



AlarmNet® 7810PC

IP Receiver Software

Version 3.2.6.xx

Installation and User Guide



UL

This product is suitable for Commercial Fire and Commercial Burglary applications.

- Product complies with UL 1076, paragraph 25A, *Central Supervisory Station Equipment*
- Product complies with UL 1610, *Standard for Central-Station Burglar-Alarm Units*.
- Product complies with UL 864, *Standard for Control Units and Accessories for Fire Alarm Systems*.

TRADEMARKS

Windows, Windows Server, SQL Server, and Excel are trademarks, or registered trademarks of Microsoft Corporation in the United States and other countries.

Intel® Core™ 2 Duo is a registered trademark and/or trademark of Intel Corporation in the U.S. and/or other countries.

All other trademarks are the properties of their respective owners.

Contents

Introduction	1
System Requirements	2
Power Requirements for UL 864 Compliance	5
Programming and Configuration for UL 1076 Compliance	6
Programming and Configuration for UL 1610 Compliance	8
Programming and Configuration for UL 864 Compliance	10
Operation.....	12
Manual Mode	12
Serial Automation Mode.....	12
TCP/IP Mode	12
Failure Indications	15
Maintenance and Testing	15
Network Maintenance and Testing	15
Testing the 7810PC IP Receiver Software	15
Installation	16
What you need.....	16
To install or Upgrade the 7810PC application.....	16
Configuring the 7810PC application.....	20
Configuring the SQL Server database (Private LAN only).....	20
Configuring a Web Server for AlarmNet Direct Private! (Private LAN only)	23
Uninstalling the 7810-PC software.....	23
Installing the DEMO License.....	24
Enterprise Setup.....	25
Using the 7810PC application	26
Alarms tab	28
Private LAN Accounts tab (Private LAN only)	29
Automation tab.....	30
AlarmNet tab	31
Installation tab (Private LAN only)	32
Network tab	33
Users tab (Private LAN only)	34
Commands tab (Private LAN only)	34
QOS tab (Private LAN only).....	34
Available Tools and Information Screens	35
Trace Tool (Tools > Trace).....	35
Network Diagnostics (Tools > Network Diagnostics)	35
Export Subscribers (Tools > Export Subscribers) (Private LAN only)	36
About License (Help > About License).....	36
Database Information (Help > About Database) (Private LAN only)	36
Using the AlarmNet Direct Private! website (Private LAN only).....	37
Log In	37
Device Status	38
View Accounts	39
View Receivers	40
View Supervisors	41
Message Formats.....	42
ADEMCO Contact ID Format.....	42
ADEMCO High-Speed Format.....	43
High-Speed Message Interpretation	44
Contact ID Format	49
Event Code Classifications	50
Contacting Technical Support.....	56

Introduction

Resideo's 7810PC IP Receiver Software (referred to as the 7810PC) is a highly upgradeable, and feature rich IP alarm receiver solution that can take the place of traditional hardware based 7810iR-ent receivers.

Alarm receivers (such as the 7810PC or the 7810iR-ent) monitor alarms, check-ins, and status messages from security systems. The 7810PC functions like the hardware based 7810iR-ent, but offers more features. See the comparison below.

Function	7810iR-ent	7810PC
Alarm Logging (Private LAN only.)	Alarms are sent to a printer.	Alarms are logged in a robust Microsoft SQL database with backup capability.
Message Storage	Messages are stored by an AlarmNet database and accessible for 30 days by the Central Station.	In addition to AlarmNet database storage, the messages are stored on <u>your local</u> SQL database and are always available. (Private LAN only.)
Search Capability (Private LAN only.)	No	Yes. The SQL database information can be easily searched and sorted.
Database Synchronization (Private LAN only.)	Only in private LAN configuration, Primary and Secondary receivers can synchronize data. AlarmNet data is not synced to 7810iR-ent devices.	Primary and Secondary 7810PC applications share a common SQL database so they are always in sync.
Subscribers	1,000	10,000
Automation Options	Manual Mode, LRR Line Card Mode, and 685 Automation Mode.	Manual Mode, Serial Automation Mode, and TCP/IP Automation.
Graphical Interface	Touch screen. Information is presented in a very terse manner. Not intuitive.	Intuitive PC application style GUI that uses a keyboard and mouse to interface with tabbed windows, fields and option drop-down boxes. Descriptive choices are more detailed and include tool tips.
Multilingual Interface	No	Capable
Message buffering	up to 49	up to 100
Printing	Uses a dedicated serial printer only.	Uses any printer supported by the operating system. Prints logs and traces.
MAC Address	Embedded in hardware.	Assigned by AlarmNet upon installation.
Diagnostics	Basic tests to check the hardware's display, audio, RTC (real time clock), screen, and encryption algorithm.	<ul style="list-style-type: none">• Network trace to AlarmNet utility• Network diagnostic utility• Database OK indicator (with database)• System OK indicator

System Requirements

UL

Model 7845i-ent has been evaluated for use with the 7810PC.

For compatible Listed communicators, see the individual installation instructions. The communicators need to be Listed to the appropriate standards.

The 7810PC must be configured as a fault tolerant system.

Hardware and Software Requirements	
<p>The specifications provided are for satisfactory system (includes; operating system, SQL database, and to provide reliable database storage) performance. For example, if the minimum system RAM for the operating system is 256MB, and the recommended RAM for SQL server is 4GB, then 4GB will be specified to ensure satisfactory performance.</p> <p>The specifications below are considered the minimum requirements. By using faster processors, multiple processors, multi-core processors, etc., better performance can be achieved. For detailed information about the operating system, SQL server, network installations, compatible network protocols, etc., refer to the Microsoft TechNet website.</p>	
<p>Workstation and Server Hardware</p> <p>The CD/DVD drive is only necessary if you are not downloading the software from the internet.</p>	<p>Processor – Intel Core 2 Duo, or compatible processor, 2.16GHz clock speed.</p> <p>RAM – 4GB</p> <p>Hard Drive Capacity – 320GB (For HD data reliability, use a RAID 1 configuration. This configuration requires two drives.)</p> <p>File System – NTFS</p> <p>CD or DVD Drive – required if not downloading for software installation.</p> <p>Ports – Serial Ports, Parallel Port, and USB ports as needed.</p> <p>Monitor – VGA 1024 x 768 resolution.</p> <p>Keyboard and Mouse – required interface.</p> <p>Network Adapters – compatible with the operating system. 10BaseT connection using CAT5 or CAT6 wiring.</p> <ul style="list-style-type: none"> • The 7810PC software must be v3.2.6.xx or later. Primary and Secondary installations MUST use the same version of the software. • Primary and Secondary 7810PC installations MUST run on separate workstations. • Each server PC must have a static IP address. • Processor, RAM, and disk space must meet or exceed the requirements of the operating system and database.
Operating System	<p>Microsoft Windows 2000 Server (with SP5 or later), Microsoft Windows Server 2003 (with SP2 or later), or Microsoft Windows Server 2008 (with SP2 or later) or Microsoft Windows 2012 Server.</p> <p>Internet Explorer 7.0 (or later) browser recommended. We recommend updating with the latest Windows Service Packs for optimum security.</p>
Database (Private LAN only.)	<p>Microsoft SQL Server 2005 (with SP3 or later), or SQL Server 2008 or SQL Server 2012.</p> <p>If a SQL backup database is desired, refer to the SQL Server documentation to setup the backup database on another server.</p>
IIS Web Hosting software	<p>Internet Information Services (IIS) 6.0.</p> <p>This application is included as part of the operating system and must be installed if an AlarmNetDirectPrivate! website is to be used.</p> <p>UL: AlarmNetDirectPrivate! website is an <u>optional part</u> of the 7810PC application used for private LAN only. It enables remote viewing of device status, alarm history and hosting of communicator software updates.</p> <p>AlarmNetDirectPrivate! is a supplementary feature. It MUST be installed on a separate dedicated server for UL.</p>
Automation System Interface	<p>An RS-232 serial interface is required from the workstation where the 7810PC application is installed to the Automation system.</p>

Hardware and Software Requirements	
Requirements for UL Compliance	
<p>The installation must meet the following requirements:</p> <ul style="list-style-type: none"> • UL 497A, <i>Standard for Secondary Protectors For Communications Circuits</i> • UL 497B, <i>Standard for Protectors for Data Communications and Fire Alarm Circuits</i> • UL 681, <i>Standard for Installation and Classification of Burglar and Holdup Alarm Systems</i> • UL 827, <i>Standard for Central Alarm Services</i> • UL 864, <i>Standard for Control Units and Accessories for Fire Alarm Systems</i> • UL 1012, <i>Standard for Power Units Other Than Class 2</i> • UL 1076, paragraph 25A, <i>Central Supervisory Station Equipment</i> • UL 1610, <i>Standard for Central-Station Burglar-Alarm Units</i> • UL 60950, <i>Standard for Information Technology Equipment</i> • NFPA 70 <i>National Electrical Code</i>, NFPA72 <i>National Fire Alarm and Signaling Code</i> 	
General	<p>Hardware must be installed in accordance with:</p> <ul style="list-style-type: none"> • The National Electrical Code, NFPA70, and National Fire Alarm and Signaling Code NFPA72. • The local authority having jurisdiction (AHJ). • The Standard for Central Station Alarm Services, UL 827 and NFPA72 <p>Software must be configured such that:</p> <ul style="list-style-type: none"> • Signal prioritization shall be set by the automation system. • Polling between the protected premise equipment and the 7810PC software receiver must not exceed 200 seconds.
HVAC Maintenance Contract (UL 864 only)	Must have an ACTIVE maintenance contract that provides restoration of the HVAC system within 24 hours, applicable 7 days a week.
Environment	<ul style="list-style-type: none"> • Equipment must be installed in a temperature controlled environment maintained between 13 – 35°C (55 – 95°F) by the HVAC system. • Twenty-four hours of standby power must be provided for the HVAC system. The standby power for the HVAC system may be supplied by an engine driven generator alone. (A standby battery is not required.) • Primary Power for all equipment must comply with the <i>Standard for Transient Voltage Surge Suppressors</i>, UL 1449, with a maximum marked rating of 330V. • Data lines for all equipment must comply with <i>Standard for Protectors for Data Communications and Fire Alarm Circuits</i>, UL 497B, and be marked for a maximum rating of 50V. • Communication circuits and network components connected to the telecommunications network shall be protected by secondary protectors for communication circuits. These protectors shall comply with the Standard for Secondary Protectors For Communications Circuits, UL 497A. These protectors shall be used only on the protected side of the telecommunications network.

Hardware and Software Requirements	
Server Equipment, Operating System SQL database 7810PC IP Receiver Software Network Equipment such as routers, switches, hubs, and modems.	<ul style="list-style-type: none"> The Central Supervisory Station Equipment must be UL Listed and comply with <i>The Standard for Information Technology Equipment</i>, UL60950. All hardware must utilize an Uninterruptible Power Supply (UPS) with sufficient capacity to enable at least 15 minutes of operation. The UPS units must comply with UL 1778, <i>Standard for Uninterruptible Power Supply Equipment</i>, or UL 1481, <i>Standard for Fire Protective Signaling Devices</i>. In addition to the main power supply and secondary power supply that are required to be provided at the central supervisory station, the system shall be provided with an uninterruptible power supply (UPS) with sufficient capacity to operate the computer equipment for a minimum of 15 minutes. If more than 15 minutes is required for the secondary power supply to supply the UPS input power, the UPS shall be capable of providing input power for at least that amount of time. To support maintenance, a means for disconnecting the input to the UPS while maintaining continuity of power to the Automation system shall be provided. <p>To ensure fault tolerance:</p> <ul style="list-style-type: none"> All hardware and software installed on workstations and database servers must be duplicated. Install the 7810PC to run as a Service to insure automatic restart if the server reboots. Install a Primary 7810PC on a server, and a Secondary 7810PC on a separate physical workstation server. Both installations must be the same version. Since the Primary 7810PC installation switches to the Secondary 7810PC installation, both systems must run concurrently. Install the SQL Server on a database server with a redundant mirrored database on a separate physical database server. (For Private LAN only.)
Power Conditioner (optional)	<ul style="list-style-type: none"> If a Power Conditioner is used, it shall comply with UL 1012, <i>Standard for Power Units Other Than Class 2</i>. To support maintenance, a means for disconnecting the input to the Power Conditioner while maintaining continuity of power to the Automation system shall be provided.
7810PC running the Receiver Supervisor option.	<p>The Receiver Supervisor option can supervise multiple 7810PCs operating without supervising partners (for example, running in Direct mode).</p> <p>The Receiver Supervisor option <u>DOES NOT</u> provide supervision for <u>UL</u>.</p> <p><u>For UL</u>, supervision REQUIRES operation of redundant 7810PC applications, properly configured to serve in the role of receiver.</p>
Automation System	<p>Must be a UL Listed UL 1981 Automation system. The Automation system must control the Priority of Signals (see below). Note that if more than 500 accounts are being serviced, then two Automation systems must be used.</p> <p>Manual Mode – Private LAN is required, and Automation Mode CANNOT be used (UL 1076).</p> <p>Serial or TCP/IP Automation Mode – Automation system must be UL 1981 Listed and must control priority of signals. It must be used in all UL 1610 configurations.</p>
<p style="text-align: center;">UL864 Priority of Signals</p> <p>When concurrent signals are received, they shall be indicated as follows in descending order of priority:</p> <ol style="list-style-type: none"> 1. Signals associated with life safety. 2. Signals associated with property safety. 3. Supervisory signals and trouble signals associated with life and/or property safety. 4. All other signals. 	
Security System Control Panels	Control Panels need to be Listed to the appropriate standards.

Power Requirements for UL 864 Compliance

Source of power	<ul style="list-style-type: none">• The supervising station processing control equipment or the enclosure housing the control equipment shall have with a permanent means for connection to the branch circuit supply which shall include provision for installing the supply conductors in conduit.• Hardware shall be powered by a UPS that complies with either the Standard for Uninterruptable Power Supply Equipment, UL 1778, or the Standard for Fire Protective Signaling Devices, UL 1481.• In order to perform maintenance and repair service, a means for disconnecting the input to a UPS and output from a UPS while maintaining continuity of power supply to the automation system shall be provided.• When a power conditioner is being used, it shall comply with the Standard for Power Units Other Than Class 2, UL 1012. In order to perform maintenance and repair service, a means for disconnecting the input to a power conditioner and output from a power conditioner while maintaining continuity of power to the automation system shall be provided.• All sources of power for the signal processing equipment shall be within the rated voltage range of the equipment.
Supply-line transient protection	Hardware shall be protected by transient voltage surge suppressors that comply with the Standard for Transient Voltage Surge Suppressors, UL 1449. The transient voltage surge suppressors for single-phase, 120/220 V AC systems shall have a marked rating of 330 volts or less. The transient voltage surge suppressors for 3-phase, 480 VAC or higher-rated systems shall have a marked rating of 400 volts or less.
Signaling-line transient protection	<ul style="list-style-type: none">• The communication circuits contained within the central-station building and not connected to the telecommunications network shall be protected by isolated loop circuit protectors. These protectors shall comply with the Standard for Protectors for Data Communication and Fire Alarm Circuits, UL 497B, and shall have a marked rating of 50 volts or less.• Communication circuits connected to the telecommunications network shall be protected by secondary protectors for communication circuits. These protectors shall comply with the Standard for Secondary Protectors for Communications Circuits, UL 497A, and shall have a marked rating of 150 volts or less. These protectors shall be used only in the protected side of the telecommunications network.

Programming and Configuration for UL 1076 Compliance

The 7810PC has configuration settings and programmable selections that allow the system to meet the UL1076 Proprietary Burglar Alarm requirements. These requirements are listed in the following table.

NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION AND OTHER INVOLVED PARTIES			
This product incorporates field-programmable software and component options. In order to comply with the requirements in the Standard for Proprietary Burglar Alarm Units and Systems, UL1076, certain programming features or options must be limited to specific settings or not used at all as indicated below.			
Program Feature or Option	Permitted in UL1076?	Possible Settings	Settings permitted in UL1076
IIS Web Hosting software Internet Information Services (IIS) 5.0 This application is included as part of the operating system and must be installed if an AlarmNetDirectPrivate! website is to be used.	Yes	Optional Installed if an AlarmNetDirectPrivate! website is desired. This website is an optional part of the 7810PC application used for private LAN only. It enables remote viewing of device status, alarm history, and hosting communicator software updates.	AlarmNetDirectPrivate! MUST be installed on a separate dedicated server. When installing hosted Software Updates, a system administrator MUST be present.
Receiver Supervisor (supplementary feature) The Receiver Supervisor can supervise multiple 7810PCs operating without supervising partners (for example, running in Direct mode).	Yes	<ul style="list-style-type: none"> • Installed – not used for supervision • Installed – used for supervision • Not Installed 	Installed – not used for supervision OR Not Installed Supervision MUST be accomplished by setting up redundant 7810PC applications, and configuring their receiver roles.
Enterprise setup This is a 7810PC setup type configuration that can be chosen during installation. Enables multiple sets of 7810PCs to share one mirrored database server. This installation is used for Private LAN only.	Yes	<ul style="list-style-type: none"> • Enterprise_Mode_ = 0 (or not specified) • Enterprise_Mode_ = 1 	Both settings: <ul style="list-style-type: none"> • MUST have a secondary 7810PC installation on a separate server. • The secondary 7810PC will receive messages in the event that the primary 7810PC loses communication.
SQL Server database	Yes	<ul style="list-style-type: none"> • Installed • Not Installed 	Installed for Private LAN mode MUST utilize redundant SQL databases. Each redundant SQL Server database MUST be on a separate server. Not Installed for AlarmNet mode
Secondary 7810PC Installation	Yes	<ul style="list-style-type: none"> • Installed • Not Installed 	Installed
<u>AlarmNet</u> tab: Account Supervision setting	Yes	<ul style="list-style-type: none"> • 24 Hours • 1 Hour • US UL Lin 6 Min • CN UL Lin Lvl 3 • US UL Lin 90 sec • CN UL Line Lvl 4 • CN UL Line Lvl 5 • None 	US UL Lin 90 sec

**NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION AND
OTHER INVOLVED PARTIES**

This product incorporates field-programmable software and component options. In order to comply with the requirements in the Standard for Proprietary Burglar Alarm Units and Systems, UL1076, certain programming features or options must be limited to specific settings or not used at all as indicated below.

Program Feature or Option	Permitted in UL1076?	Possible Settings	Settings permitted in UL1076
<u>Installation</u> tab: This Receiver's Role settings Support Supervision	Yes	<ul style="list-style-type: none"> • Checked • Unchecked 	Checked
<u>Installation</u> tab: This Receiver's Role settings <i>and</i> Other Receiver's Role settings	Yes	<ul style="list-style-type: none"> • Does Not Exist • Primary • Secondary 	<p>Does Not Exist is not permitted</p> <p>Primary when secondary is selected at the other 7810PC</p> <p>Secondary when primary is selected at the other 7810PC.</p> <p>MUST have a Primary and Secondary receiver, and their roles configured.</p> <p>MUST check Support Supervision box for each receiver.</p>
Communication Loss Report programming (at communicator)	Yes	<ul style="list-style-type: none"> • Alarm • Trouble 	Alarm
Private LAN mode	Yes	<ul style="list-style-type: none"> • Licensed • Not Licensed 	Required, Licensed
AlarmNet mode	Yes (when used in conjunction with Private LAN mode)	<ul style="list-style-type: none"> • Licensed • Not Licensed 	Optional, Licensed
<u>Automation</u> tab: Manual Mode	Yes	<ul style="list-style-type: none"> • Manual Mode 	Manual Mode
<u>Automation</u> tab: Automation Modes	No	<ul style="list-style-type: none"> • TCP/IP Mode • Serial Mode 	Manual Mode
Setting protection for the system	Yes	Set from Protected Premises only	Required

Programming and Configuration for UL 1610 Compliance

The 7810PC has configuration settings and programmable selections that allow the system to meet the UL1610 Central Station Burglar Alarm requirements. These requirements are listed in the following table.

NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION AND OTHER INVOLVED PARTIES			
This product incorporates field-programmable software and component options. In order to comply with the requirements in the Standard for Central Station Burglar Alarm Units, UL1610, certain programming features or options must be limited to specific settings or not used at all as indicated below.			
<i>Program Feature or Option</i>	<i>Permitted in UL1610?</i>	<i>Possible Settings</i>	<i>Settings permitted in UL1610</i>
IIS Web Hosting software Internet Information Services (IIS) 5.0 This application is included as part of the operating system and must be installed if an AlarmNetDirectPrivate! website is to be used.	Yes	Optional Installed if an AlarmNetDirectPrivate! website is desired. This website is an optional part of the 7810PC application used for private LAN only. It enables remote viewing of device status, alarm history, and hosting communicator software updates.	AlarmNetDirectPrivate! MUST be installed on a separate dedicated server. When installing hosted Software Updates, a system administrator MUST be present.
Receiver Supervisor (supplementary feature) The Receiver Supervisor can supervise multiple 7810PCs operating without supervising partners (for example, running in Direct mode).	Yes	<ul style="list-style-type: none">• Installed – not used for supervision• Installed – used for supervision• Not Installed	Installed – not used for supervision OR Not Installed Supervision MUST be accomplished by setting up redundant 7810PC applications, and configuring their receiver roles.
Enterprise setup This is a 7810PC setup type configuration that can be chosen during installation. Enables multiple sets of 7810PCs to share one mirrored database server. This installation is used for Private LAN only.	Yes	<ul style="list-style-type: none">• Enterprise_Mode_ = 0 (or not specified)• Enterprise_Mode_ = 1	Both settings: <ul style="list-style-type: none">• MUST have a secondary 7810PC installation on a separate server.• The secondary 7810PC will receive messages in the event that the primary 7810PC loses communication.
SQL Server database	Yes	<ul style="list-style-type: none">• Installed• Not Installed	Not Installed for AlarmNet mode Installed if Private LAN mode is optionally selected MUST utilize redundant SQL databases. Each redundant SQL Server database MUST be on a separate server.
Secondary 7810PC Installation	Yes	<ul style="list-style-type: none">• Installed• Not Installed	Installed

**NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION AND
OTHER INVOLVED PARTIES**

This product incorporates field-programmable software and component options. In order to comply with the requirements in the Standard for Central Station Burglar Alarm Units, UL1610, certain programming features or options must be limited to specific settings or not used at all as indicated below.

Program Feature or Option	Permitted in UL1610?	Possible Settings	Settings permitted in UL1610
AlarmNet tab: Account Supervision setting	Yes	<ul style="list-style-type: none"> • 24 Hours • 1 Hour • US UL Lin 6 Min • CN UL Lin Lvl 3 • US UL Lin 90 sec • CN UL Line Lvl 4 • CN UL Line Lvl 5 • None 	US UL Lin 90 sec
Installation tab: This Receiver's Role settings Support Supervision	Yes	<ul style="list-style-type: none"> • Checked • Unchecked 	Checked
Installation tab: This Receiver's Role settings <i>and</i> Other Receiver's Role settings	Yes	<ul style="list-style-type: none"> • Does Not Exist • Primary • Secondary 	<p>Does Not Exist is not permitted</p> <p>Primary when secondary is selected at the other 7810PC</p> <p>Secondary when primary is selected at the other 7810PC.</p> <p>MUST have a Primary and Secondary receiver, and their roles configured.</p> <p>MUST check Support Supervision box for each receiver.</p>
Communication Loss Report programming (at communicator)	Yes	<ul style="list-style-type: none"> • Alarm • Trouble 	Alarm
Private LAN mode	Yes (Yes, when used in conjunction with AlarmNet mode)	<ul style="list-style-type: none"> • Licensed • Not Licensed 	Optional, Licensed
AlarmNet mode	Yes	<ul style="list-style-type: none"> • Licensed • Not Licensed 	Required, Licensed
Automation tab: Manual Mode	No	<ul style="list-style-type: none"> • Manual Mode 	No
Automation tab: Automation Modes	Yes	<ul style="list-style-type: none"> • TCP/IP Mode • Serial Mode 	TCP/IP or Serial Mode

Programming and Configuration for UL 864 Compliance

The 7810PC has configuration settings and programmable selections that allow the system to meet the UL 864 Commercial Fire requirements. These requirements are listed in the following table.

NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION AND OTHER INVOLVED PARTIES			
This product incorporates field-programmable software and component options. In order to comply with the requirements in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864, certain programming features or options must be limited to specific settings or not used at all as indicated below.			
Program Feature or Option	Permitted in UL864?	Possible Settings	Settings permitted in UL864
IIS Web Hosting software Internet Information Services (IIS) 5.0 This application is included as part of the operating system and must be installed if an AlarmNetDirectPrivate! website is to be used.	Yes	Optional Installed if an AlarmNetDirectPrivate! website is desired. This website is an optional part of the 7810PC application used for private LAN only. It enables remote viewing of device status, alarm history, and hosting communicator software updates.	AlarmNetDirectPrivate! MUST be installed on a separate dedicated server. When installing hosted Software Updates, a system administrator MUST be present.
Receiver Supervisor (supplementary feature) The Receiver Supervisor can supervise multiple 7810PCs operating without supervising partners (for example, running in Direct mode).	Yes	<ul style="list-style-type: none"> Installed – not used for supervision Installed – used for supervision Not Installed 	Installed – not used for supervision OR Not Installed Supervision MUST be accomplished by setting up redundant 7810PC applications, and configuring their receiver roles.
Enterprise setup This is a 7810PC setup type configuration that can be chosen during installation. Enables multiple sets of 7810PCs to share one mirrored database server. This installation is used for Private LAN only.	Yes	<ul style="list-style-type: none"> Enterprise_Mode_ = 0 (or not specified) Enterprise_Mode_ = 1 	Both settings: <ul style="list-style-type: none"> MUST have a secondary 7810PC installation on a separate server. The secondary 7810PC will receive messages in the event that the primary 7810PC loses communication.
SQL Server database	Yes	<ul style="list-style-type: none"> Installed Not Installed 	Installed for Private LAN mode MUST utilize redundant SQL databases. Each redundant SQL Server database MUST be on a separate server. Not Installed for AlarmNet mode
SQL Server database mirroring	Yes	<ul style="list-style-type: none"> High Safety with Automatic Failover High Performance High Safety without Automatic Failover 	High safety with automatic failover
Secondary 7810PC Installation	Yes	<ul style="list-style-type: none"> Installed Not Installed 	Installed

**NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION AND
OTHER INVOLVED PARTIES**

This product incorporates field-programmable software and component options. In order to comply with the requirements in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864, certain programming features or options must be limited to specific settings or not used at all as indicated below.

<i>Program Feature or Option</i>	<i>Permitted in UL864?</i>	<i>Possible Settings</i>	<i>Settings permitted in UL864</i>
AlarmNet tab: Account Supervision setting	Yes	<ul style="list-style-type: none"> • 24 Hours • 1 Hour • US UL Lin 6 Min • CN UL Lin Lvl 3 • US UL Lin 90 sec • CN UL Line Lvl 4 • CN UL Line Lvl 5 • None 	US UL Lin 90 sec
Installation tab: This Receiver's Role settings Support Supervision	Yes	<ul style="list-style-type: none"> • Checked • Unchecked 	Checked
Installation tab: This Receiver's Role settings <i>and</i> Other Receiver's Role settings	Yes	<ul style="list-style-type: none"> • Does Not Exist • Primary • Secondary 	<p>Does Not Exist is not permitted</p> <p>Primary when secondary is selected at the other 7810PC</p> <p>Secondary when primary is selected at the other 7810PC.</p> <p>MUST have a Primary and Secondary receiver, and their roles configured.</p> <p>MUST check Support Supervision box for each receiver.</p>
Communication Loss Report programming (at communicator)	Yes	<ul style="list-style-type: none"> • Alarm • Trouble 	Trouble

Operation

The 7810PC can be used in two basic configurations, AlarmNet Configuration and Private LAN Configuration (refer to the diagrams on the following pages). Depending on the licenses purchased, both configurations can be used.

When configured for AlarmNet, the alarms and messages from the protected premise are sent to AlarmNet where they are monitored, backed up on their servers and passed to the central station. In turn, the Central Station uses a 7810PC to receive these alarms and messages.

When configured for Private LAN, the alarms and messages from the protected premise are sent via LAN to the 7810PC. These alarms and messages are then monitored, processed, and stored locally on a Microsoft SQL database. In this configuration AlarmNet is not involved.

In either configuration the 7810PC serves as a buffer; it allows the alarms and messages to be viewed and manually acknowledged by an operator or passed on to Automation systems for further processing. The 7810PC can be configured in three receiver modes, (Manual, Serial Automation, and TCP/IP) offering various degrees of intervention.

When AlarmNet and Private LAN are selected together, all signals, whether from a Private LAN account or an AlarmNet account, are processed in the same manner (i.e., the alarm is received, acknowledged, and outputted to the automation system, as usual, with no apparent difference to the monitor).

Manual Mode

Manual Mode is a standalone method of receiving alarms and messages. In this mode, the operator manually monitors and processes each alarm and message.

- Incoming messages are displayed in the New Alarm window (ADEMCO high-speed or Contact ID format).
- Operator is required to acknowledge and silence the incoming alarm by clicking the “Display Next” button. This will move it from the New Alarm window to the Alarm History window.

Serial Automation Mode

When configured for the Serial Automation Mode, the 7810PC emulates a 685 Digital Alarm Receiver. In this configuration the 7810PC routes alarms and messages directly to the Automation system. The 7810PC uses a RS232 serial interface to communicate with the Automation system.

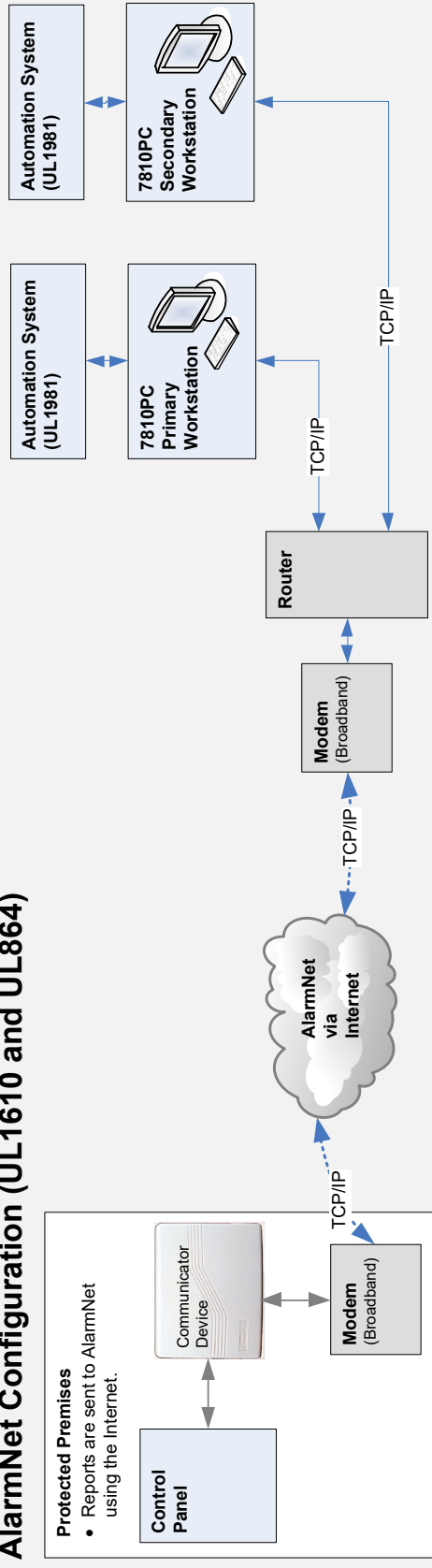
- Both the New Alarm window and the Alarm History window are first-in first-out (FIFO) buffers that are limited to 100 entries. When 100 messages have been received in either window, the next message will push the oldest alarm off the list.
- Completed alarms will be displayed in the Alarm History window with no audible alert.
- When the Automation system receives and acknowledges the alarm message, the 7810PC moves the message into the Alarm History window. This is repeated for each new alarm.
- If the “Fail to Manual” option is selected during the 7810PC programming, the 7810PC will revert to Manual Mode when communication with the Automation system is lost. When communication is restored, the 7810PC will send up to 100 unreported messages to the Automation system.
- If the “Fail to Manual” option is not selected, a loss of communications between the 7810PC and the Automation system will block all messages. This makes all incoming messages undeliverable or bounced. In this condition, all subscriber message traffic will be routed to the secondary 7810PC.

TCP/IP Mode

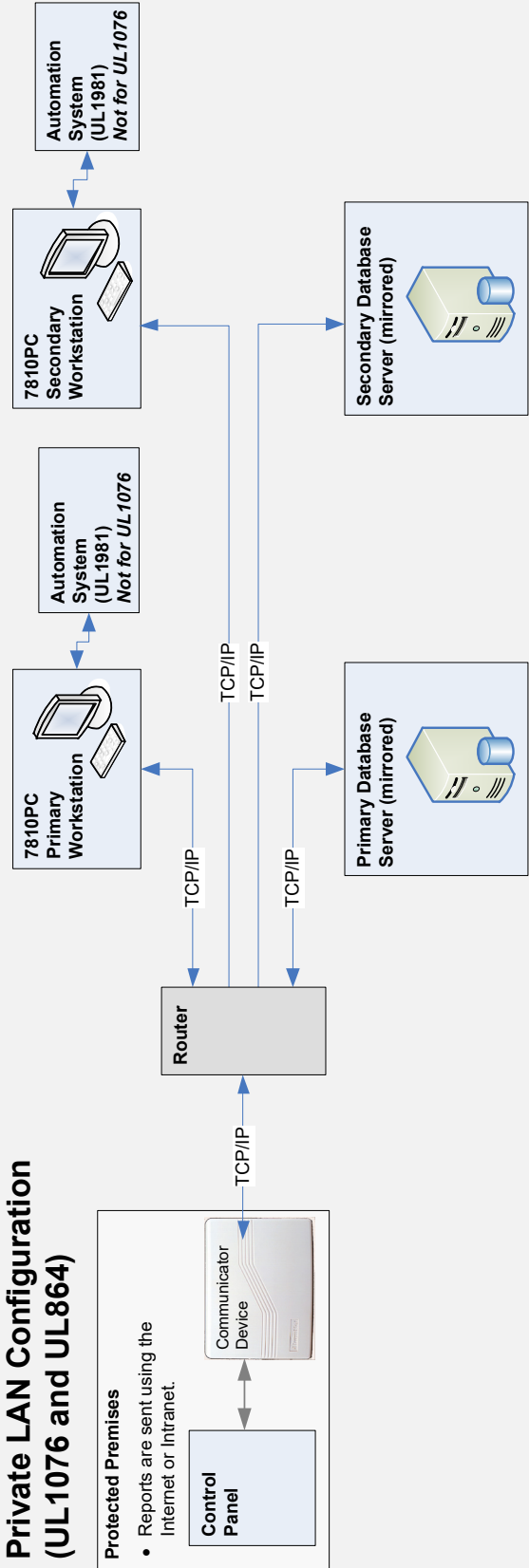
Same features as the Serial Automation Mode above. However, in this mode the 7810PC uses a TCP/IP connection to communicate with the Automation system.

UL The following illustrations depict UL tested 7810PC system configurations.

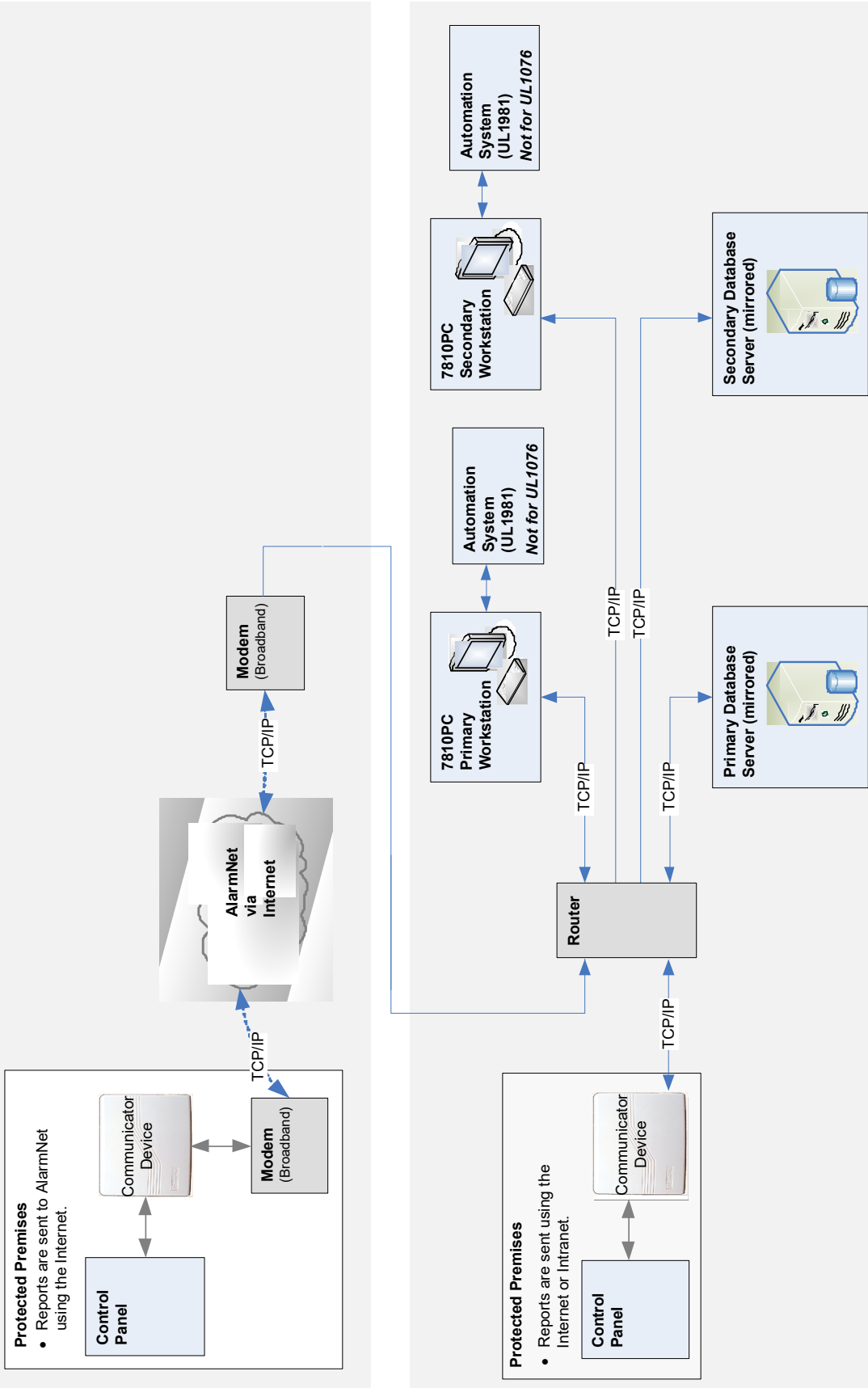
AlarmNet Configuration (UL1610 and UL864)



Private LAN Configuration (UL1076 and UL864)



Private LAN and AlarmNet Configuration (UL1610, UL864 and UL1076)



Failure Indications

UL The 7810PC must be configured as a fault tolerant system.

Configured as a fault tolerant system, the 7810PC makes a very robust security alarm message receiver. This is accomplished by using separate, redundant hardware systems, each with an uninterruptible power supply and identical software and databases. One system must function in the Primary (main) role and the other in the Secondary (backup) role.

A hardware or software failure in either workstation triggers audible and visual notification at the other workstation.

When the primary 7810PC fails, communication with the security system's communicator is lost, and the communicator automatically rolls over and communicates with the secondary 7810PC. In addition, the communicator sends the secondary 7810PC a Central Station Fail message.

When the operating system software fails as a result of a hardware component (hard drive, RAM, etc.) or the server software itself, an obvious fatal error or other message is displayed.

Further since the hardware power is protected by Uninterruptible Power Supplies (UPS), any interruption in power is indicated by audible warnings from the UPS hardware. If the UPS management software has been installed, a visual message/report of any power problems will also appear.

(Private LAN only.) When communication with the database fails, or the database itself fails, the 7810PC status indicator turns red, indicating a "Database Failure" and an E961Database Failure message is generated and posted to the Automation System.

When communication is restored, an R961 restore message is generated and posted to the Automation System.

Maintenance and Testing

The maintenance and testing tasks consists of two parts: Network Maintenance and Testing the 7810PC application.

Network Maintenance and Testing

Every month the site system administrator should perform maintenance on all network software (including the databases) and hardware components according to their manufacturer's instructions or local site procedure.

Testing the 7810PC IP Receiver Software

Every week the 7810PC administrator should use the Network Diagnostics tool (Tools > Network Diagnostics) to determine if the 7810PC is properly communicating with the site network.

Installation

Installing the 7810PC application is to be done by the site's System Administrator. The administrator must be familiar with Microsoft Server operating systems, and Microsoft SQL Server databases. Before installing the 7810PC application, understand that the installation and configuration can vary according with how the 7810PC is going to be used.

Repeat installation on Secondary 7810PC.

UL

No software other than the operating system software, database software and anti-virus/security protection software shall be installed on the primary and backup computers **and** the primary and backup database servers.

The 7810PC can receive alarm reports in a Private LAN configuration, and/or alarm reports from an AlarmNet Configuration via the internet. If used in a Private LAN configuration, a database is required.

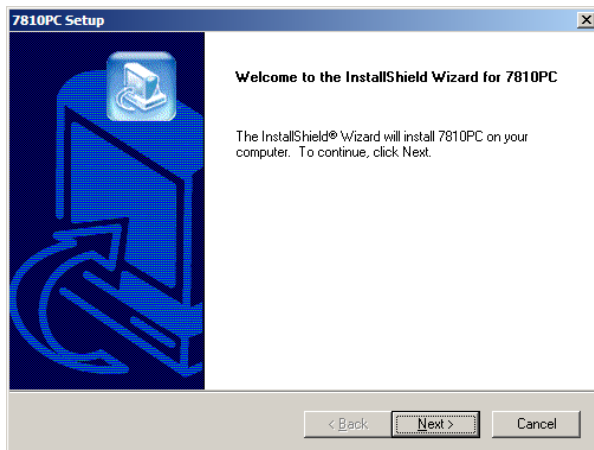
What you need

- 7810PC application software, this guide, and the *7810PC License Guide*, or the *7810PC Demo License Guide* (internet distribution files). For convenience, installing the Demo License is also covered in this guide.
- Ensure each server and workstation is assigned a static IP address and meets all the hardware and software requirements specified in the "*System Requirements*" topic.

NOTE: For **AlarmNet Only** or **Supervisor** operation, DHCP can be used.

To install or Upgrade the 7810PC application

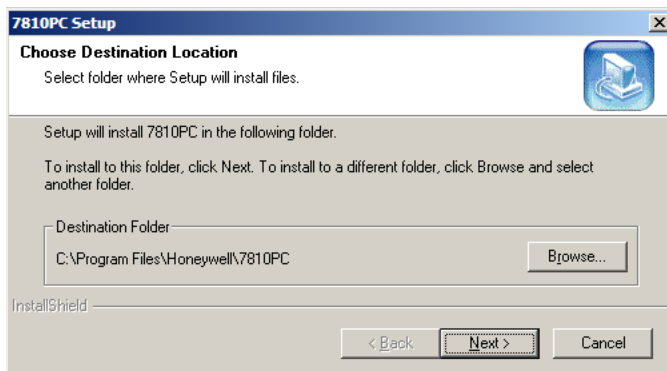
1. Copy the self-extracting application file (PC7810_Setup.exe) to a temporary folder, and double click to start the installation.



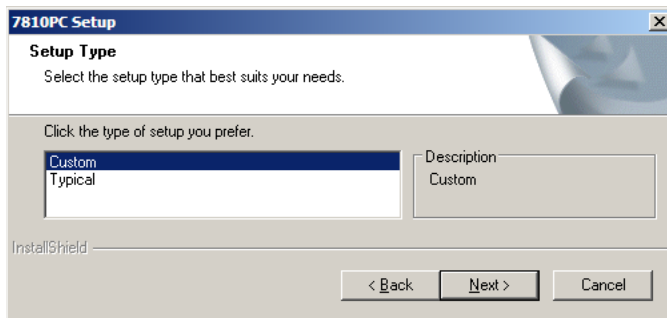
NOTES:

- If you are upgrading the 7810PC, it will detect the existing installation. A screen will appear with choices to Modify, Repair, or Remove.
- Choose Repair, then click **Next**. All of your settings and data will be retained and the upgrade will proceed with minimal intervention.
- **(Private LAN only.)** After the upgrade is complete refer to the "*Configuring the SQL Server database*" topic and update the database.

2. Click **Next**. The License Agreement screen appears.
3. Read through the license agreement and click **Yes**.
4. Click **Next** to accept the default destination, or click **Browse** to choose an alternate location.



5. Click **Next**. The Setup Type screen appears.



6. Select the Setup Type according to your requirements.

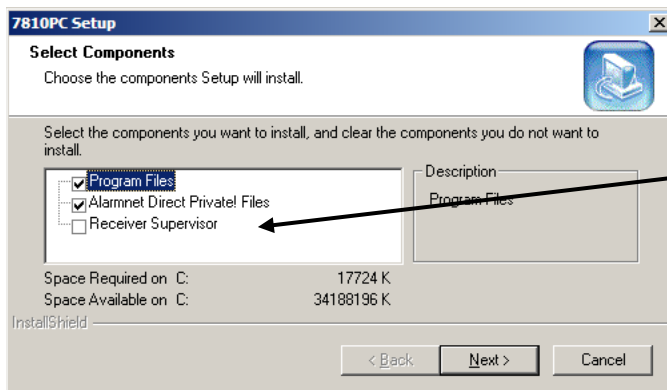
- Custom – This option also installs the supplementary features AlarmNet Direct Private! and/or Receiver Supervisor capability. **(Private LAN only.)**

AlarmNet Direct Private! enables remotely viewing alarms from a web page. This installation requires setting up a web server (on a separate server) using Microsoft's IIS component.

Receiver Supervisor enables supervising multiple 7810PCs sharing a single database. It monitors their heartbeats and sends an alarm in the event of a Comm Fail.

- Typical – This option supports receiving messages from AlarmNet, and/or Private Enterprise communications.

If you choose Custom, the following screen will appear, allowing you to choose the components. You can also choose Custom to add or remove a component from a previous installation.

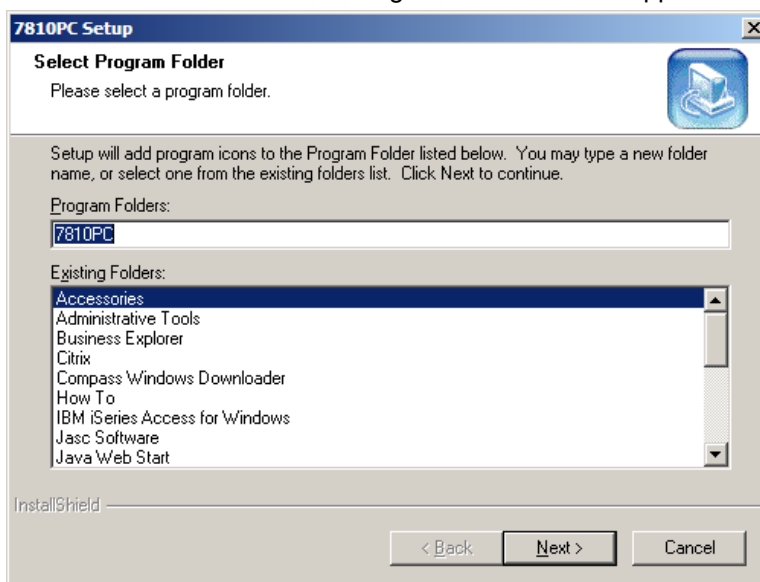


The Receiver Supervisor option can supervise multiple 7810PCs operating without supervising partners (for example, running in Direct mode). The Receiver Supervisor option DOES NOT provide supervision for UL.

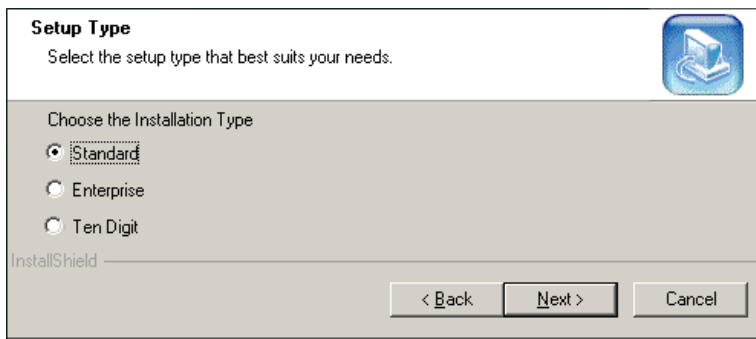
For UL, this supplementary feature must be installed on a separate server.

For UL, supervision **REQUIRES** operation of redundant 7810PC applications, properly configured for their receiver roles.

7. Then click **Next**. The Select Program Folder screen appears.



8. Accept 7810PC as the default program folder name, or enter a name, then click **Next**. The Setup Type screen appears. Review the descriptions shown at right.



Standard – One set of 7810PCs sharing one database server.

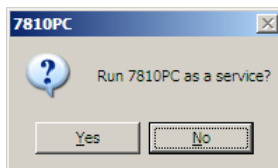
Enterprise – Enables multiple sets of 7810PCs sharing one database. This installation is used for Private LAN only.

Ten Digit – If installing in South America, choose this option to allow the use of 10-digit account numbers.

9. Choose Standard, then click **Next**.

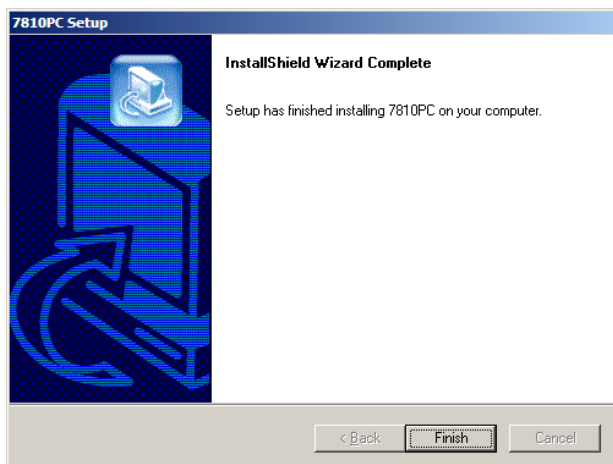
For an Enterprise installation please refer to the “*Enterprise Setup*” topic in this guide for more information.

The “Run as a Service” prompt appears.

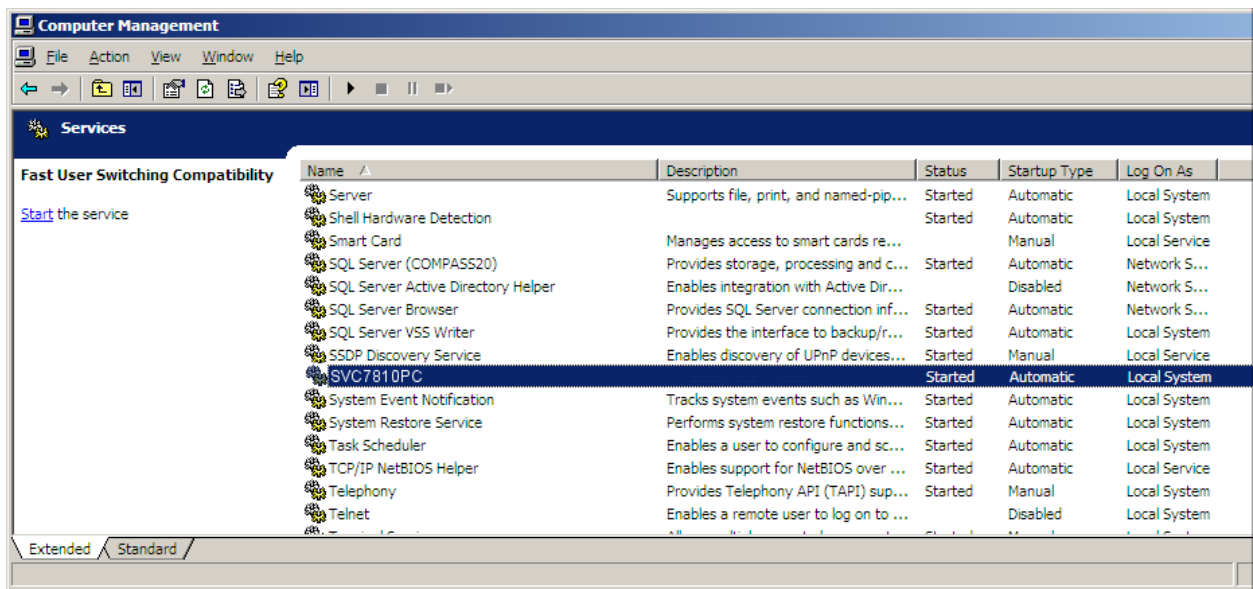


If you choose Yes to run the 7810PC as a Service, the application will start every time the server starts or reboots. If you choose No, the 7810PC will have to be manually started. (We recommend choosing Yes to run the 7810PC as a Service.) Choose **Yes** or **No**.

The Installation Complete screen appears.



10. Click **Finish**. Then reboot the server.
11. If you chose to run the 7810PC as a Service, check that the service is Started and is set to Automatic.



Running the installation again on the same server will offer options to Modify, Repair or Remove an installation.

UL

For UL compliance, you **MUST** have a secondary 7810PC. The installation procedure above must be repeated on a separate server. The secondary 7810PC will receive messages in the event that the primary 7810PC loses communication.

Configuring the 7810PC application

The configuration of the 7810PC is determined by the license you purchase. To complete your installation have the following information available:

- A license for each 7810PC installation. (Refer to the *7810PC License Guide* to obtain your license.)
- SQL Server Name, Login, and Password.
- Static IP address for the Primary PC, and Secondary PC (required for UL). On a Secondary PC, the 7810PC software installation process **MUST** be repeated.
- City, CS, and subscriber account numbers.

If you have not already created or upgraded your license, click **Help** on the menu bar at the top of the window and select **About License**, then click **License Manager** and create or upgrade your license, then continue to the next topic.

Configuring the SQL Server database (Private LAN only)

1. Ensure Microsoft SQL Server is set up (refer to the Microsoft documentation if necessary) as follows:
 - It is recommended that SQL Server be installed on a different server than the 7810PC application.
 - SQL Server must be configured to enable remote TCP/IP connection.
 - If a redundant database is desired, SQL Server must be installed on two separate servers. Both SQL Server databases must have the same username, password, and domain.

UL

This configuration **MUST** utilize redundant databases. Each redundant database **MUST** be on a separate server. The redundant databases **MUST** run on SEPARATE systems from the 7810PC applications. Both SQL Server databases must have the same username, password, and domain.

2. Set up the 7810PC database schema, stored procedures and the DSN using the **sqlscript.exe** utility. This utility resides in the 7810PC installation directory (typically c:\Program Files\Honeywell\7810PC). Execute the **sqlscript.exe** utility. Refer to the illustration in Step 4.
3. Select the server from the dropdown box or enter the server name. (The admin name and password are required to complete this step.)
4. Check **Create/Update Database**. Enter the appropriate information for the redundant SQL database (if used) in the Setup Failover Server fields.
5. Click **GO!** to finish setting up the database.

Each installation of the 7810PC database (and supplementary applications such as Receiver Supervisor and AlarmNet Direct Private!) requires a DSN to connect to the database. Therefore you must run **sqlscript.exe** for each one.

Check "Create/Update DSN on this computer" for each installation.

However, if this is an installation for a Secondary 7810PC application or supplementary application, the databases may have already been created. If that is the case, after selecting the Server and optional Failover Server, do not select "Create Database."

The screenshot shows the '7810-PC Database Setup' window. It features a 'Tools' menu and two main configuration sections. The 'Setup Server' section includes a dropdown menu for 'Select or Write SQL Server Name', input fields for 'Login Name' and 'Password', and a checkbox for 'Create/Update Database'. The 'Setup Failover Server' section includes a dropdown menu for 'Select or Write SQL Failover Server Name' (currently set to 'none'), input fields for 'Login Name' and 'Password', and a checkbox for 'Create Failover Database'. At the bottom of the window, there is a checkbox for 'Create/Update DSN on this computer' which is checked, and a 'Go!' button.

Advanced SQL Configuration (Advanced users only)

This option requires log-in.

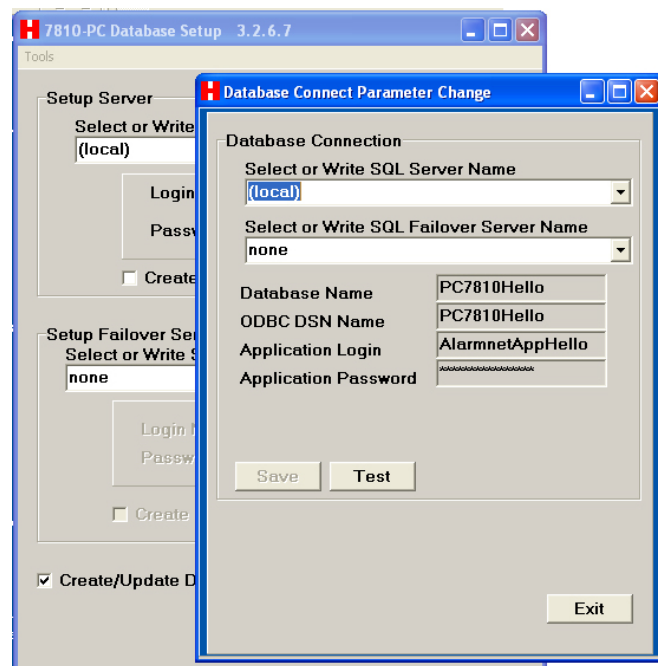
To override default configuration settings, click Tools at top left and select **Change Database Connect Params**.

Database Connect Parameter Change is a method for changing the connection string to the database for the 7810PC applications from the default. (It does **not** make changes to the database or ODBC DSN. Users must make changes manually through SQL server or by running the Main page of SQL Script.exe*).

The following parameters can be changed: **Server** name, **Mirror server** name, **Database** name, **ODBC DSN** name, **Login** name*, **Login password**. Upon Save, the new connection string is saved and will be used to create/update database* and ODBC DSN when the Main page is run subsequently.

**Login name changes are not synchronized to mirrored servers and must be done manually.*

To synchronize: From SQL Management Studio, pause Mirroring, make the login change and restart Mirroring. See "Configuring a Mirrored SQL Server Database" section (following) for details on changing login.



Configuring a Mirrored SQL Server database (Private LAN only)

This procedure is for advanced users only.

Perform this procedure only if a secondary (backup) SQL Server was set up.

1. Ensure the logins between the main SQL server and backup SQL server are synchronized.
2. Using SQL Management Studio on the main SQL server, open a new query. Enter the following code:

```
select sid from sys.sql_logins where name='AlarmnetApp'
```
3. Copy the resulting SID.
4. Using SQL Management Studio on the backup (mirror) SQL server (and witness if required), open a new query. Enter the following code substituting the SID copied from the main SQL server:

```
Drop login AlarmnetApp
create login AlarmnetApp with password='AlarmnetApp',
CHECK_EXPIRATION=OFF,
CHECK_POLICY=OFF,
sid=0xC26311B69DD2B647AFC29E678CAC5139
```

5. Setup Microsoft SQL Server Mirroring on the backup server (and witness if required), per Microsoft's directions.

When setting up a mirrored database, use the Microsoft SQL Server Management Studio to set up mirroring. The "High safety with automatic failover" option is recommended.

UL

You must use a mirrored database, and choose the "High safety with automatic failover" option.

The "High performance" and "High safety without automatic failover" options DO NOT COMPLY.

Note : This option requires a "witness" SQL server and may be installed on either of the 7810PC servers.

Configuring a Web Server for AlarmNet Direct Private! (Private LAN only)

The AlarmNetDirectPrivate! website is an optional part of the 7810PC application used for private LAN only. It enables remote viewing of:

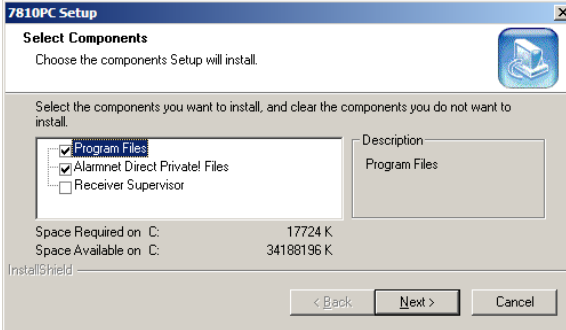
- Communicator status and configuration changes
- Receiver status and configuration changes
- Supervisor status and configuration changes
- Alarm history

The web server can also be used for hosting communicator software updates.

UL AlarmNetDirectPrivate! MUST be installed on a separate dedicated server.







Best performance is achieved by installing AlarmNetDirectPrivate! on its own dedicated server.

AlarmNetDirectPrivate! can be installed on the same server as the 7810PC application, but a configuration of this type is NOT UL compliant.

1. If the AlarmNet Direct Private! component was not installed initially, run setup again and choose **Custom Setup**. Select both **Program Files** and **AlarmNet Direct Private! Files**. Install over the previous installation.
- 
2. If the AlarmNet Direct Private! component was installed ensure the following is installed and configured on the web server.
 - The Microsoft IIS component of the server operating system (Control Panel > Add New Program > Add Windows Component > Internet Information Services).
 - ASP.NET framework 2.0 or higher.
 - Set security to ASP v2.0 or higher.
 3. If there is a problem it may be due to; another framework was installed first, or a process account error occurred. Typically the IIS mappings for ASP.NET need to be fixed. Try the following procedure by running the "Aspnet_regiis.exe" utility.
 - Click **Start** then **Run**.
 - In the Open text box, type **cmd**, then press **ENTER**. At the command prompt, type the following:
"%windir%\Microsoft.NET\Framework\{version}\aspnet_regiis.exe" -i
For *version*, enter the version number of the .NET Framework installed on the server.
 - Press **Enter**.
 4. In IIS, under "Default Web Site" add a virtual directory named AlarmNetDirectPrivate. Link this to the AlarmNetDirectPrivate directory created when the 7810PC application was installed. Typically this would be C:\Program Files\Honeywell\AlarmnetDirectPrivate.
Settings should be ASP.NET 2.0. In addition the directory must have web share turned on with read, scripts, and execute permissions.
 5. Be sure to perform the procedure outlined in *Configuring the SQL Server Database* on page 14.
 6. **Make sure** there are no conflicts (such as port assignments) with other applications on the system.
 7. If AlarmNetDirectPrivate! will be viewed remotely, make sure the PC's firewall settings allow an exception for Web Server. (Control Panel > Firewall > Advanced > Settings > Services > Web server.)

Uninstalling the 7810-PC software

1. Close any open applications.
2. Determine if the **SVC7810PC service** is running. If it is, stop the service.

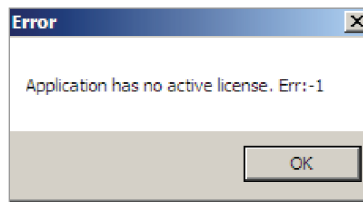
	SQL Server Active Directory Helper	Enables integration with Active Dir...	Disabled	Network S...
	SQL Server Browser	Provides SQL Server connection inf...	Started	Automatic
	SQL Server VSS Writer	Provides the interface to backup/r...	Started	Automatic
	SSDP Discovery Service	Enables discovery of UPnP devices...	Started	Manual
	SVC7810PC		Started	Automatic
	System Event Notification	Tracks system events such as Win...	Started	Automatic

3. The 7810PC application can now be removed using the Add or Remove Programs utility in the control panel. After completion, reboot.

Installing the DEMO License

This procedure is for obtaining and activating a **Demo License Certificate** for your 7810PC IP Receiver Software.

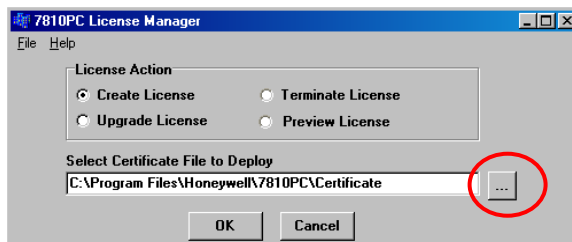
- The Demo License Certificate enables the software to be used for 90 days with a maximum of 10 subscribers. The license procedure is done after the 7810PC software is installed.
 - Requires a database.
1. Obtain the Installer software at www.alarmnet.com then navigate to **TECH SUPPORT > MyWebTech** and log in. For telephone support, call 1-800-222-6525, Monday thru Friday 8:30 am to 5:30 pm ET.
 2. Install the 7810PC IP Receiver Software. (Refer to the Installation and User Guide.)
 3. Double click the 7810PC desktop icon to start the program.
 - If an error message does not appear skip to **step #8**.
 - If an error message appears it indicates there is no license and you will have to obtain one. There may also be a **license manager** error. In this case, proceed to the next step.



4. Click **OK** to confirm the message(s) and start the License Manager.
5. Contact your AlarmNet representative at the number above and choose the technical support option.
6. Request a Demo License.
7. You will receive an email reply with your Certificate file.

At this time you may close the License Manager and 7810PC software until the Certificate from AlarmNet is received. When received, continue with the next step.

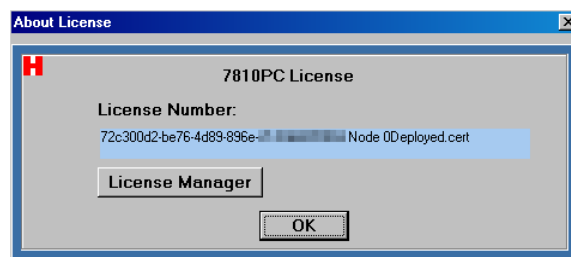
8. Copy the Certificate file to the 7810PC Certificate folder; typically **C:\Program Files\Honeywell\7810PC\Certificate**.
9. If necessary, start the 7810PC application. The License Manager starts and the following appears.



Note: There may be more than one certificate file for installations that have done a create/upgrade or have previously terminated licenses.

If you are upgrading and login with Admin credentials, the "Terminate License" option will appear.

10. Use the [...] button to navigate to the correct certificate file, then click **Create License**. Your DEMO license is now activated.
11. You can view your License information by going to **Help > About License**.

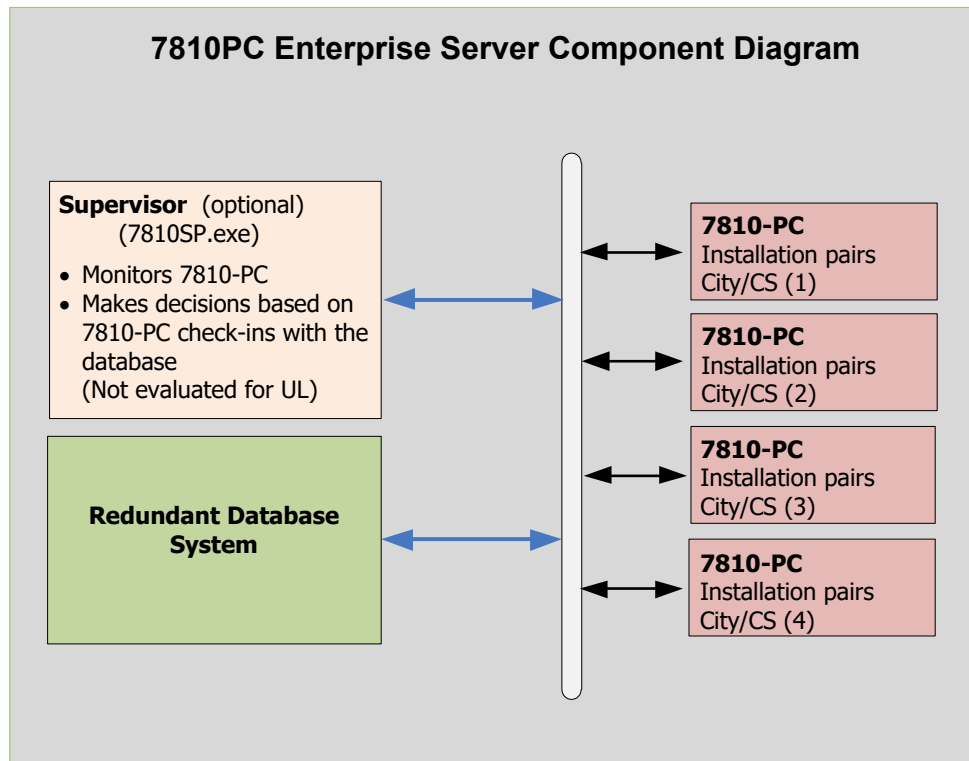


Enterprise Setup

Use the Enterprise setup if more than one installation pair of 7810PCs are to be setup using the same database and network.

- Each installation pair must have its own city/cs.
- For Private LAN accounts only, and VPN is not available.
- The Enterprise Blade Server locks each instance of 7810PC to its City/CS for supervision.
- During installation if “Enterprise” was not selected, you can run the installation again and choose Modify. Alternately you can use Notepad to edit the **7810PC.ini** file (typically [c:\Program Files\Honeywell\7810PC](#)). Edit the line ENTERPRISE_MODE_=1.

The configuration shown below is Private LAN.

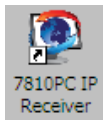


Using the 7810PC application

NOTE: Depending on the licenses purchased the screen shots depicted in this manual may vary.

Please consider the screens as reference points in the procedures.

1. You can start the application using the Start menu or by double clicking the desktop shortcut.

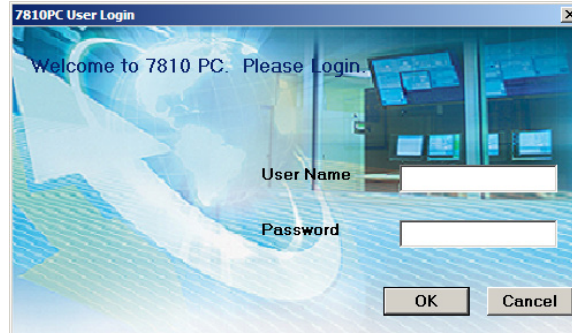
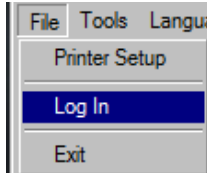


Note, if you do not have an active license, or need to upgrade an existing license refer to the “7810PC License Guide” for details.

2. A splash screen briefly appears, followed by the Alarm History viewing screen:

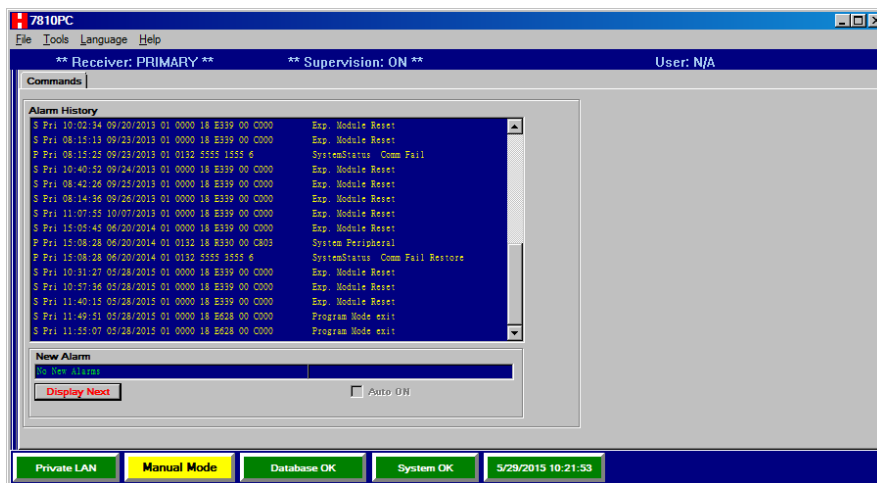


3. From the File pull-down menu, select **Log In**. The User Login screen appears, enter the User Name and Password, then click **OK**. The default User Name and Password is **Alarmnet** (case sensitive).



NOTE: For **AlarmNet Only** configurations: Uninstalling and **reinstalling** the program defaults the password.

4. The program runs; all tabs pictured below are displayed with Administrator log-in. The Administrator can set up other users (**Private LAN only**). Users that are not assigned administrator privileges can only see the Alarm History window.



Initially when you log in using the default user name and password this is an administrator account. Please visit the Users tabbed window and setup user accounts and privileges for other operators.

It is recommended that you change the default password. To change the administrative password, from the Tools pull-down menu choose **Change Password**, and follow the prompts.

A Word About Users (Private LAN only)

There are two types of users; Administrator, and Operator. Adding users and assigning their authority level, and passwords can only be done by an Administrator via the “Users” tab. Below is a chart that shows what 7810PC features are available to the “Operator”. Of course the Administrator has access to all features.

“Operator” Authority Level	
Pull-down Menu	Selections
File	Printer Setup, Login/Logout, Exit
Tools	Disable Fly-Over Help, Network Diagnostics, View Alarm History
Language	All selections available
Help	AlarmNet Home Page, About License, About Database, About
Tabs	There are no tabs available for the “Operator” authority level.

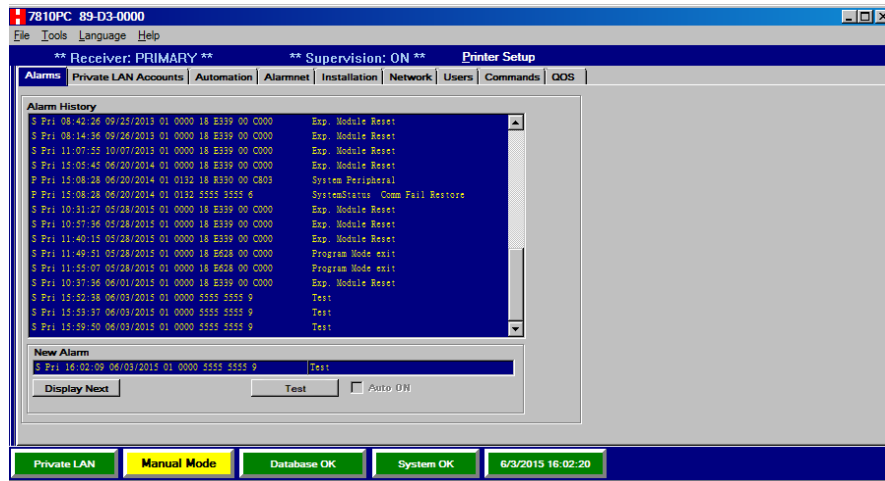
To view the status of Private LAN accounts you must log in as an Administrator, and go to the Private LAN Accounts tab.

The status of AlarmNet Accounts can only be viewed on AlarmNet websites. AlarmNet forwards its messages to the 7810PC which then reports the messages on the company’s private network automation. The 7810PC does not have knowledge of the accounts’ status directly – AlarmNet supervises them.

The following topics describe the fields on each tabbed window.

Alarms tab

This is the main operations window allowing the operator to view and process alarms.



Item	Description / Function
Alarm History	Displays the processed alarms.
New Alarm	Displays the most current alarm.
Display Next	When red, indicates a new alarm is ready for processing. The operator must click this button to acknowledge the alarm and silence audible indication at workstation. This action clears the New Alarm field and adds the event to the Alarm History window.
Test (visible when registered with AlarmNet)	Click to send a test message to AlarmNet.
Auto ON	When checked, allows the operator to quickly select Manual Mode while in Automation Mode if Fail to Manual Mode (see Automation tab) is selected.
Private LAN	Indicates the Private LAN is being monitored.
Mode	Manual: Operator acknowledgement. Automation: OK indicates normal operation and TCP/IP or Serial Mode. Auto Offline: Connection problem.
Database connection status (Private LAN only)	Green: OK ; connection operating normally. Red: Database Failure ; indicates fault in primary database. Yellow: Database Mirror Error ; indicates fault in redundant database. Yellow: Database Witness Error ; indicates fault in witness.
System status	Green: System OK ; no system faults. Red: System Trouble ; indicates a system fault.
Date / Time	Displays current date and time.

Private LAN Accounts tab (Private LAN only)

This tabbed window is used to view private LAN accounts that do not report via AlarmNet. Reports would come directly from the protected premises.

MAC Address	City ID	CS ID	Account Number	Last Heard	Account Status	Status	Supervision	IP Address	Software Version
00D02D00...	0089	00AB	0301	12/9/2011 11:35:23	Enabled	OK	US UL Line 90 Sec	10.10.100.111	2.0.131
00D02D00...	0089	00AB	07D0	11/23/2011 10:22:51	Enabled	OK	US UL Line 90 Sec	10.10.100.239	N/A
00D02D00...	0089	00AB	07D1	11/28/2011 9:21:48	Enabled	Comm Fail	US UL Line 90 Sec	10.10.100.239	N/A
00D02D00...	0089	00AB	07D2	11/23/2011 10:23:11	Enabled	OK	US UL Line 90 Sec	10.10.100.239	N/A

Item	Description / Function
Select Accounts	This grouping enables filtering the accounts by Active, Comm Fail, or Substitutable. The number of account that are associated with that filter are displayed to the right.
Sort	Enables sorting the accounts by City-CS-Account number or MAC Address.
Search	This filter enables finding a particular account by MAC Address or by the City-CS-Account number. Click the Find button to start the search.
Refresh	Enables refreshing the search criteria.
Clear Database	When changing the City and/or CS ID, clear the database after making changes.
Recovery Mode	<p>Recovery Mode is only applicable when in Private LAN Mode. In the event of a failure of the communicator (requiring replacement), Recovery mode enables the 7810PC to be updated with the 10-digit installation key of the new hardware.</p> <p>When a communicator communicates with the 7810PC and is found not in its database, a special response is sent back to the communicator, requesting it to re-register itself. The communicator then registers using the 10-digit installation key. When all accounts have been recovered, Recovery Mode can be turned off to provide better control of registration.</p> <hr/> <p>UL: Replacing a communicator requires operator intervention.</p> <hr/> <p>When a Communicator is replaced in Private LAN, click the Recovery Mode button. Then register the unit. When registration is complete, click the Recovery Mode button again to turn off recovery mode.</p>
Viewing window	Displays the private LAN accounts according to the filtering criteria. Column heads show specific account details. Navigation buttons (bottom right) enable fast navigation of accounts.
Enable, Delete, FTP/Telnet, Software Update	Maintenance and communication options for the account selected in the viewing window.
Substitute	Allows replacement of an existing system with a new one, using the same account number.
Send Test Alarm	Transmits test alarms to primary, secondary or both systems.
Configuration	Allows changes to Supervision interval , Primary central station IP address and port number , Secondary central station IP address and port number and account number .

Automation tab

This tabbed window enables configuring the 7810PC to communicate with the Automation system.

Item	Description / Function
Manual Mode	Select this to put the 7810PC in Manual mode. In Manual Mode received messages are displayed in the Alarms tabbed window and must be processed manually. Automation system will not be used.
TCP/IP Mode	Select this to enable the 7810PC to communicate with Automation system via the intranet/internet.
Auto Port	Use the default communications port displayed, or enter the number of another port.
Specify IP Address	Select this option to enter a specific IP address for automation connection when the server has multiple network cards (NICs).
IP Address	<i>Display only.</i> Indicates the IP address of the connected TCP/IP Automation system when connected.
Serial Mode	Select this to enable communications with Automation system using the server's serial data port rather than TCP/IP or manual. Connect the Automation system to the workstation's Com 1 serial port. Use the Device Manager to ensure the com port is set to the default parameters. The Comm port is defaulted to 1, however, it can be set to another port by using Notepad to edit the 7810PC.ini file (typically c:\Program Files\Honeywell\7810PC). Add or edit the line ANICOMMPORT_=x where x is the desired port.
Fail to Manual	Check this box to enable the 7810PC to go into Manual Mode if TCP/IP or serial communications fail.
Automation Baud Rate	Use this drop-down box to select the serial communications rate to the Automation system.
Report Format	
685	When selected, data is sent in 685 report format to the Automation system.
Ademco CID (5)	When selected, data is sent in Ademco CID format to the Automation system.
10 Digit Account	When selected, data is sent in the Ademco 10 Digit Account format to the Automation system.
VPN	Check this box to enable use of a Virtual Private Network.
RX Line Number	Used to select the line card number of the receiver equipment.
Save / Cancel	Use these buttons to either save or cancel your changes.
Send Test Alarm	Use this button to test your new configuration.

AlarmNet tab

This tabbed window enables configuring the 7810PC to communicate with AlarmNet.

Item	Description / Function
Receive Alarms From	<i>Display only.</i> Information is based on the license features such as AlarmNet, Private LAN, or AlarmNet and Private LAN.
Primary Account City ID, CS ID, Subscriber ID	Use these fields to specify the primary central station account that messages will be sent to.
Virtual Subsystem	Use this field to create city/cs mapping to Ademco CID 5 formatting.
Virtual Group	Use this field to create city/cs mapping to Ademco CID 5 formatting.
	If the <u>Receive Alarms From</u> display field shows Private LAN, the following controls will be disabled.
Register	Use this button to re-register to AlarmNet.
Send Test Alarm	Use this button to test the AlarmNet configuration.
Supervision Options Old Alarm Time, Account Supervision	<p>Old Alarm Time – this is only applicable for power-on reset messages and test messages.</p> <p>Account Supervision – sets the AlarmNet supervision period.</p> <p><u>UL: Must select US UL Line 90 Sec.</u></p>

Installation tab (Private LAN only)

This tabbed window enables configuring the 7810PC role as either a Primary or Secondary receiver. A Secondary role is used when communications with the Primary 7810PC is lost. If that occurs, messages are reported to the Secondary 7810PC.

Item	Description / Function
	UL: A secondary role MUST be assigned, and the “Support Supervision” check box for each receiver MUST be checked.
This Receiver's Role Primary Secondary	Use the Primary or Secondary choices to assign a role for the 7810PC. Only one receiver can be the “Primary” receiver. Note, the IP Address field is for display only. If a Secondary role is assigned, the Support Supervision feature becomes active. Check the box if the receiver is to support supervision.
Other Receiver's Role	Use to designate the role for the other receiver. Only one receiver can be the “Primary” receiver. Note, the IP Address field is for display only. When a Secondary role is assigned, the Support Supervision feature becomes active. Check the box if the receiver is to support supervision.
Installation Key	This button is used to set the 10-digit install key for private LAN use.
Alarm History Save 90 Days Do Not Save	Use these choices to determine if the alarm history for this receiver is to be saved. <u>Save 90 Days</u> – if chosen, the alarm history is stored locally for 90 days. If needed the data can be backed up for long term storage. <u>Do Not Save</u> – if chosen, the alarm history is not stored locally at the workstation, however, it is always stored in the SQL database.

Network tab

This tabbed window enables viewing the network properties of the server, and configuring the server ports.

7810PC 89-D3-0000

File Tools Language Help

** Receiver: PRIMARY ** ** Supervision: ON ** User: Alarmnet

Alarms Private LAN Accounts Automation Alarmnet Installation **Network** Users Commands

Network Properties

PC Alarmnet MAC Address

Host Name

IP Address

Alarmnet Direct Private Server IP Address

Incoming Message Ports

Listening Port 449

☒ Specify IP Address

Compass Connect Port 7777

☐ Specify IP Address

Outgoing Message Ports

Web Port 443

Save Cancel

If you installed AlarmNet Direct Private!, ensure this field is filled in.

Item	Description / Function
PC AlarmNet MAC Address	<i>Display only.</i> Indicates MAC address assigned by AlarmNet for installed 7810PC.
Host Name	<i>Display only.</i> Indicates the server name.
IP Address	<i>Display only.</i> Indicates the server's static IP address. For servers that are configured with multiple static IPs, the entries may be scrolled.
AlarmNet Direct Private Server IP Address	Enter the static IP address of the server where the AlarmNet Direct Private resides.
Firewall Blocking indicator	ONLY appears if the firewall is blocking.
Save	Use this button to save any changes.
Cancel	Discards changes to settings.
Incoming Message Ports (Private LAN only.)	
Listening Port	Specifies the port used for communication with Subscribers. Program this port and the 7810PC's IP address into Subscriber radios.
Specify IP Address	For servers with multiple network interface cards (NIC): Select to enter a specific IP address for listening to subscribers.
Compass Connect Port	Specifies the port used for communication with a Compass server.
Specify IP Address	For servers with multiple network interface cards (NIC): Select to enter a specific IP address for Compass Connect Requests.
Outgoing Message Port (AlarmNet only.)	
Web Port	This is the port used for communicating via the web.

Users tab (Private LAN only)

This tabbed window enables the administrator to manage users.

The screenshot shows the 'Users' tab in a software window. The window has a menu bar with 'File', 'Tools', 'Language', and 'Help'. Below the menu bar is a status bar with 'Receiver: PRIMARY', 'Supervision: ON', and 'User: Chris'. The 'Users' tab is selected, showing a table with columns 'User Name' and 'Authority Level'. The table contains four rows: 'Alarmnet' (Administrator), 'Ann' (Administrator), 'Jane' (Operator), and 'Robert' (Operator). Below the table are 'Add User' and 'Delete User' buttons.

User Name	Authority Level
Alarmnet	Administrator
Ann	Administrator
Jane	Operator
Robert	Operator

Add User Delete User

- The administrator can add and delete users, assign their authority level (Administrator or Operator) and assign their initial password.
- Each user can change their password by going to **Tools > Change Password**.

Commands tab (Private LAN only)

This tabbed window (only available for an Admin log in) contains subscriber configuration commands in addition to network service, software update and test alarm commands.

The screenshot shows the 'Commands' tab in the software window. The window has a menu bar with 'File', 'Tools', 'Language', and 'Help'. Below the menu bar is a status bar with 'Receiver: PRIMARY', 'Supervision: ON', and 'User: Chris'. The 'Commands' tab is selected, showing a table with columns 'MAC Address', 'Action', 'Data', 'Expiration Type', and 'Expiration Time (sec)'. Below the table is a 'Delete' button.

MAC Address	Action	Data	Expiration Type	Expiration Time (sec)
-------------	--------	------	-----------------	-----------------------

Delete

QOS tab (Private LAN only)

The QOS (Quality of Service) tab is only available for an Admin log in. It is based on the license issued, and whether the system is using GSM communicators.

This tabbed window enables Quality of Service information to be obtained. Enter the MAC Address, or the City-CS-Account number fields of the communicator, then click the **Get QOS Data** button to query the communicator. The data obtained will be listed.

The screenshot shows the 'QOS' tab in the software window. The window has a menu bar with 'File', 'Tools', 'Language', and 'Help'. Below the menu bar is a status bar with 'Receiver: PRIMARY', 'Supervision: ON', and 'User: Chris'. The 'QOS' tab is selected, showing a 'Find QOS' section with 'MAC Address' and 'City-CS-Account' input fields, a 'Get QOS Data' button, and a red message 'No QOS Data Found'. Below this is a table with columns 'MAC Address', 'Date/Time', 'Line Voltage', 'Battery Voltage', 'RX Level', 'Min Level', 'Max Level', and 'Message Type'.

Find QOS
MAC Address [] Get QOS Data
No QOS Data Found
City-CS-Account [] - []

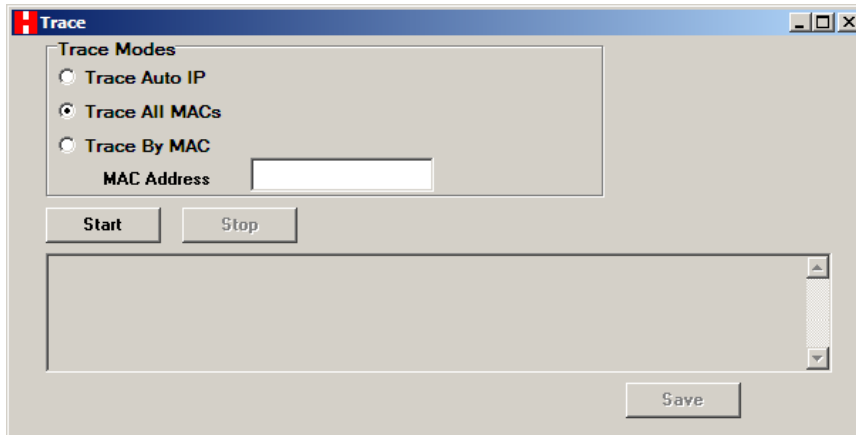
MAC Address	Date/Time	Line Voltage	Battery Voltage	RX Level	Min Level	Max Level	Message Type

Available Tools and Information Screens

There are various tools and information screens that can be accessed by using the pull-down menus. Most are self explanatory, therefore we will only cover the unique tools below.

Trace Tool (**Tools > Trace**)

The trace screen is used to watch (take out “incoming”) alarm traffic and to look for problems. Additionally it can be used to track the data from a single communicator to see how it is reacting. Choose the desired trace mode and click **Start**. Note, the Trace Tool is not available when running the 7810PC as a Service.

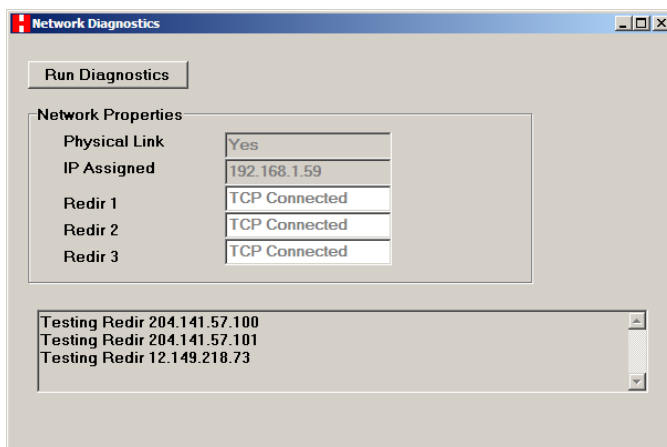


This tool is for debugging only and should not be left running as it will reduce performance.

Item	Description / Function
Trace Auto IP	Select this to view alarm traffic to and polling with IP automation.
Trace All MACs	Select this to view incoming alarm traffic.
Trace By MAC	This choice is used in conjunction with the MAC Address field to select the specific device you want to run a trace on. This acts as a filter to focus solely on the specified device.
MAC Address (field)	Enter the MAC address of the device you want to trace.

Network Diagnostics (**Tools > Network Diagnostics**)

This tool enables identifying the network redirects.



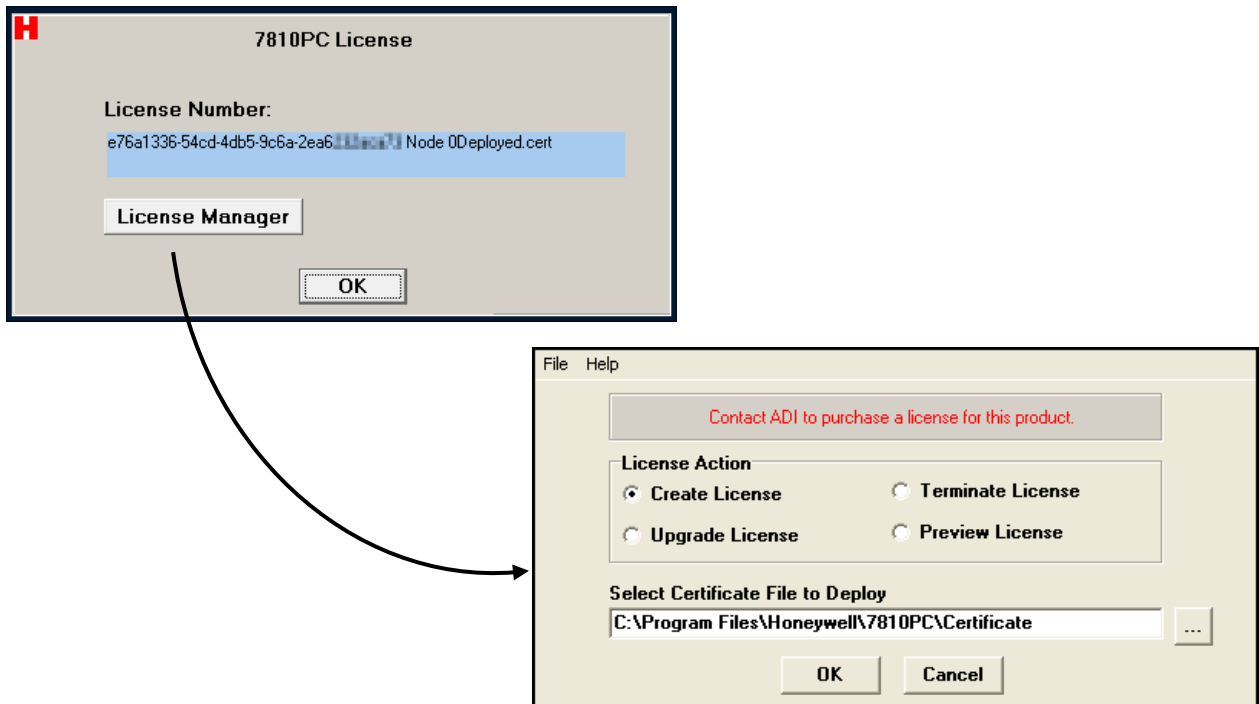
Export Subscribers (Tools > Export Subscribers) (Private LAN only)

This tool creates an Excel spreadsheet file of the subscribers. Typically this file is stored in the following path:

[C:\Program Files\Honeywell\7810PC\xx-xxSubscribers.csv](#) (The xx-xx will be the City ID, and CS ID.)

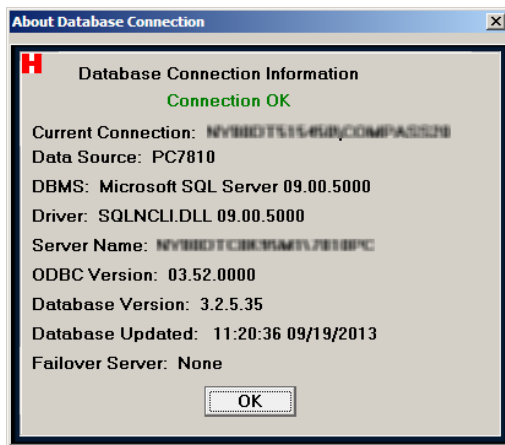
About License (Help > About License)

This information screen displays the active license number. There is a “License Manager” button that enables you to Create a new license, Upgrade an existing license, or Terminate a license (Must be logged in with Admin credentials).



Database Information (Help > About Database) (Private LAN only)

This information screen provides an overall view of the 7810PC's database configuration.



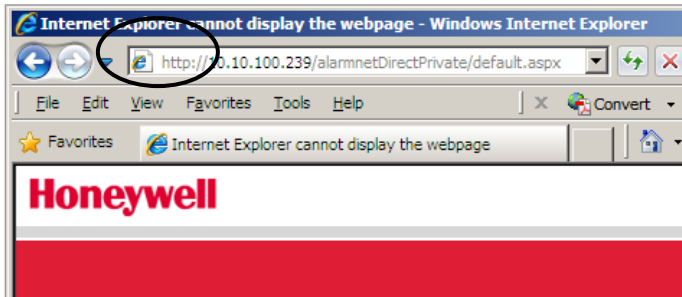
Using the AlarmNet Direct Private! website (Private LAN only)

AlarmNet Direct Private! enables viewing alarms remotely from a web browser.

To access AlarmNet Direct Private!, enter the server's IP address in your browser's address field. You will be redirected to the website. For example:

<http://10.10.100.239/alarmnetDirectPrivate/default.aspx>

After the page loads, create a desktop shortcut by positioning the cursor over the address icon, left click the mouse and drag it onto the desktop.



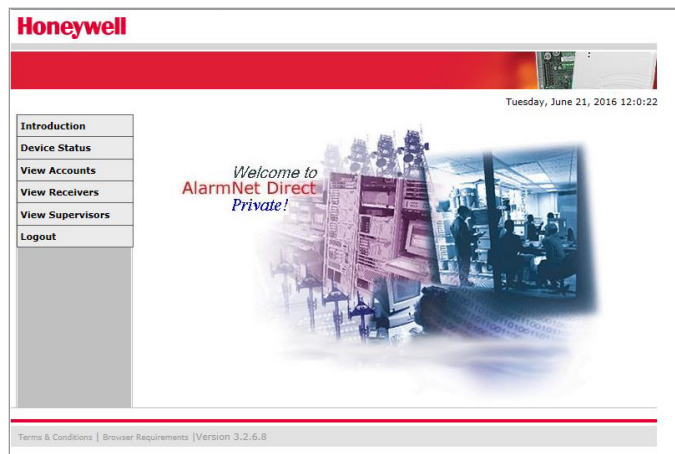
Log In

Navigate to the AlarmNet Direct Private! home page using either the desktop shortcut (created in the last paragraph) or by typing the address into the browser's address field. The Login page appears.

A screenshot of the AlarmNet Direct Private! login page. The page has a red header with the "Honeywell" logo. Below the header, there is a login form on the left with the text "Please Log In" and fields for "User Name:" and "Password:". Below these fields are "Log In" and "Reset" buttons. To the right of the form is a large, stylized image of a server room with the text "Welcome to AlarmNet Direct Private!" overlaid. At the bottom of the page, it says "AlarmNet Direct provides a vital link for our customers. Private!".

Enter your **User Name** and **Password** (same as used for the 7810PC), then press **Enter**. The "Welcome" window appears.

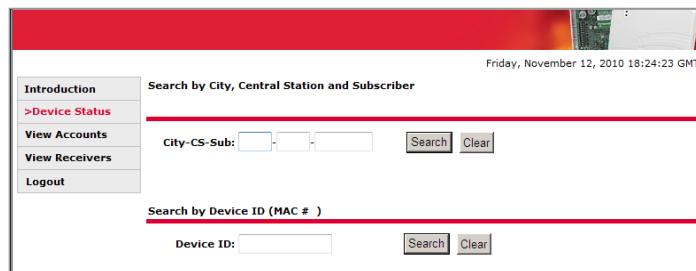
AlarmNet Direct Private! is easy to navigate. The layout consists of a navigation bar on the left, and an information window to the right.



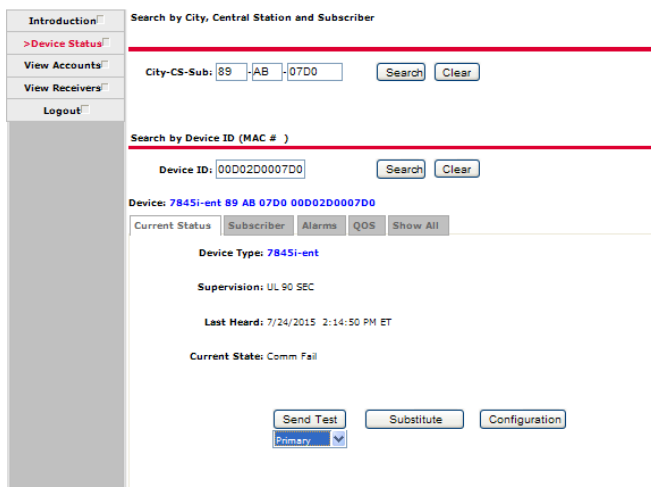
By clicking on a category in the Navigation bar, the associated information window is displayed. The selected category in the Navigation bar will appear in RED. From the information window you can view, edit, add, or delete information. Some information can be printed, or saved as a file. The following paragraphs explore the various AlarmNet Direct Private! categories.

Device Status

This category enables you to quickly check the status of a AlarmNet reporting communicator devices.



Find the device by performing a search. You can search by City code, Central Station and Subscriber number, or Device ID by entering the data and clicking the **Search** button. A detailed status screen for the device is displayed as shown below.



Send Test: Transmits test alarms to Primary, Secondary or both systems.

Substitute: Allows replacement of an existing system with a new one, using the same account number.

Configuration: Allows changes to **Supervision interval, Primary central station IP address and port number, Secondary central station IP address and port number and account number.**

Besides the Current Status information, there are tabs for Subscriber, Alarms, QOS (Quality of Service) and Show All that display more information. Some tabbed information screens allow additional functions or commands to be performed on the communications device.

View Accounts

This category enables you to quickly check the status of a Private LAN reporting communicator devices. Start by entering the City-CS information, then filling in the **Start Range** and **End Range** fields if desired.

Introduction

Device Status

>View Accounts

View Receivers

Logout

--->DISABLE POP-UP BLOCKERS FOR THIS PAGE<---

Friday, November 12, 2010 18:35:36 GMT

Disclaimer: Accounts shown on this page may not show status of pending transactions being processed

Select a City-CS

Select start and/or end range for subscriber range:

Start Range:

End Range:

SubmitReset

Refresh the page, information interrupted

Instructions:

Select a CityID-CSID

Pick filtering options (optional)

- choose a min limit for subscriber, subscribers will be >= min

- choose a max limit for subscriber, subscribers will be <= maximum

Press Submit button to display results

Press Reset to clear page and reset all controls

Upon completion, click **Submit**. An example of the search results is shown below.

Introduction

Device Status

>View Accounts

View Receivers

Logout

--->DISABLE POP-UP BLOCKERS FOR THIS PAGE<---

Friday, November 12, 2010 18:35:36 GMT

Disclaimer: Accounts shown on this page may not show status of pending transactions being processed

Select a City-CS

89

AB

Select start and/or end range for subscriber range:

Start Range:

07D5

End Range:

SubmitReset

Displaying Results [1 - 100] of 1496 Total Results on Page 1 of 15 Total Pages [Sortable Columns](#)

[Click Here](#) to download the Device List Information.

Details	City	CS	Sub	Status	CommStatus
Details	89	AB	07D5	Active	Comm Fail
Details	89	AB	07D6	Active	Comm Fail
Details	89	AB	07D7	Active	Comm Fail
Details	89	AB	07D8	Active	Comm Fail
Details	89	AB	07D9	Active	Comm Fail
Details	89	AB	07DA	Active	Comm Fail
Details	89	AB	07DB	Active	Comm Fail
Details	89	AB	07DC	Active	Comm Fail
Details	89	AB	07DD	Active	Comm Fail
Details	89	AB	07DE	Active	OK
Details	89	AB	07DF	Active	OK
Details	89	AB	07E0	Active	OK
Details	89	AB	07E1	Active	OK
Details	89	AB	07E2	Active	OK
Details	89	AB	07E3	Active	OK

« First

« Previous

Pick a Page:

1

Goto New Page

Next »

Last »

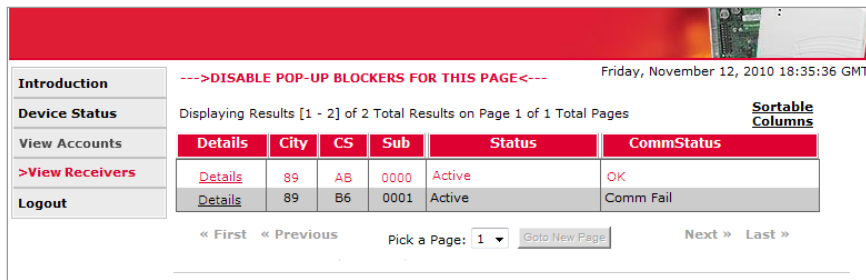
Information can further be sorted by clicking any of the column heads. The resultant sorted data can also be downloaded.

For any particular account, more detailed information can be displayed in a pop-up window by clicking **Details**.

39

View Receivers

This category enables you to view your receivers.



Introduction

Device Status

View Accounts

>View Receivers

Logout

--->DISABLE POP-UP BLOCKERS FOR THIS PAGE<---

Friday, November 12, 2010 18:35:36 GMT

Displaying Results [1 - 2] of 2 Total Results on Page 1 of 1 Total Pages

Sortable Columns

Details	City	CS	Sub	Status	CommStatus
Details	89	AB	0000	Active	OK
Details	89	B6	0001	Active	Comm Fail

« First « Previous Pick a Page: 1 Goto New Page Next » Last »

For any particular receiver, more detailed information can be displayed in a pop-up window by clicking **Details**.



Device: 7810PC Receiver

Current Status

Device Type: 7810PC Receiver

Supervision: UL 90 SEC

Last Registered: 10/18/2010 2:55:01 PM ET

Current State: Comm Fail

Status Detail: PRIVATE LAN,AUTO IP OK

Send Test

Subscriber Information

Reference ID: 10562

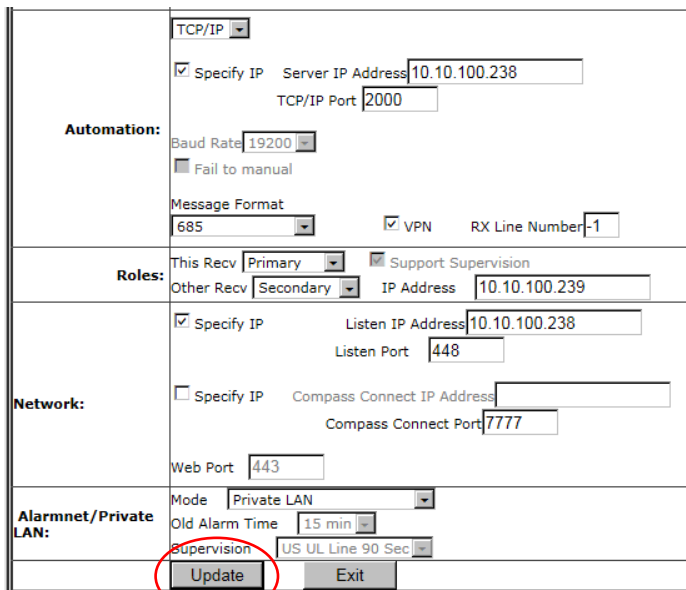
Host Name: c1022046

IP Address: 10.10.100.220

Software Version: Beta 3.2.0.0

Receiver Configuration

Clicking on **Receiver Configuration** enables you to view and configure the receiver. If you make changes, click **Update** to apply the changes, or **Exit** to cancel the changes and return to the View Receivers category.



TCP/IP

Specify IP Server IP Address 10.10.100.238

TCP/IP Port 2000

Automation:

Baud Rate 19200

Fail to manual

Message Format 685

VPN RX Line Number -1

Roles:

This Recv Primary Support Supervision

Other Recv Secondary IP Address 10.10.100.239

Network:

Specify IP Listen IP Address 10.10.100.238

Listen Port 448

Specify IP Compass Connect IP Address

Compass Connect Port 7777

Web Port 443

Alarmnet/Private LAN:

Mode Private LAN

Old Alarm Time 15 min

Supervision US UL Line 90 Sec

Update Exit

View Supervisors

This category enables you to view your supervisors.

--->DISABLE POP-UP BLOCKERS FOR THIS PAGE<---

Introduction
Device Status
View Accounts
View Receivers
>View Supervisors
Logout

Displaying Results [1 - 1] of 1 Total Results on Page 1 of 1 Total Pages

Sortable Columns

Details	City	CS	Sub	Status	CommStatus
Details	89	AB	0000	Active	OK

« First « Previous Pick a Page: 1 Goto New Page Next » Last »

For more information on a particular supervisor, click **Details** (circled above).

Device: 7810PC Supervisor 89 AB 0000 MAC:000000000000

Current Status

Device Type: 7810PC Supervisor


Last Heard: 6/21/2016 1:43:34 PM ET


Current State: OK

Status Detail: PRIVATE LAN,AUTO IP OFFLINE

[Send Test](#)

Subscriber Information

Host Name: 

IP Address: 

Software Version: 3.2.6.8


[Configuration](#)

Receiver/Supervisor Information

Edit Configuration: 89-AB-0000

Subsystem - Grp: 12 - 345

TCP/IP ☐ Fail to manual

☒ Specify IP Server IP Address 

TCP/IP Port 2001

Automation: Baud Rate 19200

Message Format Ademco CID (5) ☐ VPN RX Line Number 85

[Update](#) [Exit](#)

Clicking on **Configuration** (circled above left) enables you to view and configure the supervisor. If you make changes, click **Update** (circled above right) to apply the changes, or **Exit** to cancel the changes and return to the View Supervisors category.

Message Formats

There are two categories of messages that are sent by AlarmNet to the Central Station.

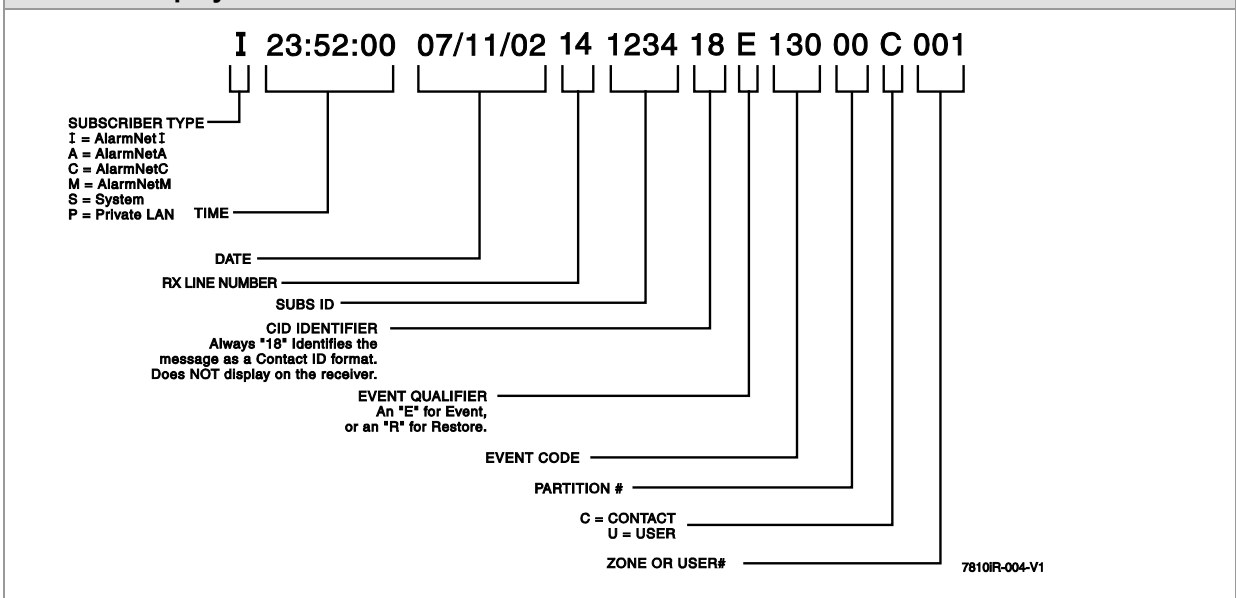
- **Subscriber Messages** – indicate alarm or trouble conditions at the subscriber premises, or identify issues with the subscriber communicator. Subscriber messages can be sent in one of two formats; ADEMCO high-speed or Contact ID.
- **Network Messages** – indicate specific conditions with the AlarmNet network, central station transceivers, and or subscribers. Network messages are sent in ADEMCO high-speed ONLY and may include messages for subscribers # 0000 or # 0001.

ADEMCO Contact ID Format

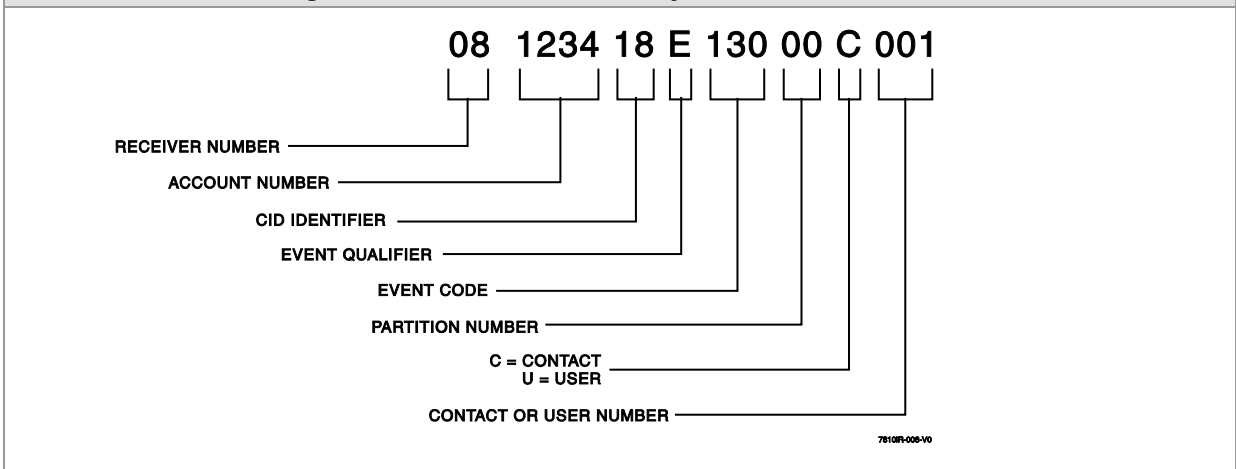
This format consists of:

- A 4-digit subscriber ID
- A 'qualifier' that indicates whether the message is an event or a restoral
- An event code indicating the type of AlarmNet
- An optional partition number
- The exact zone or user number that initiated the report

How it is displayed on the 7810PC



How Contact ID Messages are sent to Automation system in Serial Automation Mode

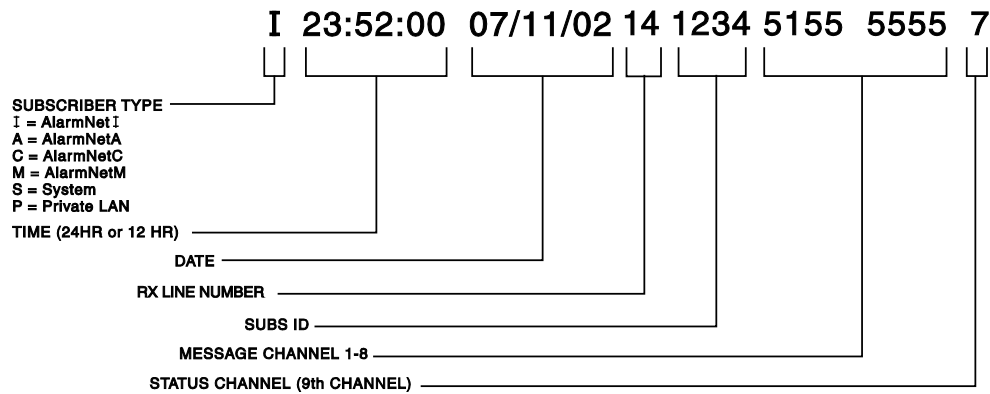


ADEMCO High-Speed Format

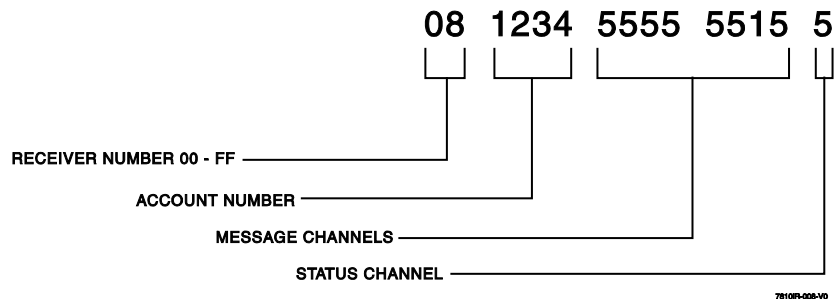
This format consists of:

- A 4-digit subscriber ID
- Eight channels of information indicating zones or other information in each message
- A ninth status digit indicating the type of report

How it is displayed on the 7810PC



How Contact ID Messages are sent to Automation system in Serial Automation Mode



Reading a High Speed Message

The status channel (9th channel) identifies the type of message, as shown below:

- 0 = Diagnostic Messages
- 1 = Notification Message
- 2 = Not applicable to radio accounts
- 3 = Not applicable to radio accounts
- 4 = Not applicable to radio accounts
- 5 = Subscriber Trouble / Special Reports
- 6 = Status Message
- 7 = Alarm Condition
- 8 = Alarm with low battery (old 7620 radio)
- 9 = Installer or network generated test message, Daily Test Message

The previous eight channels indicate the message details:

- For System messages, each channel represents a unique condition.
- For Subscriber Zone Conditions, each channel represents a zone.

High-Speed Message Interpretation

- The “Key Indicator” is a unique character in a specific channel position that can be used to identify a specific type of message.
- The letters ‘cccc’ are used to represent the customer subscriber ID number (communicator or radio account number).
- Where the subscriber account numbers “0000” and “0001” are used, these identify messages pertaining to the primary and secondary AlarmNet C/S transceivers, respectively. Messages for these accounts apply to central stations using AlarmNet-A transceivers only.
- Other lowercase letters are used to represent different codes or characters that have various meanings in certain messages, and are defined in the ‘Definitions’ column of each table.
- The messages apply to all types of subscriber devices (AlarmNet–A and –I), except where noted. Subscriber devices are also referred to as communicator devices.

A = AlarmNet A

I = AlarmNet i

Message	Definition	Applies To
Status Channel = 0 (Diagnostic Message)		
Key Indicator: “F” in 3rd channel		
cccc ngF0 s0fm 0	F-Type diagnostic (RF) n = number of the node reporting (1-9, A-F) g = node group number (0 or 1) F = F-type diagnostic s = signal strength (0-9, or A) f = frequency (always “0”, not used) m = modulation level (always “0”, not used)	A
cccc ngF0 s00t 0	F-Type diagnostic (pass/fail) n = number of the node reporting (1-9, A-F) g = node group number (0 or 1) F = F-type diagnostic 0 = unused, always “0” s = signal strength (0-9, or A) 00 = unused, always “00” t = pass/fail result: A = acceptable F = failure	A
Key Indicator: “4” in 4th channel		
cccc nng4 rrrr 0	Subscriber Command Failure (Dialer reporting) nn = number of the node reporting (01 to 15) g = node group number (0 or 1) 4 = subscriber trouble message rrrr = reason code: 0001 = Low signal strength 0002 = Frequency error 0003 = Modulation error 0004 = Keyed-on subscriber 0005 = Repeating alarm suppressed 0006 = Redundant supervision warning 0007 = Multiple nodes down 0010 = Redundant supervision restore 0011 = Multiple nodes down restore 0012 = 2-Way radio internal tamper 0013 = Authentication – no response 0014 = Authentication violation 0015 = Authentication Initialized * Messages for account # “0000” refer to the central station.	A

Message	Definition	Applies To
Key Indicator: "A" in 3rd channel		
cccc ngA0 s0fm 0	A-type diagnostic (RF) n = number of the node reporting (1-9, A-F) g = node group number (0 or 1) A = A-type diagnostic s = signal strength (0-9, or A) f = frequency (always "0", not used) m = modulation level (always "0", not used)	A
Key Indicator: "D" in 3rd channel		
cccc 00D0 0005 0	Zone swinger suppression	
cccc 00D0 010C 0	Authorized radio or subscriber substitution	I
cccc 00D0 010E 0	Unauthorized substitution attempt	I
cccc 00D0 020E 0	Service termination alarm	I
cccc 00D0 0104 0	Reset command sent	A
cccc 00D0 0103 0	Comm inquiry sent	A
cccc 00D0 0106 0	Test command sent	A
cccc ngD0 rrrr 0	Subscriber Report (RF Reporting) n = number of the node reporting (1-9, A-F) g = node group number (0 or 1) D = indicates subscriber trouble rrrr = reason code: 0001 = Low signal strength 0002 = Frequency error 0003 = Modulation error 0004 = Keyed-on subscriber 0005 = Repeating alarm suppressed 0006 = Redundant supervision warning 0007 = Multiple nodes down 000A= Redundant supervision restore 000B = Multiple nodes down restore 000C = 2-Way radio internal tamper 000D = Authentication – no response 000E = Authentication violation 000F = Authentication Initialized * Messages for account # "0000" refer to the central station.	A
0000 ngD0 00DB 0	Database update in progress n = number of the node reporting (1-9, A-F) g = node group number (0 or 1) D0 = indicates this node is being updated 00DB = indicates a database update	A
Key Indicator: "E" in 3rd channel		
0000 00E0 cccc 0	Illegal subscriber message	A
0000 ngE0 cccc 0	Illegal (unregistered) Subscriber (RF delivery) n = number of the node reporting (1-9, A-F) g = node group number (0 or 1) E = indicates subscriber trouble warning cccc = customer subscriber number reporting	A
Key Indicator: "F" in 3rd channel		
cccc 00F0 s000 0	F-Type diagnostic (s = signal strength)	A

Message	Definition	Applies To
Key Indicator: "1" in 4th channel		
cccc nng1 ssfm 0	A-type diagnostic (dialer) nn = number of the node reporting (01 to 15) g = node group number (0 or 1) 1 = indicates an A-type diagnostic ss = signal strength (0-10) f = frequency (always "0", not used) m = modulation level (always "0", not used)	A
Key Indicator: "5" in 4th channel		
0000 nng5 cccc 0	Illegal (unregistered) Subscriber (RF delivery) nn = number of the node reporting (1-15) g = node group number (0 or 1) 5 = always "5". Indicates subscriber trouble warning. cccc = customer subscriber number reporting	A
Key Indicator: "6" in 4th channel		
cccc nng6 ssfm 0	F-type diagnostic (dialer) nn = number of the node reporting (01 to 15) g = node group number (0 or 1) 6 = always "6". Indicates an F-type diagnostic ss = signal strength (0-10) f = frequency (always "0", not used) m = modulation level (always "0", not used)	A
Status Channel = 1 (Notification Message)		
0000 5555 5555 1	Network Alert Message – Tells the C/S to refer to their e-mail or fax machine for further information and instructions from AlarmNet.	All
cccc 5555 1555 1	Secondary CS Communications Failure	A
cccc 5555 3555 1	Secondary CS Communications Failure Restore	A
Status Channel = 5 (Subscriber Trouble / Special Report)		
Key Indicator: Account # = "0000" or "0001"		
0000 5555 5515 5 0001 5555 5515 5	Master Host Alarm The 685 generates this message internally. It indicates a failure to connect to the network. This may be caused by: <ul style="list-style-type: none"> • Antenna failure • Radio receiver failure • Substantial interference • Network outage 	A, I
0000 5555 3555 5 0000 5555 5535 5 0001 5555 5535 5	Master Host Alarm Restore	A, I
0000 5555 1555 5 0001 5555 1555 5	Master Host Alarm Reminder Notifies the central station that the redundant receiver has lost connection to the 685.	I
0000 5155 5555 5 0001 5155 5555 5	Check 685 Printer Tells the C/S to refer to their printer for messages that might not be reported through the Automation system.	A
	For subscriber reporting, each channel that displays these message types corresponds to a particular type of event. Because there are eight channels, it is possible for multiple events to be reported in multiple channels in only one message. (Example: The message "cccc 1555 5355 5" indicates a fault on zone 1 and a restore on zone 6.)	

cccc zzzz zzzz 5	Fire Zone Supervisory Fault z = zone number corresponding to the channel position (1 – 8) 1 = new zone fault 3 = zone restore 5 = normal zone condition 6 = previously report zone fault	7720ULF or 7920SE only
Status Channel = 6 (Status Message)		
	Each channel that displays these message types corresponds to a particular type of event. Because there are eight channels, it is possible for multiple events to be reported in multiple channels in only one message. (Example: The message “cccc 1555 5155 6” would indicate an AC loss and a Telco Fault.)	
Key Indicator: Account # = “0000” or “0001”		
0000 5555 1555 6	Central Station Communications Failure This may be received via the (800) Backup provision for an AlarmNet-A receiver, or by the secondary C/S transceiver for AlarmNet-M.	A
0000 5555 3555 6	Central Station Communications Failure Restore	A
0000 5515 5555 6	Central Station Radio Poll Timeout	A, I
0000 5535 5555 6	Central Station Radio Poll Timeout Restore	A, I
0000 5551 5555 6	Central Station Power-on Reset	A
cccc 1555 5555 6	AC Power Loss	A
cccc 3555 5555 6	AC Power Loss Restore	A
cccc 6555 5555 6	AC Power Loss Previously Reported	A
cccc 5155 5555 6	Low Battery This message indicates that the radio’s battery is low, not that of the alarm control panel.	A
cccc 5355 5555 6	Low Battery Restore	A
cccc 5655 5555 6	Low Battery Previously Reported	A
cccc 5515 5555 6	Two-Way Radio Poll Timeout	A, I
cccc 5551 5555 6	Power-on Reset	A
cccc 5555 1555 6	Primary CS Communications Failure	A
cccc 5555 3555 6	Primary CS Communications Failure Restore	A
cccc 5555 6555 6	Communications Failure Previously Reported	A
	Communications Failure Reminders	A, I
cccc 5555 5155 6	Telco Line Fault	A
cccc 5555 5355 6	Telco Line Fault Restore	A
cccc 5555 5655 6	Telco Line Fault Previously Reported	A
cccc 5555 5515 6	System Supervisory Fault	7720ULF
cccc 5555 5535 6	System Supervisory Fault Restore	7720ULF
cccc 5555 5565 6	System Supervisory Fault Previously Reported	7720ULF
cccc 5555 5551 6	Walk Test	7720ULF
cccc 5555 5553 6	Walk Test Exit	7720ULF
cccc 5353 5555 6	Exiting Battery Charge Mode	7720V2
Status Channel = 7 (Alarm condition)		
	Each channel that displays these message types corresponds to a particular type of event. Because there are eight channels, it is possible for multiple events to be reported in multiple channels in only one message. (Example: “cccc 1553 5555 7” indicates an alarm on zone 1 and a restore on zone 4.)	

cccc zzzz zzzz 7	<p>Zone Fault</p> <p>z = zone number corresponding to the channel position (1 – 8)</p> <p>1 = new zone fault</p> <p>2 = opening (system disarmed)</p> <p>3 = zone restore</p> <p>4 = closing (system armed)</p> <p>5 = normal zone condition</p> <p>6 = previously report zone fault</p> <p><u>Example:</u></p> <p>1234 5515 5555 7 indicates a new alarm on zone 3.</p> <p>1234 5165 5555 7 indicates a new alarm on zone 2, with a previously reported, un-restored condition still on zone 3. (i.e. The '6' in the third channel indicates that previously, zone 3 had gone into alarm, was reported in a message with a 1 in channel three, and remains violated.)</p> <p>1234 5335 5555 7 indicates a restore on zones 2 and 3. I.e. the conditions that caused the alarm on zones 2 and 3 have returned to a normal state.</p> <p>Sending restoral signals are optional in programming.</p> <p><u>Example:</u></p> <p>1234 5525 5555 7 indicates an Opening message.</p> <p>1234 5545 5555 7 indicates a Closing message.</p> <p>Open/Close signals are typically sent via the Control Panel's Dialer; however they may be optionally programmed to be sent via the radio as well. Open/Close messages will be sent on a particular channel when the radio is programmed properly and wired to the alarm control so that a signal is sent to the radio when the alarm is <i>Disarmed</i> (Opening) or <i>Armed</i> (Closing).</p> <p>Regarding the 7620ULF: Since the 7620ULF is not a fire alarm control, supervisory faults from the fire control panel may be used to trigger one or more of the eight channels on the 7620ULF, and thus will be reported as alarms. The central station should be aware of which of the eight channels are actually reporting supervisory conditions so alarm reports for these channels can be responded to correctly.</p>	All
cccc 5555 5551 7	AC Loss	7620ULF only
cccc 5555 5553 7	AC Loss Restore	7620ULF only
RCVB 5155 5555 7	While "Fail to manual" in LRR Line Card or 685 - Automation – Auto button unchecked	Receiver
RCVB 5551 5555 7	While "Fail to manual" in LRR Line Card or 685 - Automation – Auto button checked	Receiver
Status Channel = 8 (Alarm with low battery (older 7620 radio only))		
	<p>Each channel that displays these message types corresponds to a particular type of event. Because there are eight channels, it is possible for multiple events to be reported in multiple channels in only one message.</p> <p>(Example: "cccc 1553 5155 8" indicates an alarm on zone 1, a restore on zone 4 and a low battery.)</p>	
cccc 5555 5555 8	Low Battery Message	7620 or 7620ULF only

cccc zzzz zzzz 8	<p>Low Battery with Reported Alarms</p> <p>Alarm messages are identical to those reported when the status channel is a "7". The "8" only indicates that a low battery condition is also present. (Please refer to the description of alarm messages for status channel of "7".)</p> <p>For these radios, the low battery message will be repeated when other trouble conditions are reported (where the status channel = '6'). The low battery message will be sent directly following the trouble message.</p> <p>In addition, the low battery message will also be sent when any alarm or restore is reported.</p> <p>These radios do not have a specific Low Battery Restore message. After a low battery condition is received, a Low Battery Restore is implied when the next alarm or Open/Close message is received with a '7' in the ninth channel rather than an '8'.</p>	7620 or 7620ULF only
Status Channel = 9 (Installer generated test message)		
cccc 5555 5555 9	<p>System Test Message</p> <p>Manually triggered test from the radio.</p> <p>Test signal generated by an AlarmNet Network Technician for a specific subscriber.</p> <p>24-hour Network Acknowledgement of Subscriber Status messages.</p> <p>For older 7620 and 7620ULF radios, Zone alarms may also be sent at the same time as a test message. These messages will be in the identical formats to those alarms shown for Status Channel 5 or 8, except that the status channel will be a 9.</p>	All

Contact ID Format

Contact ID reporting takes the following format:

CCCC Q EEE GG ZZZ

Where:

CCCC = customer (subscriber account number)

Q = event qualifier, E = new event, R = restore

EEE = event code

GG = partition number, 00-08 (always 00 for non-partitioned panels)

ZZZ = zone ID number reporting the alarm (001-099), or user number for open/close reports.

* System status messages (i.e. AC Loss, Low Battery) contain zeros in the ZZZ location.

SUBSCRIBER ID #	EVENT QUALIFIER Event or Restore	EVENT CODE*	PARTITION #	ZONE OR USER #
XXXX	E or R	000	00	C000 or U000

Event Code Classifications

Not all Contact ID codes are provided by each model Control Panel. For complete Contact ID code information for your system refer to your Control Panel Installation Guide.

Medical

100	Medical	Emerg-Personal Emergency-#
101	Pendant Transmitter	Emerg-Personal Emergency-#
102	Fail to report in	Emerg-Fail to check in-#

Fire Alarms

110	Fire	Fire-Fire Alarm-#
111	Smoke w/Verification	Fire-Fire Alarm-#
112	Combustion	Fire-Combustion-#
113	Water flow	Fire-Water Flow-#
114	Heat	Fire-Heat Sensor-#
115	Pull Station	Fire-Pull Station-#
116	Duct	Fire-Duct Sensor-#
117	Flame	Fire-Flame Sensor-#
118	Near Alarm	Fire-Near Alarm-#

Panic Alarms

120	Panic Alarm	Panic-Panic-#
121	Duress	Panic-Duress- User 000, or duress zone number on low end panels
122	Silent	Panic-Silent Panic-#
123	Audible	Panic-Audible Panic-#
124	Duress-Access Granted	Panic-Duress Access Grant-#
125	Duress-Egress Granted	Panic-Duress Egress Grant-#
126	Hold-up suspicion print	User has activated trigger to indicate a suspicious condition.
129	Panic Verifier	

Burglar Alarms

130	Burglary	Burg-Burglary-#
131	Perimeter	Burg-Perimeter-#
132	Interior	Burg-Interior-#
133	24 Hr Burg (Aux)	Burg-24 Hour-#
134	Entry/Exit	Burg-Entry/Exit-#
135	Day/Night	Burg-Day/Night-#
136	Outdoor	Burg-Outdoor-#
137	Tamper	Burg-Tamper-#
138	Near Alarm	Burg-Near Alarm-#
139	Intrusion Verifier	Burg-Intrusion Verifier-#

General Alarms

140	General Alarm	Alarm-General Alarm-#
141	Polling Loop Open	Alarm-Polling Loop Open
142	Polling Loop Short (AI)	Alarm-Polling Loop Short
143	Expansion Mod Failure	Alarm-Exp. Module Tamper-#
144	Sensor Tamper	Alarm-Sensor Tamper-#
145	Expansion Module Tamper	Alarm-Exp. Module Tamper-#
146	Silent Burg	Burg-Silent Burglary-#
147	Sensor Supervision Failure	A sensor's supervisory circuit has reported a failure while the system was armed.

24 Hour Non-Burglary

150	24 Hour (Auxiliary)	Alarm-24 Hr. Non-Burg-#
151	Gas Detected	Alarm-Gas Detected-#
152	Refrigeration	Alarm-Refrigeration-#
153	Loss of Heat	Alarm-Heating System-#
154	Water Leakage	Alarm-Water Leakage-#
155	Foil Break	Trouble-Foil Break-#
156	Day Trouble	Trouble-Day Zone-#
157	Low Bottled Gas Level	Alarm-Low Gas Level-#
158	High Temp	Alarm-High Temperature-#
159	Low Temp	Alarm-Low Temperature-#
161	Loss of Air Flow	Alarm-Air Flow-#
162	Carbon Monoxide Detected	Alarm-Carbon Monoxide-#
163	Tank Level	Trouble-Tank Level-#

Fire Supervisory

200	Fire Supervisory	Super.-Fire Supervisory-#
201	Low Water Pressure	Super.-Low Water Pressure-#
202	Low CO2	Super.-Low CO2-#
203	Gate Valve Sensor	Super.-Gate Valve-#
204	Low Water Level	Super.-Low Water Level-#
205	Pump Activated	Super.-Pump Activation-#
206	Pump Failure	Super.-Pump Failure-#

System Troubles

300	System Trouble	Trouble-System Trouble
301	Ac Loss	Trouble-Ac Power
302	Low System Batt	Trouble-Low Battery (AC is lost, battery is getting low)
303	RAM Checksum Bad	Trouble-Bad RAM Checksum (Restore Not Applicable)
304	ROM Checksum Bad	Trouble-Bad ROM Checksum (Restore Not Applicable)
305	System Reset	Trouble-System Reset (Restore Not Applicable)
306	Panel Prog Change	Trouble-Programming Changed (Restore Not Applicable)
307	Self-Test Failure	Trouble-Self Test Failure
308	System Shutdown	Trouble-System Shutdown
309	Battery Test Fail	Trouble-Battery Test Failure (Battery failed at test interval)
310	Ground Fault	Trouble-Ground Fault-#
311	Battery Missing/Dead	Trouble-Battery is Missing or Dead
312	Power Supply Overcurrent	Trouble-Pwr. Supp. Overcur.-#
313	Engineer Reset	Status-Engineer Reset – User # (Restore Not Applicable)
314	Radio battery charger failure	The system's primary power supply has failed a supervision test. Radio devices indicate this when the backup battery charging circuit has failed its supervision test.
316	System Tamper	A tamper occurred while the system was armed.
317	Tamper while disarmed	A tamper occurred while the system was disarmed.

Sounder/Relay Troubles

320	Sounder / Relay	Trouble-Sounder/Relay-#
321	Bell 1	Trouble-Bell/Siren #1 (Event An Restore)
322	Bell 2	Trouble-Bell/Siren #2 (Event an Restore)
323	Alarm Relay	Trouble-Alarm Relay
324	Trouble Relay	Trouble-Trouble Relay
325	Reversing Relay	Trouble-Telco Reversing Relay
326	Notification Appliance Ckt. # 3	Trouble-Notification Appl. Ckt#3
327	Notification Appliance Ckt. # 4	Trouble-Notification Appl. Ckt#4

System Peripheral Troubles

330	System Peripheral	Trouble-Sys. Peripheral-#
331	Polling Loop Open	Trouble-Polling Loop Open
332	Polling Loop Short	Trouble-Polling Loop Short
333	Exp. Module Failure	Trouble-Exp. Module Fail-#
334	Repeater Failure	Trouble-Repeater Failure-#
335	Local Printer Paper Out	Trouble-Printer Paper Out
336	Local Printer Failure	Trouble-Local Printer
337	Exp. Mod. DC Loss	Trouble-Exp. Mod. DC Loss-#
338	Exp. Mod. Low Bat	Trouble-Exp. Mod. Low Batt-#
339	Exp. Mod. Reset	Trouble-Exp. Mod. Reset-#
341	Exp. Mod. Tamper	Trouble-Exp. Mod. Tamper-# (5881ENHC)
342	Exp. Module AC Loss	Trouble-Exp. Module AC Loss-#
343	Exp. Module Self-Test Fail	Trouble-Exp. Self-Test Fail-#
344	RF Rcvr Jam Detect #	Trouble-RF Rcvr Jam Detect-#
345	AES Encryption	An encryption trouble occurred.

Communication Troubles

350	Communication	Trouble-Communication Failure
351	Telco 1 Fault	Trouble-Phone Line # 1 (Comes in as Zone 1 on a V20 Panel.)
352	Telco 2 Fault	Trouble-Phone Line # 2
353	LR Radio Xmitter Fault	Trouble-Radio Transmitter
354	Failure To Communicate	Trouble-Fail to Communicate
355	Loss of Radio Super.	Trouble-Radio Supervision
356	Loss of Central Polling	Trouble-Central Radio Polling
357	LRR XMTR. VSWR	Trouble-Radio Xmitter. VSWR-#
358	Periodic Comm Test Fail/Restore	A periodic Communication path test has failed.

Protection Loop

370	Protection Loop	Trouble-Protection Loop-# (zone type 19)
-----	-----------------	--

Uplink®/Sierra Wireless® cellular backup devices send Zone 99 for Low Battery and Zone 97 for Communication Failure (no response from poll). These will report as contact ID E370 (protection loop). These signals are produced by the Uplink device itself to indicate its status. Other codes from the Uplink device may include Zones 81-86, which correspond to hardwire inputs 1-6. The contact ID message for these is determined by Uplink. Central stations may assume these messages come from a security system panel. If an unusual zone 97 or 99 is being reported, the Uplink device may be its source. Contact Uplink at 1-888-987-5465 for more information.

371	Protection Loop Open	Trouble-Prot. Loop Open-#
372	Protection Loop Short	Trouble-Prot. Loop Short-#
373	Fire Trouble	Trouble-Fire Loop-# (Supervision Loss)
374	Exit Error (By User)	Alarm-Exit Error-#
375	Panic Zone Trouble	Trouble-PA Trouble-#
376	Hold-Up Zone Trouble	Trouble-Hold-Up Trouble-#
377	Swinger Trouble	A fault has occurred on a zone that has been shut down due to excessive alarms.
378	Cross-zone Trouble	The specified zone in a cross-zone configuration has faulted without a fault on its corresponding cross-zone in a specific time period.

Sensor

380	Sensor Trbl - Global	Trouble-Sensor Trouble-#
381	Loss Of Suprvsn - RF	Trouble-RF Sensor Super.-#
382	Loss Of Suprvsn - RPM	Trouble-Rpm Sensor Super.-#
383	Sensor Tamper	Trouble-Sensor Tamper-#
384	RF Low Battery	Trouble-RF Sensor Battery-#
385	Smoke Hi Sens.	Trouble-Smoke Hi Sens.-#
386	Smoke Lo Sens.	Trouble-Smoke Lo Sens.-#
387	Intrusion Hi Sens.	Trouble-Intrusion Hi Sens.-#
388	Intrusion Lo Sens.	Trouble-Intrusion Lo Sens.-# - These codes are similar to those used for smart smoke detectors. The idea is to report a problem developing in the detector's operation.
389	Sensor Self Test Fail	Trouble-Sensor Test Fail-#
391	Sensor Watch Failure	Trouble-Sensor Watch Fail-#
392	Drift Comp. Error	Trouble-Drift Comp. Error-# - Reported by Firelite panels. The panel is not able to adjust its thresholds to balance out drift in the normal operating point of a smoke detector.
393	Maintenance Alert	Trouble-Maintenance Alert-#
394	CO Detector needs replacement	The specified Carbon Monoxide detector has reached end-of-life.

Open/Close

400	Open/Close	Opening/Closing E = Open, R = Close
401	Open/Close By User	Opening-User # / Closing-User #
402	Group O/C	Closing-Group User #
403	Automatic Open/Close	Opening-Automatic / Closing-Automatic
404	Late to O/C	Opening-Late / Closing-Late
405	Deferred O/C	Event & Restore Not Applicable
406	Cancel (By User)	Opening-Cancel
407	Remote Arm/Disarm	Opening-Remote / Closing-Remote
408	Quick Arm	Event Not Applicable For Opening / Closing-Quick Arm
409	Keyswitch Open/Close	Opening-Keyswitch / Closing-Keyswitch
441	Armed Stay	Opening-Armed Stay / Closing-Armed Stay
442	Keyswitch Armed Stay	Opening-Keysw. Arm Stay / Opening-Keysw. Arm Stay
443	Armed w/System Trouble Override	The specified user has armed the system while overriding a trouble condition.
450	Exception O/C	Opening-Exception / Closing-Exception
451	Early O/C	Opening-Early / Closing-Early-User #
452	Late O/C	Opening-Late / Closing-Late-User #
453	Failed to Open	Trouble-Fail to Open (Restore not applicable)
454	Failed to Close	Trouble-Fail to Close (Restore not applicable)
455	Auto-Arm Failed	Trouble-Auto Arm Failed (Restore not applicable)
456	Partial Arm	Closing-Partial arm-User #
457	Exit Error (User)	Closing-Exit Error-User #
458	User on Premises	Opening-User on Prem. – User #
459	Recent Close	Trouble-Recent Close – User # (Restore not appl)
461	Wrong Code Entry	Access – Wrong Code entry (Restore not applicable)
462	Legal Code Entry	Access-Legal Code entry – user # (Restore not appl)
463	Re-arm after Alarm	Status-Re Arm After Alarm-User # (Restore not appl)
464	Auto Arm Time Extended	Status-Auto Arm Time Ext. – User # (Restore not appl)
465	Panic Alarm Reset	Status-PA Reset (Restore not applicable)
466	Service On/Off Premises	A service person has entered or exited the premises.

Remote Access

411	Callback Requested	Remote-Callback Requested (No Restore) Enabled with O/C reports.
412	Success-Download/access	Remote-Successful Access (Restore Not Applicable)
413	Unsuccessful Access	Remote-Unsuccessful Access (Restore Not Applicable)
414	System Shutdown	Remote-System Shutdown
415	Dialer Shutdown	Remote-Dialer Shutdown
416	Successful Upload	Remote-Successful Upload (Restore Not Applicable)

Access Control

421	Access Denied	Access-Access Denied-User # (Restore Not Applicable)
422	Access Report by User	Access-Access Gained –User# (Restore Not Applicable)
423	Forced Access	Panic-Forced Access-#
424	Egress Denied	Access-Egress Denied (Restore Not Applicable)
425	Egress Granted	Access-Egress Granted-# (Restore Not Applicable)
426	Access Door Propped Open	Access-Door Propped Open-#
427	Access Point DSM Trouble	Access-ACS Point DSM Trbl.-# (Door Status Monitor)
428	Access Point RTE Trouble	Access-ACS Point RTE Trbl.-# (Request to Exit)
429	Access Program Mode Entry	Access-ACS Prog. Entry-User # (Restore Not Applicable)
430	Access Program Mode Exit	Access-ACS Prog. Exit-User # (Restore Not Applicable)
431	Access Threat Level Change	Access-ACS Threat Level Chg.
432	Access Relay/Trigger Fail	Access-ACS Relay/Trig. Fail-#
433	Access RTE Shunt	Access-ACS RTE Shunt-#
434	Access DSM Shunt	Access-ACS DSM Shunt-#

System Disables

501	Access Reader Disable	Disable-Access Rdr. Disable-#
-----	-----------------------	-------------------------------

Sounder/Relay Disables

520	Sounder/Relay Disable	Disable-Sounder/Relay-#
521	Bell 1 Disable	Disable-Bell/Siren # 1
522	Bell 2 Disable	Disable-Bell/Siren # 2
523	Alarm Relay Disable	Disable-Alarm Relay
524	Trouble Relay Disable	Disable-Trouble Relay
525	Reversing Relay Disable	Disable-Reversing Relay
526	Notification Appliance Ckt # 3	Disable-Notification Appl. Ckt#3
527	Notification Appliance Ckt # 4	Disable-Notification Appl. Ckt#4

System Peripheral Disables

531	Module Added	Super.-Module Added (Restore Not Applicable)
532	Module Removed	Super.-Module Removed (Restore Not Applicable)

Communication Disables

551	Dialer Disabled	Disable-Dialer Disable
552	Radio Xmitter Disabled	Disable-Radio Disable
553	Remote Upload/Download	Disable-Rem. Up/Download Disable

Bypasses

570	Zone/Sensor Bypass	Bypass-Zone Bypass-#
571	Fire Bypass	Bypass-Fire Bypass-#
572	24 Hour Zone Bypass	Bypass-24 Hour Bypass-#
573	Burg. Bypass	Bypass-Burg. Bypass-#
574	Group Bypass	Bypass-Group Bypass-User #
575	Swinger Bypass	Bypass-Swinger Bypass-#
576	Access Zone Shunt	Access-ACS Zone Shunt-#
577	Access Point Bypass	Access-ACS Point Bypass-#
578	Vault Bypass	The specified vault zone has been bypassed.
579	Vent Zone Bypass	The specified vent zone has been bypassed and will no longer report any activity.

Test / Misc

601	Manual Test	Test-Manually Triggered (Restore Not Applicable)
602	Periodic Test	Test-Periodic (Restore Not Applicable)
603	Periodic RF Xmission	Test-Periodic Radio (Restore Not Applicable)
604	Fire Test	Test-Fire Walk Test-User #
605	Status Report To Follow	Test-Fire Walk Test-User #
606	Listen-In To Follow	Listen-Listen-In Active (Restore Not Applicable)
607	Walk-Test Mode	Test-Walk Test Mode-User #
608	System Trouble Present	Test-System Trouble Present (Restore Not Applicable)
609	Video Xmtr Active	Listen-Video Xmitter Active (Restore Not Applicable)
611	Point Tested Ok	Test-Point Tested Ok-# (Restore Not Applicable)
612	Point Not Tested	Test-Point Not Tested-# (Restore Not Applicable)
613	Intrusion Zone Walk Tested	Test-Intrn Zone Walk Test-# (Restore Not Applicable)
614	Fire Zone Walk Tested	Test-Fire Zone Walk Test-# (Restore Not Applicable)
615	Panic Zone Walk Tested	Test-PA Zone Walk Test (Restore Not Applicable)
616	Service Request	Trouble-Service Request
621	Event Log Reset	Trouble-Event Log Reset (Restore Not Applicable)
622	Event Log 50% Full	Trouble-Event Log 50% Full (Restore Not Applicable)
623	Event Log 90% Full	Trouble-Event Log 90% Full (Restore Not Applicable)
624	Event Log Overflow	Trouble-Event Log Overflow (Restore Not Applicable)
625	Time/Date Reset	Trouble-Time/Date Reset-User # (Restore Not Appl)
626	Time/Date Inaccurate	Trouble-Time/Date Invalid (clock not stamping to log correctly)
627	Program Mode Entry	Trouble-Program Mode Entry (Restore Not Applicable)
628	Program Mode Exit	Trouble-Program Mode Exit (Restore Not Applicable)
629	32 Hour Event log marker	In the last 31.9 hours (1 and 1/3 days), nothing has been posted to the event log. There is nothing new to read. Does not send to central station and only occurs in the Vista-20/SE and FA sister products.

Scheduling

630	Schedule Change	Trouble-Schedule Changed (Restore Not Applicable)
631	Exception Sched. Change	Trouble-Esc. Sched. Changed (Restore Not Applicable)
632	Access Schedule Change	Trouble-Access Sched. Changed (Restore Not Applicable)

Personnel Monitoring

641	Senior Watch Trouble	Trouble-Senior Watch Trouble – Also referred to as ‘up and about’, meaning that a person has not moved about their home for a preset period of time.
642	Latch-key Supervision	Status-Latch-key Super-User # (Restore Not Applicable). Used to report when a certain user has returned home and disarmed the alarm.

Special Codes

651	Code sent to identify the control panel as an ADT® Authorized Dealer.	
652	Reserved	
653	Reserved	
654	System Inactivity	System has not been operated for x days.
655	User Code X modified by installer	The installer has modified the specified User's code.
703	Auxiliary #3	
704	Installer Test	
750-789	These codes are used by Protection One® and can be assigned any unique non-standard Event code, which Protection One will be tracking. Also can be used on custom zone types.	
796	Unable to output signal (Derived Channel)	
798	STU Controller down (Derived Channel)	
900	Download Abort	The specified Downloader ID has aborted a download sequence in progress.
901	Download Start/End	Downloader has started or ended a download sequence to the panel.
902	Download Interrupted	A download sequence has been interrupted.
903	Device Flash Update Started	
904	Device Flash Update Failure	

Continued

910	Auto-close with Bypass	An auto-close sequence has been started and the specified zone has been bypassed.
911	Bypass Closing	
912	Fire Alarm Silence	The fire alarm has been silenced.
913	Supervisory Point test Start/End	A fire supervisory device has been tested.
914	Hold-up test Start/End	The specified user has started or ended a hold-up test.
915	Burg. Test Print Start/End	The printed progress of a burglary test has been started or ended.
916	Supervisory Test Print Start/End	The printed progress of a supervisory test has been started or ended.
917	Burg. Diagnostics Start/End	A burglary system diagnostic test has been started or ended.
918	Fire Diagnostics Start/End	A fire system diagnostic test has been started or ended.
919	Untyped diagnostics	
920	Trouble Closing (closed with burg. during exit).	
921	Access Denied Code Unknown	Access has been denied because the system did not recognize the supplied access code as valid.
922	Supervisory Point Alarm	The specified supervisory point has reported an alarm condition.
923	Supervisory Point Bypass	The specified supervisory point has been bypassed.
924	Supervisory Point Trouble	The specified supervisory point has reported a trouble condition.
925	Hold-up Point Bypass	The specified hold-up point has been bypassed.
926	AC Failure for 4 hours	There has been a loss of AC power for at least four hours.
927	Output Trouble	The specified output has reported a trouble condition.
928	User code for event	This message contains the ID of the user who triggered the previous event.
929	Log-off	The specified user has logged-off of the system.
954	Communication Failure	Comm fail to the primary (zone 951) or secondary (zone 952) 7810PC in private LAN mode.
961	Database Failure	Indicates a database communication failure.
962	License Expiration Notify	Indicates product license has expired.

Event Log

999	1 and 1/3 Day No Read Log	In the last 31.9 hours (1 and 1/3 days), nothing has been posted to the event log. There is nothing new to read. Does not send to central station and only occurs in the Vista-20/SE and FA sister products.
-----	---------------------------	--

Contacting Technical Support

Before you contact Technical Support, be sure that:

- You have followed this manual accurately.
- Entered all data correctly and did not enter the letter O for the number zero.
- Note your customer account number.

Please have this information handy and contact your security system dealer.



resideo

www.resideo.com

Resideo Technologies, Inc
2 Corporate Center Drive, Suite 100
P.O. Box 9040, Melville, NY 11747

© 2020 Resideo Technologies, Inc. All rights reserved.

The Honeywell Home trademark is used under license from Honeywell International, Inc.

This product is manufactured by Resideo Technologies, Inc. and its affiliates.



800-09798V2C 8/15 Rev C