



FEDERAL SIGNAL
Safety and Security Systems

PAGASYS® GEN II Network Solution

Description, Installation, and User Manual

Limited Warranty

This product is subject to and covered by a limited warranty, a copy of which can be found at www.fedsig.com/SSG-Warranty. A copy of this limited warranty can also be obtained by written request to Federal Signal Corporation, 2645 Federal Signal Drive, University Park, IL 60484, email to info@fedsig.com or call +1 708-534-3400.

This limited warranty is in lieu of all other warranties, express or implied, contractual or statutory, including, but not limited to the warranty of merchantability, warranty of fitness for a particular purpose and any warranty against failure of its essential purpose.



FEDERAL SIGNAL
Safety and Security Systems

2645 Federal Signal Drive
University Park, Illinois 60484

www.fedsig.com

Technical Support 800-524-3021

All product names or trademarks are properties of their respective owners.

Contents

1.0 Safety Messages	5
1.1 Safety Messages to Installers.....	5
2.0 General Description	8
2.1 Introduction.....	8
2.2 Overview.....	8
3.0 Using the PAGASYS Status Concentrator	13
3.1 Introduction.....	13
3.2 NetConfig Import	14
3.3 NetConfig Export	14
3.4 NetConfig Editor	15
3.4.1 NetConfig Editor > Nodes.....	16
3.4.2 NetConfig Editor > NetZones.....	18
3.4.3 NetConfig Editor > NetCasts	20
3.4.4 NetConfig Editor > NetAlarms	23
4.0 Using the Global Access Panel (GAP)	25
4.1 GAP Kiosk Window	27
4.1.1 Rack Status	27
4.1.2 Zone Select Status	28
4.1.3 Zone Status	28
4.1.4 System Status	29
4.1.5 Actions	30
4.2 Initiate Action from Kiosk Window	31
4.3 GAP Installation and Configuration	31
5.0 Network Models and Configuration	32
6.0 Upgrading to a Networked Solution	32
6.1 Updating the Hardware	32
6.2 Configuring the Software	33
7.0 Getting Service	34

Tables

Table 1 NetZone Example	11
Table 2 Zone Select Status	28
Table 3 Zone Status.....	28
Table 4 Faults.....	30

Figures

Figure 1 PAGASYS GEN II Network Topology	9
Figure 2 NetConfig Context Diagram.....	10
Figure 3 PAGASYS GEN II GAP Operations.....	25
Figure 4 PAGASYS GEN II Dante® Digital Audio Sharing	26
Figure 5 System Controller PCB that is Network Enabled (P-NET-G-IP).....	32

1.0 Safety Messages

WARNING

It is important to follow all instructions shipped with this product. This device is to be installed by trained personnel who are thoroughly familiar with the country electric codes and will follow these guidelines as well as local codes and ordinances, including any state or local noise control ordinances.

Planning

- If suitable warning equipment is not selected, the installation site for the system is not selected properly or the system is not installed properly, it may not produce the intended optimum audible warning. Follow Federal Emergency Management Agency (FEMA) recommendations.
- If the system is not activated in a timely manner when an emergency condition exists, it cannot provide the intended audible warning. It is imperative that knowledgeable people, who are provided with the necessary information, be available at all times to authorize activation.
- The sound output of the system is capable of causing permanent hearing damage. To prevent excessive exposure, carefully plan placement, post warnings, and restrict access to areas near loudspeakers. Review and comply with any local or state noise control ordinances as well as OSHA noise exposure regulations and guidelines.
- Activating the system may not result in people taking the desired actions if those to be warned are not properly trained about the meaning of warning sounds. Users should follow FEMA recommendations and instruct those to be warned of correct actions to be taken.

After installation, service, or maintenance, test the system to confirm that it is operating properly. Test the system regularly to confirm that it will be operational in an emergency.

1.1 Safety Messages to Installers

People's lives depend on your safe installation of our products. It is important to follow all instructions shipped with this product. This device is to be installed by a trained electrician who is thoroughly familiar with the National Electrical Code and/or Canadian Electrical Code and will follow the NEC and/or CEC Guidelines as well as all local codes.

The selection of the mounting location for this system, its controls and the routing of the wiring are to be accomplished under the direction of the Facilities Engineer and the Safety Engineer. Listed below are some other important safety instructions and precautions you should follow:

- Electrocution or severe personal injury can occur when performing various installation and service functions such as making electrical connections, drilling holes, or lifting equipment. Therefore, only experienced electricians should install this product in accordance with national, state and any other electrical codes having jurisdiction. Perform all work under the direction of the installation or service crew safety foreman.

Safety Messages

- Read and understand all instructions before installing, operating, or servicing this equipment.
- All effective warning sounds may, in certain circumstances, cause permanent hearing loss. Take appropriate precautions such as wearing hearing protection. Maximum sound level exposure limits specified in OSHA 29 CFR 1910 should not be exceeded.
- For optimum sound distribution do not install the loudspeakers where objects would block any portion of the front of the system.
- Establish a procedure to routinely check the signal system for proper activation and operation.
- Any maintenance to the unit **MUST** be performed by a trained electrician in accordance with NEC Guidelines and local codes or a Federal Signal certified Service Provider.
- Never alter the unit in any manner.
- The nameplate should **NOT** be obscured, as it contains cautionary and/or other information of importance to maintenance personnel.
- After installation and completion of initial system test, provide a copy of these instructions to all personnel responsible for operation, periodic testing, and maintenance of the equipment.
- File these instructions in a safe place and refer to them when maintaining and/or reinstalling the device.

Failure to follow all safety precautions and instructions may result in property damage, serious injury, or death.

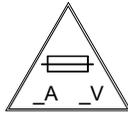
Installation and Service

- After installation or service, test the system to confirm that it is operating properly. Test the system regularly to confirm that it will be operational in an emergency.
- If future service and operating personnel do not have these instructions to refer to, the system may not provide the intended audible warning, and service personnel may be exposed to death, permanent hearing loss, or other bodily injury. File these instructions in a safe place and refer to them periodically. Give a copy of these instructions to new recruits and trainees. Also give a copy to anyone who is going to service or repair the system.
- To reduce the risk of electric shock, do not perform any servicing other than what is contained in the operating instructions unless you are qualified to do so. Refer all servicing to qualified service personnel. Always test the system before using after repairs have been made.

Ethernet Wiring

- Unless shielded or run in conduit, Ethernet wiring must be at least six feet from bare power wiring or lightning rods and associated wires, and at least six inches from other wire (for example, antenna wires, doorbell wires, wires from transformers to neon signs), steam or hot water pipes, and heating ducts.
- Do not place Ethernet wiring or connections in any conduit, outlet or junction box containing high voltage electrical wiring.

Symbol Definition



Indicates to reduce the risk of fire, replace fuse as marked.

Pay careful attention to the notice located on the equipment.

Read and understand the information contained in this manual before attempting to install or service the system.

2.0 General Description

2.1 Introduction

This document is a description, installation, and user manual for the PAGASYS GEN II networking solution. Its intended audience are those assigned to use and maintain the system.

2.2 Overview

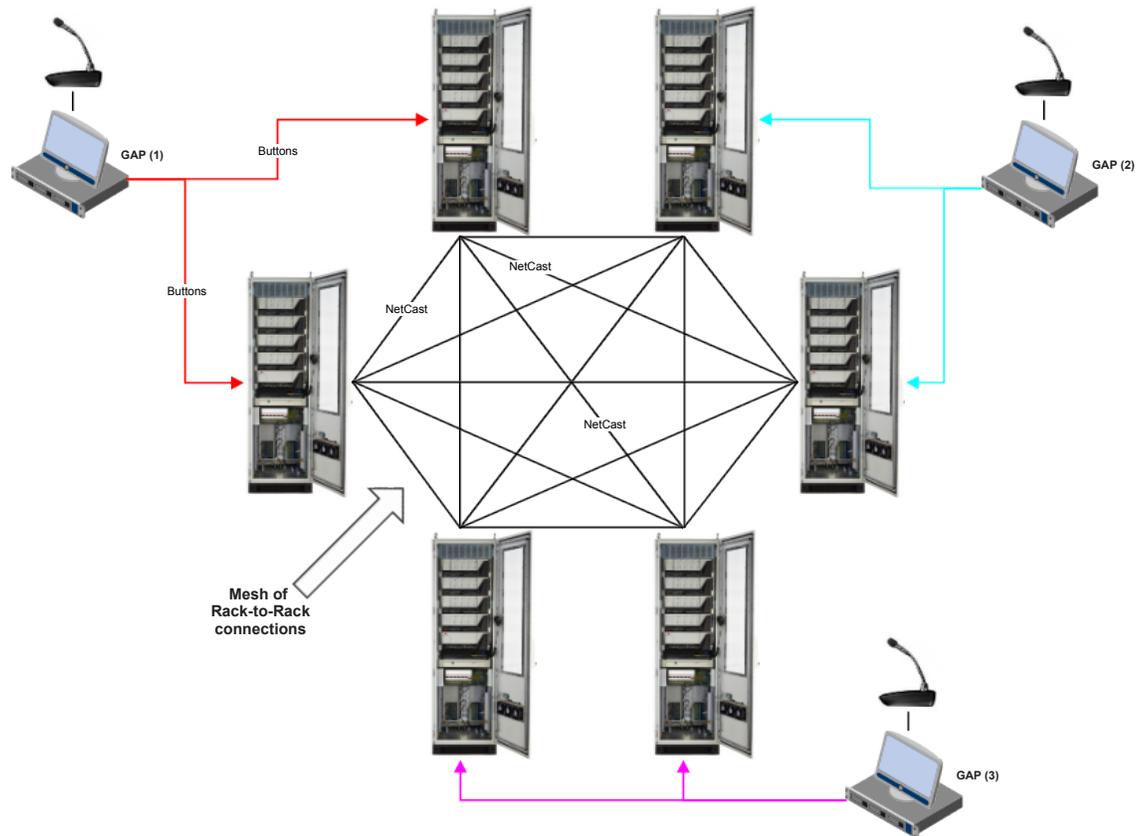
The current PAGASYS GEN II design provides a robust and powerful System Manager to support, command, and control the PAGASYS GEN II controller. The PAGASYS GEN II networking features offer additional redundancy using IP networking and enables sharing of audio across an IP enabled Digital Audio Network Through Ethernet (Dante®) interface. This manual describes the current product design and network design features, as well as new features that are part of the new PAGASYS GEN II network release.

The Dante® module on the system controller communicates with a Dante® application on remote Global Access Panels (GAPs) and other networked system controllers to share up to 16 channels of digital audio initiated from local microphones on the remote GAPs. Use of the Dante® module and application eliminates the need for a separate audio distribution hardware solution or protocol.

The PAGASYS GEN II network release involves a system design that uses Global Access Panels (GAPs) that communicate with one or more networked PAGASYS GEN II systems. A GAP sends all control and button status/broadcast requests to its connected Controllers using an IP-based interface. The GAP is a form of access panel that provides the ability to initiate broadcasts to any zone in a networked PAGASYS GEN II system.

The PAGASYS GEN II networked Controllers, when receiving a request to initiate a network broadcast, will coordinate with all network connected Controllers to ensure the requested broadcast is sent to all Controller/Zones specified in the network broadcast.

Figure 1 PAGASYS GEN II Network Topology



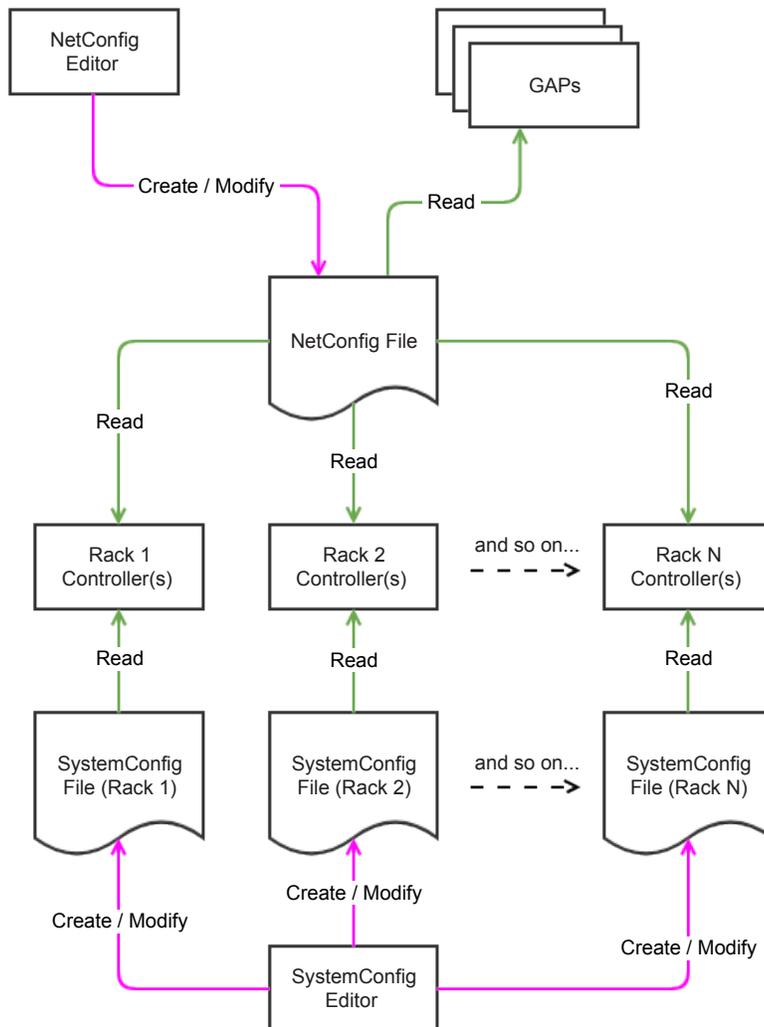
In a networked system, the PAGASYS Controllers and GAPs need to know about any device that they communicate with over the network, collectively referred to as “NetNodes.”

- Other PAGASYS Controllers: all PAGASYS Controllers are fully interconnected using a mesh-network configuration.
- GAPs: Global Access Panel that communicates with designated System Controllers through IP interfaces.

The PAGASYS GEN II system must operate on a dedicated network because of its safety critical nature and the bandwidth required. Operator and maintenance access can be restricted using passwords for both computer access and software access.

Network configuration is supported by a shared network configuration file, which is used to configure the respective network PAGASYS GEN II GAP and system controllers. The network configuration file is called the NetConfig file. The NetConfig file contains network node attributes and context, NetAlarms, NetCasts, and network zones (NetZones). The NetConfig file is created using a NetConfig Editor.

Figure 2 NetConfig Context Diagram



On the PAGASYS GEN II system, local broadcasts of alarms and announcements can be made from each node using a local access Control Panel. These access control points usually take the form of a hardware panel with buttons and indicators, or a System Manager hosted on a local server included with the PAGASYS GEN II rack and provide the means for local broadcasts from that node only or hardware access panel. In the unlikely event a node loses communications with the IP network, this local control point still allows broadcasts to be made. This method of initiating alarms and announcements is the primary method used by non-networked PA/GA systems.

Global broadcasts of alarms and announcements are made from Global Access Panels (GAPs), which are remote computers running GAP software. This software communicates directly with the network control equipment and can provide various broadcast and monitoring features. Networked PAGASYS GEN II racks are also able to initiate network broadcasts from the local access panel if required.

PAGASYS GEN II network operation uses NetZones, which are a subset of all the zones on all the racks in the networked system. An example of a NetZone accessing multiple zones on multiple racks is reflected in Table 1.

NOTE: NetZone IDs are numbered from 1 to 1024.

Table 1 NetZone Example

Network Zone ID	Network Zone Name	Rack 1	Rack 2	Rack 3	Comments
1	All zones	*	*	*	All zones on all racks
2	All zones in Tank Farm	*	*	none	All local zones on racks 1 and 2
3	Offices	none	none	3,4	Specific local zones on specific racks
4	Accommodation	1	none	1	Local zone 1 on all racks (except rack 2, which has no accommodation zones)

In a networked configuration, the system can broadcast NetAlarms, which are similar to current context PAGASYS broadcasts, but must be only alarm or message type.

When a NetAlarm is initiated from a GAP, the NetAlarm can originate from multiple racks. If all connected racks go down, the NetAlarm can failover repeatedly to other racks in the network. As long as one rack in the network is still functional, the NetAlarm will continue to sound. This behavior provides high fault-tolerance in the face of multiple rack or network faults.

A NetAlarm is similar to current context PAGASYS broadcasts except for the following:

- NetAlarm must be an ALARM or MESSAGE type (for example, Alarm, Routine Message), not a PAGE type (for example, Emergency Page, Routine Page, etc.).
- NetAlarm includes the IDs of all racks capable of originating the NetAlarm, sorted by priority.
- NetAlarm includes the IDs of all possible receiving racks.

All other NetAlarm properties (for example, priority, name, slice_sequences, etc.) are the same as for a normal Controller local broadcast.

The networked system also allows the user to broadcast NetCasts, which are similar to current context PAGASYS paging broadcasts. Support of NetCasts on a GAP or rack is dependent on the GAP/rack being configured with a microphone.

NetCasts typically originate from a single GAP paging microphone, but they can be routed to several PAGASYS GEN II racks. By routing to multiple racks, the NetCast will be fault tolerant to a rack outage, but fault tolerance is only available at least one rack directly connected to the originating GAP is available to distribute the NetCast. If all racks connected to the originating GAP go down, the paging capability from a GAP will be lost.

General Description

A NetCast is similar to current context PAGASYS broadcasts except for the following:

- NetCast must be a PAGE type (for example, Emergency Page, Routine Page, etc.), not an ALARM or MESSAGE type.
- NetCast cannot be muted.
- NetCast cannot be ducked.
- NetCast includes the ID of the originating rack and all possible receiving racks.

All other NetCast properties (for example, priority, name, slice_sequences, etc.) are the same as for a normal Controller local broadcast.

3.0 Using the PAGASYS Status Concentrator

3.1 Introduction

The PAGASYS Status Concentrator is a Windows® web-based process that resides on one or more of the computers in the PAGASYS GEN II network. The Status Concentrator supports the NetConfig Editor and manages the network communications between PAGASYS GEN II controllers and GAPS.

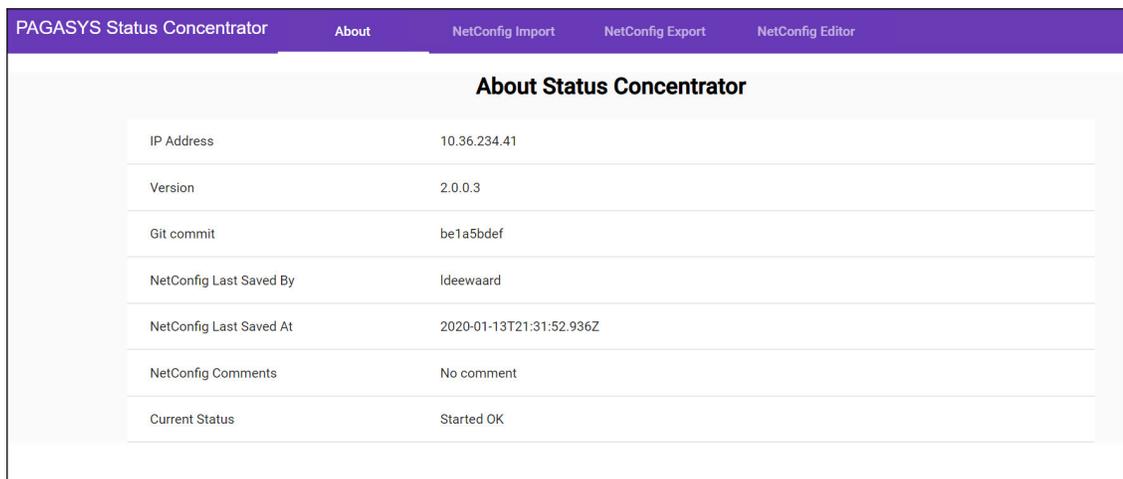
To access the Status Concentrator:

1. Open a new browser window on the host computer.
2. Enter the local website

localhost:808x

where: 808x is the IP port where the Status Concentrator was installed with 8081 the default IP port

The PAGASYS Status Concentrator window appears. The About window is the initial entry point for the Status Concentrator.



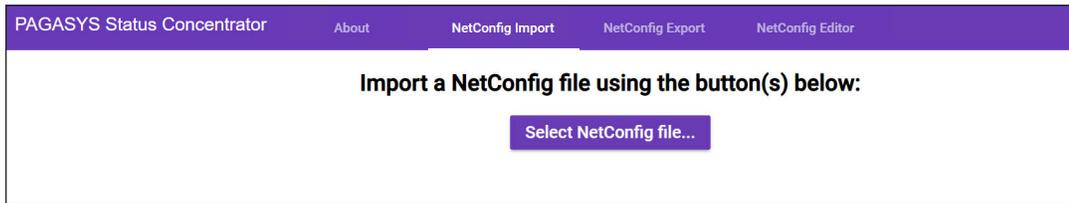
About Status Concentrator	
IP Address	10.36.234.41
Version	2.0.0.3
Git commit	be1a5bdef
NetConfig Last Saved By	Ideewaard
NetConfig Last Saved At	2020-01-13T21:31:52.936Z
NetConfig Comments	No comment
Current Status	Started OK

Fields	Description
IP Address	Displays the IP address of the computer hosting the Status Concentrator.
Version	Displays the Status Concentrator software version.
Git commit	Displays the Local build commit number of the software.
NetConfig Last Saved By	Displays the User login for user making last update to the configuration.
NetConfig Last Saved At	Displays the date and time of last update to configuration.
NetConfig Comments	Displays the user's comments for Status Concentrator.
Current Status	Displays the realtime status of the Status Concentrator.

3.2 NetConfig Import

The NetConfig Import window for the Status Concentrator editor allows the user to import an existing netconfig file into the editor. This allows the user to reuse an existing netconfig file to reduce the editing required.

To view the NetConfig Import window, click the NetConfig Import tab. The NetConfig Import window appears.



Click the Select NetConfig file button to open a window to browse the local computer for the existing netconfig file.

3.3 NetConfig Export

The NetConfig Export window for the Status Concentrator editor allows the user to export a netconfig file after it is created or modified in the editor. This allows the user to save a netconfig file to back up the file and distribute to network nodes that use the NetConfig.

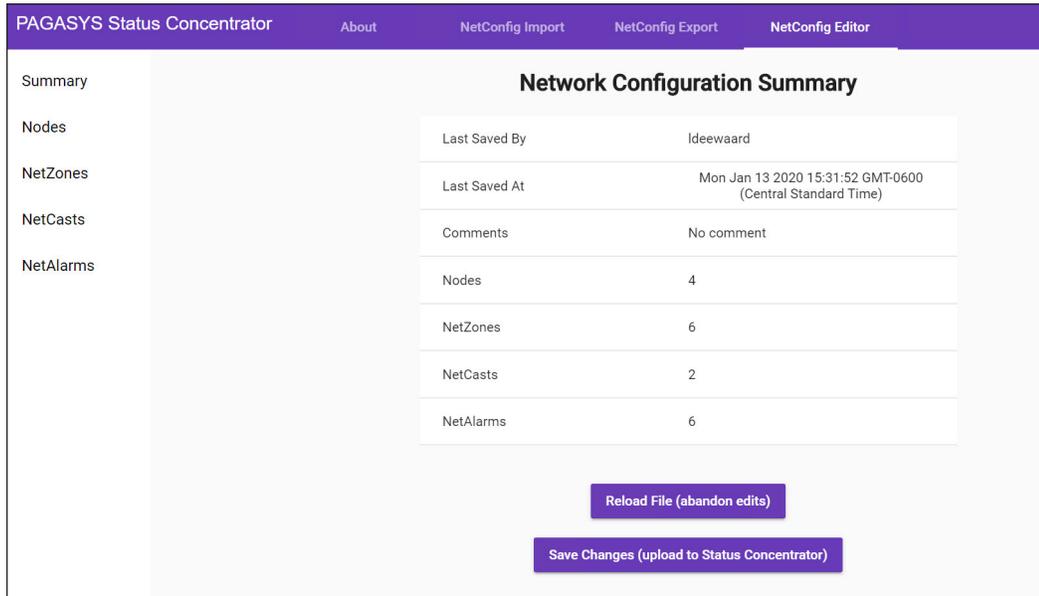
To view the NetConfig Export window, click the NetConfig Export tab. The NetConfig Export window appears.



Click the netconfig button to export the netconfig file to the local computer to save.

3.4 NetConfig Editor

To view the NetConfig Editor window, click the NetConfig Editor tab. The NetConfig Editor window appears.



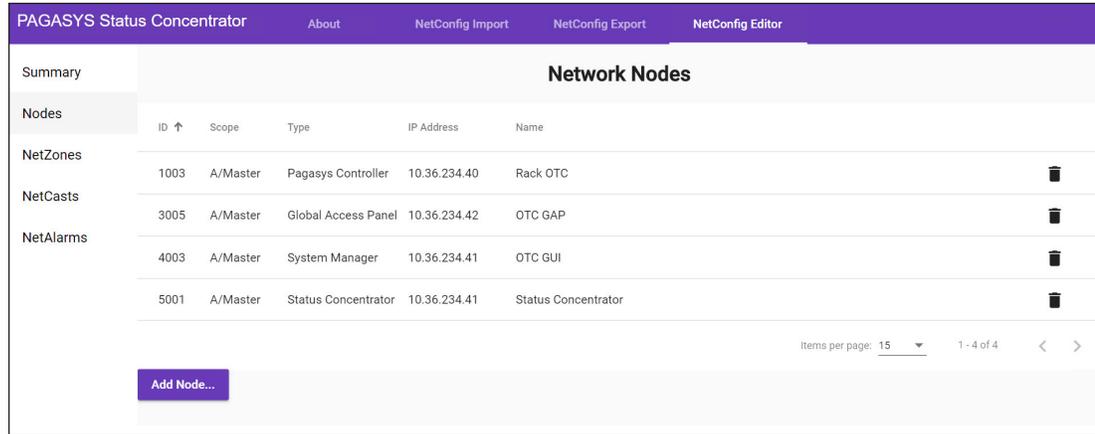
The Status Concentrator NetConfig Editor Summary window shows the user the current NetConfig status.

Fields	Description
Last Saved By	Displays the user login name of user making last update to the configuration.
Last Saved At	Displays the date and time of last update to configuration.
Comments	Displays the user's comments for Status Concentrator.
Nodes	Displays the number of network nodes in the NetConfig.
NetZones	Displays the number of network zones in the NetConfig.
NetCasts	Displays the number of network broadcasts in the NetConfig.
NetAlarms	Displays the number of network alarms in the NetConfig.
Reload File (abandon edits)	Click this button to abandon any changes to the NetConfig and reload the existing file from disk.
Save Changes (upload to Status Concentrator)	Click this button to upload any changes to the Status Concentrator.

3.4.1 NetConfig Editor > Nodes

The Status Concentrator Network Nodes window shows all of the existing network nodes in the NetConfig on the Status Concentrator. The user can delete any of the nodes or can add a new node.

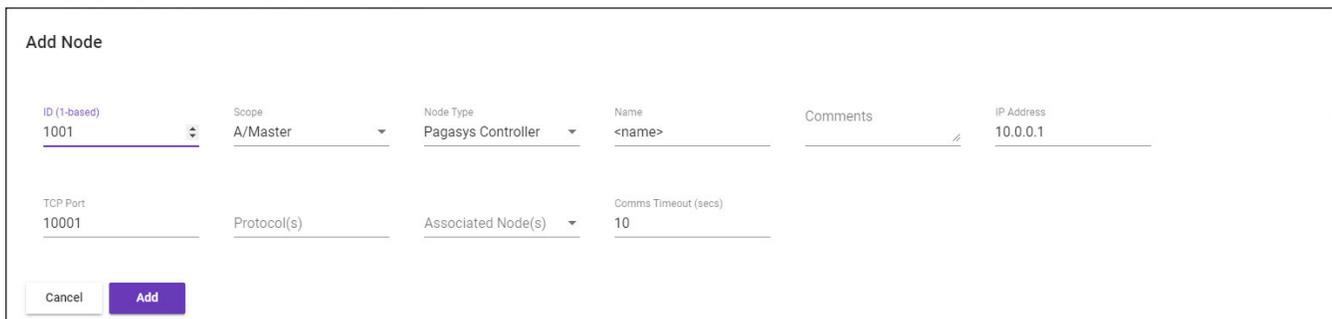
To access the Network Nodes, click Nodes. The Network Nodes window appears.



To delete a node, select the trash can icon next to the node you want to delete.

3.4.1.1 Adding New Nodes

To add a node, click the Add Node button. The Add Node dialog box appears.



The Status Concentrator NetConfig Editor Add Node window allows the user to add new network nodes to the NetConfig.

Fields	Description
ID	Select the network ID for the new node being added to the network. Range 1001 and higher.
Scope	Select either A/Master or B/Standby for PAGASYS controllers, System Managers, and NIONs, or Duplicated for GAPs and Status Concentrators.
Node Type	Select the type of the node. Options are Global Access Panel, NION, Pagasys Controller, Status Concentrator, or System Manager.
Name	Enter the user-defined name for the new node.
Comments	Enter comments for the new node.
IP Address	Displays the IP address of the new node.

Fields	Description
TCP Port	Select the TCP port for the new node, typically 1000x.
Protocol(s)	Enter the protocols used to access the new node.
Associated Node(s)	Select the other nodes in the system that the new node needs access to, such as GAPS or other controllers.
Comms Timeout (secs)	Select the timeout for node communications.
Cancel	Click to cancel adding the new node.
Add	Click to add the new node with current parameters.

3.4.1.2 Editing Nodes

The Status Concentrator NetConfig Editor View/Edit Node window allows the user to edit existing network nodes to the NetConfig. The View/Edit Node window uses the same fields as the Add Nodes window.

To edit a node, click the node you want to edit. The View/Edit Node dialog box appears.

The screenshot shows the 'View/Edit Node - OTC GUI' dialog box. The interface includes a sidebar with categories: Summary, Nodes, NetZones, NetCasts, and NetAlarms. The main area contains the following fields:

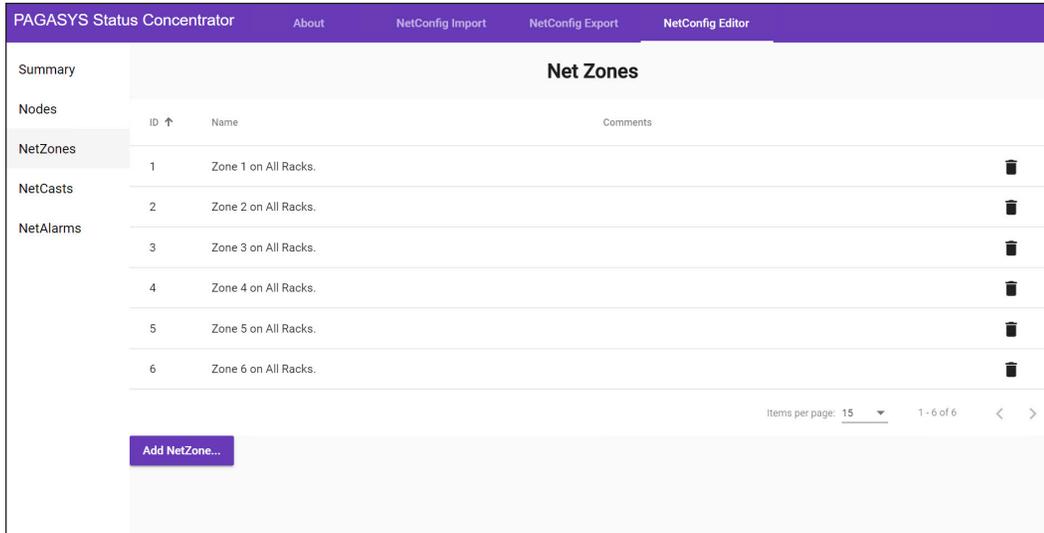
- ID (1-based):** 4003
- Scope:** A/Master
- Node Type:** System Manager
- Name:** OTC GUI
- Comments:** (Text area)
- IP Address:** 10.36.234.41
- TCP Port:** 8092
- Protocol(s):** HTTP
- Associated Node(s):** 1003 (Rack OTC)
- Comms Timeout (secs):** 10

A 'Save Changes' button is located at the bottom of the form.

3.4.2 NetConfig Editor > NetZones

The Status Concentrator NetConfig NetZone window shows all of the existing network zones in the NetConfig on the Status Concentrator. The user can delete any of the network zones or can add a new zone.

To access the Net Zones window, click NetZones. The Net Zones window appears.



To delete a NetZone, select the trash can icon next to the NetZone you want to delete.

3.4.2.1 Adding New NetZones

To add a NetZone, click the Add NetZone button. The Add NetZone dialog box appears.



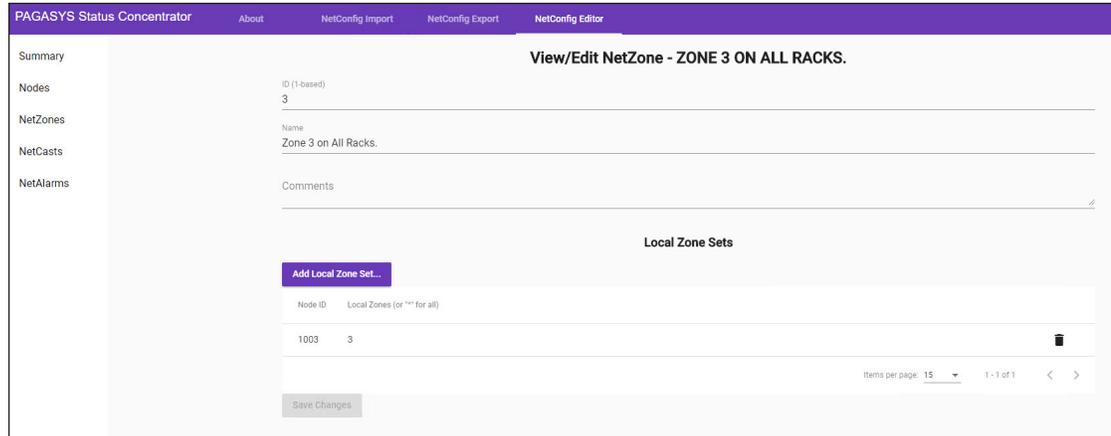
The Status Concentrator NetConfig Editor Add NetZone window allows the user to add new network zones to the NetConfig.

Fields	Description
ID	Select the ID for the new zone being added to the network. Range 1 to 1024.
Name	Enter the name of the new network zone.
Comments	Enter comments for the new network zone.
Cancel	Click to cancel adding the new network zone.
Add	Click to add the new zone with current parameters.

3.4.2.2 Editing NetZones

The Status Concentrator NetConfig Editor View/Edit NetZone window allows the user to edit existing network zones to the NetConfig.

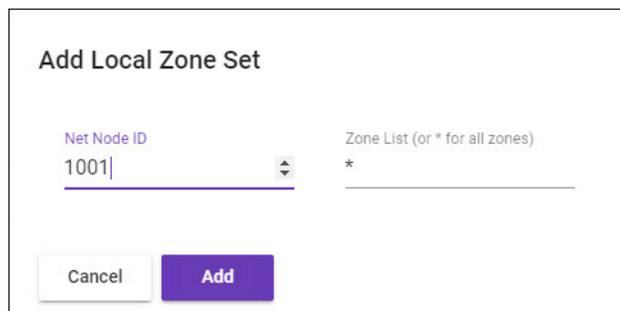
To edit a zone, click the zone you want to edit. The View/Edit NetZone dialog box appears.



Fields	Description
ID	Select ID for the new zone being added to the network.
Name	Enter the name of the new network zone.
Comments	Enter comments for the new network zone.
Add Local Zone Set	Click to add local zone setting to the new network zone.
Save Changes	Click to save changes after editing a NetZone.

Adding Local Zone Settings

To add local zone setting to the new network zone, click the Add Local Zone Set button. The Add Local Zone Set dialog box appears.

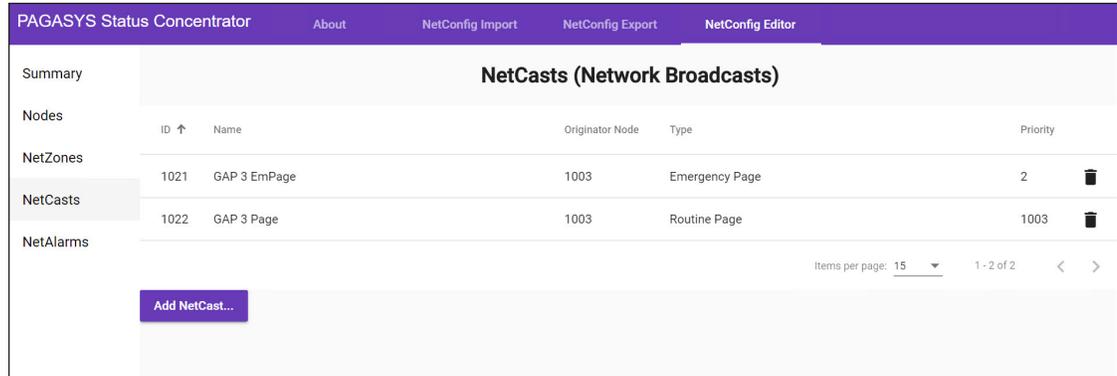


Fields	Description
Net Node ID	Select the network node ID for the node affected by the new zone.
Zone List	Define the list of zones on the target node that are included in the new network zone.
Cancel	Click to cancel the local zone settings change.
Add	Click to add the new settings for the local zone on the target node.

3.4.3 NetConfig Editor > NetCasts

The Status Concentrator NetConfig Editor NetCasts window shows all of the existing network broadcast sources in the NetConfig on the Status Concentrator.

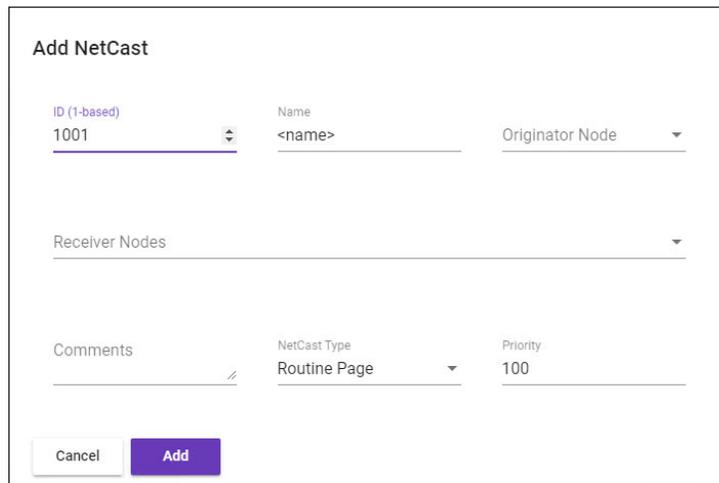
To access the Network Broadcast, click NetCasts. The Network Broadcasts window appears.



To delete a network broadcast, select the trash can icon next to the network broadcast you want to delete.

3.4.3.1 Adding New Broadcasts

To add a Network Broadcasts, click the Add NetCasts button. The Add NetCast dialog box appears.



The Status Concentrator NetConfig Editor Add NetCasts window allows the user to add new network broadcast sources to the NetConfig.

Fields	Description
ID	Select the ID for the new broadcast source being added to the network. Range is 1 to 9999.
Name	Enter the name of the new network broadcast source.
Originator Node	Select the network node that will originate the new network broadcast.

Fields	Description
Receiver Nodes	Select the network nodes that can receive the new network broadcast, or leave blank for 'all nodes'. The nodes that actually receive the broadcast will depend on which NetZones are selected at the time.
Comments	Enter comments for the new network broadcast source.
NetCast Type	Select the NetCast type. Options are Emergency Page, Priority Page, or Routine Page.
Priority	Select a numeric priority. (Lower numbers have higher priority.)
Cancel	Click to cancel adding the new network broadcast source.
Add	Click to add the new broadcast source with current parameters.

3.4.3.2 Editing Broadcasts

The Status Concentrator NetConfig Editor View/Edit NetCast window allows the user to edit existing NetCast to the NetConfig.

To edit a network broadcast, click the network broadcast you want to edit. The View/Edit NetCast dialog box appears.

Fields	Description
ID	Select the ID for the new broadcast source being added to the network.
Name	Enter the name of the new network broadcast source.
Comments	Enter the comments for the new network broadcast source.
Originator Node	Select the network node that will originate the new network broadcast.
Receiver Nodes	Select the network nodes that will receive the new network broadcast.
Priority	Select a numeric priority. (Lower numbers have higher priority.)

Fields	Description
NetCast Type	Select option from Emergency Page, Priority Page, or Routine Page.
Save Changes	Click to save changes after editing a network broadcast source.
Add Slice	Click to add a new audio source to the Primary or Secondary sequence for the new NetCast.

Adding Primary/Secondary Slice

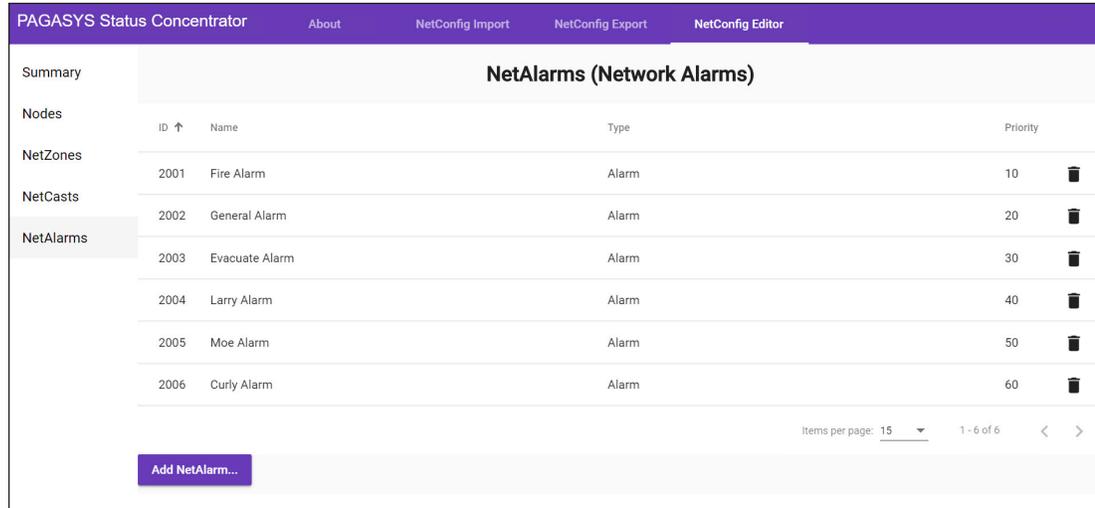
To add a new audio source to the Primary or Secondary sequence for the new NetCast, click the Add Slice button. The Add Primary Slice dialog box appears.

Fields	Description
Slice ID	Select the add sequence number for the audio source, starting at 1.
Jump	Select the field that indicates which sequence number to play after current sequence or zero to just play the next slice.
Widget ID	Select the ID of internal function Widget, if available.
Live Source	Click to use live source.
Source	Select from the source of the broadcast.
Source Scope	Select option from A / Master, B / Standby, or Duplicated.
Cancel	Click to cancel adding the primary/secondary slice.
Add	Click to add a new audio source to the Primary or Secondary sequence for the new NetCast.

3.4.4 NetConfig Editor > NetAlarms

The Status Concentrator NetConfig Editor NetAlarms window shows all of the existing network alarms in the NetConfig on the Status Concentrator.

To access the Network Alarms, click NetAlarms. The NetAlarms (Network Alarms) window appears.



To delete a network alarm, select the trash can icon next to the network alarm you want to delete.

3.4.4.1 Adding New Network Alarms

The Status Concentrator NetConfig Editor Add NetAlarm window allows the user to add new network alarms to the NetConfig.

To add a network alarm, click the Add NetAlarm button. The Add NetAlarm dialog box appears.

Add NetAlarm

ID (1-based):

Name:

Originator Nodes:

Comments:

NetAlarm Type:

Priority:

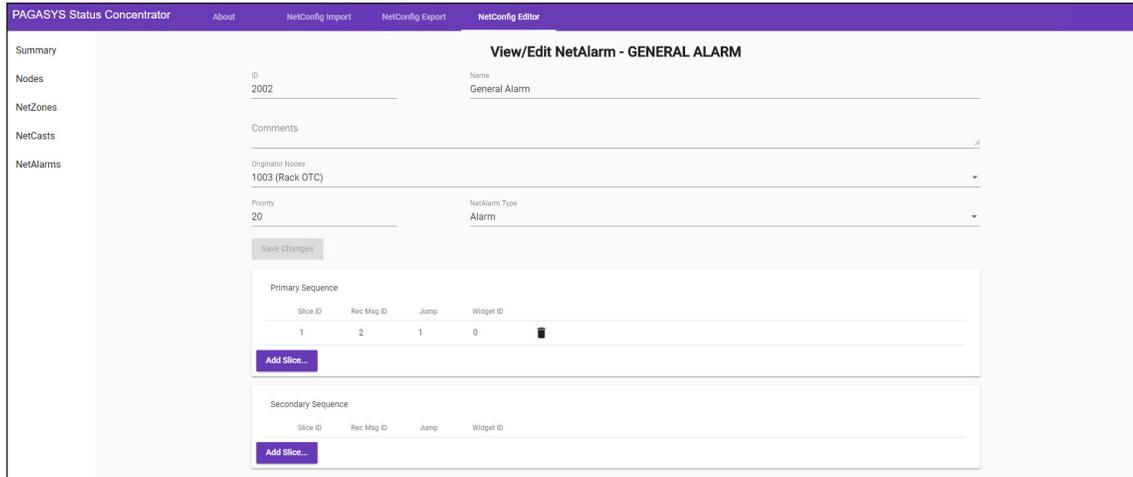
Fields	Description
ID	Select the ID for the new alarm being added to the network.
Name	Enter the name of the new network alarm.

Fields	Description
Originator Nodes	Select the network nodes that can originate the new network alarm (that is, all nodes that may need to sound this alarm).
Comments	Enter comments for the new network alarm.
NetAlarm Type	Select the NetAlarm type. Options are Alarm, Duckable Alarm, or Routine Message.
Priority	Enter a numeric priority. (Lower numbers have higher priority.)
Cancel	Select to cancel adding the new network alarm.
Add	Select to add the new alarm with current parameters.

3.4.4.2 Editing Network Alarms

The Status Concentrator NetConfig Editor View/Edit NetAlarm window allows the user to edit existing NetAlarm to the NetConfig.

To edit a network alarm, click the network alarm you want to edit. The View/Edit NetAlarm dialog box appears.



Fields	Description
ID	Select the ID for the new alarm being added to the network.
Name	Enter the name of the new network alarm.
Comments	Enter comments for the new network alarm.
Originator Nodes	Select the network nodes that will originate the new network alarm.
Priority	Enter a numeric priority. (Lower numbers have higher priority.)
NetAlarm Type	Select the NetAlarm type. Options are Alarm, Duckable Alarm, or Routine Message.
Save Changes	Click to save changes after editing the network alarm.
Add Slice	Select to add a new alarm with current parameters.

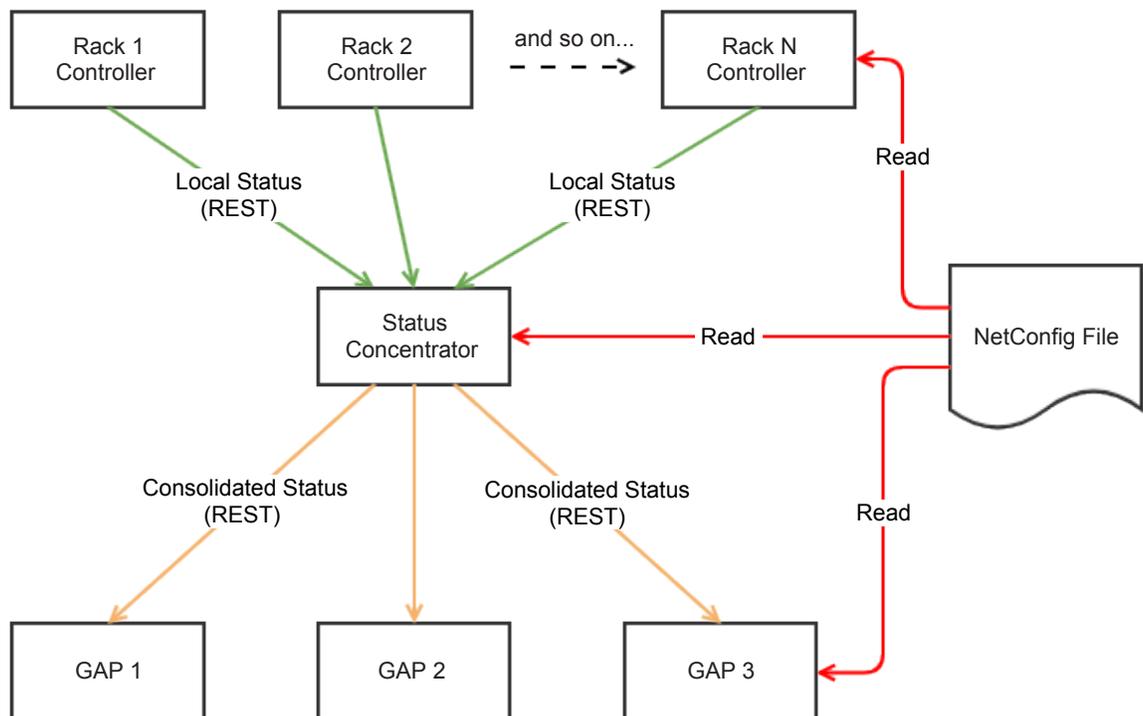
4.0 Using the Global Access Panel (GAP)

A PAGASYS GEN II networked system includes GAPs communicating with select controllers and the network of system controllers (racks) that share control and status information important to the network.

The GAP software supports many of the operations supported by the PAGASYS GEN II System Manager, including the following: user login, a Control Panel, User Admin, and importing and exporting Control Panel design. You must design the GAP Control Panel on a System Manager, because the GAP does not have the capability to design its own Control Panel.

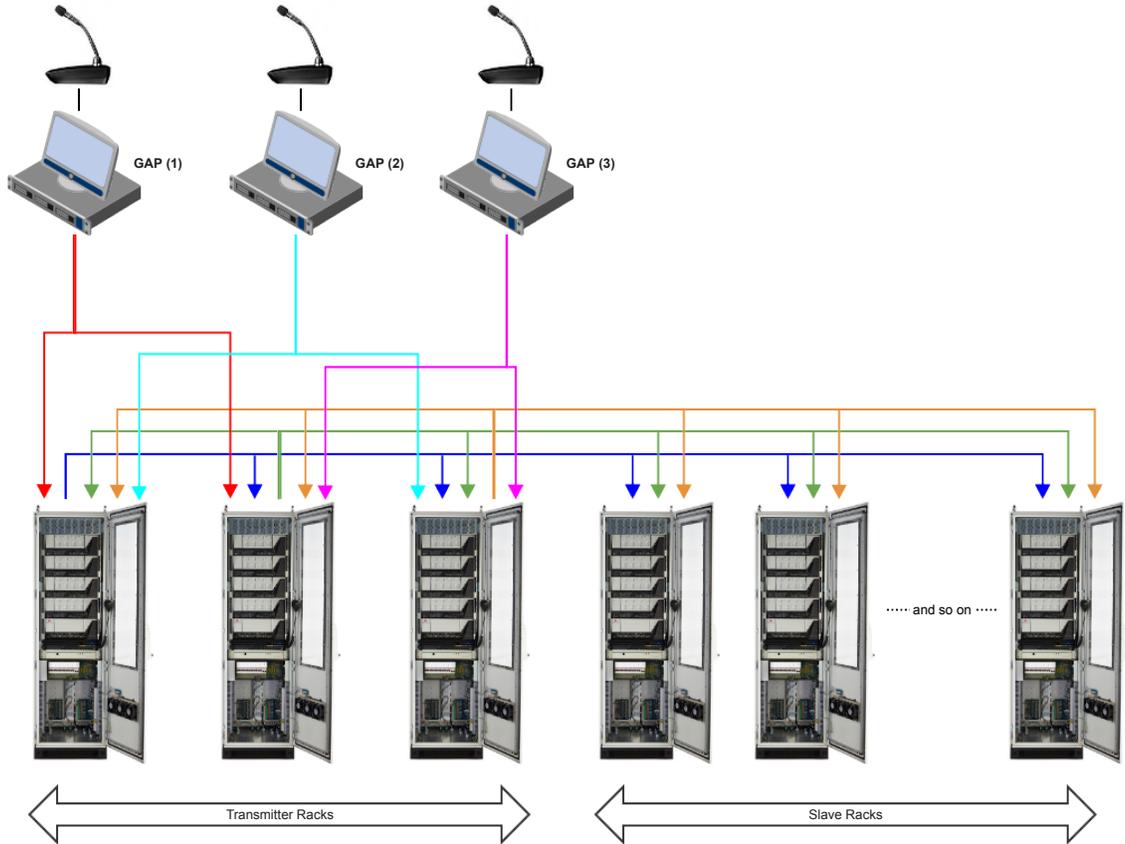
GAP operations also include alarm and paging initiation with system controllers, as well as Controller faults status display. A GAP receives real-time data on Controller status for current broadcasts and faults/status in the network, displaying collated network data on the GAP status windows.

Figure 3 PAGASYS GEN II GAP Operations



GAPs in the PAGASYS GEN II networked system may share live audio using IP-based Dante® channels. Dante® audio routing is configured using the Dante® Controller software from Audinate. Each rack Controller selects up to six channels out of a possible 16 channels received from connected GAPs.

Figure 4 PAGASYS GEN II Dante® Digital Audio Sharing



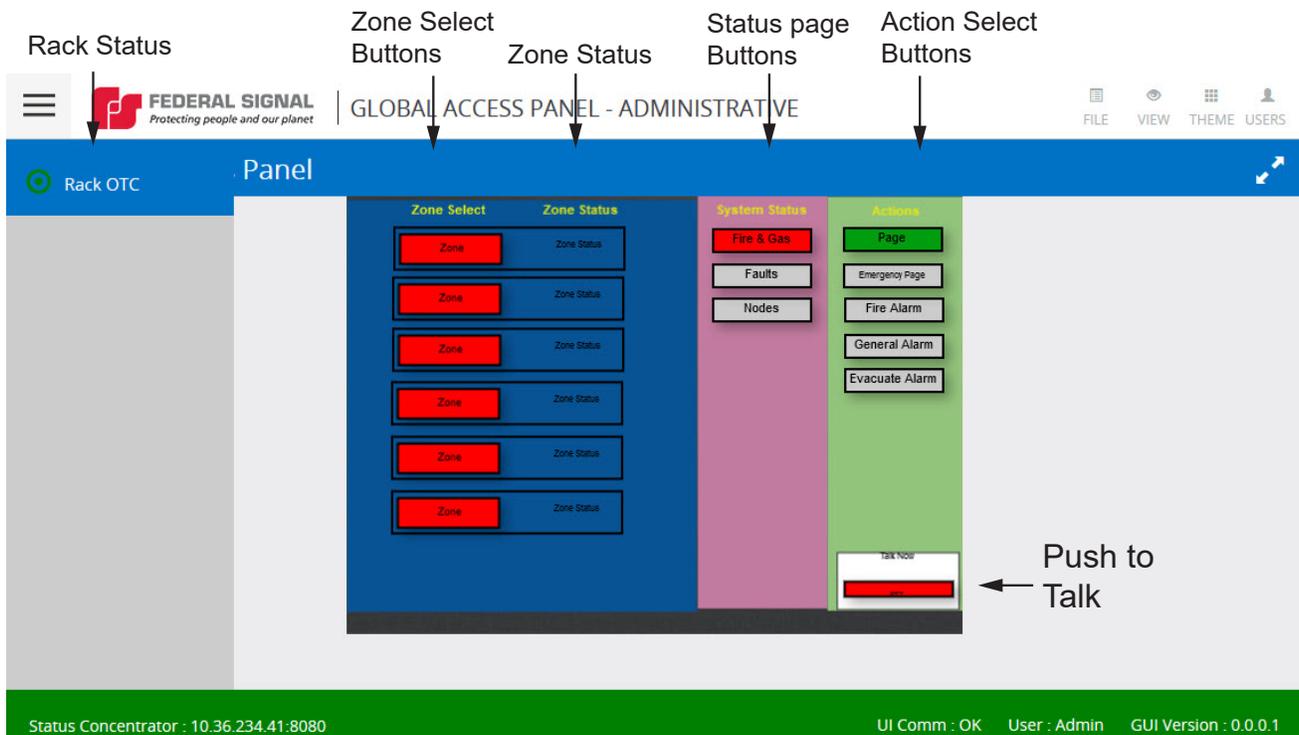
Like the PAGASYS GEN II System Manager, the GAP application has GUI display windows to allow the user to initiate broadcasts or view system status. The GAP display windows include the GAP kiosk window and system status windows, including Fire & Gas and Faults.

4.1 GAP Kiosk Window

Upon initial entry after user login, the default GAP page is the Kiosk window. The GAP Kiosk window is a representation of a user kiosk that allows network zone selection. The Kiosk also displays Broadcast Status and System Status.

The GAP communicates with the PAGASYS GEN II network through the Status Concentrators in the network. The GAP connection status bar on the Kiosk window reflects the connection status between the GAP and the Status Concentrator. The bar is green when the connection is good. The IP address and port of the connected Status Concentrator is displayed on the left side of the bar. The bar is yellow when connection is lost. Multiple Status Concentrators can be used for redundancy, with the GAP switching between Status Concentrators when connection is lost.

The Kiosk window appears. The appearance and position of controls are completely user-defined, but the illustration below shows a typical layout.



4.1.1 Rack Status

On the left side of the Kiosk window is the rack status. The rack status lists the controller nodes which the GAP is connected to through the Status Concentrator. Typically, a GAP is connected to at least two racks for redundancy but can be connected to more than two. The rack status only shows nodes when the user is logged in as the admin user. When logging into the GAP as a kiosk user, the rack status will be blank.

4.1.2 Zone Select Status

In the center of the Kiosk window is Zone Select status. The Zone Select column displays user-defined colors that reflect Zone Select status related to connected racks. The network zones displayed on the GAP can include multiple local zones on different PAGASYS racks.

Zone Select conditions are listed in the table below.

Table 2 Zone Select Status

Zone Select Status	Description	Color	Text
On	All racks show this zone selected	User defined (for example, Green)	Network Zone ID
Off	All racks show this zone un-selected	User defined (for example, Grey)	Network Zone ID
Conflicted	Racks do not agree on Zone Select status (typically a fault, when one of the racks may not be communicating normally)	User defined (for example, Yellow)	Network Zone ID

4.1.3 Zone Status

When a broadcast is active on a network zone, the color of the Zone Status reflects the current broadcast status for the network zone, including all local zones in the network zone. In addition, the Zone Status displays text representing the active broadcast in that network zone. Zone Status conditions are listed in the table below.

Table 3 Zone Status

Zone Select Status	Description	Color	Text
SILENT	All local zones in this network zone are silent	User defined (for example, Transparent)	No text
SAME	All local zones playing the same broadcast	User defined (for example Orange)	Broadcast name
PARTIAL	Some local zones playing the broadcast, but some silent	User defined (for example, Blue)	Broadcast name followed by asterisk symbol (*) (for example, "Fire Alarm*")
DIFF	Some of the local zones are playing one broadcast, while others are playing a different broadcast.	User defined (for example, Red)	Name of highest priority broadcast or name of broadcast playing in most of the local zones, encapsulated by the number symbol (#) (for example, #Fire Alarm#)
STALE	All of the specified zones have stale data.	User defined (for example, Yellow)	None

Zone Status example

Zone 2 has condition SILENT, and Zone 26 has condition SAME, and is playing broadcast “Fire Alarm.”



4.1.4 System Status

The System Status window includes configurable status buttons that can be configured to support:

- Indication of any named inputs/outputs that are active (such as Fire & Gas)
- List of any active faults, which can be filtered by multiple parameters
- List of named Broadcasts that are active in the system

The sections below describe common examples of status windows, Fire & Gas and Faults.

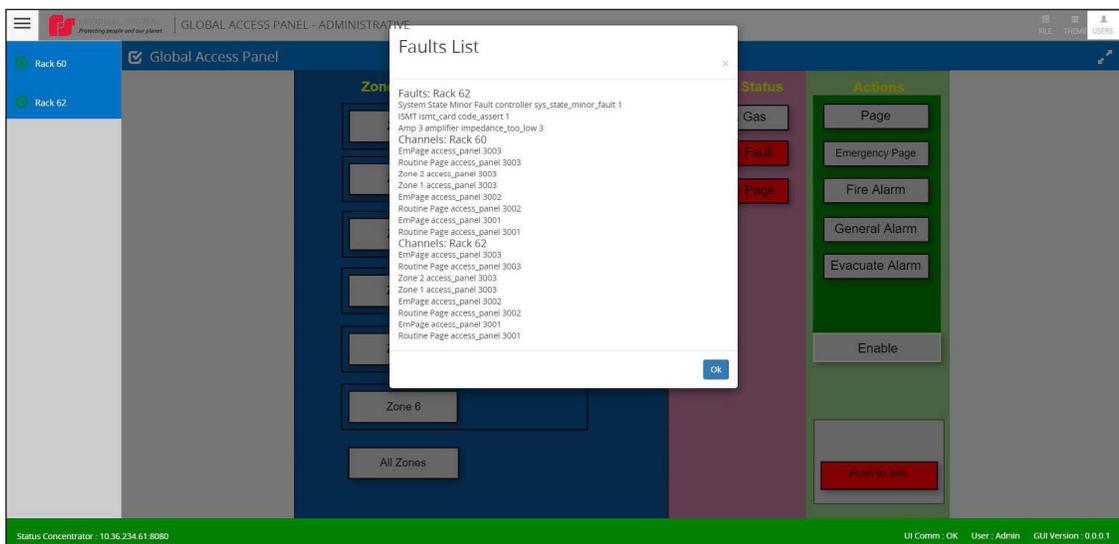
Fire & Gas Indicator

You can wire multiple fire and gas activations into the remote racks and configure to automatically activate fire and gas alarms in the racks. If there is an “active” trigger from the fire and gas system to any node in the system, then the Fire & Gas indicator lights. Click the Fire & Gas indicator to display a page that lists the rack(s) in the system that are reporting the Fire or Gas alarm.

Faults Button

The PAGASYS GEN II GAP supports Faults status from all racks connected to the local GAP. This data is collected from Controller Hosts and collated for display.

Click the Faults button to display a NetNodes faults page that lists active faults on connected racks. See the following example.



NetNodes Faults page columns reflect the current state of faults for connected PAGASYS racks. NetNodes fault fields are listed in the following table.

Table 4 Faults

Field	Description
Node ID	Controller ID reporting the fault
Status Type	The type of fault being reported
Entity Type	The equipment reported to have the fault
Entity ID	A local rack ID for the equipment reported to have the fault
Sub Entity ID	A local rack ID for further resolution of equipment reported to have the fault for example, the channel on an input card.

4.1.5 Actions

The GAP Kiosk Actions buttons provide actions that you can initiate on selected NetZones. While the actions can vary depending on what actions are configured during configuration of the GAP Kiosk, typical actions include Page (routine and emergency), Fire Alarm, General Alarm, and Evacuation Alarm. In addition, the Actions buttons can require the selection of an Enable button before activating alarms, in the same manner supported on the System Manager Control Panel. The Actions buttons can also include a Push to Talk button for live paging.

Page

The Page button enables the user to make live routine pages from the GAP when it is configured with a microphone.

To make live routine pages, click the Page button and then select the Push-to-Talk button while speaking into the microphone.

To stop capturing speech, release the Push-to-Talk button.

Emergency Page

Similar to the Page button operation, the Emergency Page button allows the user to make pages from the GAP when it is configured with a microphone. Emergency page is typically set to a higher priority than routine Page. The Emergency Page button is typically configured so that the user is required to click the Enable button before selecting the Emergency Page button. The Emergency Page button also requires Push to Talk while speaking into the microphone.

Fire Alarm

The Fire Alarm button allows the user to initiate a fire alarm broadcast to any selected NetZones. The Fire Alarm button is typically configured so that the user is required to click the Enable button before selecting the Fire Alarm button.

General Alarm

The General Alarm button allows the user to initiate a General Alarm broadcast to any selected NetZones. The General Alarm button is typically configured so that the user is required to click the Enable button before selecting the General Alarm button.

Evacuate Alarm

The Evacuate Alarm button allows the user to initiate an Evacuate Alarm broadcast to any selected NetZones. The Evacuate Alarm button is typically configured so that the user is required to click the Enable button before selecting the Evacuate Alarm button.

Enable

The Enable button must be selected prior to selecting higher priority Action buttons.

Push to Talk

The Push to Talk (PTT) button is used to enable the microphone when the GAP user wants to broadcast live speech to the selected NetZones. This button must be continuously held while broadcasting.

4.2 Initiate Action from Kiosk Window

To initiate an Action from the Kiosk window (Broadcast or live voice page):

1. Select at least one Zone Select button. (Select the All Zones button to select all zones.)
2. Select an Action button. In some cases, the Enable button needs to be selected before selecting an action button, for example when attempting an emergency page.
3. The broadcast or page is requested by the connected Status Concentrator to the selected racks/zones.

Once the broadcast is initiated, local zones defined in the NetZone represented by the Zone Select button will play the broadcast. The broadcast can be routed to additional NetZones by selecting their Zone Select buttons on the GAP. To stop the broadcast, deselect the Zone Select button or the Action button.

4.3 GAP Installation and Configuration

The GAP is a Microsoft Windows server that may include a touch screen user interface and an optional microphone when live audio is desired. The server hardware and software prerequisites and requirements are the same as needed for the PAGASYS GEN II System Manager. (See section 2.3 of the PAGASYS GEN II System Manager Manual for operating requirements.) The GAP software uses the same automated installer program as the System Manager. (See section 3.1 of the PAGASYS GEN II System Manager Manual for the installation procedure.) Live audio from the optional microphone on a GAP is routed to connected controllers using a Dante® application running on the GAP server. The Dante® software is installed with the GAP software when using the automated installer program.

The GAP-specific attributes or personalities are enabled after software installation during license activation, contact Federal Signal Customer Service to obtain a GAP license.

5.0 Network Models and Configuration

To configure a PAGASYS GEN II system as a networked system, a new Controller Chassis (P-NET-G-IP) needs to replace the standard Controller Chassis (P-NET-G) in the PAGASYS GEN II cabinet. The system also requires licensing of the System Manager software as networked, and installation and configuration of the Status Concentrator software on one of the Windows® servers in the network.

Order Global Access Panels using model P-GAP-G and the System Manager software on the GAP will be licensed as networked and as a GAP.

6.0 Upgrading to a Networked Solution

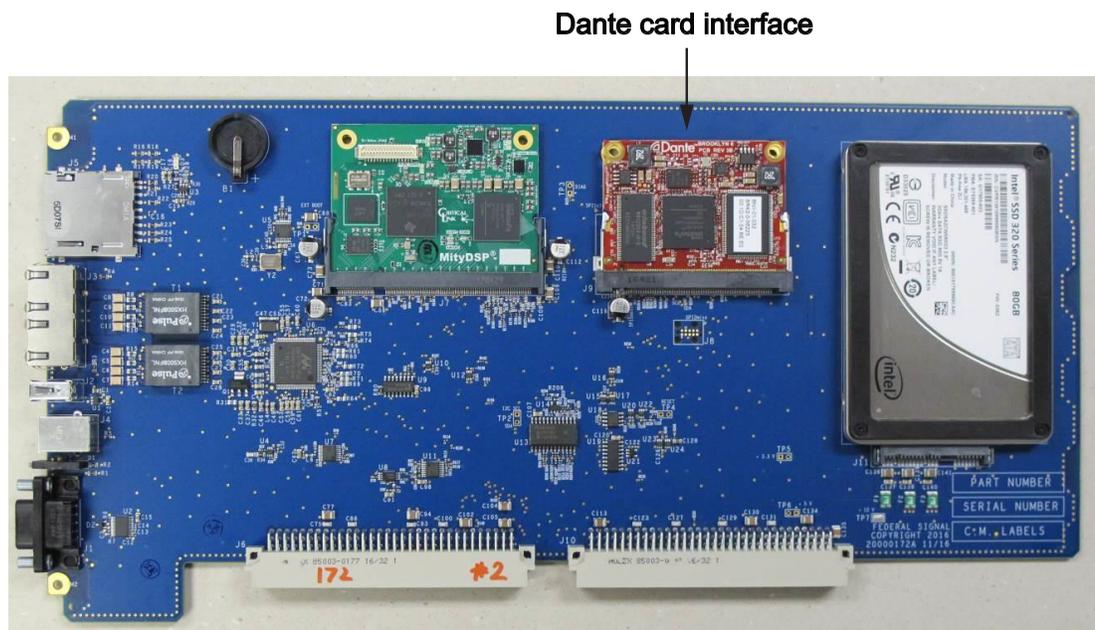
A non-networked PAGASYS GEN II system can be transitioned to a networked solution with hardware and configuration changes.

6.1 Updating the Hardware

A networked PAGASYS GEN II system requires a system controller that is enabled for Dante® digital audio. Federal Signal offers the system controller in two models: one that is not network-enabled (P-NET-G), and one that is network enabled (P-NET-G-IP). If the system already contains the non-network enabled controller chassis, transitioning the controller hardware to be network-enabled requires a change to the system controller PCB in the Controller Chassis.

The system controller PCB (P-CPC-G) includes a Dante® card interface. See Figure 5.

Figure 5 System Controller PCB that is Network Enabled (P-NET-G-IP)



The Dante® card interface is unpopulated in a non-networked Controller Chassis and is populated with the Dante® card in a networked Controller Chassis.

When transitioning a non-networked system to a networked system, a network transition kit (K-P-DANTE-G) can be purchased that includes the Dante® card, standoffs, and screws necessary to mount the Dante® card onto the non-networked controller card. After the Dante® card is installed on the controller card, configuration changes are also required to enable network mode.

6.2 Configuring the Software

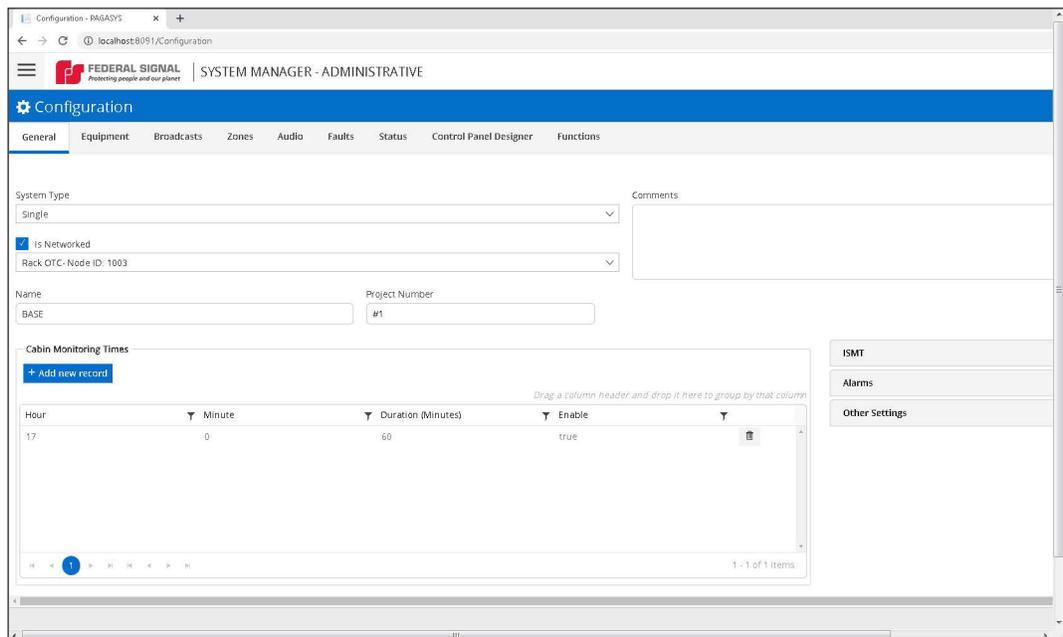
Once the hardware changes are made to the controller card, the PAGASYS GEN II system should be configured to support networking.

The local System Manager software should be licensed to support networking. Federal Signal Customer Service can provide network licensing for the local System Manager when ordering the network transition kit (K-P-DANTE-G). Once licensed for networking, the local System Manager software can be configured to use the local networked controller.

To configure the local System Manager software to use the local networked controller:

1. In the System Manager software, click Configuration > General tab.
2. Click the Is Networked check box.
3. Use the drop-down arrow to select the local controller that is being configured as networked.

IMPORTANT: This last step assumes that the NetConfig file has been created on the local Status Concentrator and distributed to networked nodes that include the local System Manager software and the connected, networked controller.



Once the system is set up as networked, the system can use the Dante® network audio to route audio from networked GAPS and remote controllers and amplifiers.

7.0 Getting Service

If you are experiencing any difficulties, contact Federal Signal Technical Support at 800-524-3021 or through e-mail at techsupport@fedsig.com. For instruction manuals and information on related products, visit <http://www.fedsig.com/>



FEDERAL SIGNAL
Safety and Security Systems

2645 Federal Signal Drive
University Park, Illinois 60484-3167

www.fedsig.com

Technical Support 800-524-3021



FEDERAL SIGNAL
Safety and Security Systems

2645 Federal Signal Drive
University Park, Illinois 60484-3167

www.fedsig.com

Technical Support

800-524-3021