FocalPoint™ Receivers Gateway

Installation & Operation Manual

DACR Gateway
Version 3.10.110
Serial Number: 10437
This Product Installed at: FCI Test Key
Software Licensed to: Rick Suel
Local Computer Name: KY09DTHJHRT21
Local IP Address: 101.101.101.101
Language: English

Gamewell FCI FIRE CONTROL INSTRUMENTS by Honeywell

Published in U.S.A.
P/N: 53251 A
ECN: 08-901

12 Clintonville Road, Northford, CT 06472, 203-484-7161, FAX 203-484-7118
www.gamewell-fci.com

IMPORTANT INFORMATION

This manual is designed for use by factory trained installers and operators of the Gamewell/FCI FocalPoint System. All illustrations, functional descriptions, operating and installation procedures, and other relevant information are contained in this manual.

The contents of this manual are important, and the manual must be kept with the system at all times. If building ownership is changed, this manual, including any testing and maintenance information, must be passed along to the new owner(s).

Manuals and instructions for other devices forming part of the FocalPoint System should be kept together. Purchasers who install this system for use by others must leave the instructions with the user. A copy of these instructions is included with each product and is available from the manufacturer.

This equipment is Listed by various listing agencies for use in emergency evacuation and fire alarm systems. Use only components that are compatible with this FocalPoint System. The installation MUST be in accordance with the instructions in this manual.

Therefore:

- DO NOT deviate from the procedures described in this manual.
- DO NOT assume any details not shown in this manual.
- DO NOT modify any electrical or mechanical features.
- DO comply with all codes and standards set forth by the Authority Having Jurisdiction.

The term “Authority Having Jurisdiction” has become a standard term in the fire alarm industry. An acceptable definition of “Authority Having Jurisdiction” is:

Fire alarm systems installed in the USA fall under the jurisdiction of some authority. In some areas, this may be a local fire department; in other areas, it may be a building inspector, insurance firm, etc. Different authorities may have their own local requirements for the way the fire alarm system is installed and used. Most local authorities based their requirements on the NFPA (National Fire Protection Association) codes, but there may be important differences. You must install this system in the way in which the Authority Having Jurisdiction requires. If you do not know which authority has jurisdiction in your area, contact your local fire department or building inspector for guidance.

It is important that you tell users to be aware of any requirements defined by the Authority Having Jurisdiction.

The installation MUST be in accordance with the following standards:

- National Fire Alarm Code (NFPA 72)
- National Electrical Code (NFPA 70)
- Life Safety Code (NFPA 101)

WARNING: Touching components, which are improperly installed, applied or operated, could be hazardous and possibly fatal. Short circuits could cause arcing that could result in molten metal injuries. Therefore, only qualified technicians familiar with electrical hazards should perform checkout procedures. Safety glasses should be worn, and test equipment used for voltage measurements should be designed for this purpose and be in good working order.

ENVIRONMENTAL CONSIDERATIONS

It is important that this equipment be operated within its specifications: Recommended operating temperature range: 0°C to 49°C (32°F to 120°F) and at a relative humidity 93% ± 2% RH (non-condensing) at 32°C ± 2°C (90°F ± 3°F).

INSTALLATION CONSIDERATIONS

Check that you have all the equipment you need to complete the installation. Follow the field wiring diagrams and installation notes in this manual.

Install the equipment in a clean, dry environment (minimal dust). Avoid installing the equipment where vibrations will occur.

Remove all electronic assemblies prior to drilling, filing, reaming, or punching the enclosure. When possible, make all cable entries from the side, being careful to separate the power-limited conductors from the non power-limited conductors. Before making modifications, verify that they will not interfere with battery, transformer, and printed circuit board location.

Do not over tighten screw terminals. Over tightening may damage threads, resulting in reduced terminal contact pressure and difficulty with screw terminal removal.

Disconnect all sources of power before servicing, removing, or inserting any circuit board. Control unit and associated equipment may be damaged by removing and/or inserting cards, subassemblies, or interconnecting cables while the unit is energized.

FocalPoint is a trademark of Honeywell International.

WIRING CONSIDERATIONS

A Gamewell/FCI fire alarm control panel contains power-limited circuits. You cannot connect external sources of power to these circuits without invalidating their approval.

Verify that wiring sizes are adequate for all initiating device and notification appliance circuits. Most devices cannot tolerate more than a 10% drop from the specified voltage.

The installer must ensure that the wiring and devices installed in the system meet the current National Electrical Code, NFPA 70, and all applicable state and local building code requirements.

Use the conductor size and type required by local codes (see NFPA 70, Article 760). Wiring resistance must not be more than that shown on the field wiring diagrams.

To reduce errors and help in servicing the system, all conductors should be labeled or otherwise coded and logged at installation to identify circuit assignment and polarity. If the conductors are logged with a code, keep the log that explains the code with the manual, so that it is available to other people working on the panel.

Like all solid state electronic devices, this system may operate erratically or be damaged when subjected to lightning induced transients. Although no system is completely immune to lightning transients and interference, proper grounding will reduce susceptibility. Gamewell/FCI does not recommend the use of overhead or outside aerial wiring due to the increased susceptibility to nearby lightning strikes. Consult with the Gamewell/FCI Technical Support Department if any problems are anticipated or encountered.

To prevent the spread of fire, use proper patching materials to areas where system wiring passes through fire-rated walls or floors.

SURVIVABILITY

Per the National Fire Alarm Code, NFPA 72, all circuits necessary for the operation of the notification appliances shall be protected until they enter the evacuation signaling zone that they serve. Any of the following methods shall be considered acceptable as meeting these requirements:

- A two-hour rated cable or cable system.
- A two-hour rated enclosure.
- Performance alternatives approved by Authority Having Jurisdiction.

MAINTENANCE

To keep your fire alarm system in excellent working order, ongoing maintenance is required per the manufacturer's recommendations and UL and NFPA Standards, and applicable state and local codes. At a minimum, the requirements of Chapter 7 of NFPA, the National Fire Alarm Code, shall be followed. A preventative maintenance agreement should be arranged through the manufacturer's local representative. Though smoke detectors are designed for long life, they may fail at any time. Any smoke detector, fire alarm system, or any component of that system shall be repaired or replaced immediately.

SYSTEM RE-ACCEPTANCE TEST

To ensure proper system operation, this product must be tested in accordance with NFPA 72, Chapter 7. Re-acceptance testing is required after any modification, repair, or adjustment to system hardware, wiring, or programming.

All components, circuits, or system operations known to be affected by a change must be 100% tested. In addition, to ensure that other operations are not inadvertently affected, at least 10% of initiating devices that are not directly affected by the change, up to a maximum of 50 devices, must also be tested and proper system operation verified.

Equipment used in the system may not be technically compatible with the control panel. It is essential to use only equipment Listed for service with the control panel.

OTHER CONSIDERATIONS

The equipment was tested according to EC directive 89/336/EEC for Class A equipment and was verified to the limits and methods of EN 55022. FCC WARNING: This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for Class A computing devices pursuant to Subpart B of Part 15 of FCC Rules, which is designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his own expense.

If these instructions are not clear, or if additional information or clarification is needed, please consult your local authorized Gamewell/FCI distributor.

Because of design changes and product improvements, the information in this manual will be subject to change without notice. Gamewell/FCI reserves the right to change hardware and/or software design, which may subsequently affect the contents of this manual. Gamewell/FCI assumes no responsibility for any errors that may appear in this manual.

Neither this manual nor any part of it may be reproduced without the advance written permission of Gamewell/FCI.

LIMITATIONS OF FIRE ALARM SYSTEMS

Gamewell/FCI recommends that smoke and/or heat detectors be located throughout the protected premises following the recommendations of the current edition of the National Fire Protection Association Standard 72, the National Fire Alarm Code (NFPA 72), manufacturer's recommendations, State and local codes, and the recommendations contained in the Guide for the Proper Use of System Smoke Detectors, which is made available at no charge to all installing dealers. A study by the Federal Emergency Management Agency (an agency of the United States government) indicated that smoke detectors may not go into alarm or give early warning in as many as 35% of all fires. While fire alarm systems are designed to provide warning against fire, they do not guarantee warning or protection against fire. Any alarm system is subject to compromise or failure to warn for a variety of reasons. For example:

Particles of combustion or "smoke" from a developing fire may not reach the sensing chambers of a smoke detector because:

- Barriers such as closed or partially closed doors, walls, or chimneys may inhibit air flow.
- Smoke particles may become "cold" and stratify, and may not reach the ceiling or upper walls where detectors are located.
- Smoke particles may be blown away from detectors by air outlets.
- Smoke particles may be drawn into air returns before reaching the detector.

In general, smoke detectors on one level of a structure cannot be expected to sense fires developing on another level.

The amount of "smoke" present may be insufficient to alarm smoke detectors. Smoke detectors are designed to alarm at various levels of smoke density. If such density levels are not created by a developing fire at the location of detectors, the detectors will not go into alarm.

Smoke detectors, even when working properly, have sensing limitations. Detectors that have photo-electronic sensing chambers tend to detect smoldering fires earlier than flaming fires, which have little visible smoke. Detectors that have ionization-type sensing chambers tend to detect fast flaming fires earlier than smoldering fires. Because fires develop in different ways and are often unpredictable in their growth, neither type of detector is necessarily best and a given type of detector may not provide adequate warning of a fire.

Smoke detectors are subject to unwanted or nuisance alarms. For example, a smoke detector located in or near a kitchen may go into nuisance alarm during normal operation of kitchen appliances. In addition, dusty or steamy environments may cause a smoke detector to alarm unnecessarily. If the location of a smoke detector causes an abundance of unwanted or nuisance alarms, do not disconnect the smoke detector; call a professional to analyze the situation and recommend a solution.

Smoke detectors cannot be expected to provide adequate warning of a fire caused by arson, children playing with matches (especially in bedrooms), smoking in bed, violent explosions (caused by escaping gas, improper storage of flammable materials, etc.).

Heat detectors do not sense particles of combustion and are designed to alarm only when heat on their sensors increase at a predetermined rate or reaches a predetermined level. Heat detectors are designed to protect property, not life.

Warning devices (including horns, sirens, bells, and speakers) may not alert people or awaken sleepers who are located on the other side of closed or partially open doors. A warning device that activates on a different floor or level of a dwelling or structure is less likely to awaken or alert people. Even persons who are awake may not notice the warning if the alarm is muffled by noise from a stereo, radio, air conditioner or other appliance, or by passing traffic. Audible warning devices may not alert the hearing-impaired (strobes or other devices should be provided to warn these people). Any warning device may fail to alert people with a disability, deep sleepers, people who have recently used alcohol or drugs, or people on medication or sleeping pills.

Please note that:

- Strobes can, under certain circumstances, cause seizures in people with conditions such as epilepsy.
- Studies have shown that certain people, even when they hear a fire alarm signal, do not respond or comprehend the meaning of the signal. It is the property owner's responsibility to conduct fire drills and other training exercises to make people aware of the fire alarm signals and instruct on the proper reaction to alarm signals.
- In rare instances, the sounding of a warning device can cause temporary or permanent hearing loss.

Telephone lines needed to transmit alarm signals from a premise to a central station may be out of service or temporarily out of service. For added protection against telephone line failure, backup radio transmission systems are recommended.

System components, though designed to last many years, can fail at any time. As a precautionary measure, it is recommended that smoke detectors be checked, maintained, and replaced per manufacturer's recommendations.

System components will not work without electrical power. If system batteries are not serviced or replaced regularly, they may not provide adequate standby when AC power fails.

Environments with high air velocity or that are dusty or dirty require more frequent maintenance.

In general, fire alarm systems and devices will not work without power and will not function properly unless they are maintained and tested regularly.

While installing a fire alarm system may make the owner eligible for a lower insurance rate, a fire alarm system is not a substitute for insurance. Property owners should continue to act prudently in protecting the premises and the people on the premises and should properly insure life and property and buy sufficient amounts of liability insurance to meet their needs.

Table of Contents

Section 1 About Receivers Gateways

1.1 FPT Receivers Gateway Description

The Receivers Gateway (FPT-DACR-GW) acts as a bridge between the supported digital alarm receivers and the FocalPoint system. A Receivers Gateway processes information coming from a connected receiver and passes the information to FocalPoint components. A FocalPoint Workstation on the system will annunciate events from control panels to receivers using a DACT. Each Receivers Gateway is capable of monitoring up to 20 digital alarm receivers.

Supported receiver types are:

- ADEMCO 685.
- Radionics D6600.
- Silent Knight 9500/9800.
- Teldat VisorALARM.

Supported protocols for these receivers are:

- ADEMCO Contact ID.

Receivers connect to the Workstation using:

- A COM port on the Workstation’s computer.

1.2 FPT Receivers Gateway System Architecture

An FocalPoint system must have at least one capable UL or ULC listed computer, that is appropriate for use with fire protective signaling units with the FocalPoint Workstation software application installed.

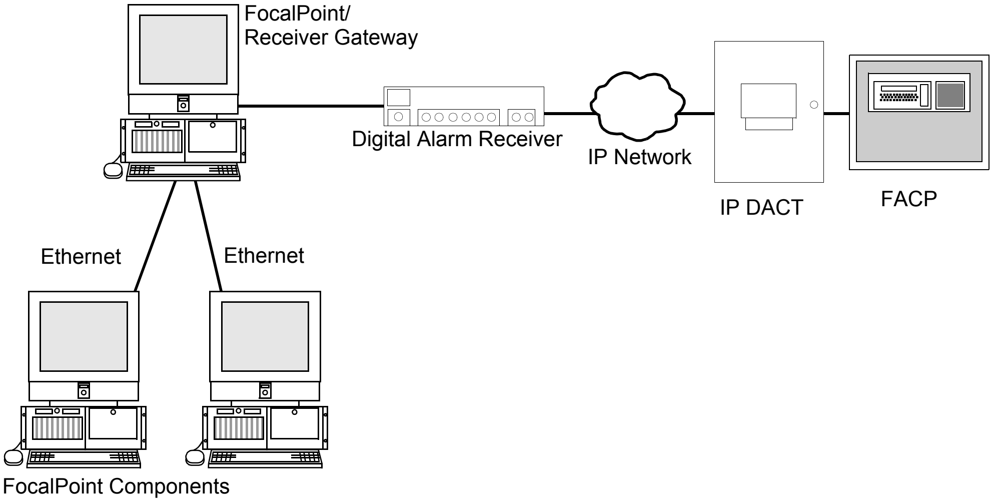


Figure 1.1 Receivers IP Network Architecture Diagram

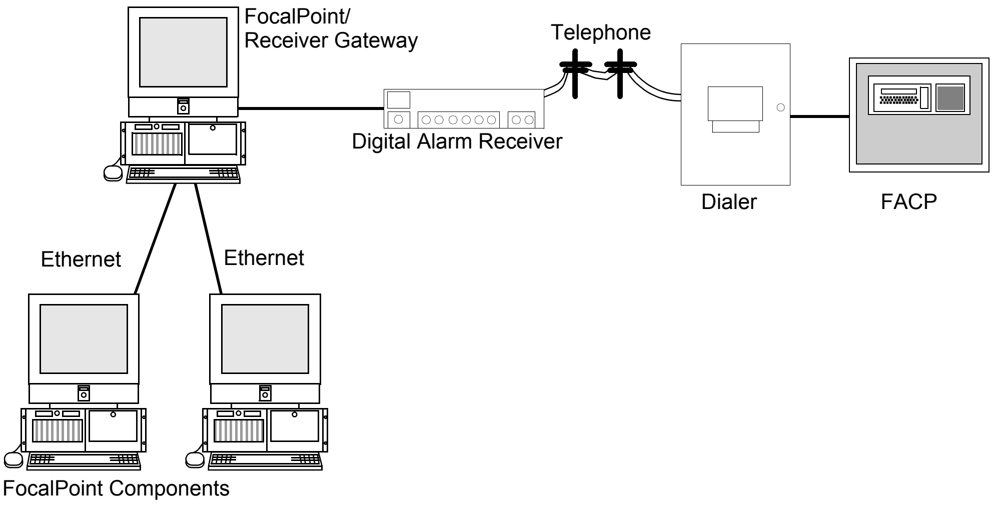


Figure 1.2 Receivers Telephone Architecture Diagram

1.3 Agency Listings

NOTE:
UL 864, 9th Edition—FocalPoint systems work with products that have been UL 864, 9th Edition listed as well as products that have not received UL 864, 9th Edition certification. Operation of systems that are comprised of equipment that is UL 864, 9th Edition listed together with products that are not UL 864, 9th Edition listed requires the approval of the local Authority Having Jurisdiction (AHJ).
CAN/ULC-S559-04, 1st Edition—FocalPoint systems work with products that have been CAN/ULC-S559-04, 1st Edition listed as well as products that have not received CAN/ULC-S559-04, 1st Edition certification. Operation of systems that are comprised of equipment that is CAN/ULC-S559-04, 1st Edition listed together with products that are not CAN/ULC-S559-04, 1st Edition listed requires the approval of the local Authority Having Jurisdiction (AHJ).

1.3.1 Compliance

This product has been investigated to, and found to be in compliance with the following standards.

National Fire Protection Association

- **NFPA 72**—National Fire Alarm Code

Underwriters Laboratories

- **UL-864**—Control Units for Fire Alarm Systems, Ninth Edition
- **UL-1076**—Proprietary Burglar Alarm Units and Systems, Fifth Edition
- **UL-2017**—General-Purpose Signaling Devices and Systems, First Edition

Underwriters Laboratories Canada

- **CAN/ULC-S527-99**—Standard for Control Units for Fire Alarm Systems, Second Edition
- **CAN/ULC-S559-04**—Equipment for Fire Signal Receiving Centres and Systems, First Edition

1.3.2 Installation

This product is intended to be installed in accordance with the following regulatory agencies.

Local

- **AHJ**—Authority Having Jurisdiction

National Fire Protection Association

- **NFPA 70**—National Electrical Code
- **NFPA 72**—National Fire Alarm Code
- **NFPA 101**—Life Safety Code

Underwriters Laboratories

- **UL-1076**—In certified applications, the unit shall be installed in accordance with Proprietary Burglar Alarm Units and Systems, Fifth Edition

Underwriters Laboratories Canada

- **CAN/ULC-S524-06**—Standard for the Installation of Fire Alarm Systems, Fifth Edition
- **CAN/ULC-S561-03**—Installation and Services for Fire Signal Receiving Centres and Systems, First Edition

Canada

- **CSA C22.1**—Canadian Electrical Code, Part I, Safety Standard for Electrical Installations

WARNING: Installation
Improper installation, maintenance, and lack of routine testing could result in system malfunction.

1.4 Environmental Requirements

This product must be installed in the following environmental conditions:

- Temperature range of 0°C to 49°C (32°F - 120°F).
- 93% humidity non-condensing at 30°C (86°F).

1.5 Related Documentation

The following is a list of documentation resources related to the FocalPoint system.

- *FocalPoint Gateway (P/N 52649)*
- *FocalPoint Workstation (P/N 52561)*
- *FocalPoint Configuration Tool (P/N 53381)*

NOTE: The contents of this manual are important and must be kept in close proximity of the Workstation. If building ownership is changed, this manual including all other testing and maintenance information must also be passed to the current owner of the facility. A copy of this manual was shipped with the equipment and is also available from the manufacturer.

Section 2 Digital Receivers Installation and Configuration

2.1 Digital Receiver Setup Guidelines

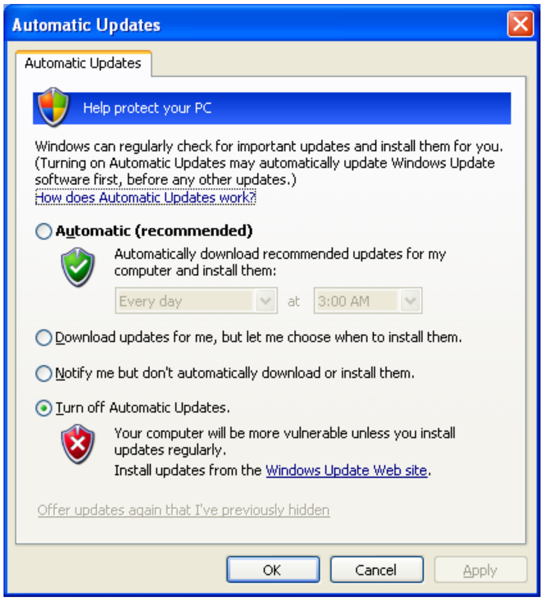
The supported Digital receivers must be installed according to the following guidelines:

- Receivers may be placed on a single Gateway or distributed among several.
- A receiver may be attached to any available COM port on a Receiver Gateway capable UL or ULC listed computer, that is appropriate for use with fire protective signaling units.
- Every device that calls a receiver must have an account code that uses a supported protocol.
- Each account code must be unique throughout the entire system.
- Each device or panel must utilize the monitored receiver's account code to which it reports.
- Multiple account codes per device are not supported.

2.1.1 Automatic Updates

NOTE: Automatic Updates must be turned **OFF** for the Receiver Gateway to function correctly.

To verify automatic updates are turned off, follow the path: Start > Control Panel > Security Center > Automatic Updates.



Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)
How does Automatic Updates work?

○ **Automatic (recommended)**

Automatically download recommended updates for my computer and install them:

Every day at 3:00 AM

○ Download updates for me, but let me choose when to install them.

○ Notify me but don't automatically download or install them.

● Turn off Automatic Updates.

Your computer will be more vulnerable unless you install updates regularly.
Install updates from the Windows Update Web site.

Offer updates again that I've previously hidden

You may still update your Windows operating system manually. To manually update Windows, open a web browser and go to http://www.update.microsoft.com/microsoftupdate/v6/default.aspx?.

2.2 ADEMCO 685 Setup

2.2.1 685 Cable Configuration

NOTE: All connections must be no more than 20 feet in length and run in conduit.

Use the following figure to configure the cable that connects the 685’s J103 port to a unused COM port on your Receiver Gateway capable Workstation computer.

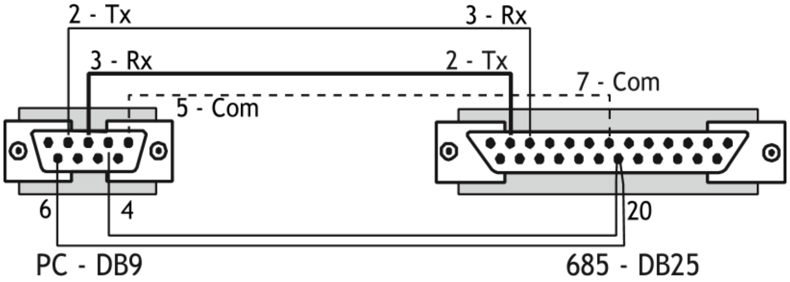


Figure 2.1 ADEMCO 685 Cable Connections

2.2.2 685 Jumper Settings

On the 685's memory card, make the following jumper settings:

- Jumper P7 - Pins 2 and 3 (Parallel Printer On).
- Jumper P10 - Pins 1 and 2 (With Computer).

2.2.3 685 DIP Switch Settings

Inside the ADEMCO 685 receiver there is a DIP switch; set the switches as:

- Switch 4: PRN-OFF - PRN (Off)
- Switch 8: OFF-COM - OFF (Off)

2.2.4 685 Supported Formats

The supported address format is ADEMCO Contact ID.

2.2.5 685 Parallel Printer Requirements

A parallel printer MUST remain connected to the 685 receiver at all times because it is used by the 685 to print the events it receives.

2.2.6 685 Communication Settings

From the Receivers Gateway main screen, single click on the desired receiver, then double click on the communication setting you wish to configure: Baud Rate=600, Parity=N, Data Bits=8 and Stop Bits=1.

2.2.7 685 Device Addressing and Supervision

The Receivers Gateway monitors a 685 receiver for trouble conditions and reports these events to Workstations as a pop-up window.

Once the ADEMCO 685 is connected to the Gateway, the Workstation will auto-create an icon for the 685 receiver. 685 site names will look similar to this: 685 DACR - #### (where #### is the account code for the panel that is dialing in).

685 panels generate a periodic test message. The Gateway uses that test message to supervise the site.

2.2.8 685 Device Addresses Reported by the Gateway

Device addresses reported by dialers on panels will vary when using the 685 receiver compared to panels monitored by NIONs. The reported format is dependent on the dialer format used and the native panel format. In most cases, the reported format will either match the native format or be very similar. In all cases field tests should be performed to confirm the reported format of panel devices.

2.2.9 685 Site IDs

When using dialers to communicate with the 685 receiver, each dialer is treated as an individual site. Therefore, each panel reporting through a dialer is reported as a standalone site. The site ID format is as follows: 685 DACR-*XXXX*, where *XXXX* is the three- or four-digit account code for the dialer. Example: Dialer account 24 would report as 685 DACR-0024.

2.2.10 685 Device IDs

The Gateway reformats all devices reported by the ADEMCO 685 receiver to fit the standard FocalPoint system format of an 8-character point ID:

NOTE: Since there is no actual node or sub-node located at the panel, the Gateway always pads the node/sub-node position with *001000*. Each device ID reported through the ADEMCO 685 receiver will begin this way. As described above, the 8-character device ID will depend on the native device format and the dialer format used.

2.3 Radionics D6600 Setup

Digital receivers must be installed according to the "Digital Receiver Setup Guidelines" on page 11.

2.3.1 D6600 Description

The Receivers Gateway is the software interface between the Radionics receiver and the FocalPoint network monitoring system. The Receivers Gateway redirects information from a remote site and displays alarm and trouble event information that can be used in conjunction with a Workstation and other FocalPoint clients. The Radionics D6600 receiver is a modular multi-format digital receiver designed to receive, display and route data received from the Internet or private Intranet. The system that is created between the Radionics receivers and the Receivers Gateway allows the Workstation to display events that use the 6500 Contact ID format.

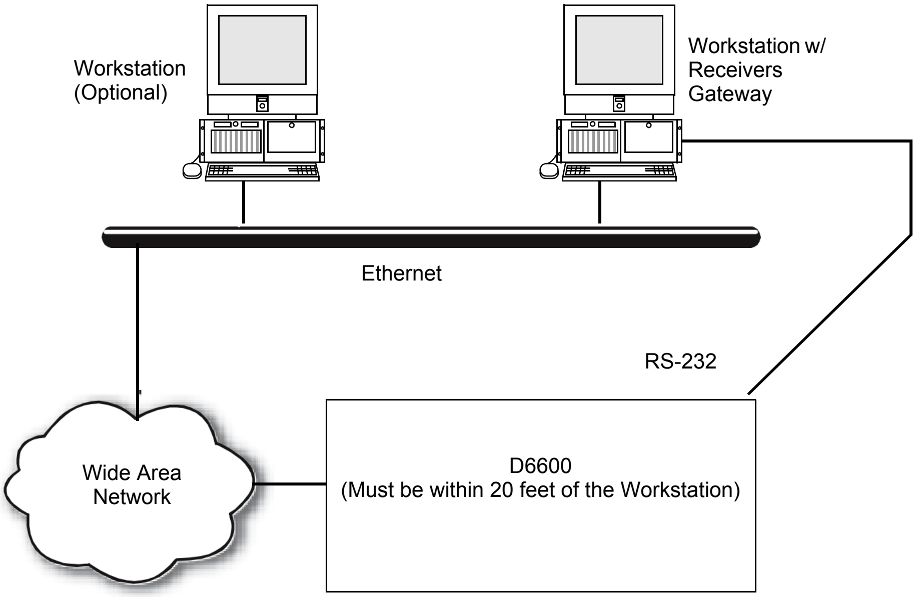

Workstation (Optional)
Workstation w/ Receivers Gateway
Ethernet
RS-232
Wide Area Network
D6600
(Must be within 20 feet of the Workstation)

Figure 2.2 Radionics D6600 Receiver Application Example

2.3.2 Supported Formats

The D6500 Mode ADEMCO Contact-ID Format is the supported address format.

2.3.3 D6600 Serial Communication Connection

Use the following figure to configure the cable that connects the Radionics D6600's COM3 port to a unused COM port on your Receiver Gateway capable Workstation computer. You can use a standard null modem cable to connect the Radionics D6600 to the Receivers Gateway.

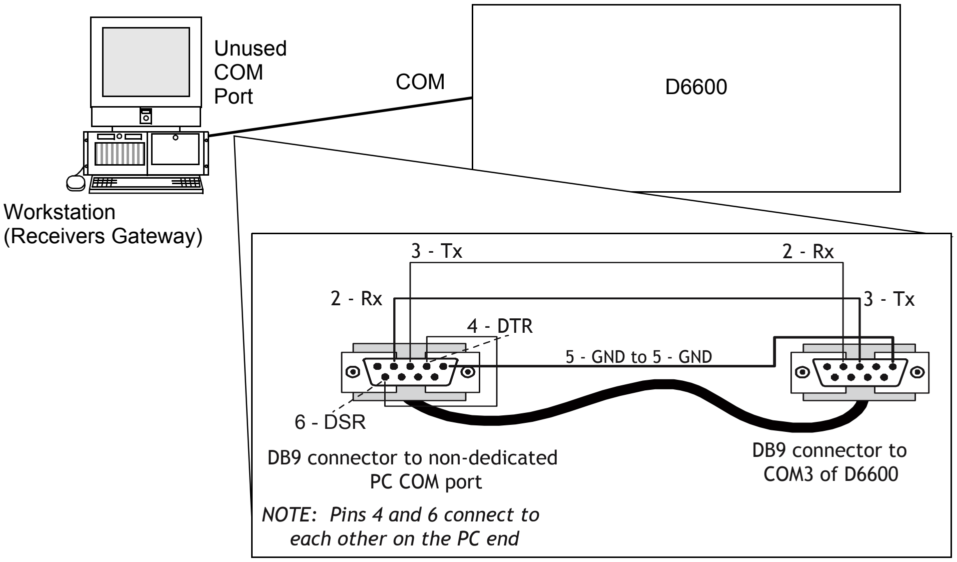


Figure 2.3 D6600 To Gateway Serial Connection

2.3.4 D6600 Setup

The default settings of the D6600 may be used with the following exception:

The Trailer (menu item 2.5.9 on the D6600) needs to be set to 0. Refer to the table below for D6600 settings. For more detailed information, see the Radionics D6600 Program Entry Guide.

Table 2.1 D6600/Receivers Gateway Configuration Settings

D6600 Menu Item	Menu Item Name/Description	D6600 Value for WAS Configuration
2.5.2	Baud	110 - 38400
2.5.3	Data Bit	8
2.5.4	Parity	0 - None
2.5.6	Link Test	30 seconds
2.5.7	Automation Wait	4 seconds
2.5.8	Header	00 No Header
2.5.9	Trailer	0D
2.5.15	Output Format	1 6500 format output
3.1.9.2	Receiver Type	0 Radionics
3.1.9.5	Output for Modem II/III Formats	0 Disable Network Automation Output
6.3.6	Network Automation Output Format	0 Disable Network Automation Output

Table 2.1 D6600/Receivers Gateway Configuration Settings

D6600 Menu Item	Menu Item Name/Description	D6600 Value for WAS Configuration
6.3.7	Device	2 - Utilize COM3 RS-232 Automation

2.3.5 D6600 Configuration

Device Addressing and Supervision

The Receivers Gateway monitors digital alarm receivers for trouble conditions and reports these events to Workstations. Once the receiver is connected to the Receivers Gateway, the Workstation will auto-create an icon for the receiver.

Receiver Site Names and Supervision

When using dialers to communicate with the Radionics D6600 receiver, each dialer is treated as an individual site. Therefore, each panel reporting through a dialer is reported as a standalone site. Site names will look similar to this: D6600 - #### (where #### is the account code for the panel that is dialing in). Example: Dialer account 24 would report as D6600-0024.

Receiver sites are supervised by the Workstation. Panels connected to receivers generate a periodic test message. The Receivers Gateway uses that test message to supervise the site. In the Gateway's configuration window, Site supervision hours are set at 24 hours and it can not be changed in the gateway.

Heartbeat/Link Test

The Heartbeat and link test are the same thing. The Radionics D6600 sends a message to the Receivers Gateway every 30 seconds. The Gateway then sends a reply back to the D6600. This message allows the Gateway to determine if the D6600 is present (if it receives the message within 45 seconds, then the D6600 is OK). The D6600 knows that the Receivers Gateway is OK if it received the Gateway's reply to the message that it sent.

2.3.6 D6600 Operation and Event Handling

Device Addresses as Reported via the Receivers Gateway

Device addresses reported by dialers on panels will vary when using receivers compared to panels monitored by NIONs. The reported format is dependent on the dialer format used and the native panel format. In most cases, the reported format will either match the native format or be very similar. In all cases, field tests should be performed to confirm the reported format of panel devices.

Device IDs

The Receivers Gateway reformats all devices reported by Radionics D6600 receivers to fit the standard system format of an 8-character point ID.

Because there is no actual node or sub-node located at the panel, the Receivers Gateway always pads the node/sub-node positions with zero spacers (001000). Each device ID reported through the receiver will begin this way. As described above, the 8-character device ID will depend on the event and device.

Event Handling and Multiple Instances of an Event

An event reported from account number *XXXX* will have the same device ID in the FocalPoint system, regardless of the Receivers Gateway or receiver that reported the event to the Gateway. If the same event from the same point at the same account number is reported to other Receivers Gateways, the Gateway will disregard the second instance of the event.

2.4 Silent Knight 9500/9800 Receiver Setup

A Receiver Gateway capable Workstation is capable of monitoring 10 Silent Knight 9500/9800 digital alarm receiver's devices reporting alarm and trouble information. Digital receivers must be installed according to the "Digital Receiver Setup Guidelines" on page 11.

2.4.1 9500/9800 Cable Configuration

NOTE: All connections must be no more than 20 feet in length and run in conduit.

Use the following figure to configure the serial cable running from the automation port of the receiver to a non-dedicated COM port of the PC on which the Receivers Gateway is running:

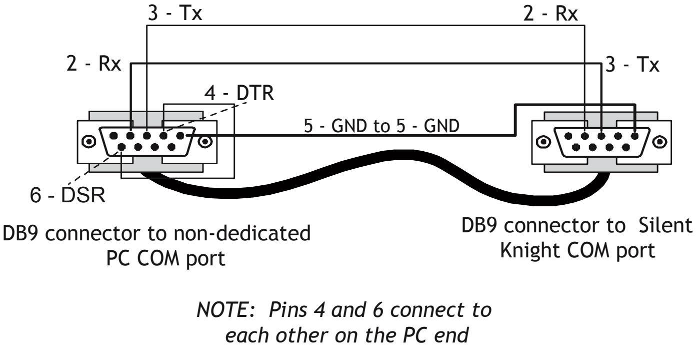

3 - Tx
2 - Rx
2 - Rx
3 - Tx
4 - DTR
5 - GND to 5 - GND
6 - DSR
DB9 connector to non-dedicated PC COM port
DB9 connector to Silent Knight COM port
NOTE: Pins 4 and 6 connect to each other on the PC end

Figure 2.4 Silent Knight Serial Cable Pinouts

2.4.2 9500/9800 Supported Formats

The following format is supported:

- ADEMCO Contact ID
- Receiver Settings and Configuration

2.4.3 9500/9800 Receiver Settings

Table 2.2 Silent Knight/Receivers Gateway Configuration Settings

Configuration Feature	Value
Receiver Operation Mode	Automatic
CID Format Display Option	Code
Automation Port Communication Settings	
Baud Rate	600
Data Bits	8
Parity	None
Stop Bits	1
Port Monitor	No
Flow Control	None
Automation Configuration Settings	
Format	ADEMCO685
Heartbeat	No
Ack Timeout	15
Ack	06

2.4.4 9500/9800 Device Addressing and Supervision

The Receivers Gateway monitors digital alarm receivers for trouble conditions and reports these events to Workstations in a pop-up dialog box. Once the receiver is connected to the Gateway, the Workstation will auto-create an icon for the receiver.

2.4.5 9500/9800 Site IDs

When using dialers to communicate with the Silent Knight 9500/9800 receiver, each dialer is treated as an individual site. Therefore, each panel reporting through a dialer is reported as a standalone site. Site names will look similar to this: SK9500 - #### or SK9800 - #### (where #### is the account code for the panel that is dialing in). Example: Dialer account 24 would report as SK9500 - #### or SK9800 - ####.

Receiver sites are supervised by the Workstation. Panels connected to receivers generate a periodic test message. The Receivers Gateway uses that test message to supervise the site. In the Gateway's configuration window. Site supervision hours are set at 24 hours and it can not be changed in the gateway.

2.4.6 9500/9800 Device Addresses Reported by the Gateway

Device addresses reported by dialers on panels will vary when using receivers compared to panels monitored by NIONs. The reported format is dependent on the dialer format used and the native panel format. In most cases the reported format will either match the native format or be very similar. In all cases field tests should be performed to confirm the reported format of panel devices.

2.4.7 9500/9800 Device IDs

The Receivers Gateway reformats all devices reported by Silent Knight 9500/9800 receivers to fit the FocalPoint system format of an 8-character point ID.

Since there is no actual node or sub-node located at the panel, the Gateway always pads the node/ sub-node position with zero spacers (001000). Each device ID reported through the receiver will begin this way. As described above, the 8-character device ID will depend on the native device format and the dialer format used.

2.5 Teldat VisorALARM Receiver Setup

VisorALARM is an IP Receiver which can receive event messages via IP networks from configured IP digital alarm control transmitters (IPDACTs).

2.5.1 VisorALARM Cable Configuration

NOTE: All connections must be no more than 20 feet in length and run in conduit.

Use the following figure to configure the cable that connects the receiver to a unused COM port on your Receiver Gateway capable Workstation computer.

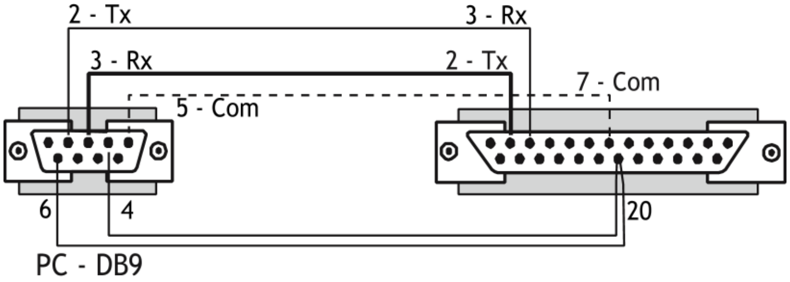


Figure 2.5 VisorALARM Cable Connections

2.5.2 VisorALARM Serial Communication Connection

The VisorALARM also connects via an Ethernet cable into the intranet where it can receive events from any programmed IPDACT registered with the receiver.

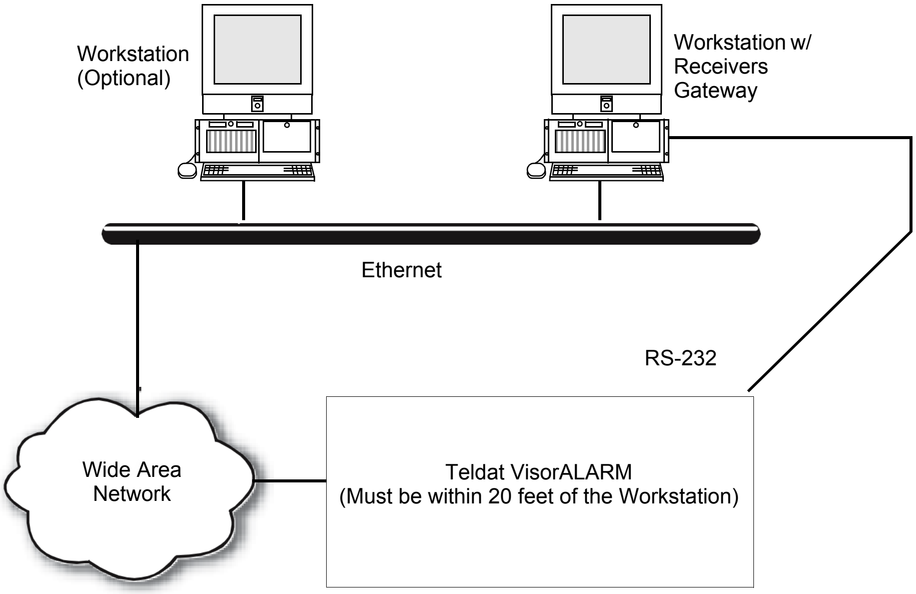


Figure 2.6 Teldat VisorALARM Receiver Application Example

2.5.3 VisorALARM Configurations

There are some configurations that need to be made to setup the receiver and the IPDACTs refer to the receiver's documentation for those details.

2.5.4 VisorALARM Supported Formats

The following format is supported:

- ADEMCO Contact ID.

2.5.5 VisorALARM Communication Settings

Recommended as Baud Rate=9600, Parity=N, Data Bits=8 and Stop Bits=1.

2.5.6 VisorALARM Device Addressing and Supervision

Receivers Gateway monitors the VisorALARM for trouble conditions and reports them to connected Workstations. The Workstation will auto-create an icon for this receiver, and will display as VisorALARM - #### (where #### is the account number). Also the VisorALARM sends a periodic heartbeat in which the Receivers Gateway supervises the connection to the receiver.

2.5.7 Device Addresses Reported

Point type addresses vary.

Site ID

VisorALARM Site IDs display as VisorALARM - ####.

Device ID

VisorALARM point IDs will be an 8-character device ID (XXXXXXXX) and their format depends on the point type.

Section 3 Receivers Gateway Installation and Configuration

3.1 Receivers Gateway Installation Overview

NOTE: The Workstation and FPT Receivers Gateway must be logged into before any of its settings can be configured. A User that has the Security Option to configure settings needs to login to change an existing setting. The factory defined User "Admin" has such an Security Option. Information in this document is written assuming that a User with the equivalent Security Option of the "Admin" User will be performing the procedures in this document.

The sequence in which these tasks are performed is determined by the Admin User performing them and this list is a suggested guideline.

1. Install Receivers in desired locations (refer to individual Receiver manuals).
2. Setup these supported digital receiver(s).
   - "ADEMCO 685 Setup" on page 12.
   - "Radionics D6600 Setup" on page 14.
   - "Silent Knight 9500/9800 Receiver Setup" on page 17.
   - "Teldat VisorALARM Receiver Setup" on page 20.
3. Start the FocalPoint Workstation software applications. Refer to "Workstation Startup" on page 23 and "Receivers Gateway Startup" on page 24.
4. Use the Receivers Gateway to configure network communications settings. Refer to "Receivers Gateway Network Communication Configuration" on page 24.

System Limitations

Each instance of the Receivers Gateway can support a maximum of 20 receivers.

3.2 Workstation Startup

Refer to the Workstation manual or to "Login" on page 28 for more details.

Step 1. Select Start > >All Programs >Facilities Monitoring >Workstation.

Step 2. From the Workstation menu bar select File > Login. The User Login window displays.

Step 3. Click on a User name with system administrator privileges.

Step 4. Type the user's password into the Password field and then click OK.

3.3 Receivers Gateway Startup

Step 1. Double click on the Receivers Gateway icon in the Windows system tray. The Receivers Gateway window displays.

Step 2. From the Receivers Gateway window select File >Login. The User Login window displays.

Step 3. Click on a User name in the Available Users list.

Step 4. Type in the User's password in the password field, and then click OK. The login will log in the current user at their assign Security Profile access level. Refer to the Workstation manual for details about Security Profiles.

3.3.1 Closing and Shutting Down the Gateway

- File >Close will minimize the Receivers Gateway screen; the Receivers Gateway is still running, and its icon appears in the System Tray.
- File >Shut Down Gateway will shut down the Receivers Gateway running on the current Workstation. Meaning the Gateway will no longer display events of panels connected.

3.4 Receivers Gateway Network Communication Configuration

These are the configuration settings to be specified for a Receivers Gateway that will be connected and communicating over the FocalPoint network:

- IP address of Gateway (set in the Workstation)
- Port Configuration (set for each receiver from the Receivers Gateway user interface)

3.4.1 Establish Receivers Gateway/Workstation Communication

Each instance of a Receivers Gateway must be configured in the Workstation for events to be annunciated properly.

3.4.2 Receivers Gateway's Port Configuration

The Admin User creates a Network name and then adds a gateway. Network Names and gateway connections are created using the Configuration Tool which is launched from Workstation's main menu

Network Connection Configuration Procedure

Step 1. Login to the Workstation.

Step 2. Launch the Configuration Tool from the Workstation's Main Menu (select Configure >Launch Configuration Tool). The Network Configuration window displays.

Step 3. Select Network >Add Network... The Network Properties window displays.

Step 4. Type in the network's name into the Alias field.

Step 5. Select the Type down arrow and select the type of network from the list of choices.

Step 6. Click on the Gateway Connection field's Add Gateway icon (mouse over). The Gateway Properties window displays.

Step 7. Add the gateway using one of the following:

- Type in the Gateway's IP Address.
- Select a gateway from the list of Online Gateways.

Step 8. Click on the OK button.

Step 9. Exit the Configuration Tool and respond to the confirmation window prompt. Yes means the database will be updated.

Once the Gateway is configured in the Receivers Gateway from the Workstation, individual receivers can now be configured.

Receiver Gateway's Ports Configuration Procedure

Step 1. Verify that all receivers are connected to one of the Workstation computer's COM ports.

Step 2. Select the appropriate Receiver or Port to configure from the Connections list.

Step 3. In the Receiver Type Value field select your receiver type from the drop down menu. Refer to the setup information for the following supported digital receivers:

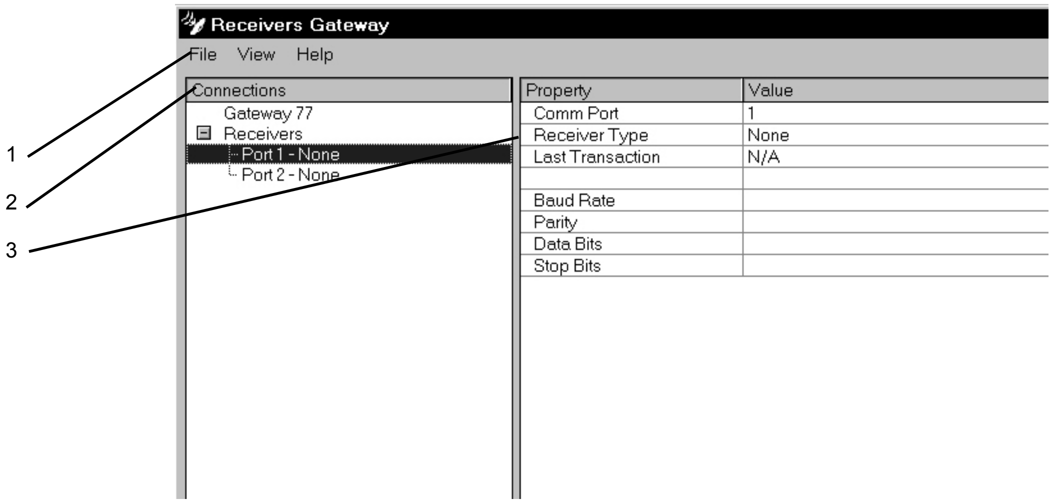
- "ADEMCO 685 Setup" on page 12.
- "Radionics D6600 Setup" on page 14.
- "Silent Knight 9500/9800 Receiver Setup" on page 17.
- "Teldat VisorALARM Receiver Setup" on page 20

Step 4. Verify the preset Baud rate, Parity, Data Bits, and Stop Bits all of which contain the pertinent digital receiver's default values. Digital Alarm Control Receiver values and Receivers Gateway values must be the same value. It is not recommended that different values be used unless directed to do so by technical services personnel.

Section 4 Receivers Gateway Reference Information

4.1 Layout of the Receivers Gateway Window

The Receivers Gateway allows a FocalPoint Workstation to view events and other data originating from digital alarm control receivers. Events that occur on connected digital alarm control receivers's devices will be reported to the Workstation and appear in the Events Box like any other FocalPoint system event. Refer to the FocalPoint Workstation manual for details concerning the Events Box and event handling of the FocalPoint system.



Connections

- Gateway 77
- Receivers
  - Port 1 - None
  - Port 2 - None

Property	Value
Comm Port	1
Receiver Type	None
Last Transaction	N/A
Baud Rate	
Parity	
Data Bits	
Stop Bits	

Figure 4.1 Receivers Gateway Configuration Window

1. The Main Menu that has drop-down style menus.
2. The Connection section lists all receivers on the network, including the node number and a user defined node description if it was specified.
3. The Property/Value section displays details about the selected item highlighted in the Connections list.

4.2 File Menu Descriptions

4.2.1 Login

The Workstation or FPT Receivers Gateway software applications must be logged into before any of its settings can be configured. A User that has the Security Profile to change a password needs to login to change an existing User's password or to add a User and their password. The factory defined User "Admin" has such an access level.

Factory default Workstation software application passwords have been created for the factory defined User profiles. Factory defined User profiles can not be deleted.

User Name	Password
Admin	admin
Default	default

Step 1. Select Start >Facilities Monitoring >FPT Receivers Gateway. The FPT Receivers Gateway window displays.

Step 2. From its menu select File > Login. The User Login window displays.

Step 3. Click-on to highlight a user name that has appropriate user privileges.

Step 4. Type in that user's password into the Password field and then click OK.

4.2.2 Close

Minimizes the Receivers Gateway interface and places its icon in the Window system. The connected devices will continue to report events to the Workstation(s).

4.2.3 Shut Down Gateway

Shuts down the Receivers Gateway and will not report events to the Workstation from any of the connected digital alarm control receivers.

4.3 View Menu Descriptions

View Clients - displays all network connections and is updated every second as long as it is open.

4.4 Help Menu Descriptions

About - displays the application's splash screen displaying *version information*.

Appendix A: Radionics D6600 Internal Message Mapping

The following table displays what messages will look like in the History Manager database:

Table A.1 Radionics D6600 Internal Message Mapping

Event	Zone	Description	Action
X	2	TIME SET	Recorded in the history database as D6600 %DACR% TIME SET
X	9	BATTERY MISSING	Report as event Trouble on device BATT with device type Battery
X	11	BATTERY LOW	Report as event Battery Low on device BATT with device type Battery
X	12	BATTERY RESTORE	Report as event Return To Normal (Spc) on device BATT with device type Battery
X	13	AC FAIL	Report as event AC Power Failure on device ACPWR with device type Power Supply
X	14	AC RESTORE	Report as event AC Power Restored on device ACPWR with device type Power Supply
X	45	REMOTE PARM PROGRAM IN	Report as event Program Entry on device PROG with device type Processor
X	46	REMOTE PARM PROGRAM OK	Report as event Program Exit on device PROG with device type Processor
X	47	REMOTE SOFTWARE PROGRAM IN	Report as event Program Entry on device PROG with device type Processor
X	48	REMOTE SOFTWARE PROGRAM SUCCESS	Report as event Program Exit on device PROG with device type Processor
X	49	REMOTE PROGRAM FAILURE	Report as event Program Exit on device PROG with device type Processor
X	21	EXTERNAL PRINTER ERROR	Report as event Trouble on device EXTPRN with device type Printer
X	22	EXTERNAL PRINTER RESTORE	Report as event Trouble Restored on device EXTPRN with device type Printer
B		BUSY SECONDS %ACC%%	Recorded in the History database as D6600 %DACR% BUSY SECONDS %ACC%%
X	30	COMPUTER ERROR	Report as event Fault Condition on device COMPUTER with device type Communication
X	33	UPS AC FAIL	Report as event Trouble on device UPSACPWR with device type Power Supply
X	34	UPS AC RESTORE	Report as event Trouble Restored on device UPSACPWR with device type Power Supply
X	35	UPS BATTERY LOW	Report as event Battery Low on device UPSBATT with device type Battery
X	36	UPS BATTERY RESTORED	Report as event Battery OK on device UPSBATT with device type Battery

Table A.1 Radionics D6600 Internal Message Mapping (Continued)

Event	Zone	Description	Action
X	37	SYSTEM RESET	Report as event Reset on device RECEIVER with device type Network Device
X	39	SYSTEM TEMPERATURE HIGH	Report as event Trouble on device TEMP with device type Temperature Sensor
X	40	TEMPERATURE RESTORE	Report as event Trouble Restored on device TEMP with device type Temperature Sensor
X	5	PHONE LINE FAULT %LINE%	Report as event Fault Condition on device LINE%LINE% with device type Telephone
X	6	PHONE LINE RESTORE %LINE%	Report as event Fault Condition Restored on device LINE%LINE% with device type Telephone
X	7	LINE CARD TROUBLE %LINE%	Report as event Trouble on device CARD%LINE% with device type Communication
X	8	LINE CARD RESTORE %LINE%	Report as event Trouble Restored on device CARD%LINE% with device type Communication
*		AUDIO IN %LINE%	Report as event Offline on device AUDIO%LINE% with device type Audio System
L		AUDIO DONE %LINE%	Report as event Offline Restored on device AUDIO%LINE% with device type Audio System
X	62	DATA ERROR %LINE%	Report as event Advise on device E62 L%LINE% with device type Telephone
X	62	NO DATA RECEIVED %LINE%	Report as event Advise on device E63 L%LINE% with device type Telephone
X	64	RESET %LINE%	Report as event Reset on device LINE%LINE% with device type Telephone
P		PRIVATE CALL %LINE%	Recorded in the history database as D6600 %DACR% PRIVATE CALL %LINE%
N		NO CALL NUMBER %LINE%	Recorded in the history database as D6600 %DACR% NO CALL NUMBER %LINE%
U		CALLER UNKNOWN %LINE%	Recorded in the history database as D6600 %DACR% CALLER UNKNOWN %LINE%
X	51	DATE SET	Recorded in the history database as D6600 %DACR% DATE SET
X	52	TWO WAY AUDIO STOP	Recorded in the history database as D6600 %DACR% TWO WAY AUDIO STOP
X	54	NETWORK TROUBLE	Report as event Trouble on device NETWORK with device type Network Device
X	55	NETWORK RESTORE	Report as event Trouble Restored on device NETWORK with device type Network Device
X	56	COMMUNICATIONS FAILURE	Report as event Trouble on device 00100COMM with device type Communication

Table A.1 Radionics D6600 Internal Message Mapping (Continued)

Event	Zone	Description	Action
X	57	COMMUNICATIONS RESTORED	Report as event Trouble Restored on device 00100COMM with device type Communication
X	88	SWITCH TO INTERCEPT MODE	Recorded in the history database as D6600 %DACR% SWITCH TO INTERCEPT MODE
X	81	SWITCH TO FALLBACK MODE	Recorded in the history database as D6600 %DACR% SWITCH TO FALLBACK MODE
X	83	DISABLE INTERCEPT MODE	Recorded in the history database as D6600 %DACR% DISABLE INTERCEPT MODE
X	84	ACTIVATE OUTPUT	Report as event Addressable Output On on device OUT1 with device type Common Generic Control Output
X	86	DEACTIVATE OUTPUT	Report as event Addressable Output Off on device OUT1 with device type Common Generic Control Output
X	59	C900 REBOOT	Report as event Reset on device C900 with device type Panel Internal Devices
X	58	C900 BATTERY LOW	Report as event Battery Low on device C900BATT with device type Battery
X	68	C900 BATTERY RESTORE	Report as event Battery OK on device C900BATT with device type Battery
X	87	C900 SWITCHED TO INTERCEPT	Report as event Device Re-enabled on device C900INTR with device type Communication
X	82	C900 SWITCHED TO FALLBACK	Report as event Device Disabled on device C900INTR with device type Communication
X	85	C900 OUTPUT ACTIVATED	Report as event Addressable Output On on device C900OUT1 with device type Common Generic Control Output
X	94	C900 OUTPUT DEACTIVATED	Report as event Addressable Output Off on device C900OUT1 with device type Common Generic Control Output
X	89	C900 INPUT SHORTED	Report as event Short Circuit on device C900IN1 with device type Digital Input
X	90	C900 INPUT OPEN	Report as event Open Circuit on device C900IN1 with device type Digital Input
X	91	C900 INPUT RESTORE	Report as event Return To Normal (Spc) on device C900IN1 with device type Digital Input
X	92	C900 INTERCEPT ENABLED	Report as event Device Re-enabled on device C900INTR with device type Communication
X	93	C900 INTERCEPT DISABLED	Report as event Device Disabled on device C900INTR with device type Communication
X	71	NO ACKNOWLEDGMENT RECEIVED	Report as event Advise on device EVENT 71 with device type Communication
X	72	NOT DIALING	Report as event Advise on device EVENT 72 with device type Communication

Table A.1 Radionics D6600 Internal Message Mapping (Continued)

Event	Zone	Description	Action
X	73	DIALING ERROR	Report as event Advise on device EVENT 73 with device type Communication
X	74	NO RESPONSE TO HANDSHAKE	Report as event Advise on device EVENT 74 with device type Communication
X	75	NO RESPONSE TO ACK	Report as event Advise on device EVENT 75 with device type Communication
X	76	MESSAGE UNKNOWN	Report as event Advise on device EVENT 76 with device type Communication
X	77	INVALID MESSAGE	Report as event Advise on device EVENT 77 with device type Communication
X	95	30 MIN SINCE FALLBACK CMD	Recorded in the history database as D6600 %DACR% 30 MIN SINCE FALLBACK CMD

Appendix B: Contact ID Reporting Formats

The following table shows the Contact ID Reporting Formats for FocalPoint messages:

Table B.1 Contact ID Reporting Formats

Contact ID Event Code	Device message w/ Group=0 Device ID	Device message w/ Group>0 Device ID	User Message Device ID	Matrix Point Type	Event Description
100	ZONE ###	G##ZO###	GROUP##	Medical	Medical - #
101	ZONE ###	G##ZO###	GROUP##	Medical	Pendant Transmitter - #
102	ZONE ###	G##ZO###	GROUP##	Medical	Fail to report in - #
110	ZONE ###	G##ZO###	GROUP##	Zone	Fire Alarm - #
111	ZONE ###	G##ZO###	GROUP##	Conventional Smoke Detector	Smoke - #
112	ZONE ###	G##ZO###	GROUP##	Combo Detector	Combustion - #
113	ZONE ###	G##ZO###	GROUP##	Waterflow	Water flow - #
114	ZONE ###	G##ZO###	GROUP##	Heat Detector	Heat - #
115	ZONE ###	G##ZO###	GROUP##	Pullstation	Pull Station - #
116	ZONE ###	G##ZO###	GROUP##	Duct Detector	Duct - #
117	ZONE ###	G##ZO###	GROUP##	Flame Detector	Flame - #
118	ZONE ###	G##ZO###	GROUP##	Zone	Near Alarm - #
120	ZONE ###	G##ZO###	GROUP##	Panic Button	Panic Alarm - #
121	ZONE ###	G##ZO###	GROUP##	Zone	Duress - User #
122	ZONE ###	G##ZO###	GROUP##	Zone	Silent - #
123	ZONE ###	G##ZO###	GROUP##	Zone	Audible - #
124	ZONE ###	G##ZO###	GROUP##	Security	Duress - Access granted - #
125	ZONE ###	G##ZO###	GROUP##	Security	Duress - Egress granted - #
130	ZONE ###	G##ZO###	GROUP##	Security	Burglary - #
131	ZONE ###	G##ZO###	GROUP##	Zone	Perimeter - #
132	ZONE ###	G##ZO###	GROUP##	Zone	Interior - #
133	ZONE ###	G##ZO###	GROUP##	Zone	24-Hour - #
134	ZONE ###	G##ZO###	GROUP##	Zone	Entry/Exit - #
135	ZONE ###	G##ZO###	GROUP##	Zone	Day/night - #
136	ZONE ###	G##ZO###	GROUP##	Security	Outdoor - #

Table B.1 Contact ID Reporting Formats (Continued)

137	ZONE ###	G##ZO###	GROUP##	Tamper Switch	Tamper - #
138	ZONE ###	G##ZO###	GROUP##	Security	Near alarm - #
139	ZONE ###	G##ZO###	GROUP##	Security	Intrusion verifier - #
140	ZONE ###	G##ZO###	GROUP##	Zone	General Alarm - #
141	ZONE ###	G##ZO###	GROUP##	Loop	Polling loop open
142	ZONE ###	G##ZO###	GROUP##	Loop	Polling loop short
143	ZONE ###	G##ZO###	GROUP##	Control Panel	Expansion module failure - #
144	ZONE ###	G##ZO###	GROUP##	Security	Sensor tamper - #
145	ZONE ###	G##ZO###	GROUP##	Control Panel	Expansion module tamper - #
146	ZONE ###	G##ZO###	GROUP##	Security	Silent Burglary - #
147	ZONE ###	G##ZO###	GROUP##	Zone	Sensor Supervision - #
150	ZONE ###	G##ZO###	GROUP##	Zone	24 Hour Non-Burg - #
151	ZONE ###	G##ZO###	GROUP##	Gas Leak Detector	Gas detected - #
152	ZONE ###	G##ZO###	GROUP##	Leak Detector	Refrigeration - #
153	ZONE ###	G##ZO###	GROUP##	Heat Detector	Loss of heat - #
154	ZONE ###	G##ZO###	GROUP##	Waterflow	Water Leakage - #
155	ZONE ###	G##ZO###	GROUP##	Security	Foil Break - #
156	ZONE ###	G##ZO###	GROUP##	Zone	Day Trouble - #
157	ZONE ###	G##ZO###	GROUP##	Tank	Low bottled gas level - #
158	ZONE ###	G##ZO###	GROUP##	Temperature Sensor	High temp - #
159	ZONE ###	G##ZO###	GROUP##	Temperature Sensor	Low temp - #
161	ZONE ###	G##ZO###	GROUP##	Fan	Loss of air flow - #
162	ZONE ###	G##ZO###	GROUP##	Toxic Gas	Carbon Monoxide detected - #
163	ZONE ###	G##ZO###	GROUP##	Tank	Tank level - #
200	ZONE ###	G##ZO###	GROUP##	Zone	Fire Supervisory - #
201	ZONE ###	G##ZO###	GROUP##	Tank	Low water pressure - #
202	ZONE ###	G##ZO###	GROUP##	CO2 Sensor	Low CO2 - #
203	ZONE ###	G##ZO###	GROUP##	Gate Sensor	Gate valve sensor - #
204	ZONE ###	G##ZO###	GROUP##	Tank	Low water level - #
205	ZONE ###	G##ZO###	GROUP##	Fire Pump	Pump activated - #

Table B.1 Contact ID Reporting Formats (Continued)

206	ZONE ###	G##ZO###	GROUP##	Fire Pump	Pump failure - #
300	PANEL###	G##PA###	GROUP##	Control Panel	System Trouble
301	ACPWR###	G##AC###	GROUP##	Power Supply	AC Loss
302	BATT ###	G##BA###	GROUP##	Battery	Low system battery
303	PANEL###	G##PA###	GROUP##	Control Panel	RAM Checksum bad
304	PANEL###	G##PA###	GROUP##	Control Panel	ROM Checksum bad
305	PANEL###	G##PA###	GROUP##	Control Panel	System reset
306	PROG ###	G##PR###	GROUP##	Zone	Panel program changed
307	PANEL###	G##PA###	GROUP##	Control Panel	Self-test failure
308	PANEL###	G##PA###	GROUP##	Control Panel	System shutdown
309	BATT ###	G##BA###	GROUP##	Battery	Battery test failure
310	PANEL###	G##PA###	GROUP##	Control Panel	Ground fault - #
311	PANEL###	G##PA###	GROUP##	Battery	Battery Missing
312	ACPWR###	G##AC###	GROUP##	Power Supply	Power Supply Overcurrent - #
313	SRVC ###	G##SR###	GROUP##	Zone	Engineer Reset - User #
314	ACPWR###	G##AC###	GROUP##	Power Supply	Primary Power Supply Failure - #
320	RELAY###	G##RE###	GROUP##	Audible Output	Sounder/Relay - #
321	BELL1###	G##BE###	GROUP##	Common Bell Output	Bell 1
322	BELL2###	G##BE###	GROUP##	Common Bell Output	Bell 2
323	RELAY###	G##RE###	GROUP##	Common Generic Control Output	Alarm relay
324	RELAY###	G##RE###	GROUP##	Common Generic Control Output	Trouble relay
325	RELAY###	G##RE###	GROUP##	Common Generic Control Output	Reversing relay
326	NAC3 ###	G##NA###	GROUP##	Common Bell Output	Notification Appliance Ckt. 3
327	NAC4 ###	G##NA###	GROUP##	Common Bell Output	Notification Appliance Ckt. 4
330	PANEL###	G##PA###	GROUP##	Zone	System Peripheral - #
331	ZONE ###	G##ZO###	GROUP##	Loop	Polling loop open
332	ZONE ###	G##ZO###	GROUP##	Zone	Polling loop short
333	PANEL###	G##PA###	GROUP##	Panel Internal Devices	Exp. module failure - #
334	ZONE ###	G##ZO###	GROUP##	Repeater	Repeater failure - #
335	PRINT###	G##PR###	GROUP##	Printer	Local printer paper out

Table B.1 Contact ID Reporting Formats (Continued)

336	PRINT###	G##PR###	GROUP##	Printer	Local printer failure
337	ACPWR###	G##AC###	GROUP##	Power Supply	Exp. module DC loss - #
338	ACPWR###	G##AC###	GROUP##	Power Supply	Exp. module Low Batt - #
339	ACPWR###	G##AC###	GROUP##	Power Supply	Exp. module Reset - #
341	ACPWR###	G##AC###	GROUP##	Power Supply	Exp. module Tamper - #
342	ACPWR###	G##AC###	GROUP##	Power Supply	Exp. Module AC loss - #
343	ACPWR###	G##AC###	GROUP##	Power Supply	Exp. Module self-test fail - #
344	ZONE ###	G##ZO###	GROUP##	Panel Internal Devices	RF DACR Jam Detect - #
350	COMM ###	G##CO###	GROUP##	Communication	Communication
351	LINE1###	G##LI###	GROUP##	Telephone	Telco 1 fault
352	LINE2###	G##LI###	GROUP##	Telephone	Telco 2 fault
353	RFXMT###	G##RF###	GROUP##	Communication	LR Radio xmitter fault
354	COMM ###	G##CO###	GROUP##	Communication	Fail to communicate
355	RFSUP###	G##RF###	GROUP##	Communication	Loss of radio supervision
356	RFPOL###	G##RF###	GROUP##	Communication	Loss of central polling
357	ZONE ###	G##ZO###	GROUP##	Panel Internal Devices	LR Radio VSWR - #
358	DACR ###	G##DA###	GROUP##	Control Panel	Backup Receiver Down
370	ZONE ###	G##ZO###	GROUP##	Loop	Protection Loop - #
371	ZONE ###	G##ZO###	GROUP##	Loop	Protection loop open - #
372	ZONE ###	G##ZO###	GROUP##	Loop	Protection loop short - #
373	ZONE ###	G##ZO###	GROUP##	Smoke Detector Ionization	Fire trouble - #
374	ZONE ###	G##ZO###	GROUP##	Zone	Exit error alarm (zone) - #
375	ZONE ###	G##ZO###	GROUP##	Security	Panic zone trouble - #
376	ZONE ###	G##ZO###	GROUP##	Speaker	Hold-up zone trouble - #
377	ZONE ###	G##ZO###	GROUP##	Zone	Swinger Trouble - #
378	ZONE ###	G##ZO###	GROUP##	Zone	Cross Zone Trouble - #
380	ZONE ###	G##ZO###	GROUP##	Monitor Module	Sensor trouble - #
381	RFSUP###	G##RF###	GROUP##	Zone	Loss of super. - RF - #
382	RPMSP###	G##RP###	GROUP##	Zone	Loss of super. - RPM - #
383	ZONE ###	G##ZO###	GROUP##	Security	Sensor tamper - #

Table B.1 Contact ID Reporting Formats (Continued)

384	RFBAT###	G##RF###	GROUP##	Battery	RF low battery - #
385	ZONE ###	G##ZO###	GROUP##	Smoke Detector	Smoke det. Hi sens - #
386	ZONE ###	G##ZO###	GROUP##	Smoke Detector	Smoke det. Lo sens - #
387	ZONE ###	G##ZO###	GROUP##	Security	Intrusion det. Hi sens - #
388	ZONE ###	G##ZO###	GROUP##	Security	Intrusion det. Lo sens - #
389	ZONE ###	G##ZO###	GROUP##	Zone	Sensor self-test failure - #
391	ZONE ###	G##ZO###	GROUP##	Zone	Sensor Watch failure - #
392	ZONE ###	G##ZO###	GROUP##	Smoke Detector	Drift Comp. Error - #
393	ZONE ###	G##ZO###	GROUP##	Smoke Detector	Maintenance Alert - #
394	COMM ###	G##CO###	GROUP##	Communication	MIP Communication Failure
395	COMM ###	G##CO###	GROUP##	Communication	MIP Configuration Error
396	DACR ###	G##DA###	GROUP##	Control Panel	Primary Receiver Active
397	COMM ###	G##CO###	GROUP##	Communication	Primary Receiver Down
398	DACR ###	G##DA###	GROUP##	Control Panel	Backup Receiver Active
399	DACR ###	G##DA###	GROUP##	Control Panel	Receiver in Backup Mode
400	ZONE ###	G##ZO###	GROUP##	Zone	Open/Close
401	ZONE ###	G##ZO###	GROUP##	Zone	O/C by User - User #
402	ZONE ###	G##ZO###	GROUP##	Zone	Group O/C - User #
403	ZONE ###	G##ZO###	GROUP##	Zone	Automatic O/C
404	ZONE ###	G##ZO###	GROUP##	Zone	Late to O/C
405	ZONE ###	G##ZO###	GROUP##	Zone	Deferred O/C
406	ZONE ###	G##ZO###	GROUP##	Zone	Cancel
407	RMT ###	G##RM###	GROUP##	Zone	Remote arm/disarm
408	ZONE ###	G##ZO###	GROUP##	Zone	Quick Arm
409	KEYSW###	G##KE###	GROUP##	Zone	Keyswitch O/C
411	RMT ###	G##RM###	GROUP##	Zone	Callback request made
412	RMT ###	G##RM###	GROUP##	Control Panel	Success- download/access
413	RMT ###	G##RM###	GROUP##	Control Panel	Unsuccessful access
414	RMT ###	G##RM###	GROUP##	Control Panel	System shutdown
415	RMT ###	G##RM###	GROUP##	Digital Dialer	Dialer shutdown

Table B.1 Contact ID Reporting Formats (Continued)

416	RMT ###	G##RM###	GROUP##	Control Panel	Successful upload
421	ZONE ###	G##ZO###	GROUP##	Card Reader	Access denied - User #
422	ZONE ###	G##ZO###	GROUP##	Card Reader	Access report by user - User #
423	GROUP###	G##GR###	GROUP##	Security	Forced Access - #
424	ZONE ###	G##ZO###	GROUP##	Security	Egress Denied - #
425	ZONE ###	G##ZO###	GROUP##	Zone	Egress Granted - #
426	ZONE ###	G##ZO###	GROUP##	Zone	Access Door propped open - #
427	ZONE ###	G##ZO###	GROUP##	Zone	Access point DSM trouble - #
428	ZONE ###	G##ZO###	GROUP##	Zone	Access point RTE trouble - #
429	ZONE ###	G##ZO###	GROUP##	Zone	Access program mode entry - User #
430	ZONE ###	G##ZO###	GROUP##	Zone	Access program mode exit - User #
431	ZONE ###	G##ZO###	GROUP##	Zone	Access threat level change
432	ZONE ###	G##ZO###	GROUP##	Zone	Access relay/trigger fail - #
433	ZONE ###	G##ZO###	GROUP##	Zone	Access RTE shunt - #
434	ZONE ###	G##ZO###	GROUP##	Zone	Access DSM shunt - #
435	ZONE ###	G##ZO###	GROUP##	Door	Second Person Access - #
436	ZONE ###	G##ZO###	GROUP##	Door	Irregular Access - User #
441	GROUP###	G##GR###	GROUP##	Zone	Armed STAY - User #
442	GROUP###	G##GR###	GROUP##	Zone	Keyswitch Armed STAY - User #
450	GROUP###	G##GR###	GROUP##	Zone	Exception O/C
451	GROUP###	G##GR###	GROUP##	Zone	Early O/C - User #
452	GROUP###	G##GR###	GROUP##	Zone	Late O/C User #
453	GROUP###	G##GR###	GROUP##	Zone	Failed to Open
454	GROUP###	G##GR###	GROUP##	Zone	Failed to Close
455	GROUP###	G##GR###	GROUP##	Zone	Auto-arm Failed
456	GROUP###	G##GR###	GROUP##	Zone	Partial Arm - User #
457	GROUP###	G##GR###	GROUP##	Zone	Exit Error by User
458	GROUP###	G##GR###	GROUP##	Zone	User on premises - User #
459	GROUP###	G##GR###	GROUP##	Zone	Recent Close
461	GROUP###	G##GR###	GROUP##	Zone	Wrong Code Entry

Table B.1 Contact ID Reporting Formats (Continued)

462	GROUP###	G##GR###	GROUP##	Zone	Legal Code Entry - User #
463	GROUP###	G##GR###	GROUP##	Zone	Re-arm after Alarm - User #
464	GROUP###	G##GR###	GROUP##	Zone	Auto-arm Time Extended - User #
465	GROUP###	G##GR###	GROUP##	Zone	Panic Alarm Reset
466	ZONE ###	G##ZO###	GROUP##	Door	Service Premises - User #
501	ZONE ###	G##ZO###	GROUP##	Zone	Access reader disable - #
520	ZONE ###	G##ZO###	GROUP##	Audible Output	Sounder/Relay Disable - #
521	BELL1###	G##BE###	GROUP##	Common Bell Output	Bell 1 disable
522	BELL2###	G##BE###	GROUP##	Common Bell Output	Bell 2 disable
523	RELAY###	G##RE###	GROUP##	Common Generic Control Output	Alarm relay disable
524	RELAY###	G##RE###	GROUP##	Common Generic Control Output	Trouble relay disable
525	RELAY###	G##RE###	GROUP##	Common Generic Control Output	Reversing relay disable
526	NAC3 ###	G##NA###	GROUP##	Common Bell Output	Notification Appliance Ckt 3 disable
527	NAC4 ###	G##NA###	GROUP##	Common Bell Output	Notification Appliance Ckt 4 disable
531	ZONE ###	G##ZO###	GROUP##	Zone	Module Added
532	ZONE ###	G##ZO###	GROUP##	Zone	Module Removed
551	DIAL ###	G##DI###	GROUP##	Digital Dialer	Dialer disabled
552	RFXMT###	G##RF###	GROUP##	Zone	Radio xmitter disabled
553	ZONE ###	G##ZO###	GROUP##	Zone	Remote Upload/Download disabled
570	ZONE ###	G##ZO###	GROUP##	Zone	Zone bypass - #
571	ZONE ###	G##ZO###	GROUP##	Fire Device	Fire bypass - #
572	ZONE ###	G##ZO###	GROUP##	Zone	24 Hour zone bypass - #
573	ZONE ###	G##ZO###	GROUP##	Security	Burg. bypass - #
574	GROUP###	G##GR###	GROUP##	Zone	Group bypass - #
575	ZONE ###	G##ZO###	GROUP##	Zone	Swinger Bypass - #
576	ZONE ###	G##ZO###	GROUP##	Zone	Access zone shunt - #
577	ZONE ###	G##ZO###	GROUP##	Zone	Access point bypass - #
578	ZONE ###	G##ZO###	GROUP##	Zone	Vault Bypass - #
579	ZONE ###	G##ZO###	GROUP##	Zone	Vent Zone Bypass - #
601	TEST ###	G##TE###	GROUP##	Zone	Manually triggered test

Table B.1 Contact ID Reporting Formats (Continued)

602	TEST ###	G##TE###	GROUP##	Zone	Periodic test report
603	TEST ###	G##TE###	GROUP##	Zone	Periodic RF xmission
604	TEST ###	G##TE###	GROUP##	Zone	Fire test - User #
605	ZONE ###	G##ZO###	GROUP##	Zone	Status report to follow
606	ZONE ###	G##ZO###	GROUP##	Zone	Listen-in to follow
607	TEST ###	G##TE###	GROUP##	Zone	Walk test mode - User #
608	TEST ###	G##TE###	GROUP##	Zone	System Trouble Present
609	ZONE ###	G##ZO###	GROUP##	Zone	Video xmitter active
611	TEST ###	G##TE###	GROUP##	Zone	Point tested OK - #
612	TEST ###	G##TE###	GROUP##	Zone	Point not tested - #
613	TEST ###	G##TE###	GROUP##	Zone	Intrusion Zone Walk Tested - #
614	TEST ###	G##TE###	GROUP##	Zone	Fire Zone Walk Tested - #
615	TEST ###	G##TE###	GROUP##	Zone	Panic Zone Walk Tested
616	ZONE ###	G##ZO###	GROUP##	Zone	Service Request"},
621	ZONE ###	G##ZO###	GROUP##	Zone	Event Log reset
622	ZONE ###	G##ZO###	GROUP##	Control Panel	Event Log 50 full
623	ZONE ###	G##ZO###	GROUP##	Control Panel	Event Log 90 full
624	PANEL###	G##PA###	GROUP##	Control Panel	Event Log overflow
625	ZONE ###	G##ZO###	GROUP##	Zone	Time/Date reset - User #
626	PANEL###	G##PA###	GROUP##	Control Panel	Time/Date inaccurate
627	ZONE ###	G##ZO###	GROUP##	Zone	Program mode entry
628	ZONE ###	G##ZO###	GROUP##	Zone	Program mode exit
630	ZONE ###	G##ZO###	GROUP##	Zone	Schedule change
631	ZONE ###	G##ZO###	GROUP##	Zone	Exception schedule change
632	ZONE ###	G##ZO###	GROUP##	Zone	Access schedule change
633	DACR ###	G##DA###	GROUP##	Control Panel	Receiver Alarm Buffer Below 25%
634	DACR ###	G##DA###	GROUP##	Control Panel	Receiver Alarm Buffer Below 75%
635	DACR ###	G##DA###	GROUP##	Control Panel	Receiver Alarm Buffer Full
641	ZONE ###	G##ZO###	GROUP##	Zone	Senior Watch Trouble
642	ZONE ###	G##ZO###	GROUP##	Zone	Latch-key Supervision - User #

Table B.1 Contact ID Reporting Formats (Continued)

654	ZONE ###	G##ZO###	GROUP##	Control Panel	System Inactivity
900	ZONE ###	G##ZO###	GROUP##	Control Panel	Download Abort
901	ZONE ###	G##ZO###	GROUP##	Control Panel	Download Start - #
902	ZONE ###	G##ZO###	GROUP##	Control Panel	Download Interrupt - #
910	ZONE ###	G##ZO###	GROUP##	Zone	Auto Close-Bypass - #
911	ZONE ###	G##ZO###	GROUP##	Zone	Bypass Closing - #

Index

Manufacturer Warranties and Limitation of Liability

Manufacturer Warranties. Subject to the limitations set forth herein, Manufacturer warrants that the Products manufactured by it in its Northford, Connecticut facility and sold by it to its authorized Distributors shall be free, under normal use and service, from defects in material and workmanship for a period of thirty six months (36) months from the date of manufacture (effective Jan. 1, 2009). The Products manufactured and sold by Manufacturer are date stamped at the time of production. Manufacturer does not warrant Products that are not manufactured by it in its Northford, Connecticut facility but assigns to its Distributor, to the extent possible, any warranty offered by the manufacturer of such product. This warranty shall be void if a Product is altered, serviced or repaired by anyone other than Manufacturer or its authorized Distributors. This warranty shall also be void if there is a failure to maintain the Products and the systems in which they operate in proper working conditions.

MANUFACTURER MAKES NO FURTHER WARRANTIES, AND DISCLAIMS ANY AND ALL OTHER WARRANTIES, EITHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE PRODUCTS, TRADEMARKS, PROGRAMS AND SERVICES RENDERED BY MANUFACTURER INCLUDING WITHOUT LIMITATION, INFRINGEMENT, TITLE, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. MANUFACTURER SHALL NOT BE LIABLE FOR ANY PERSONAL INJURY OR DEATH WHICH MAY ARISE IN THE COURSE OF, OR AS A RESULT OF, PERSONAL, COMMERCIAL OR INDUSTRIAL USES OF ITS PRODUCTS.

This document constitutes the only warranty made by Manufacturer with respect to its products and replaces all previous warranties and is the only warranty made by Manufacturer. No increase or alteration, written or verbal, of the obligation of this warranty is authorized. Manufacturer does not represent that its products will prevent any loss by fire or otherwise.

Warranty Claims. Manufacturer shall replace or repair, at Manufacturer's discretion, each part returned by its authorized Distributor and acknowledged by Manufacturer to be defective, provided that such part shall have been returned to Manufacturer with all charges prepaid and the authorized Distributor has completed Manufacturer's Return Material Authorization form. The replacement part shall come from Manufacturer's stock and may be new or refurbished. THE FOREGOING IS DISTRIBUTOR'S SOLE AND EXCLUSIVE REMEDY IN THE EVENT OF A WARRANTY CLAIM.

Warn-HL-08-2009.fm

Gamewell
FCI FIRE CONTROL INSTRUMENTS

by Honeywell

Gamewell-FCI
12 Clintonville Road
Northford, CT 06472-1610 USA
203-484-7161
fax 203-484-7118

www.gamewell-fci.com

ISO 9001
CERTIFIED
ENGINEERING & MANUFACTURING
QUALITY SYSTEMS