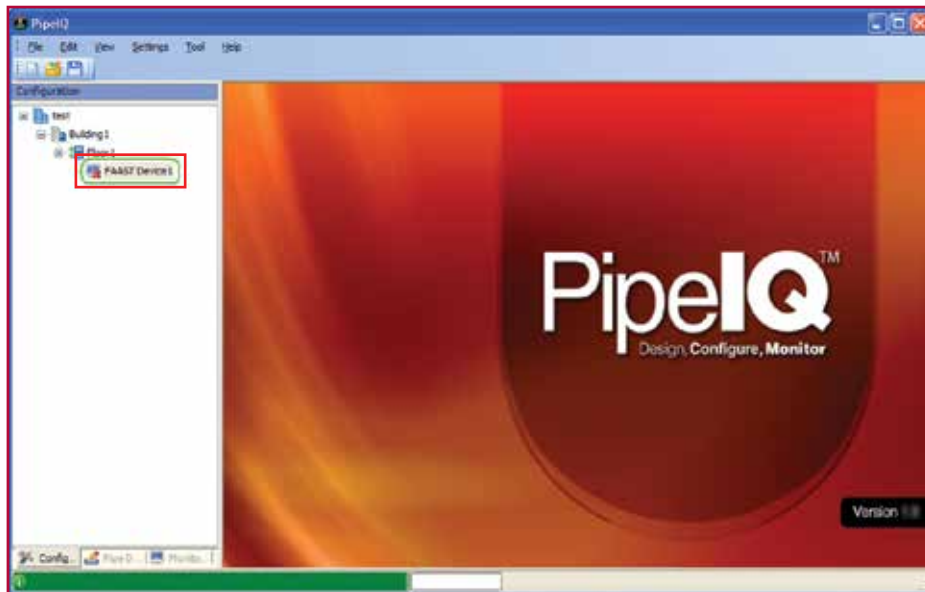


Configuration

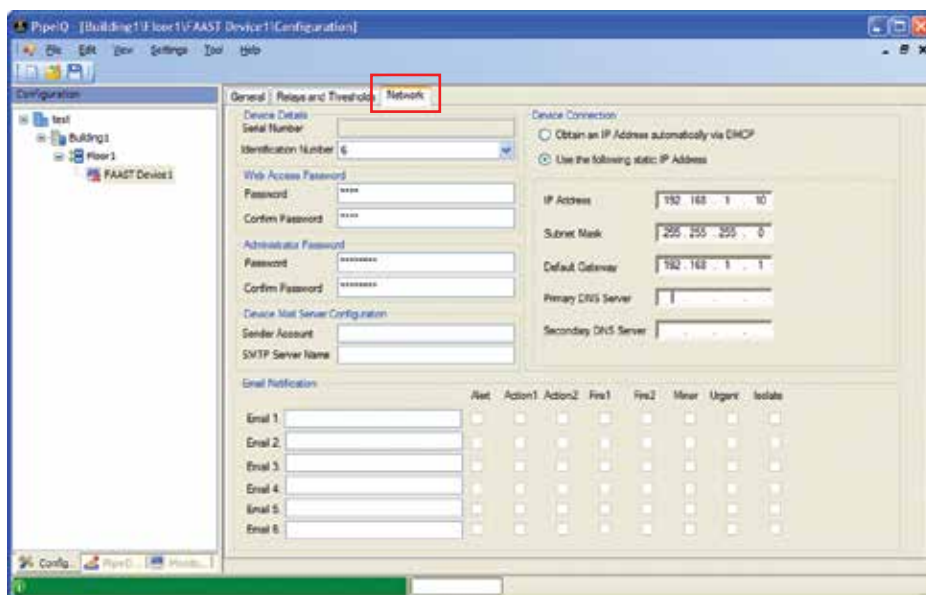
The first step in deploying a networked FAAST detector is determining the IP address it should use and the method by which the address will be assigned. IP addresses can either be assigned statically and programmed into the device or assigned dynamically by a special server using the DHCP protocol. The FAAST detector supports either method of address assignment. If you are unsure of the method and address to use, contact your network administrator for assistance.

The PipelQ software is required to change the network configuration of the FAAST detector. Instructions for IP configuration are shown below.

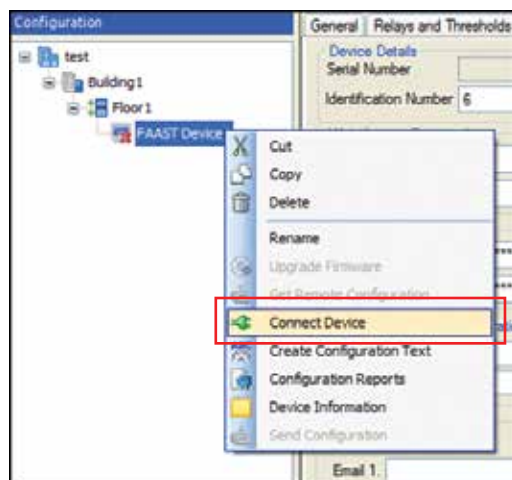
1. Start the PipelQ software application.
2. If you have previously created a project, open it using *File -> Open*. Otherwise, create a new project using *File -> New*.
3. Double-click *FAAST Device1* from the navigation pane to open the Configuration window.



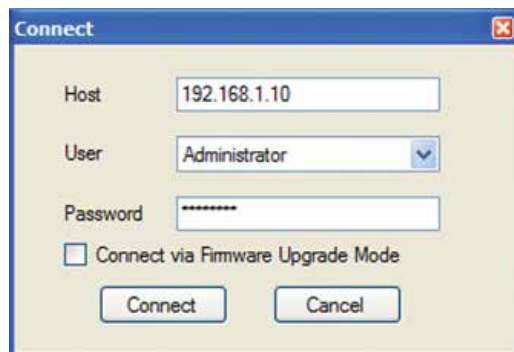
- Click the **Network** tab to display the network parameters.



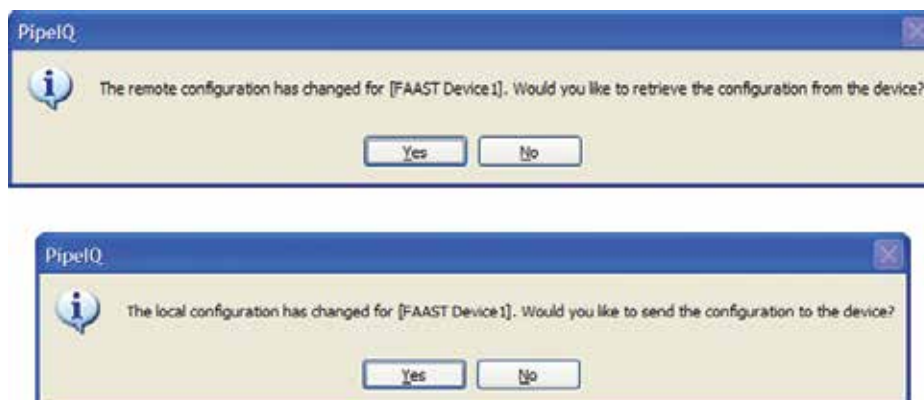
- Connect to the detector by right-clicking and selecting **Connect Device**.



- In the Connect window, ensure the correct IP address for the detector is entered in the Host field. Change the User from **Read-Only** to **Administrator**. Finally, enter the password for the detector in the Password field. The default password is "password". Click **Connect**.



7. Upon connection, you may receive one of the following messages.



If you receive the first message, select **Yes** to copy the settings from the detector into your PipelQ project file. If you receive the second message, select **No**.

8. Edit the IP settings for the detector using the Device Connection group. The FAAST detector can operate using either a static IP address or a dynamic IP address assigned via a DHCP server. When using DHCP, all the IP settings are provided by the server and static settings are disabled. The fields are described in the table below.




Static IP

Dynamic IP

Field	Description
IP Address	The address uniquely identifying the FAAST detector on an IP network
Subnet Mask	Used to determine the subnet to which the detector belongs
Default Gateway	A router for the detector to use when contacting external networks
Primary DNS Server	The IP address of a server to handle name resolution requests
Secondary DNS Server	The IP address of a second server to handle name resolution requests

Note: Choose these values carefully. Illegal IP address / subnet mask combinations will make it impossible to connect to the device.

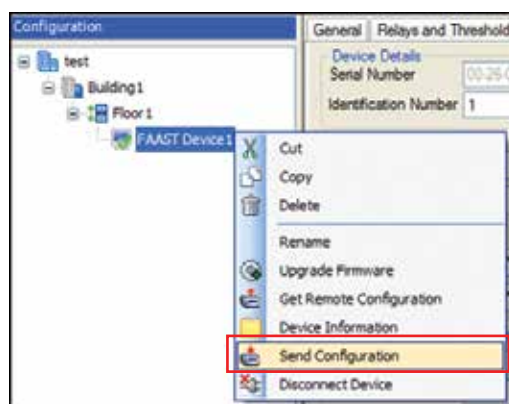
9. When the desired IP settings have been entered, click the **Save**  icon:

10. The following message will appear:



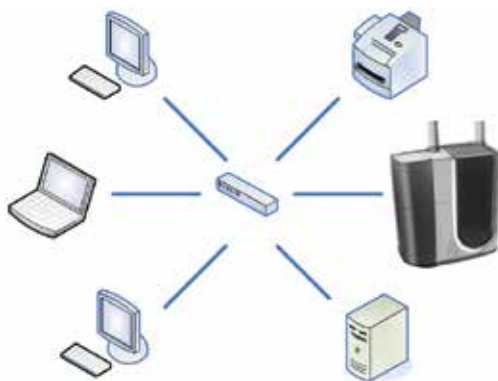
*If all settings are correct, select **Yes** to send the new configuration to the detector. If you would like to make further changes, select **No**.*

Note: To send the configuration to the detector manually, right-click on the device and select **Send Configuration**.



11. After receiving the configuration, the detector will shut down and restart. The detector will then begin operating using the new IP address.

LAN Connection

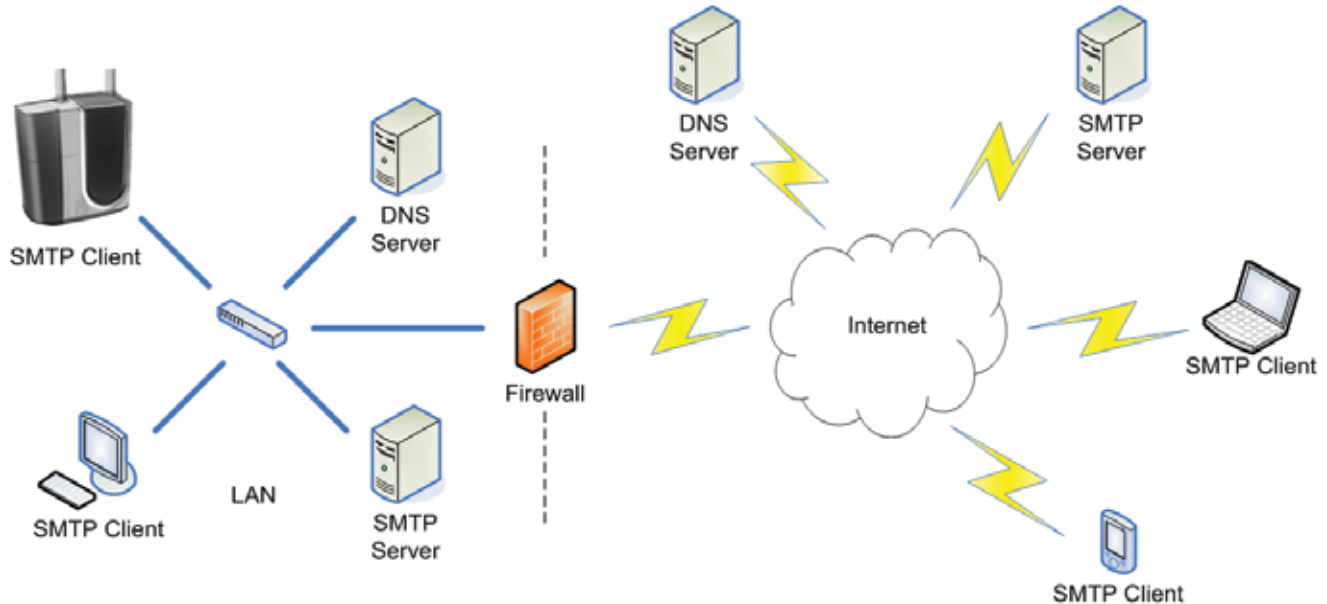


To fully realize the potential of the networking features offered by the FAAST detector, connection to a Local Area Network (LAN) is recommended. When connected to a LAN, other computers can connect to the detector for remote monitoring either using a Web browser or the PipeIQ software. If remote access to a LAN is provided by a Virtual Private Network (VPN), this remote monitoring can take place from virtually anywhere you can access the Internet. If an e-mail server resides in the LAN, FAAST can be configured to forward e-mail notifications via this server.

Connecting the FAAST detector to a LAN requires knowledge of the local network topology, configuration, and security policy. With this information, the appropriate IP and e-mail settings for the FAAST detector can be selected. Because networking environments vary widely, your local IT professional will be in the best position to integrate the detector into existing infrastructure. If you are unsure how to proceed with a permanent network deployment, contact your network administrator for assistance.

Remote Connection (VPN)

In many instances, it is desirable to access private network resources from a remote location. A common example is connecting to a networked file server using a laptop when traveling. Access in this fashion makes a computer in a remote location appear as if it were directly connected to the local network even though it is connected through the public Internet. The infrastructure that makes this possible is called a VPN. A VPN creates a “tunnel” between the remote machine and the local network that is secured from eavesdropping.



Because the FAAST detector can operate just like another peer on a LAN, it can also be accessed by a remote machine connected via a VPN tunnel. Additional VPN hardware and software infrastructure is required. Contact your local IT administrator for information on how to access your local network resources including the FAAST detector remotely.

Notes on Operation

Initialization Time

When configured for DHCP, the FAAST detector may require up to 5 minutes to register with DNS after power-up. The detector will not be reachable via its hostname during this time.

Troubleshooting

Because IP connectivity is required for any of the other network services on the FAAST detector to operate properly, it is imperative that TCP/IP functionality be verified prior to attempting to use the other functions. See the section titled **Testing Connectivity** for instructions on verifying the IP connection.

Note: For more help with troubleshooting TCP/IP, visit the Microsoft Support site: <http://support.microsoft.com/kb/314067>

FAQ: TCP/IP Connectivity

What IP address does the FAAST detector use by default?

The default IP address is 192.168.1.10. The default subnet mask is 255.255.255.0.

I'm directly plugged into the detector but I am not able to connect to it. What should I do?

Verify you have correctly configured the network adapter for your PC. Then test for IP connectivity using the ping command. In some cases, even when the IP address of the PC is set correctly a reboot of the PC is required for it to take effect.

What IP address should I assign the detector?

Networking environments vary. Contact your network administrator for the IP address you should use.

How can I determine the current IP address a particular FAAST detector is using?

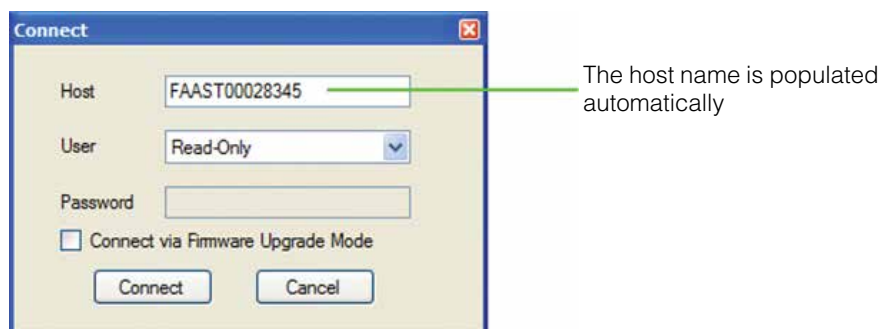
The FAAST detector has an "IP Address Blink Mode," which can be used to display the current IP address. To initiate the blink mode, press and hold the **Reset** button for 20 seconds, until the **high flow** indicator illuminates yellow. For more information, see the product manual.

I do not have VPN infrastructure on my network. Can I just attach FAAST to the Internet?

While it is theoretically possible to connect a detector directly to the Internet, this approach is not recommended and may not be supported by your ISP. Always control public access to the FAAST detector via firewalls.

How do I determine the hostname of the FAAST detector? Is it configurable?

First, configure the detector for DHCP addressing. After sending the configuration to the device, attempt to connect to it using the **Connect Device** command. The PipelQ software will automatically populate the **Host** field of the **Connect** window with the hostname of the detector. The hostname is not configurable.



PC Configuration and Monitoring

The FAAST aspiration smoke detector is configured using the PipeIQ software program and the network interface. The PipeIQ software also provides tools for remotely monitoring the detector and reading historical event logs.

User Levels

The FAAST detector provides two different levels of remote access via the PipeIQ software. The access level is selected when connecting to a device.

Administrator

The Administrator user level provides access to all remote monitoring and configuration functions. Administrative access is required to change the configuration of a FAAST detector or initiate a Test, Reset or Isolate the unit remotely. A password is required for Administrative access.

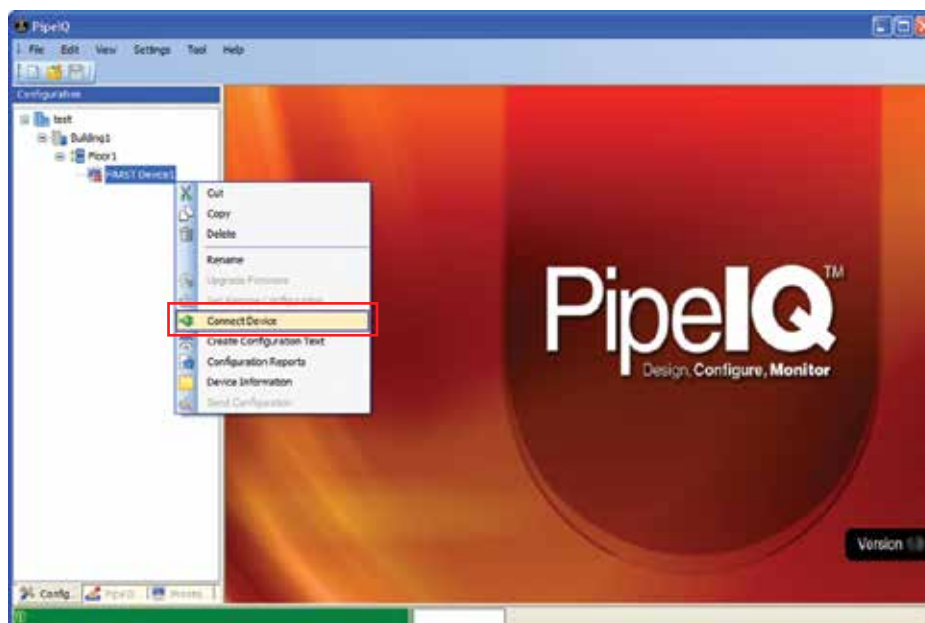
Read-Only

The Read-Only user level provides access to the detector's remote monitoring features. Read-Only users may also view configuration data. Read-Only users cannot change a detector's configuration or issue a remote Test, Reset or Isolate. No password is required for Read-Only access.

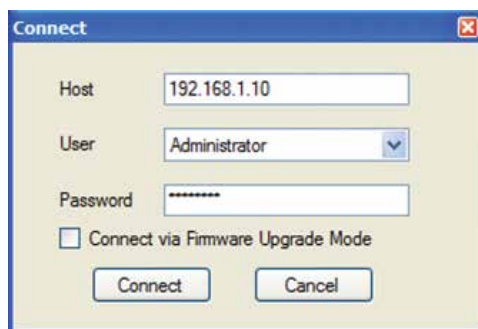
Connection

To connect to the FAAST detector using the PipeIQ software, follow these steps:

1. Start the PipeIQ software application.
2. If you have previously created a project, open it using **File -> Open**. Or create a new project using **File -> New**.
3. Connect to the detector by right-clicking it and selecting **Connect Device**.



4. In the Connect window, ensure the correct IP address or hostname for the detector is entered in the **Host** field. Select the desired user level. If required, enter the password for the detector in the **Password** field. The default Administrator password is "password". Click **Connect**.



Connection Status

The connection status of a FAAST detector can be determined by its icon.



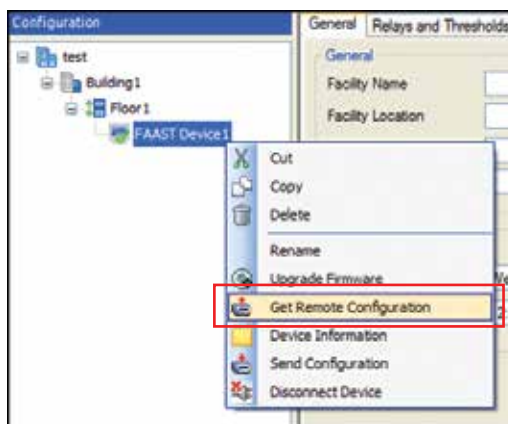
Configuration

The FAAST detector has a number of configurable parameters that can be used to control its behavior. Parameters include the smoke thresholds at which the unit will enter alarm, the latching behavior of the relay outputs, networking and e-mail settings, and more. These parameters are stored in the device when it is configured. The PipelQ software provides a means of retrieving, editing, saving, and sending configuration data.

Retrieval



The current configuration data in a FAAST detector can be retrieved and copied into a device profile using the PipelQ software. This is accomplished by right-clicking on the detector and selecting the **Get Remote Configuration** command.

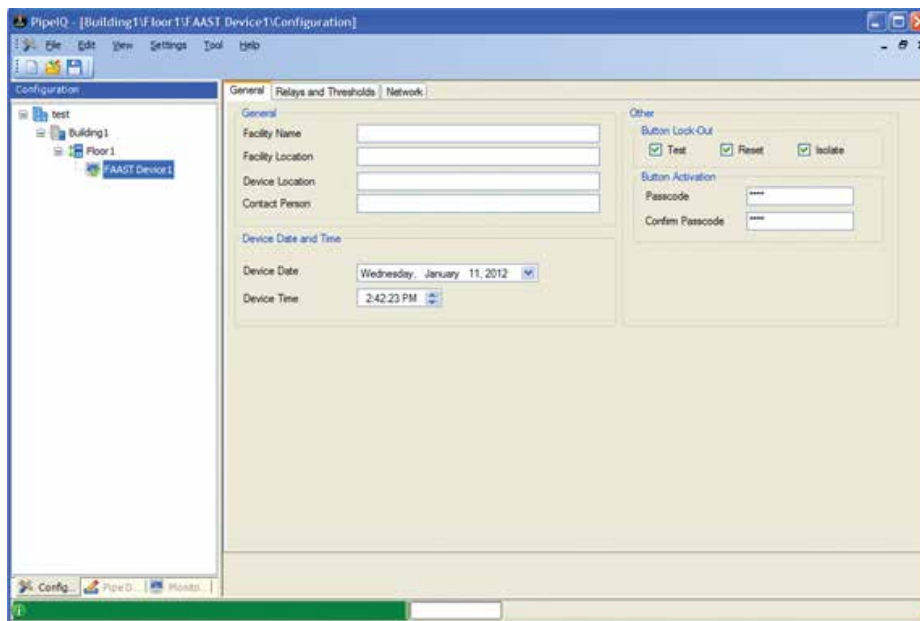


The PipelQ software will confirm the retrieval was successful with the following message.



Editing and Saving

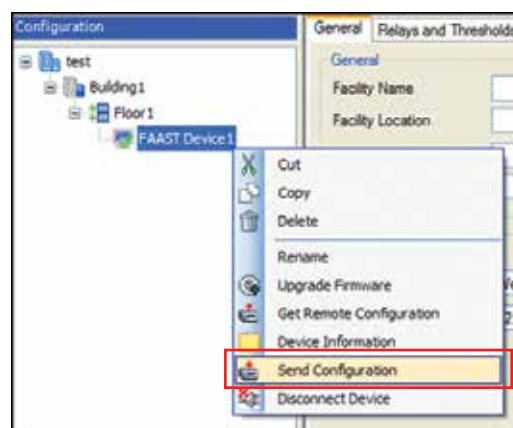
Once a configuration has been created or retrieved, the software can be used to edit the configuration parameters of the detector. Parameters are divided into three categories: **General**, **Relays and Thresholds**, and **Network**. When all the detector parameters have been set, the configuration can be saved to the project file using the **File -> Save** command.



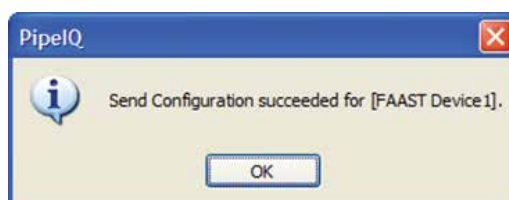
Changing Detector Configuration



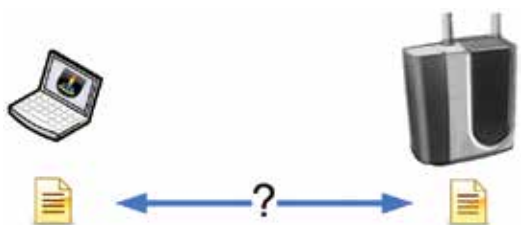
When the configuration has been edited to the desired state, it can then be sent to the detector using the **Send Configuration** command.



The PipeIQ software will confirm the configuration change with the following message and the detector will shut down and restart.



Synchronization



Because the detector and the PipelQ project file each maintain a copy of the detector configuration, it is possible that they may not always be in sync with one another. Such a situation could occur if different PCs are used to configure a detector or the original project file is lost.

The PipelQ software will detect when the configuration on the detector does not match the configuration stored in the project file. The software will then prompt you to correct the situation with one of the following messages:

Upon connection, the configuration in the detector does not match the configuration in the PipelQ project file. Choose **Yes** to overwrite the current device configuration in the PipelQ project file. Choose **No** to leave the current PipelQ configuration unchanged.



While connected to the detector, the PipelQ configuration file was saved with changes. Choose **Yes** to send the new configuration to the detector. Choose **No** to keep the existing configuration in the detector.



Monitoring

The PipelQ software includes capabilities for remotely monitoring a FAAST detector connected to an IP network. The monitoring features include a virtual view of the detector's front panel, a real-time particulate trend graph, and a real-time event viewer. In addition, the historical particulate trend and event log can be retrieved for analysis.

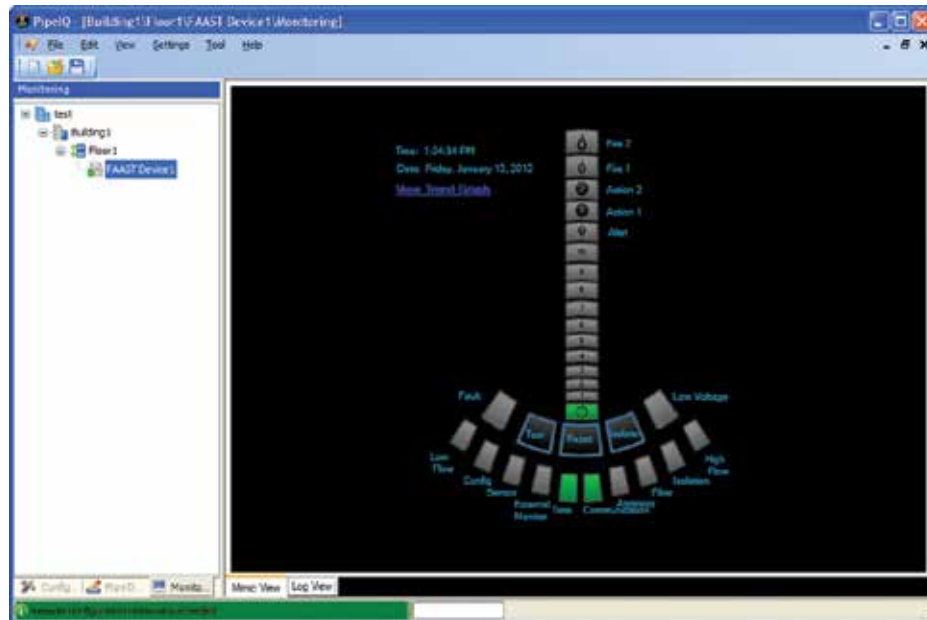
Live View

The Live or Mimic View shows a graphical representation of the detector's front panel. Users are able to see the current particulate, air flow and alarm levels as well as any faults. When logged in as an Administrator, the **Test**, **Reset**, and **Isolate** buttons can be used to initiate those functions.

To begin a Live View monitoring session:

1. Connect to a detector. For instructions, see **Connection** earlier in this guide.
2. Switch to the Monitoring function by either selecting **View -> Monitoring** from the menu bar or clicking the **Monitoring** tab in the lower left corner of the screen.

- Double-click on the detector icon to open the Mimic View. A graphical representation of the front panel will appear. For detailed information on the front panel, see the product manual.

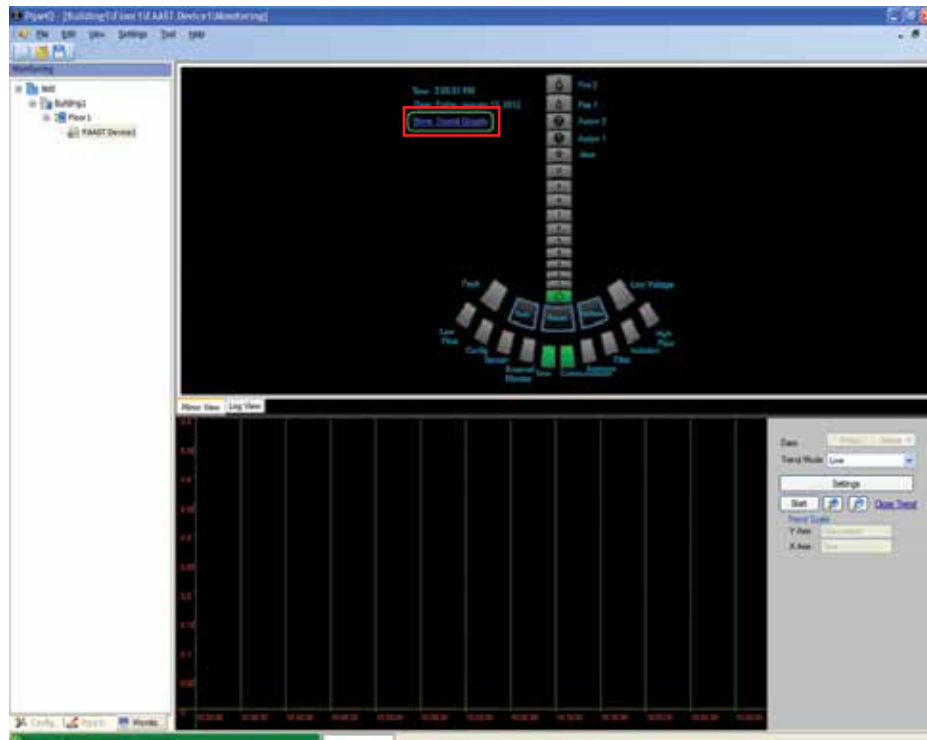


- Within 15 seconds, the indicators will illuminate, showing the current status. From then on, the display will continue to update every 15 seconds.

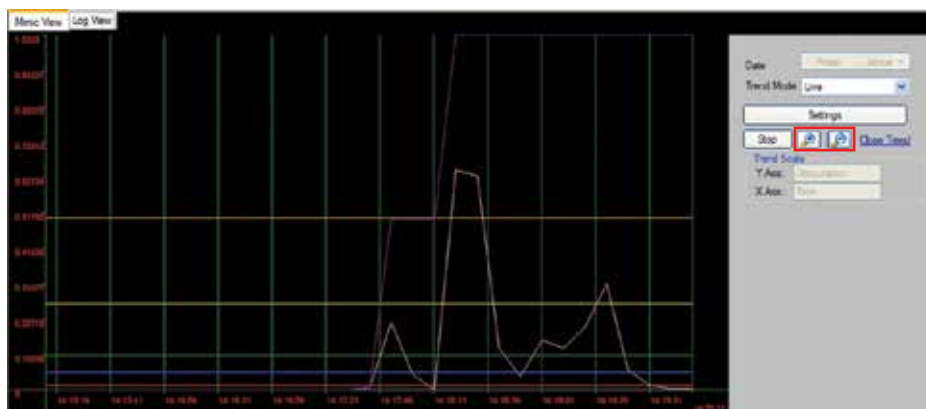
Live Trend Graph

The PipelQ trend graph plots a reading of the particulate level in real-time. To begin a live trend graph monitoring session:

- Connect to the detector and switch to the Monitoring View. For instructions, see the previous section.
- From the Mimic View, click the blue **View Trend Graph** text to open the trend graph. The trend graph opens below the Mimic View.

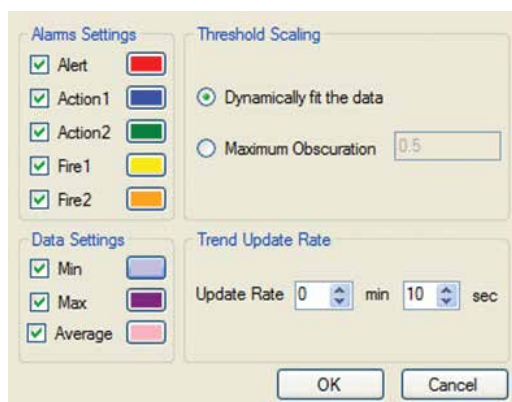


- Click **Start** to begin plotting the particulate level. Click the button several times to zoom in. Click the button to zoom out.
- As time passes, the average particulate level, the maximum and minimum particulate level, and the alarm thresholds will be plotted on the graph. The average signal is pink and the maximum is purple.



Note: The trend graph control can be resized by moving the cursor to the black-gray border just above the **Date** menu. When the cursor changes, click to drag and resize.

- The signals that are displayed and the update rate may be customized via the **Settings** button. The minimum update rate is 5 seconds.



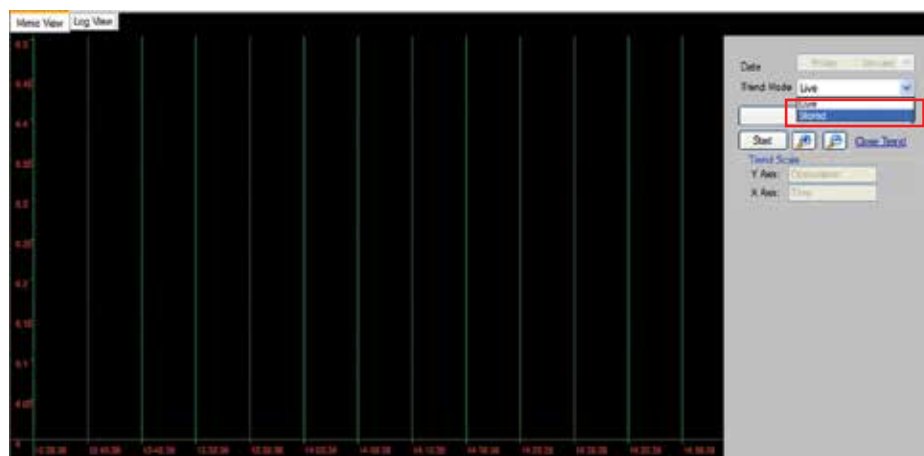
The Threshold Scaling group can be used to modify the behavior of the Y axis. The Dynamically fit the data option will automatically increase the range of the Y axis when the particulate level increases. When the Maximum Obscuration option is selected, the range of the Y axis will remain fixed.

Historical Trend Graph

The FAAST detector records the daily minimum, average, and maximum particulate level for the last year of operation. This information can be retrieved and plotted on a graph using the Stored Trend Mode. To retrieve the stored particulate data, follow these steps:

- Connect to the detector and switch to the Monitoring View. For instructions, see the previous section.
- From the Mimic View, click the blue **View Trend Graph** text to open the trend graph. The trend graph opens below the Mimic View.

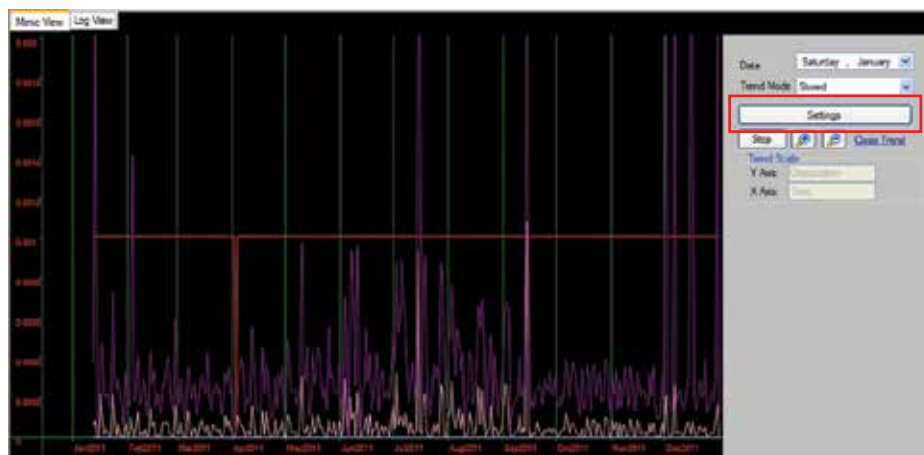
- From the Trend Mode menu, select the **Stored** option.



- Click **Start** to begin retrieval of the historical trend data. Retrieval may take several seconds. The status will be shown in the progress bar at the bottom of the window.



- Once the historical data has been retrieved, use the **Date** control to select the date where data viewing will begin. Use the and buttons to zoom to the desired time resolution. The resolution on the Y axis can be adjusted by clicking **Settings** and setting the **Maximum Obscuration**.



Note: The trend graph control can be resized by moving the cursor to the black-gray border just above the **Date** menu. When the cursor changes, click to drag and resize.

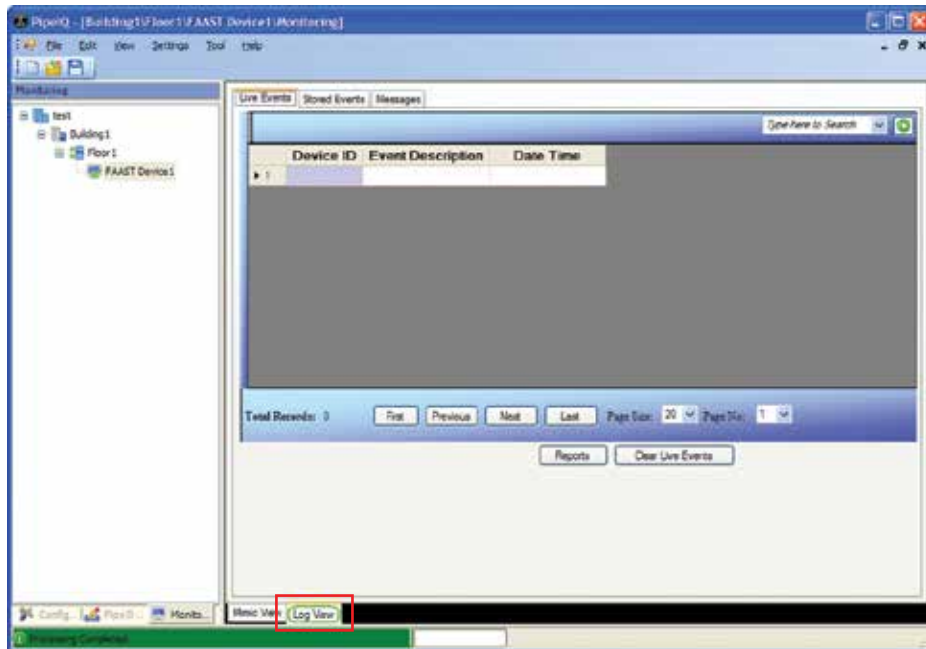
Log View

The Log View provides a way to remotely view detector events as they occur as well as retrieve the event log that is stored on the detector. It also provides the facility to create and view short text messages that may be stored on the detector. These messages may be useful for documenting maintenance or configuration changes.

To use the Log View, follow these steps:

- Connect to the detector and switch to the Monitoring View. For instructions, see the previous section.

- From the Mimic View, click the **Log View** tab at the bottom of the window. The Live Events viewer appears.



Live Events

As the FAAST detector operates, different events may occur. Examples of events include faults and alarms as well as configuration changes and power outages. Using the PipelQ software, a user can monitor a device and see when these events occur. To watch for events, click the **Live Events** tab.

Stored Events

Each time an event occurs, the FAAST detector logs the occurrence in its non-volatile memory. Up to 18,000 events may be stored. To view or clear this record, click the **Stored Events** tab. Depending on the number of events, retrieval may take several seconds. The status of the event retrieval is shown in the progress bar at the bottom of the window.

Messages

During the life of the detector, it may be advantageous to keep a record of maintenance activities or configuration changes. Using the message log, this record can be maintained in the detector itself. To view or create stored text messages, click the **Messages** tab.

FAQ: PC Configuration and Monitoring

I am unable to connect to the FAAST detector with the PipelQ software. What should I do?

Verify your networking adapter is properly configured and you have IP connectivity to the detector. See **Testing Connectivity** for more details.

What is the default Administrator password?

The default Administrator password is "password". After logging in, it may be changed via the **Administrator Password** field on the **Network** tab. See **Configuration** for instructions on changing the detector configuration.

I lost the Administrator password. How do I log in to the detector again?

Contact System Sensor Customer Service for assistance. You will need to provide your contact information and the recovery code you receive when attempting to log in to the detector. See the **Appendix** for contact information.

How many PCs can I connect to a FAAST detector at a time?

One PipelQ client may connect to a given FAAST detector at a time.

What are the General text fields such as Facility Name used for? What characters can I use?

The text fields appear on the Web server and e-mail messages and assist in identifying the detector. The fields accommodate up to 32 alphanumeric characters. The **Contact Person** field supports additional symbols.

Web Server

The FAAST detector comes equipped with an integral Web server, enabling remote access using a Web browser. Features include:

- Configuration viewer
- Live view of front panel
- Log viewer
- Access control via configurable password

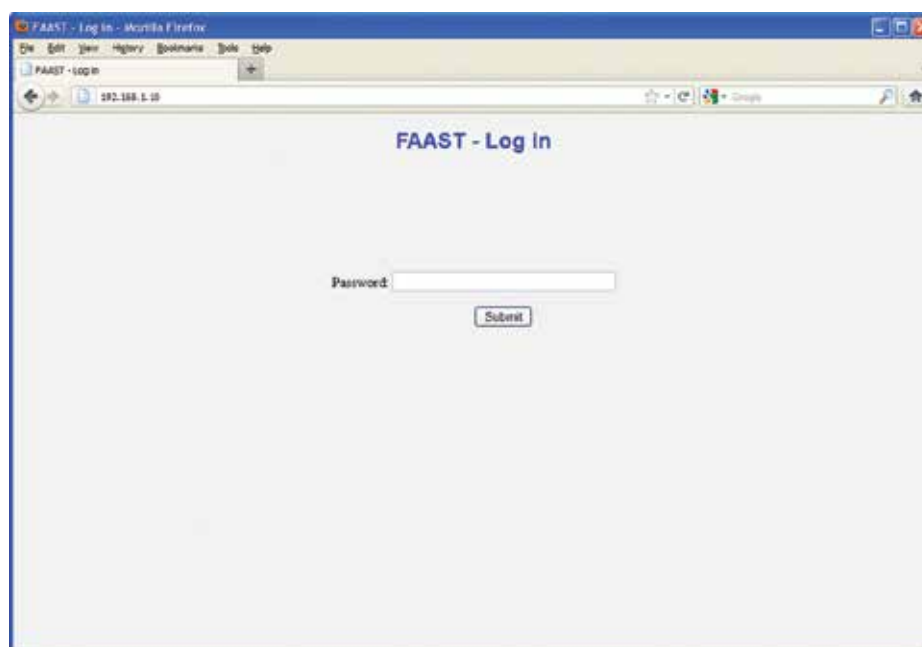
Requirements

- Internet Explorer® 6 or later –or– Mozilla Firefox® 3.6 or later
- TCP port 80 must be open

Connection

To connect to the Web server, follow these steps.

1. Open the Web browser.
2. In the address bar, type the IP address of the FAAST detector you are trying to access. If the detector is configured to obtain an IP address via DHCP, you may enter the hostname.
3. The login page will appear. If you are unable to access the login page, verify IP connectivity using the ping utility as described in *Testing Connectivity*.



4. Type in the password and press **Submit**. The default password is “1234” and may be configured using the PipelQ software. For details, see **Configuration**.

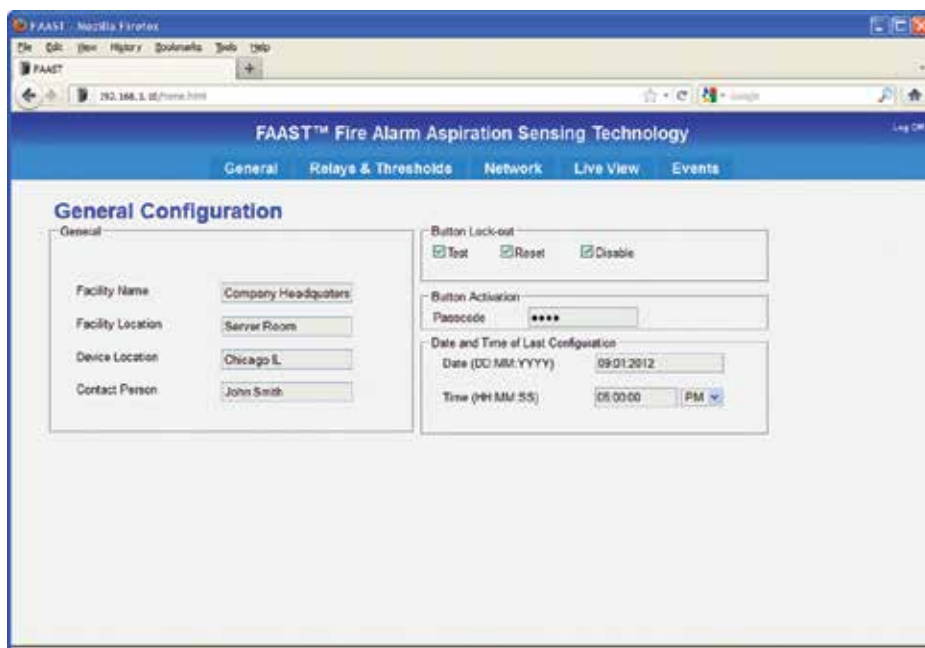


5. Upon successful login, the General Configuration is displayed.

Configuration Viewer

The integral Web server enables remote viewing of all the configurable parameters of the FAAST detector. Parameters are arranged exactly how they appear in the PipelQ software and are accessible from the menu bar at the top of the page. The Web server provides read-only access to configuration data. To change the configuration, the PipelQ software is required.

General Configuration



Relays and Thresholds Configuration

The screenshot shows the 'Network Configuration' page of the FAAST web interface. The page has a blue header with the title 'FAAST™ Fire Alarm Aspiration Sensing Technology' and a 'Log Out' link. Below the header is a navigation bar with tabs: 'General', 'Relays & Thresholds', 'Network', 'Live View', and 'Events'. The 'Network' tab is currently selected.

The main content area is titled 'Network Configuration' and contains several sections:

- Device Details:** Includes fields for 'Serial Number' (00-26-c8-00-00-01) and 'Identification Number' (1).
- Device Mail Server Configuration:** Includes fields for 'Sender Account' and 'SMTP Server Name'.
- Device Connection:** Includes radio buttons for 'DHCP Enabled' and 'Static Ip Enabled' (which is selected). Below this are fields for 'IP Address' (192.168.1.10), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (192.168.1.1), 'Primary DNS Server' (0.0.0.0), and 'Secondary DNS Server' (0.0.0.0).
- E-mail Notification:** A table with columns for 'Email', 'Alert', 'Action 1', 'Action 2', 'Fire 1', 'Fire 2', 'Minor', 'Urgent', and 'Isolate'. There are six rows for 'Email 1' through 'Email 6', each with checkboxes in the subsequent columns.

Network Configuration

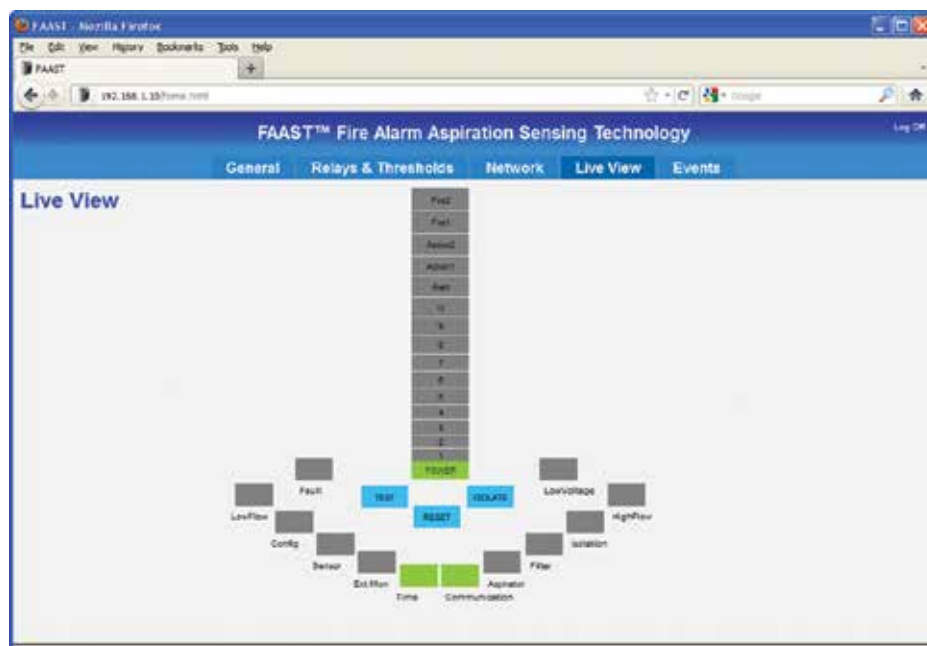
The screenshot shows the 'Relays and Thresholds Configuration' page of the FAAST web interface. The page has the same blue header and navigation bar as the previous screenshot, with the 'Relays & Thresholds' tab selected.

The main content area is titled 'Relays and Thresholds Configuration' and contains several sections:

- Alarm/Fault Relay Latching:** Includes checkboxes for 'Alert', 'Action 1', 'Action 2', 'Fire 1', 'Fire 2', and 'Minor'.
- Accumulate Mode:** Includes radio buttons for 'Enable' and 'Disable' (which is selected).
- Night Mode:** Includes fields for 'Start Time (HH:MM:SS)' (01:16:10) and 'End Time (HH:MM:SS)' (01:16:10), along with dropdown menus for 'PM' and 'PM'.
- Alarm Thresholds and Delays:** A table with columns for 'Day', 'Night', 'Weekend', 'Min', and 'Max'. Below this are fields for 'Alert', 'Action 1', 'Action 2', 'Fire 1', and 'Fire 2'. To the right of the table is a column for 'Delay (sec)' with input fields for each row.

Live View

The Web server Live View provides a graphical depiction of the front panel of the detector. Users are able to see the current particulate, air flow, and alarm levels as well as any faults.



Note: For a more detailed explanation of the front panel see the product user manual.

Events View

The FAAST detector logs a number of different events, including alarms and faults. This historical record may be helpful when diagnosing system problems or trying to determine when a smoke event occurred.



The arrow buttons at the bottom of the page are used to navigate through the available events.

Navigation Buttons	Function
<<	Go to first page
<	Go back one page
>	Go forward one page
>>	Go to last page

FAQ: Web Server

[What is the Web server password? How do I change it?](#)

The default Web server password is "1234". It may be changed using the **Web Access Password** field in the PipeIQ software.

[I am unable to access the login page using my browser. What should I do?](#)

First, verify connectivity to the detector following the instructions in **Testing Connectivity**. If you are able to ping the detector but still unable to access the login page, make sure that port 80 is not blocked by a firewall in your network environment.

[Is the Web server compatible with the Safari®, Chrome™ or Opera® browsers?](#)

The Web server has been tested with desktop versions of Internet Explorer 6 and 8 and Mozilla Firefox 3.6 and 10. Other browsers may or may not work properly.

[Is the Web server compatible with iOS, Android® or Blackberry® devices?](#)

It is possible to access the Web server using certain mobile devices. If the General Configuration does not appear after logging in, attempt to access the home page directly by typing `http://192.168.1.10/home.html` into the address bar, substituting the detector IP address as appropriate.

[Can I access the Web server remotely using my PC or mobile device?](#)

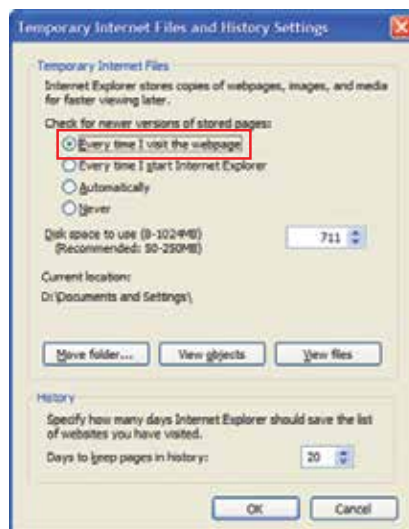
Yes, it is possible to access the FAAST Web server remotely. However, it is dependent on having the properly configured remote access infrastructure in place. Contact your local IT administrator for assistance and see the **Remote Access (VPN)** section for more details.

[How many clients may connect to the Web server at a time?](#)

Up to two clients may connect to the Web server simultaneously.

[The Live View does not appear to be updating when using Internet Explorer. How do I fix it?](#)

Go to **Tools -> Internet Options**. On the **General** tab under **Browsing history**, select **Settings**. Set the **Check for newer versions of stored pages** option to **Every time I visit the Webpage** and click **OK**.



E-mail Client

One of the exciting features offered by the FAAST aspiration smoke detector is the ability to generate e-mail notifications of alarm and fault conditions. With this technology, users may be alerted to changes in the system whenever and wherever they are.

Features

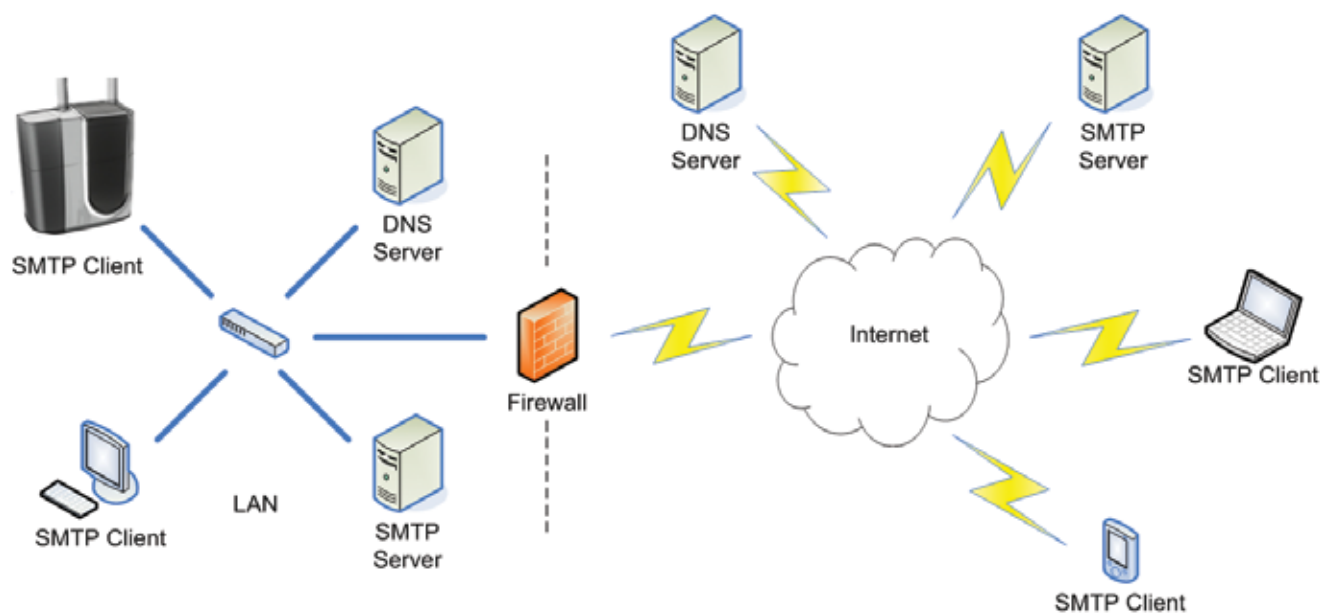
The 8100 series is equipped with an integrated SMTP client capable of forwarding alarm and fault e-mail notifications to a properly configured SMTP mail server. In addition, the detector has DNS name resolution capability for locating a mail server inside a LAN.

Configurable features of the SMTP client include:

- The name of the SMTP server used for relaying messages
- The sender e-mail account used for relaying messages
- Up to 6 unique e-mail recipients
- An independent collection of alarm and fault notifications for each e-mail recipient

The integrated SMTP client is configured using the PipelQ software.

Network Requirements



Before the integrated client can forward messages to the mail server, it must be able to make a connection to it. For this to occur, the following are required:

- The detector must be connected to a TCP/IP network via Ethernet and have a properly assigned IP address. Dynamic IP address assignment via DHCP is supported; however, for permanent installations, static IP addressing is recommended.
- The detector must be configured to forward messages to the machine where the SMTP server resides. The mail server must be specified by its hostname. Specifying the IP address of the mail server directly is not supported. If the mail server and detector are not part of the same domain, the FQDN (fully qualified domain name) should be specified.
- In order for the FAAST detector to connect to the mail server, it must be able to resolve the hostname. This is accomplished using DNS. For proper operation, the Primary and/or Secondary DNS servers the device will use for name resolution must be configured. The device will query these servers when attempting to resolve the name of the mail server. The DNS servers must be capable of resolving the name of the mail server or petitioning other DNS servers that can.

Server Requirements

The mail server will accept messages from the FAAST detector and attempt to relay them to the specified recipients. This server must meet the following requirements:

- Accept and deliver messages from the e-mail address specified in the **Sender Account** field.
- Accept and relay SMTP messages from port 25 without requiring authentication.
- Have connectivity and DNS service to networks (such as the Internet) where recipient mail servers reside.

E-mail Client Requirements

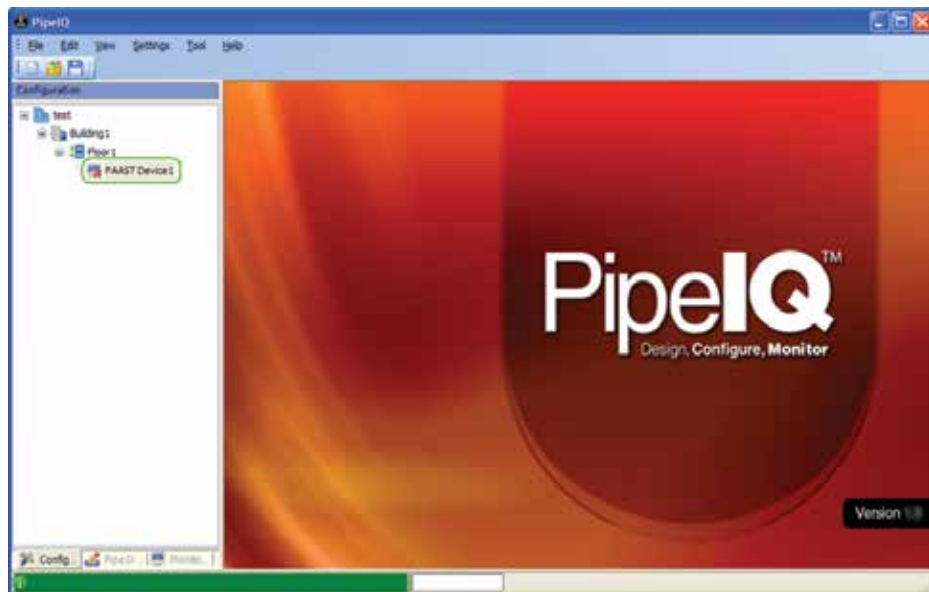
Once connectivity to the mail server is established, the integrated SMTP client will communicate with the server to deliver alarm and fault e-mail notifications. For the client to work properly, the following are required:

- The **Sender Account** field is used to populate the SMTP "**From**" field and specifies where an e-mail message originates. This field should be populated with an e-mail address specifically reserved for the detector. An e-mail account may need to be created and added to the mail server by the server administrator.
- Up to 6 recipient e-mail addresses and desired notifications must be configured.

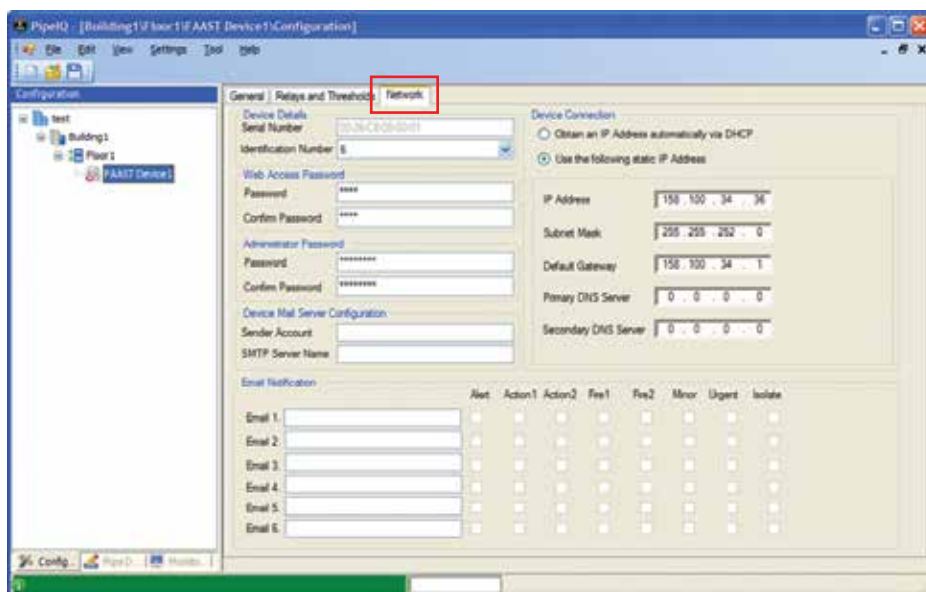
E-mail Client Configuration

The integral SMTP client is configured using the PipeIQ software. Before attempting to configure the e-mail client, the IP configuration of the detector should be completed and network connectivity verified. For instructions, see the **TCP/IP Connectivity** section earlier in this guide.

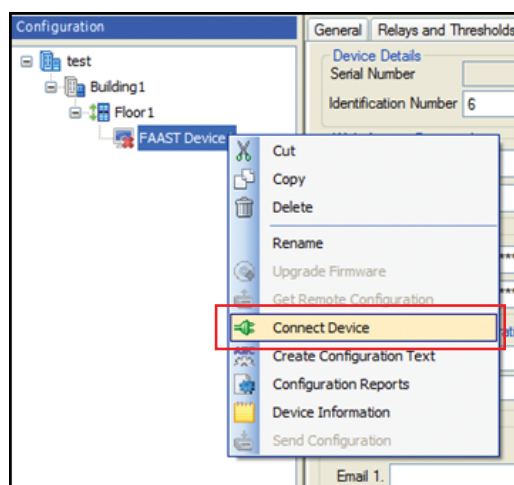
1. Start the PipeIQ software application.
2. Open the project for it using **File -> Open**.
3. Double-click the desired device to open the Configuration window.



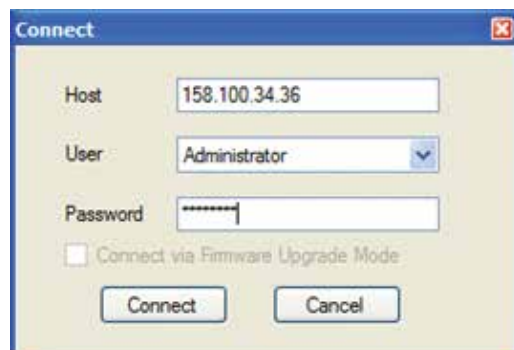
4. Click the **Network** tab to display the network parameters.



5. Connect to the detector by right-clicking and select **Connect Device**.



6. In the **Connect** window, ensure the correct IP address for the detector is entered in the **Host** field. Change the User from **Read-Only** to **Administrator**. Finally, enter the password for the detector in the **Password** field. The default password is "password". Click **Connect**.



7. The e-mail client uses name resolution technology to connect to the mail server. For DNS to work properly, the client must be made aware of a DNS server. Examine the IP settings for the detector using the **Device Connection** group. If the detector is configured to obtain an IP address automatically, it will also receive the addresses of a DNS server to use. If configured with a static address, be sure to populate the **Primary** and **Secondary DNS Server** fields.

Static IP

Dynamic IP

Note: If you are unsure what DNS servers to use, contact your local IT administrator for assistance.

8. Locate the **Device Mail Server Configuration** group and enter the **Sender Account** and **SMTP Server Name**.

Field	Description
Sender Account	The e-mail address the device will use to populate the From field of outgoing e-mail messages.
SMTP Server Name	The name of the machine where the SMTP server is running.


Note: The mail server administrator may need to configure the server to accept messages from the specified sender account. If you are unsure what e-mail address to use for the sender account, contact your server administrator for assistance.

Note: The **SMTP Server Name** field must be populated with a name, not an IP address. The machine name must be resolvable using the DNS servers specified in the previous step.

9. Locate the **Email Notification** group and enter the e-mail addresses of the recipients wishing to receive notification. Check the boxes corresponding to the notifications each recipient should receive.

	Alert	Action1	Action2	Fire1	Fire2	Minor	Urgent	Isolate
Email 1. t.worker@mydomain.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Email 2. t.admin@mydomain.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Email 3. security@mydomain.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Email 4. building.eng@mydomain.com	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Email 5.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Email 6.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Field	Description
Email	The e-mail address of the recipient to receive notification
Alert	E-mail generated when the device has reached the specified alarm level
Action 1	
Action 2	
Fire 1	
Fire 2	
Minor	E-mail generated when the device detects a Minor Fault
Urgent	E-mail generated when the device detects an Urgent Fault
Isolate	E-mail generated when the device has been placed into <i>Isolate Mode</i>

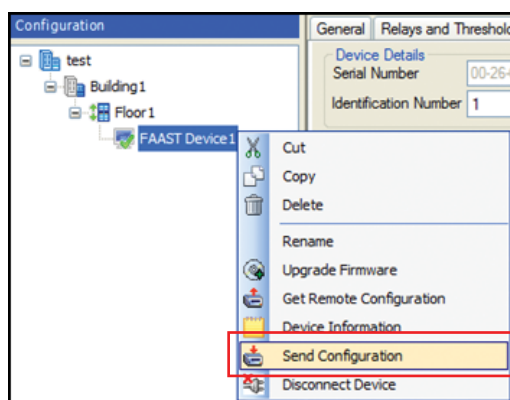
10. When the desired e-mail settings have been entered, click the **Save**  icon

11. The following message will appear



If all settings are correct, select **Yes** to send the new configuration to the detector. If you would like to make changes, select **No**.

Note: To send the configuration to the detector manually, right-click on the device and select **Send Configuration**.



12. After receiving the configuration, the detector will shut down and restart. The detector will then begin operating using the new e-mail settings.

Note: The e-mail client requires 5 minutes from power-on to initialize. No e-mails will be sent during this period.

Testing and Verification

Before attempting to send e-mails using the FAAST detector, it is recommended that the mail server configuration be tested using a simple PC-based SMTP client. This may aid in troubleshooting any server configuration problems prior to deploying the detector.

Bmail from BeyondLogic is one of many free tools that can be used to test the mail server. See below for an example.

```

C:\WINDOWS\system32\cmd.exe
G:\>bmail
Command Line SMTP EMailer V1.07
Copyright(C) 2002-2004 Craig.Peacock@beyondlogic.org
Date: Fri, 13 Jan 2012 16:52:10 -0600
Usage: bmail [options]
    -s SMTP Server Name
    -p SMTP Port Number (optional, defaults to 25)
    -t To: Address
    -f From: Address
    -b Text Body of Message (optional)
    -h Generate Headers
    -a Subject (optional)
    -n Filename (optional) Use file as Body of Message
    -c Prefix above file with CR/LF to separate body from header
    -d Debug (Show all mail server communications)

G:\>bmail -s smtp.mydomain.com -f faast@mydomain.com -t it.worker@mydomain.com
Command Line SMTP EMailer V1.07
Copyright(C) 2002-2004 Craig.Peacock@beyondlogic.org
Opening connection to smtp.mydomain.com [216.34.94.184] on port 25
  
```

Parameter	Description	PipeIQ field	Example Value
s	SMTP Server Name	SMTP Server Name	smtp.mydomain.com
f	From: Address	Sender Account	faast@mydomain.com
t	To: Address	E-mail 1	it.worker@mydomain.com

If mail delivery fails using a PC SMTP client, the FAAST SMTP client will likely also fail. In the event that you are unable to deliver mail in this fashion, the bmail debug output switch (-d) may help identify the source of the problem. If even more troubleshooting is necessary, network capture tools such as Microsoft Network Monitor or Wireshark can be used. If required, your local IT administrator will be in the best position to help troubleshoot these types of problems.

Note: System Sensor cannot make any warranty regarding these third-party tools nor provide support pertaining to their use. USE AT YOUR OWN RISK.

Notes on Operation

Initialization Time

The FAAST e-mail client requires 5 minutes to initialize after power-up and will not attempt to send any notifications during this time.

FAQ: E-mail Client

What value do I put in the *SMTP Server Name* field?

This is the hostname or FQDN of the SMTP mail server (i.e., smtp.domain.com). Contact your network or server administrator for the correct name.

Does the FAAST SMTP client support authentication or TLS/SSL connections?

The FAAST SMTP client is able to identify itself to the server via the **Sender Account** (MAIL FROM:) field. However, the client has no method of providing authentication via password and does not support TLS or SSL connections.

Is the SMTP client compatible with Web-based e-mail services like Gmail or Hotmail?

These services normally require authentication and secure connections when sending messages to prevent spam. It is possible to use these services as the sender account, but only if a locally deployed e-mail server not requiring authentication or secure connections is used as an intermediary.

When properly configured to use an SMTP mail server for message forwarding, the client will be able to send e-mails to any e-mail address, including Gmail and Hotmail accounts.

I'm not able to receive any e-mails. Who do I contact for help?

Because network and server configurations vary widely, the local network or server administrator will be in the best position to help troubleshoot any integration issues you may encounter. For questions specific to the operation of the SMTP client, please contact System Sensor.

I received an e-mail notification but I am unable to connect to the Web server using the embedded hyperlink. Why?

The embedded hyperlink will only work if you are able to connect to the detector from your computer or mobile device. A VPN may be required. See **Remote Connection** for more information.

How reliable is e-mail as a means of alarm notification?

While every effort has been made to ensure that the FAAST SMTP client operates reliably, it is still subject to the drawbacks inherent in IP and SMTP technology. There are many computers and networks that must work in concert to deliver an e-mail message, and its timely receipt cannot be guaranteed. Therefore, e-mail is provided as a supplemental rather than primary means of alarm notification. As always, follow local codes and Authority Having Jurisdiction (AHJ) requirements when deploying a system.

Appendix

Glossary

Authentication	A process to confirm the identity of an individual, often using a password
DHCP	Dynamic Host Configuration Protocol - A network protocol for automatically assigning IP addresses to host devices
DNS	Domain Name System - A hierarchal system of naming networks and devices on the Internet
Domain	A name that uniquely identifies a network and a sphere of administrative authority
Ethernet	A collection of wired local area network technologies
FAAST	Fire Alarm Aspiration Sensing Technology
FQDN	Fully Qualified Domain Name - The concatenation of a hostname and domain name with a period such as: hostname.domain.com
Hostname	A human-readable label assigned to a device on a network and mapped to an IP address
IT	Information Technology
IP Address	A 32-bit number assigned to each device in an IP network – usually represented as four decimal numbers such as: 192.168.1.10
LAN	Local Area Network
MAC Address	Media Access Control Address - A unique address assigned to every Ethernet interface by the device manufacturer.
NetBIOS	An alternative name resolution system found on Microsoft Windows networks
PipeIQ	A desktop software application for managing aspiration smoke detectors
SMTP	Simple Mail Transfer Protocol - A protocol used by clients and servers to transmit e-mail messages
SMTP Client	A device that connects to a mail server in order to send e-mail messages
SMTP Server	A computer that accepts incoming e-mail messages from clients and delivers them to other e-mail servers or e-mail recipients
TCP/IP	Transport Control Protocol / Internet Protocol - A common suite of addressing and routing protocols used on the Internet
TLS/SSL	Transport Layer Security/Secure Sockets Layer - Protocols that use encryption to provide secure communications over the Internet

Specifications

Ethernet		Comments
802.3 Compliant	Yes	
Speed	10/100 Mbit	
Auto MDI-X	Yes	Crossover cable not required
OUI	00-26-c8	MAC addresses: 00-26-c8-xx-xx-xx
TCP/IP		
Version	IPv4	
DHCP	Optional	
DHCP Retry Period	5 x 50 seconds	
DNS Name Resolution	Yes	
NetBIOS Name Resolution	Yes	When receiving its IP address via DHCP, the detector will register its name with a NetBIOS network and be accessible by its hostname.
Automatic Private IP Addressing	Yes	
IP Address (default)	192.168.1.10	
Subnet Mask (default)	255.255.255.0	
PC (PipeIQ) Server		
TCP Port	1937	
Password Protected	Yes	Administrator password required to change configuration; not required for monitoring
Administrator Password (default)	password	
Configuration Changes	Yes	
Live View Refresh Period	15 seconds	
Minimum Trend Graph Update Period	5 seconds	
Maximum Simultaneous Connections	1	
Web Server		
TCP port	80	
Password Protected	Yes	Web-Access password required for monitoring
Web Access Password (default)	1234	
Configuration Changes	No	
Automatic Logoff Period	60 minutes	
Live View Refresh Period	10 seconds	
Maximum Simultaneous Connections	2	
SMTP E-mail Client		
TCP port	25	
Initialization Time	5 minutes	
SSL/TLS	No	
Password Authentication	No	
Maximum SMTP Server Name Length	48 characters	
Maximum E-mail Address Length	48 characters	

Technical Support

System Sensor strives to provide our customers with outstanding support for the FAAST Fire Alarm Aspiration Sensing Technology® and all our products. For more information, contact us using one of the methods below:

Web:	E-mail:	Phone:
systemsensor.com/faast	systemsensor.com/contact	800.736.7672 (press 2) Mon-Fri, 7:30 a.m. – 5:00 p.m. CST

