Honeywell | MAXPRO® Cloud

MPICRX Installation and User's Guide

Document Number: 800-25755-1 Rev B **July 2020**

TABLE OF CONTENTS

TABLE OF CONTENTS

1. Introduction

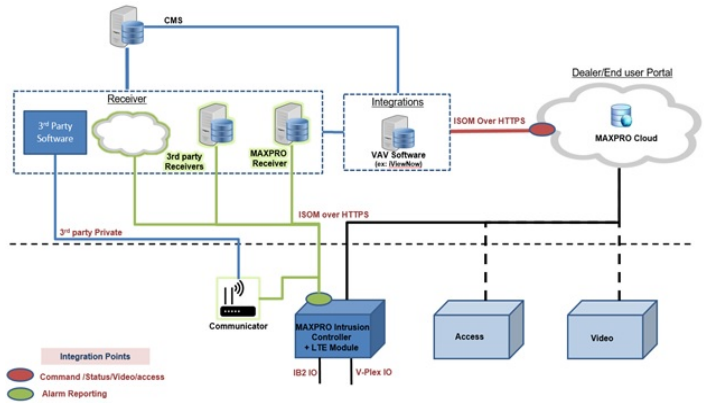
Honeywell's MPICRX Software (referred to as the *Maxpro Intrusion Central Station Receiver*) is a highly upgradeable, and feature rich IP alarm receiver solution that can take the place of traditional hardware based 7810iR-ent receivers.

MAXPRO Intrusion is an integrated (all-in-one) commercial security solution delivering Intrusion Detection, with built-in Fire Detection, Access Control and Video Alarm Verification.

The system will manage all the available security related information from the site to deliver the relevant information, to each of the people who need to react to it, in the clearest, simplest manner. This will reduce confusion and false alarms, speed up reaction to real events and deliver a safer, more comfortable environment to our customers

MAXPRO Intrusion is open system which enables integration of third-party systems through multiple secure integrations.

The following diagram illustrates major components of MAXPRO Intrusion system along with integration points (red and green bubbles) for possible third-party system integrations (highlighted in green color).



Green bubble in the above diagram represents the alarm reporting integration point for receivers/gateways to integrate for the alarms.

The following list contains the key characteristics of MAXPRO Intrusion alarm reporting.

- Secure communication; end to end encrypted, bi-directional node authentication and firewall friendly
- Based on open technologies (PKI, REST, HTTP and JSON)
- Context rich information along with alarm condition being reported
- Device and communication path supervision

2. System Requirements

2.1. Hardware and Software Requirements

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.

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.

Workstation and Server Hardware	
Processor	Intel Core 2 Duo, or compatible processor, 2.16GHz clock speed
RAM	8GB
Hard Drive Capacity	320GB (For HD data reliability, use a RAID 1 configuration. This configuration requires two drives.)
File System	NTFS
Ports	Serial Ports, Parallel Port, and USB ports as needed
Monitor	VGA 1024 x 768 resolution
Keyboard and Mouse	Required interface
Network Adapters	• Compatible with the operating system. 10BaseT connection using CAT5 or CAT6 wiring. • The Maxpro Intrusion Central Station Receiver software must be 1.0.0 or later. Primary and Secondary installations MUST use the same version of the software. • Primary and Secondary Maxpro Intrusion Central Station Receiver installations MUST run on separate workstations. • Each server computer 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	• Microsoft Windows 2012 Server and Microsoft Windows 2016 Server • Windows Server 2012 (all editions) includes the .NET Framework 4.5 as an OS component, and it is installed by default. • Windows Server 2012 R2 (all editions) includes the .NET Framework 4.5.1 as an OS component, and it is installed by default. • Windows Server 2016 (all editions) includes the NET Framework 4.6.2 as an OS component, and it is installed by default. • Internet Explorer 7.0 (or later) browser recommended. Honeywell recommends updating with the latest Windows Service Packs for optimum security.
Database (Private LAN only)	Microsoft SQL Server 2008 or SQL Server 2012. If a SQL backup database is desired, setup the backup database on another server.
Automation System Interface	An RS-232 serial interface is required from the workstation where the Honeywell's Maxpro Intrusion Central Station Receiver application is installed to the Automation system.

3. Installation

Installing the Maxpro Intrusion Central Station Receiver (MPICRX) 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 MPICRX application, understand that the installation and configuration can vary according with how the MPICRX is going to be used.

Repeat installation on Secondary MPICRX for secondary server.

3.1. Prerequisites

- 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.
- Securely receive the product and know that it has not been tampered with en-route.
- Windows Signed installation application
- Signed by Honeywell
- Ensure to use Host Intrusion Detection System and Anti-malware software installed on the device. Outputs from these can be collected by the centralized system.

3.1.1 Password Configuration

Complexity requirements should be enforced when passwords are changed or created.

Honeywell recommends you to have a password generator which will generate passwords based on the defined policy.

Administrator and system account passwords should be at least 15 characters long and contain a mixture of numbers, letters and special characters.

- English uppercase characters (A -Z)
- English lowercase characters (a -z)
- Base 10 digits (0 - 9)
- Non-alphabetic characters (!, $, #, %)

3.1.2 Workstation Configuration

- Honeywell approved Microsoft Windows update should be applied to avoid downtime on the MAXPRO receiver

Approved Honeywell Windows updates should be applied as soon as the base operating system install is completed.

Additional windows updates should be applied during maintenance windows.

3.2. Obtaining Honeywell authorized PKI certificate

Note:

MPICRX will only operate with a valid Honeywell PKI certificate.

1. Access the shared drive and install the software. (Refer to the *Installation and User Guide*.)

2. Install the MPICRX IP Receiver Software. (Refer to the *Installation and User Guide*.)
3. Double click the MPICRX desktop icon to start the program.
   - If an error message does not appear skip to step #9.
   - 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 then start the **License Manager**.
5. Locate the voucher ID found in your welcome letter.
6. Next navigate to your MPICRX installation folder (typically **C:\Program Files\Honeywell\MPICRX**) and locate the HostFile.hid file. This file was generated when the License Manager started.
7. Send an email to license.server@honeywell.com with the voucher number in the Subject line. Also attach your HostFile.hid file.

   The license server requires e-mails submissions to be provided in a specific format to facilitate automated processing. If a request complies with submission requirements, the license server will reply with a resulting license file as the attachment. Please use this format to submit your e-mail to the license server:

For New Vouchers:

To: License.Server@Honeywell.com

Subject: VOUCHID:VoucherID-should-be-entered-here

Attachment: Host ID (*.hid) file

For Upgrade or Supersede Vouchers:

To: License.Server@Honeywell.com

Subject: VOUCHID:VoucherID-should-be-entered-here

Attachment: Host ID (*.hid) file

For Transfer License Requests for Existing Voucher:

To: License.Server@Honeywell.com

Subject: VOUCHID:VoucherID-should-be-entered-here

Attachment: Host ID file and Termination file (*.term)

If upgrade licenses are active on the machine, then separate transfer requests should be

carried out for each active license. [Base and upgrade(s).]

Note:

Please generate the Host ID (*.hid) file with the latest product version installed on your machine.

8. You will receive an email reply with your Certificate file.

Note:

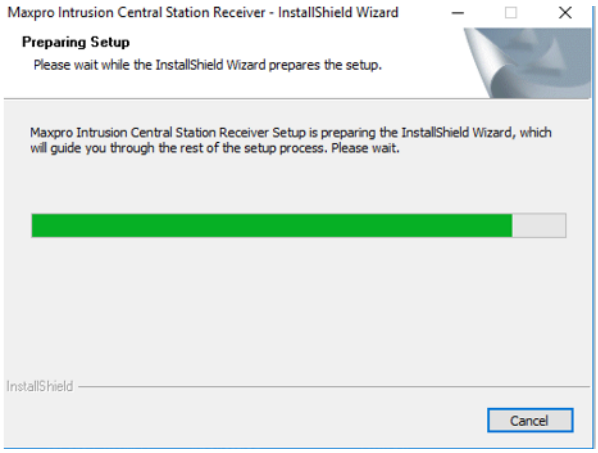
You can close the License Manager and the MPICRX software until you receive the certificate from AlarmNet. After you receive the certificate, continue with the next step.

9. Copy the Certificate file to the MPICRX Certificate folder, typically: **C:\Program Files\Honeywell\MPICRX\Certificate**.
10. If necessary, start the MPICRX application. The **License Manager** starts and the following appears.
11. Use [**...**] to navigate to the correct certificate file, then click **Create License**. Your license is now activated.
12. You can view your License information by going **Help > About License**.

3.3. Installing or upgrading the MPICRX application

To install or upgrade:

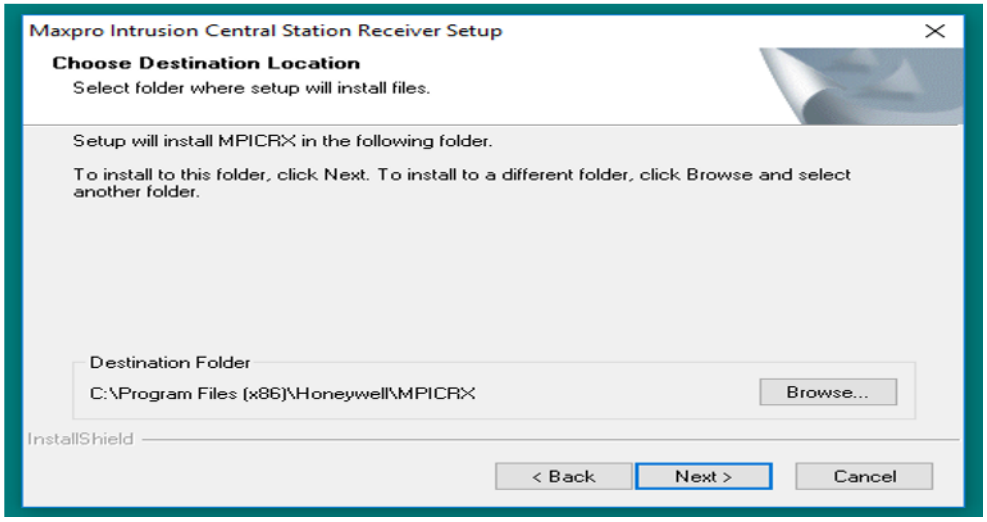
1. Copy the self-extracting application file (MPICRX_Setup.exe) to a temporary folder and double click to begin the installation.



Notes:

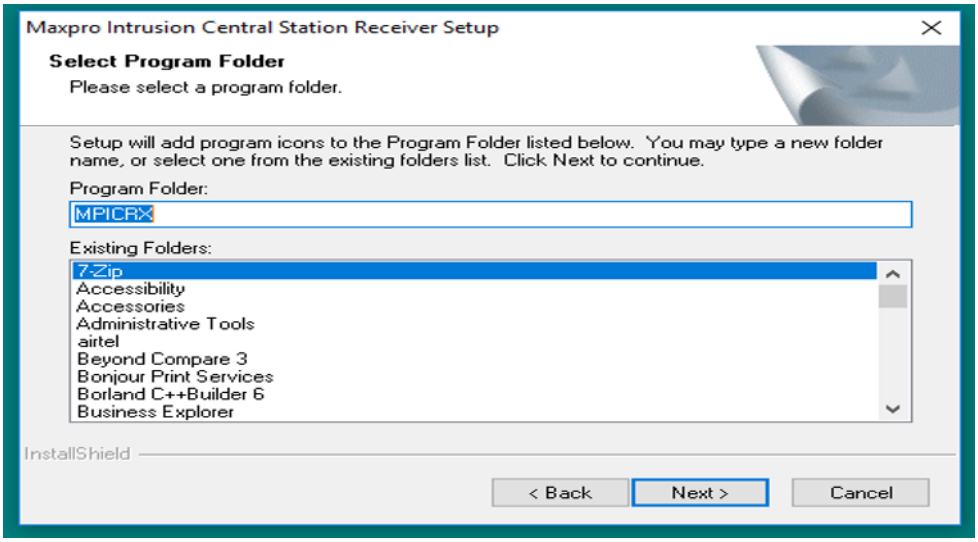
- The existing installation of **MPICRX** is detected if you are choosing to upgrade. A dialog box, with choices to **Repair** or **Remove** appears.
- Choose **Repair**, and then click **Next**. The settings and data will be retained and the upgrade will proceed with minimal intervention.
- After the upgrade is complete, refer to **Configuring the SQL Server database** 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.

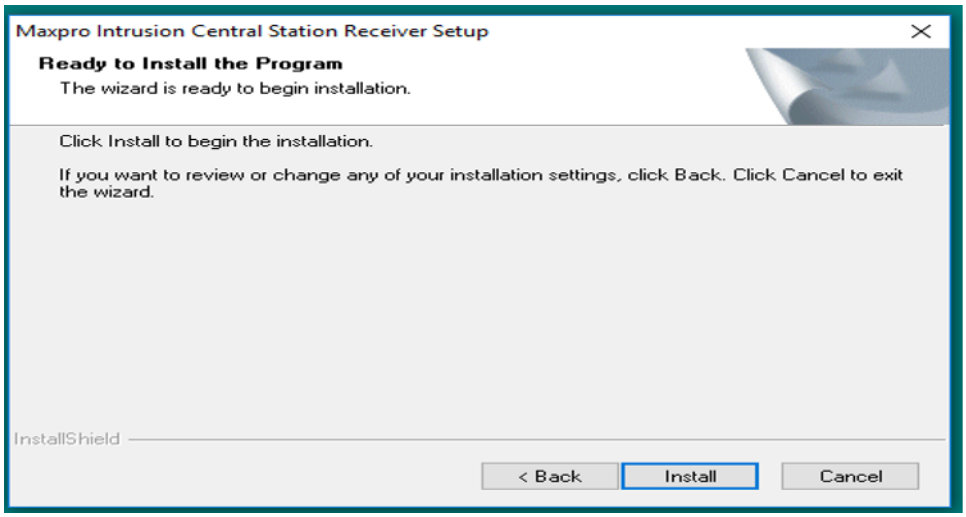


5. Click **Next.** The **Setup Type** dialog box appears.

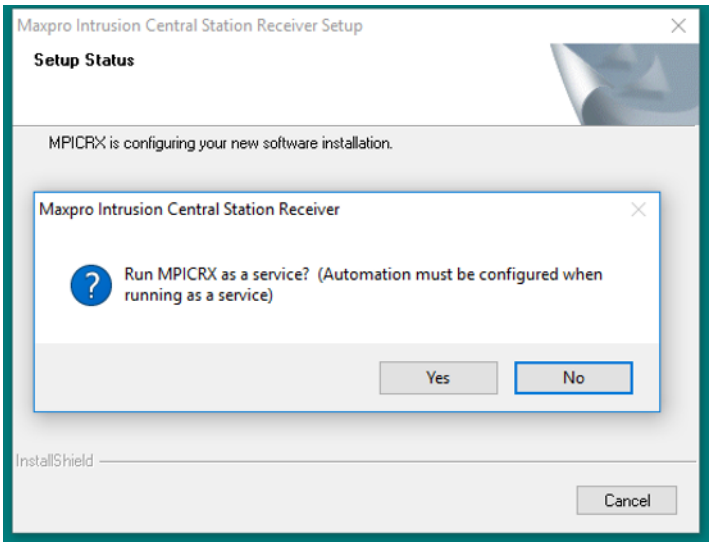
6. Select the **Setup Type** as **Typical** and then click **Next**. The **Select Program Folder** dialog box appears.



7. Accept **MPICRX** as the default program folder name or enter a name and then click **Next**. The **Setup Type** dialog box appears. Review the descriptions shown at right.



8. Choose **Standard** and then click **Next**. The **Run as a Service** prompt appears.

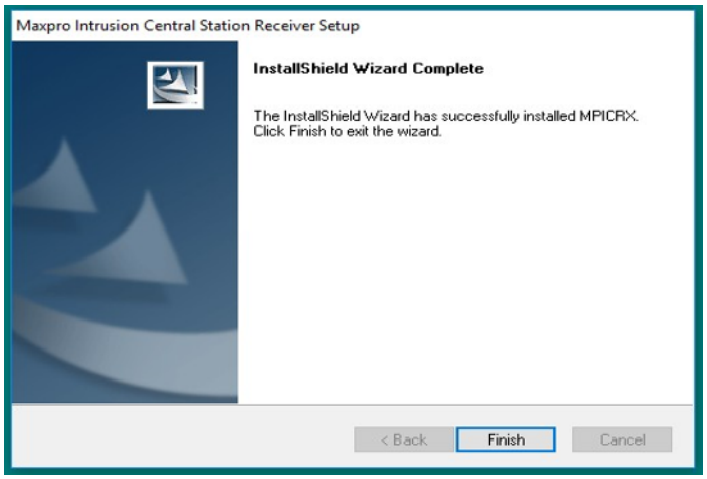


If you click **Yes** to run the Maxpro Intrusion Central Station Receiver as a Service, the application will start every time the server starts or reboots.

OR

If you click **No**, the Maxpro Intrusion Central Station Receiver will be manually started with monitor mode. Honeywell recommends you to choose **Yes** to run the Maxpro Intrusion Central Station Receiver as a **Service**.

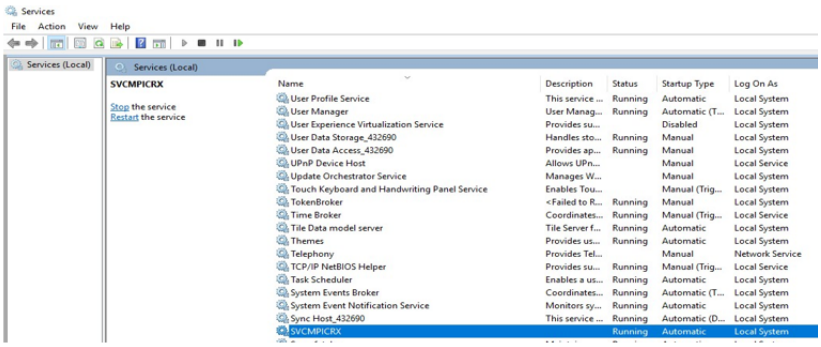
The **Installation Complete** dialog box appears.



9. Click **Finish**.

Notes:

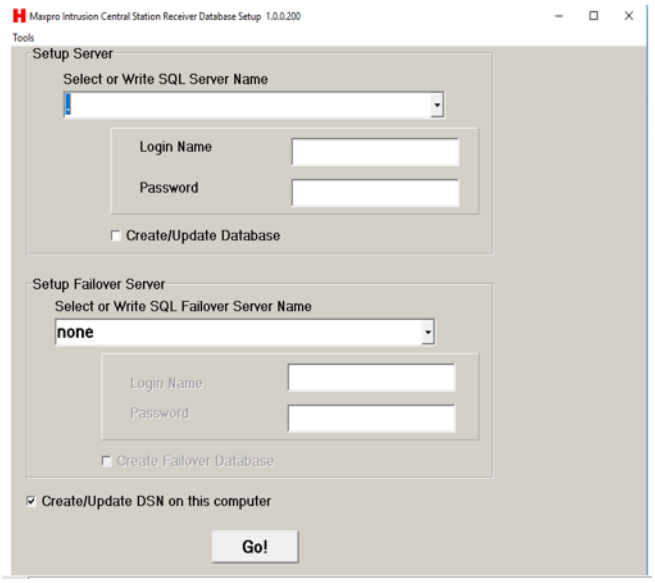
If you chose to run the Maxpro Intrusion Central Station Receiver as a Service, check that the service is **Started** and is set to **Automatic**.



Also, running the installation again on the same server will offer options to **Repair** or **Remove** an installation.

3.4. Configuring the SQL Server database

1. Ensure Microsoft SQL Server is set up (refer to the Microsoft documentation, if necessary) as follows:
   - It is recommended to install SQL Server on a different server than the **Maxpro IP Alarm Receiver 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 user name, password, and domain.
2. Set up the receiver database schema, stored procedures and the **DSN** using the **sqlscript.exe** utility. This utility resides in the receiver installation directory (typically **C:\Program Files (x86)\Honeywell\MPICRX**).
3. Execute the **sqlscript.exe** utility. Refer to the illustration in Step 4.
4. Click to select the server name from the drop down list or enter the server name. Ensure to login with administrator credentials.
5. Check **Create/Update Database**. Under **Setup Failover Server**, enter the appropriate information for the redundant SQL database (if used).



6. Click **GO!** to finish the database setup.

Every new installation of the receiver database requires a DSN to connect to the database. Hence, for every installation, you must:

- Run **sqlscript.exe**
- Select **Create/Update DSN on this computer**

However, if the installation is for a Secondary Maxpro IP Alarm Receiver application or supplementary application, the databases may have already been created. Hence, after selecting the **Server** and the optional **Failover Server**, DO NOT select **Create Database**.

Notes:

- If the SQL server is unable to connect, the following scripts have to be executed, with default selection using **Run as Administrator**.
  - msodbcsql_x64.msi
  - MsSqlCmdLnUtils_x64.msi
  - sqlncli_x64.msi
- **DO NOT** restart the machine during SQL script installation. Ignore the restart required popup message.

4. Configuring the MPICRX application

The configuration of the MPICRX is determined by the license you purchase. To complete your installation, the following details are necessary:

- A license for each Maxpro Intrusion Central Station Receiver installation. (Refer to *the MPICRX license installation guide* to obtain your license.)
- SQL Server Name, Login, and Password.
- Static IP address for the primary computer and secondary computer (required for UL). On the secondary computer, the Maxpro Intrusion Central Station Receiver software installation process MUST be repeated.

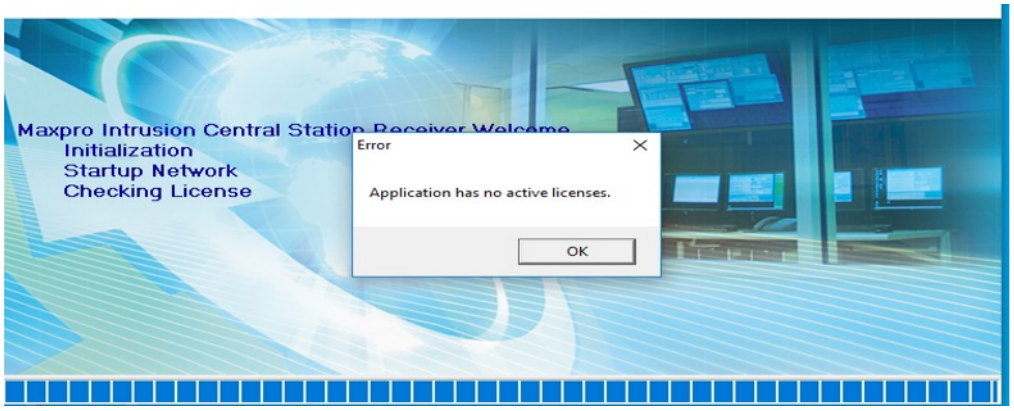
Note:

The current version of MPICRX supports 4 digit account number.

If you are yet to begin the license creation or upgrade, 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.

4.1. MPICRX Central Station Receiver license installation

1. Double click the IP Receiver desktop icon to start the program.
   - If an error message does not appear, skip to step #6.
   - 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.
2. Click **OK** to confirm the message(s) and then start the **License Manager**.



3. Get the voucher ID from Honeywell.
4. Next navigate to your Receiver installation folder (typically **C:\Program Files (x86)\Honeywell\MPICRX**) and locate the HostFile.hid file. This file was generated when the License Manager started.
5. Send an email to License.Server@Honeywell.com with the voucher number in the Subject line. Also attach your HostFile.hid file.

The license server requires e-mails submissions to be provided in a specific format to facilitate automated processing. If a request complies with submission requirements, the license server will reply with a resulting license file as the attachment. Please use this format to submit your e-mail to the license server:

For New Vouchers:

To: License.Server@Honeywell.com

Subject: VOUCHID:VoucherID-should-be-entered-here

Attachment: Host ID (*.hid) file

For Upgrade or Supersede Vouchers:

To: License.Server@Honeywell.com

Subject: VOUCHID:VoucherID-should-be-entered-here

Attachment: Host ID (*.hid) file

For Transfer license requests for existing voucher:

To: License.Server@Honeywell.com

Subject: VOUCHID:VoucherID-should-be-entered-here

Attachment: Host ID file and Termination file (*.term)

If upgrade licenses are active on the machine, then separate transfer requests should be carried out for each active license. [Base and upgrade(s).]

Note:

Please generate the Host ID (*.hid) file with the latest product version installed on your machine.

6. You will receive an email reply with your Certificate file.

Note:

You can close the License Manager and the receiver software until you receive the certificate from Honeywell. After you receive the certificate, continue with the next step.

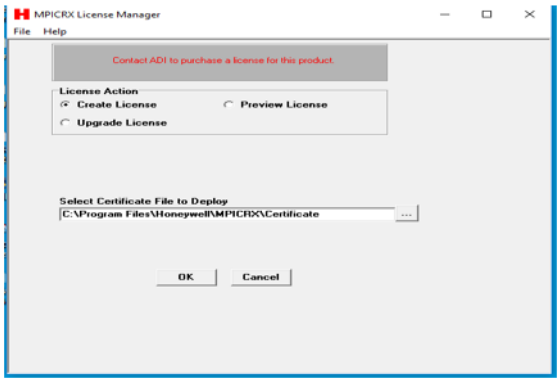
7. Copy the Certificate file to the receiver installation Certificate folder (typically, **C:\Program Files\Honeywell\MPICRX\Certificate**).

8. If necessary, start the Maxpro IP Alarm Receiver application. The License Manager starts and the following appears.

Note:

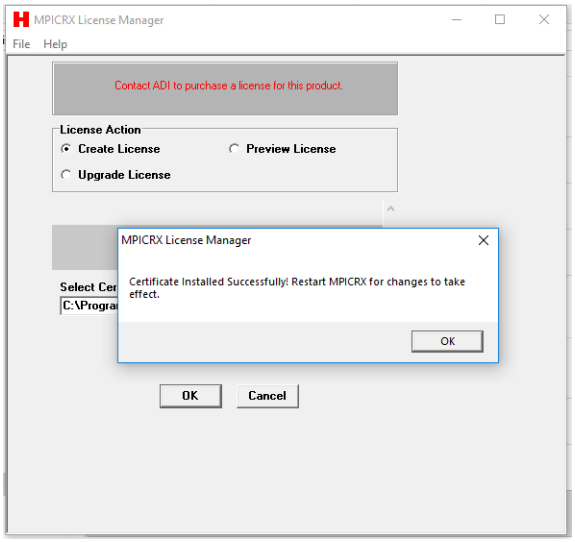
There may be more than one certificate file for installations which have had a create/upgrade or have previously terminated licenses.

If you are upgrading and if you login with Admin credentials, the **Terminate License** option appears.



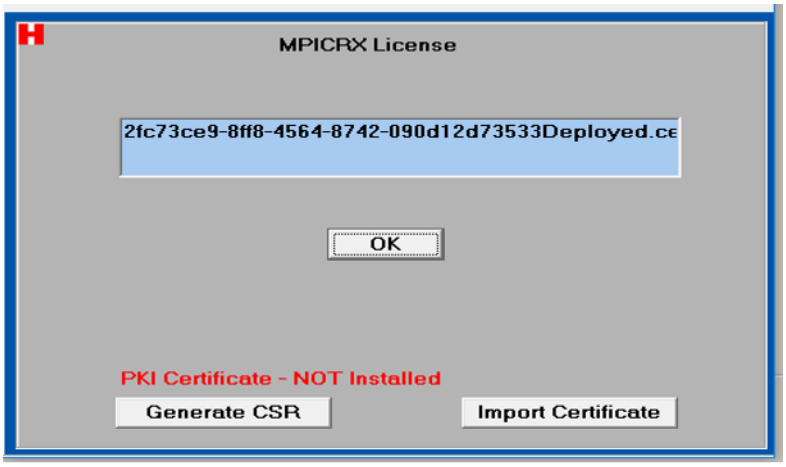
9. Click **[...]** to navigate to the correct certificate file and then click **Create License**. Your license is now activated.

10. Your license is activated successfully and the following dialog box appears.

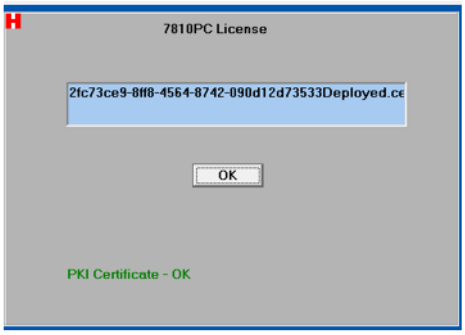


4.2. Maxpro Intrusion Central Station Receiver PKI installation

1. Go to **Help > About License**. Click **Generate CSR**.



2. Navigate to MPICRX installation folder (typically, **C:\Program Files (x86)\Honeywell\MPICRX\ Certificate**) and locate the Hon-CSR.csr file. This file was generated when Generate CSR was clicked.
3. Send an email to **hsguktechsupport@honeywell.com** with the license voucher number in the Subject line. Also attach your Hon-CSR.csr file.
4. You will receive an email reply with your Certificate file hon-cert.pem
5. Copy the Certificate file to the receiver installation Certificate folder, typically: **C:\Program Files (x86)\Honeywell\MPICRX\Certificate**.
6. If necessary, start the MPICRX application. Go to Help **> About License**. Click **Import Certificate**.
7. Once the PKI is imported successfully, the following screen appears.



8. Verify if the HTTPS status is good.

4.3. Demo License Configuration

This procedure is for obtaining and activating a Demo License Certificate for your MPICRXIP Receiver Software.

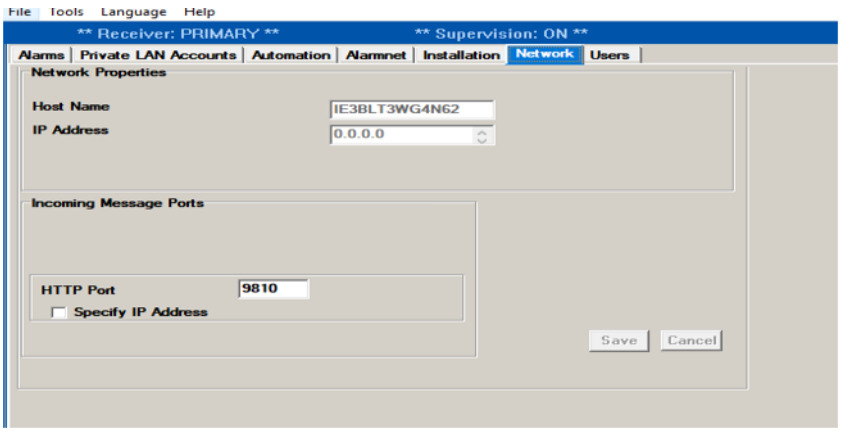
- The Demo License Certificate enables the software to be used for 90 days with a maximum of 10 subscribers.
- The license procedure is done after the MPICRX software is installed.

1. Access the Installer software through the FTP.
2. To obtain the user ID and password, check the email you would have received from the Tech Support Team.

3. Install the MPICRX IP Receiver Software. (Refer to the *Installation and User Guide*.)
4. Double click the MPICRX desktop icon to begin 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.
5. Click **OK** to confirm the message(s) and start the **License Manager**.
6. You will receive an email reply with your Certificate file.
7. At this time you may close the License Manager and MPICRX software until the Certificate from Honeywell is received. When received, continue with the next step.
8. Copy the Certificate file to the MPICRX Certificate folder; typically **C:\Program Files\Honeywell\MPICRX\Certificate**.
9. If necessary, start the MPICRX application. The **License Manager** begins.
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**.

4.4. Panel connectivity changes to connect with PKI certificate

- Receiver name to be used in panels: MPICRX-VoucherNumber.
- For example, MPICRX-2fc73ce9-8ff8-4564-8742-090d12d73533.
- There should not be space between receiver name.
- Port and IP of receiver need to configured in panel using ISP. Same port need to be configured in Maxpro IP Alarm Receiver app as shown below. (to configure port, login to the app using the default username and password as **Maxpro**)

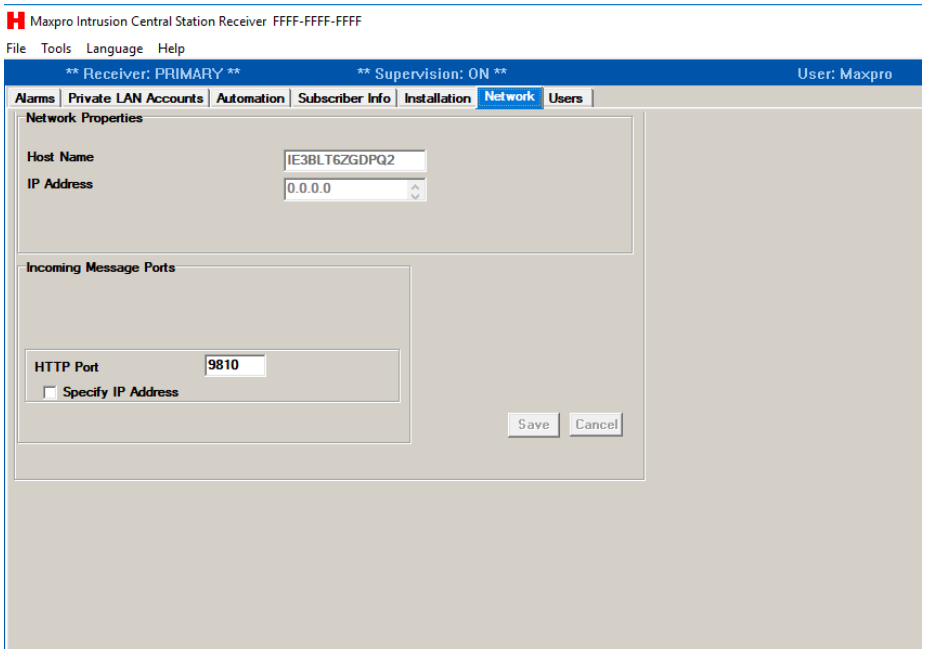


4.5. End Point Configuration

Describes how the panel communicates with the MPICRX Receiver (also known as the End Point receiver), using the static IP and the port number (provide link to firewall section).

Before you begin, you (customer) must:

- Set a static IP for the system.
- Ensure you do not provide remote access to the MPICRX system.



Note:

The IP can be purchased from the Network providers.

1. In the **MPICRX Receiver** window, click the **Network** tab.
2. Under **HTTP Port** (listening port), specify the **Receiver** port number. For example, **9810**.

Note:

Listening Port specifies the port used for communication with Subscribers. Configure this port and the MPICRX's IP address into the Subscriber panels.

4.6. Panel Replacement

When replacing a panel on MPICRX, on the **Subscriber** screen, select current panel and click Substitutable. This alerts the MPICRX that CMS wants replacement and it is not a takeover.

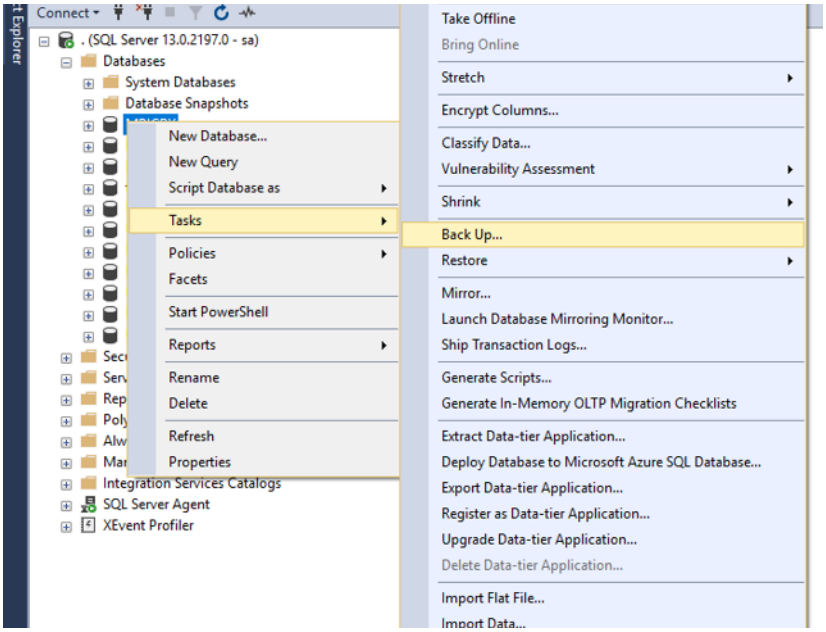
Alarm reporting Security relies on the certificate and associated private key.

4.7. Database Backup

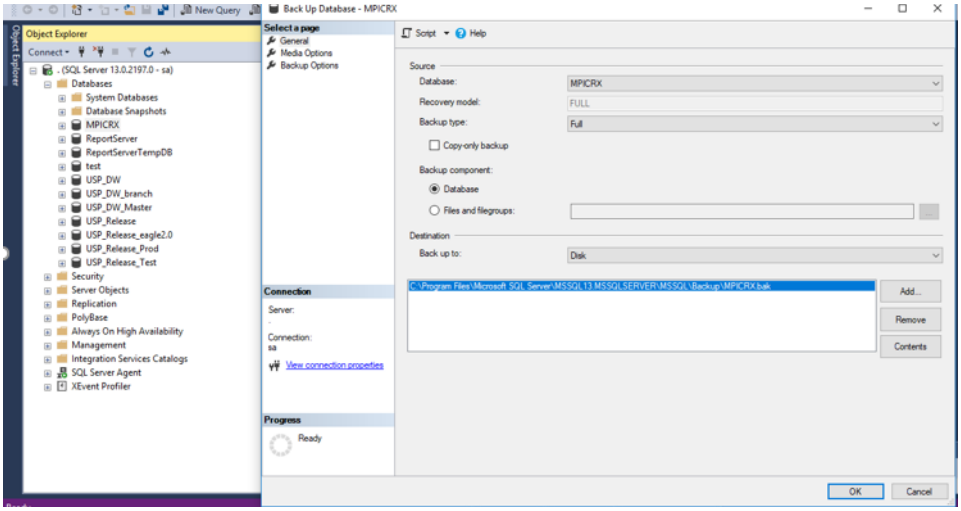
Obtaining database backup is a manual process. The following screens illustrates the method to perform a manual backup.

1. In the **Microsoft SQL Server Management Studio**, select the MPICRX database

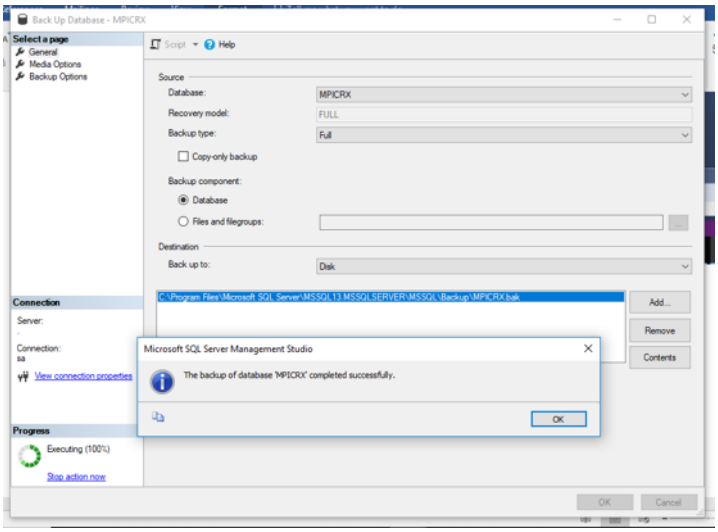
and then right click to select **Tasks > Back Up**.



2. Click **OK**.



The backup successful message appears.



It is recommended to opt for continuous backup. If the primary server goes down, the secondary server will take over.

5. Security Hardening of MPICRX receiver

Note:

Denial of Service Attacks:

Max Pro Receiver mitigates DoS attacks by refusing connections with invalid certificate. MPRX **will not** accept a connection without a **valid certificate** and **common name** validation.

This product is configured "secure by default" and any changes that may leave the product less secure should be clearly communicated to the user(s).

Therefore, we want to make sure that any options to configure the product less securely have very prominent warnings that a reasonable person would not fail to see or misunderstand.

- Location and installation of the server on which the software is to be installed is secured appropriate to the level of risk and any regulatory requirements
- Ensure to check the current setup of Windows matches the recommended Windows version
- Ensure to place the receiver at a secure location and enable access only by authorized personnel
- Default passwords are changed prior to use. Refer to **“Password Configuration” in Section 3.1.1.** for more information
- Check that the software is the latest version
- Check that the server has the correct version of Windows. Refer to Installation **“Prerequisites” in Section 3.1**.

The MAXPRO receiver (MPICRX) is intended to run on a HTTP/1.1 REST server within the customer’s environment. Data transmission is based on open source protocols PKI, REST, HTTP and JSON the open-standard file format for data interchange.

Protection against unauthorized substitution of the SPT with an identical MAXPRO intrusion SPT or with simulation equipment is provided by bi-directional node authentication. Authentication must be successful before the alarm receiver will accept a connection from another device. Each alarm receiver has its own certificate with and a unique Common Name ID that is generated at the time of installation. During authentication Common Name ID is checked against local data sent from the MAXPRO intrusion panel.

Max Pro Receiver mitigates DoS attacks by refusing connections with an invalid certificate.

MAXPRO products will not accept a connection without a valid certificate and ‘common name’ validated.

Protection measures to prevent unauthorized reading and unauthorized modification of the information transmitted by the Alarm Transmission System (ATS)S are provided by end to end encryption based on TLS 1.2. Each message transmitted includes an integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission. Asymmetric cryptography is used to encrypt the data transmitted between the client and the server using AES 128bit with 256bit public and private keys. The private key is securely stored in the alarm receiver server and cannot be

extracted or exported.

Elliptic Curve Digital Signature Algorithm (ECDSA) with SHA256 (NIST p-256 curve) is used for the 256 bit public key with an Elliptic-curve Diffie–Hellman (ECDH) key agreement protocol that allows client and server, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel.

The identity of the client and server are authenticated with client side validation.

Any attempt to modify the transmitted data or substitute a message will result in the data being identified as corrupted since it will not have a valid key.

6. Network Security

- The MPICRX is designed to work in a trusted or protected network with Internet connection protected by a firewall.
- Do not put it in a DMZ (demilitarized zone).
- The Receiver is not designed to be directly connected to the Internet without a firewall.
- Ensure to isolate the MPICRX system from any non-secure internal network.
- The MPICRX database system is designed to work in a trusted or protected network.

6.1. Network Firewall Settings

Set the following items in the firewall of the network to ensure network communication to/ from MPICRX, and to limit access to the Receiver:

1. **Inbound allowed**: Only for ports as specified in **"End Point Configuration" in Section 4.5**.
2. **Outbound denied**: None.
3. **Outbound for local LAN**: Refer to **"TCP/IP Mode" in Section 7.3** for port information.

6.2. Continuous monitoring

The IPS/IDS are not part of MPICRX. To increase the security of the network, its advised to install IDS/IPS to monitor the network traffic and internal or external security breach.

- *IDS* = Intrusion Detection System
- *IPS* = Intrusion Prevention System

6.3. Password Policy

- The MPICRX has a default user name and password. It is recommended to change the user name and password at the first login instance.
- Only authorized user should access the system. You must ensure that the system is locked when not in use.
- It is also recommended to change the password periodically.
- Multi factor authentication is not supported in the MPICRX.

6.4. Backup

Verifying and ensuring the integrity of the backup is the responsibility of the end user. Refer to **"Database Backup" in Section 4.7** for more information.

6.5. System Security

Installing the spyware, Malware, or other virus scan and enabling of windows defender is customer's responsibility for continuous monitoring of the system.

The MPICRX does not contain any process that would check the integrity of the application or its behavior.

7. Operation

The MPICRX can be used Private LAN Configuration (refer to the diagram on the following pages).

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

The MPICRX 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 c can be configured in three receiver modes, (Manual, Serial Automation, and TCP/IP) offering various degrees of intervention.

7.1. 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 (685 format (Contact ID), SIA DC-03 format, or SIA MLR2 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.

7.2. Serial Automation Mode

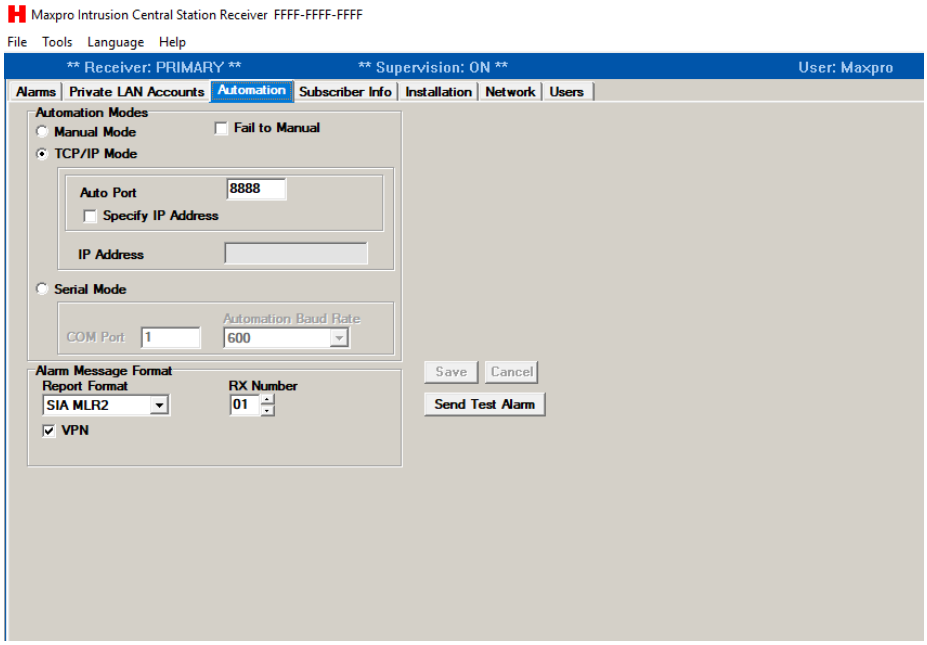
When configured for the Serial Automation Mode, the MPICRX emulates a 685 Digital Alarm Receiver. In this configuration, the Maxpro receiver routes alarms and messages directly to the Automation system. The MPICRX uses a RS232 serial interface to communicate with the Automation system.

- 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 MPICRX 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 MPICRX programming, the it will revert to Manual Mode when communication with the Automation system is lost. When communication is restored, the Maxpro receiver 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 Maxpro Receiver 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 MPICRX.

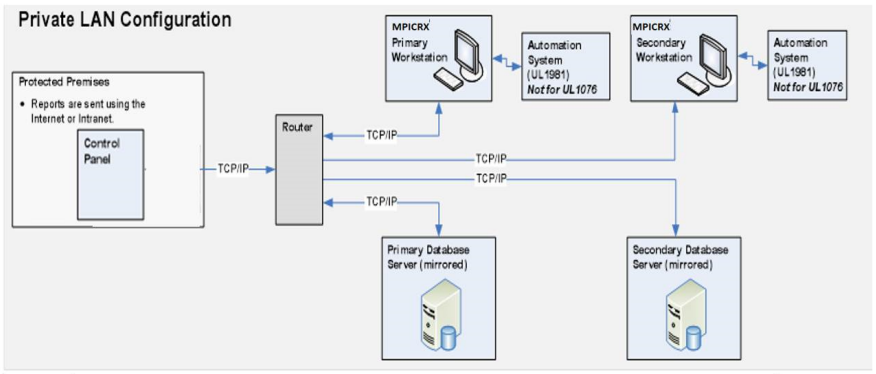
7.3. TCP/IP Mode

Same features as the Serial Automation Mode above. However, in this mode the MPICRX

uses a TCP/IP connection to communicate with the Automation system.



The following illustration depict UL tested Maxpro IP Alarm Receiver system configurations.



7.4. Failure Indications

The MPICRX must be configured as a fault tolerant system.

Configured as a fault tolerant system, the Maxpro Intrusion Central Station Receiver 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 MPICRX fails, communication with the security system's communicator is lost, and the communicator automatically rolls over and communicates with the secondary MPICRX. In addition, the communicator sends the secondary MPICRX 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.

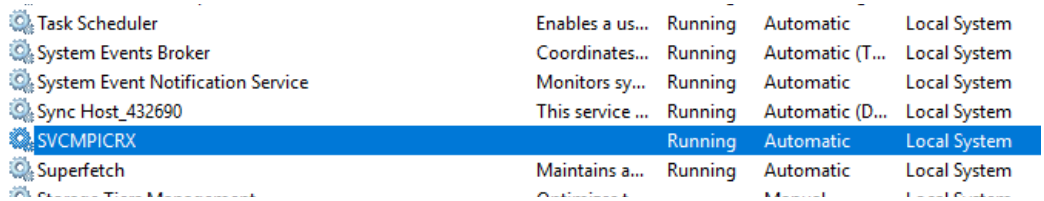
Further since the hardware power is protected by Uninterrupted Power Supplies (UPS), any interruption in power is indicated by audible warnings from the UPS hardware. If the UPS management software has been installed, a visual message/report of any power problems will also appear.

When communication with the database fails, or the database itself fails, the MPICRX 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.

8. Uninstalling the MPICRX software

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



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

8.1. Statement about information stored and GDPR

'X' inform stored, not personally identifiable

Best practice to delete account accounts on decommission to avoid possible attacks (e.g. Man-in-the-middle)

9. Using MPICRX application

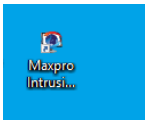
- Securely use the product, including any special security provisions such as monitoring, logging, GDPR compliance, and so on
- DoS

1. Monitoring, logging to find issues

Note:

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

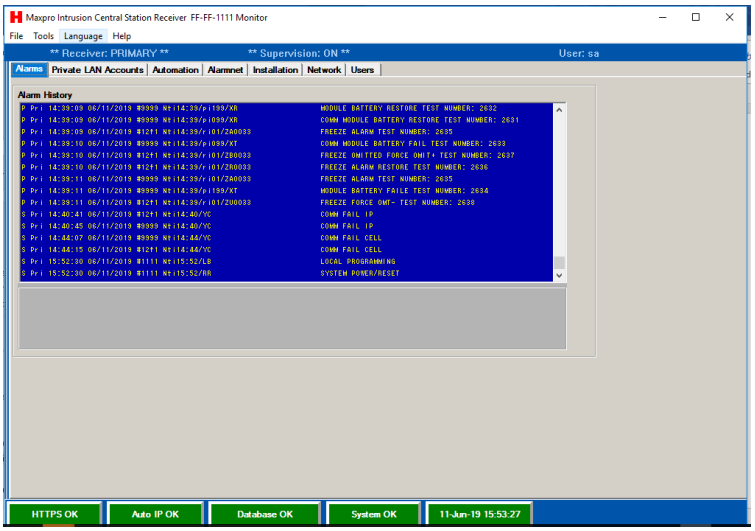
2. Click **Start > Programs > Honeywell > MPICRX** or double-click the desktop shortcut.



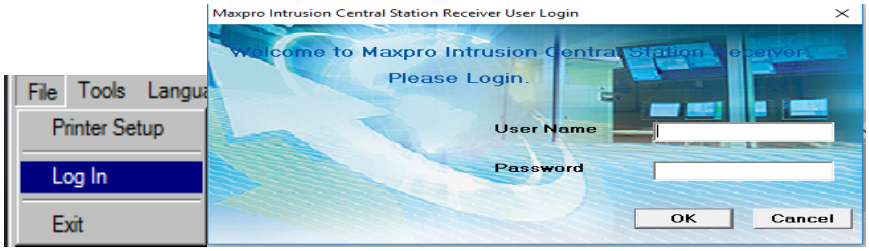
Note:

If you do not have an active license, or need to upgrade an existing license refer to the “Maxpro Intrusion Central Station Receiver License Guide” for details.

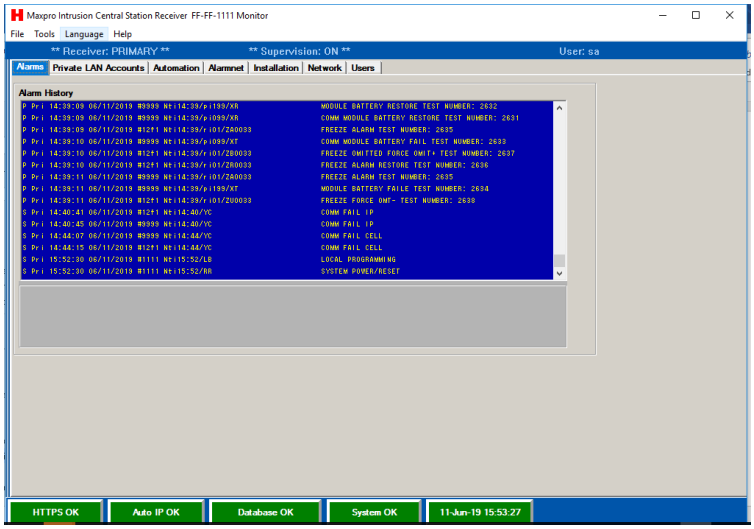
3. A splash screen briefly appears, followed by the Alarm History viewing screen:



4. From the File pull-down menu, select **Log In**. The User Login screen appears.
5. Login using the default user name and password as **Maxpro** and then click **OK**.



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



Initially, when you log in using the default user name and password, it is an administrator account. Please visit the **Users** tab 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.

9.1.1 A Word About Users (Private LAN Only)

We have two types of users:

- Administrator
- 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 Maxpro receiver features that are available to the **Operator**. The Administrator has access to all features.

Pull-down Menu	Selections
File	Printer Setup, Login/Logout, Exit

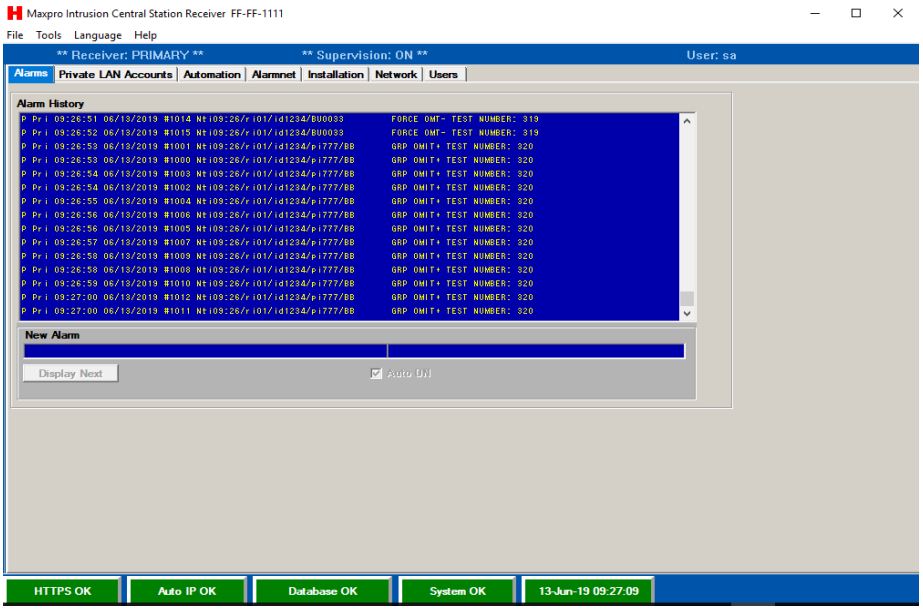
Tools	Disable Fly-Over Help
Language	All selections available
Help	Honeywell Home Page, About License, About Database, About
Tabs	There are no tabs available for the **Operator** authority level.

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

The following topics describe the fields on each tabbed window.

9.2. Alarms tab

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

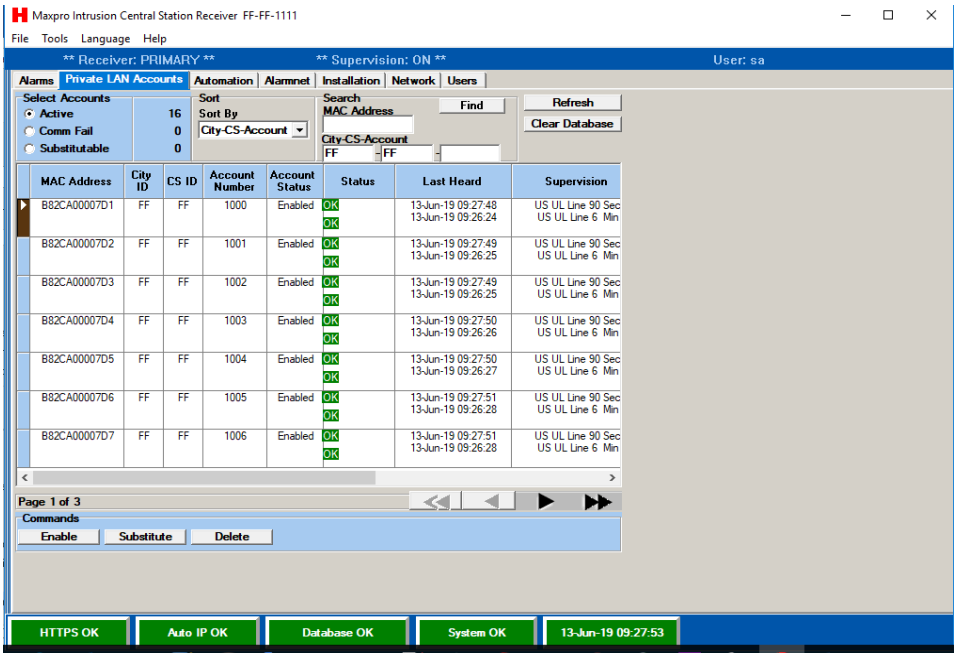


Item	Description / Function
Alarm History	Displays the processed alarms.
New Alarm	Displays the most current alarm.
Display Next	When red, indicates a new alarm is ready for processing. The operator must click this button to acknowledge the alarm and silence audible indication at workstation. This action clears the New Alarm field and adds the event to the Alarm History window.

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.
HTTPS OK	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.

9.1.1 Private LAN Accounts tab (Private LAN Only)

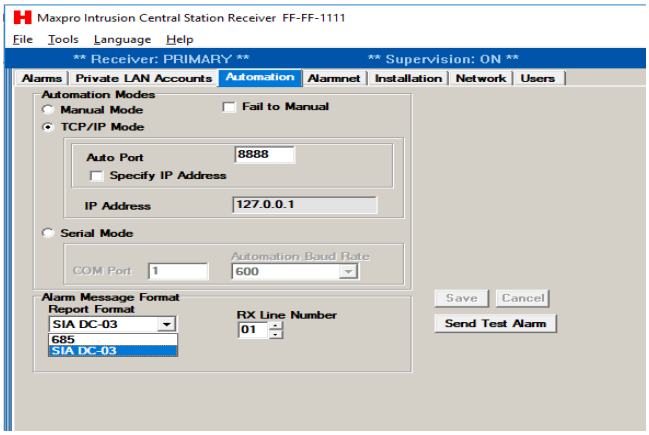
This tabbed window is used to view private LAN accounts that do not report via AlarmNet. Reports would come directly from the protected premises.



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.
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	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.

9.2. Automation tab

This tabbed window enables configuring the Maxpro Intrusion Central Station Receiver to communicate with the Automation system.

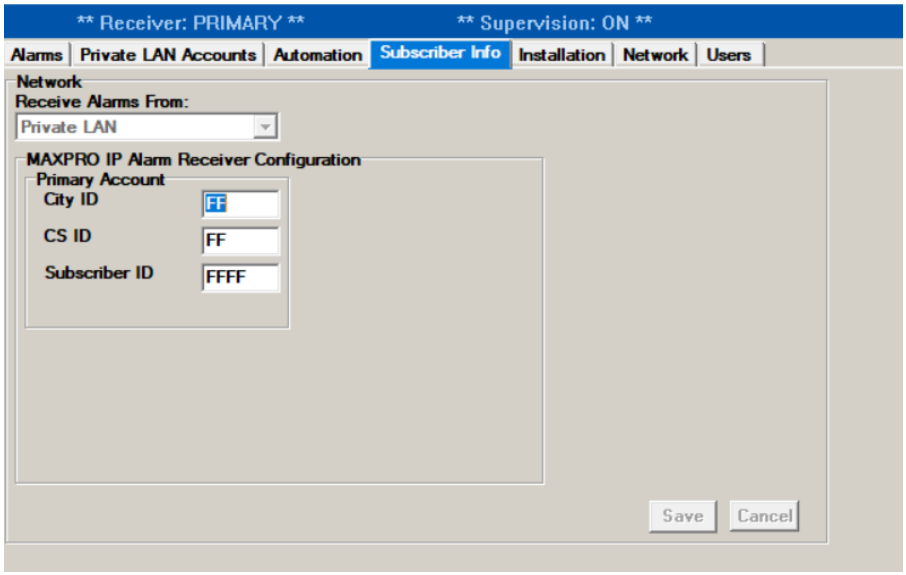


Item	Description / Function
Manual Mode	Select this to put the Maxpro Intrusion Central Station Receiver in Manual mode. In Manual Mode received messages are displayed in the Alarms tabbed window and must be processed manually. Automation system will not be used.
TCP/IP Mode	Select this to enable the Maxpro Intrusion Central Station Receiver 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	*Display only*. 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 **MPICRX.ini** file (typically **C:\Program Files\Honeywell\MPICRX**). Add or edit the line ANICOMMPORT_=x where x is the desired port.

Fail to Manual	Check this box to enable the Maxpro Intrusion Central Station Receiver 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.
685	When selected, data is sent in 685 report format to the Automation system.
SIA DC-03	When selected, data is sent in Honeywell's SIA 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.

9.3. Subscriber Info

This tabbed window enables configuring primary central station account.

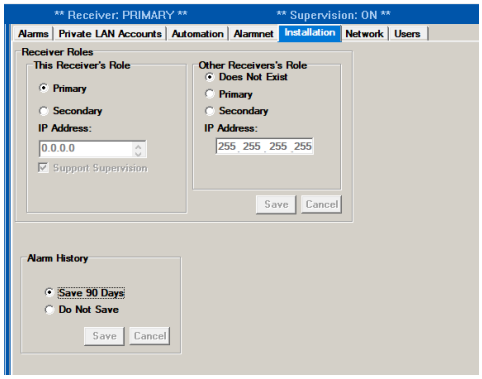


Item	Description / Function

Primary Account City ID, CS ID, Subscriber ID	Use these fields to specify the primary central station account that messages will be sent to.

9.4. Installation tab (Private LAN Only)

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

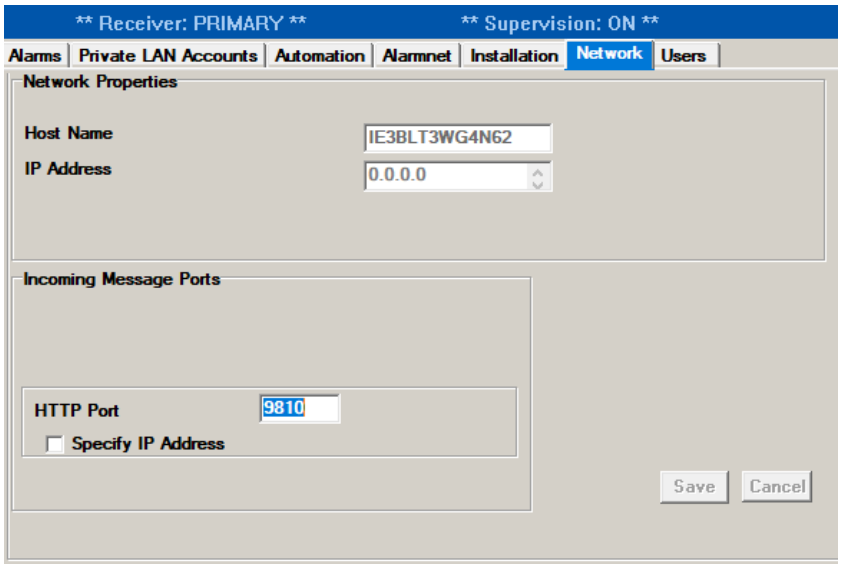


Item	Description / Function
	UL: A secondary role MUST be assigned, and the "**Support Supervision**" check box for each receiver MUST be selected.
This Receiver's Role Primary Secondary	Use the Primary or Secondary choices to assign a role for the Maxpro Intrusion Central Station Receiver. Only one 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. Select the option if the receiver has 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. Select the option if the receiver has to support supervision.
Alarm History Save 90 Days Do Not Save	Use these choices to determine if the alarm history for this receiver is to be saved. Save 90 Days – if chosen, the alarm history is stored locally for 90 days. If needed the data can be backed up for long term storage. Do Not Save – if chosen, the alarm history is not stored locally at the workstation, however, it is always stored in the SQL database.

9.5. Network tab

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

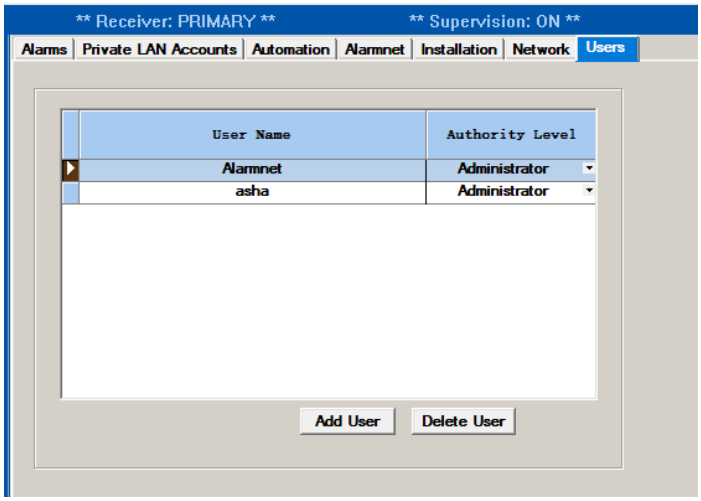


Item	Description / Function
Host Name	Display only. Indicates the server name.

IP Address	Display only. Indicates the server's static IP address. For servers that are configured with multiple static IPs, the entries may be scrolled.
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 Maxpro Intrusion Central Station Receiver's IP address into Subscriber panels.
Specify IP Address	For servers with multiple network interface cards (NIC): Select to enter a specific IP address for listening to subscribers.

9.6. Users tab (Private LAN only)

This tabbed window enables the administrator to manage users.

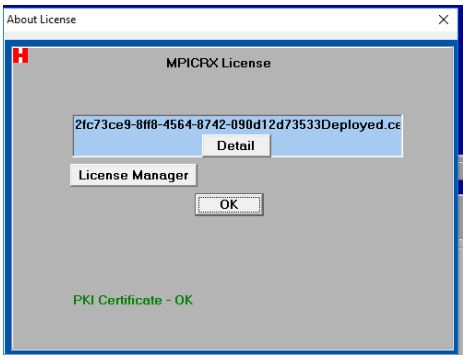


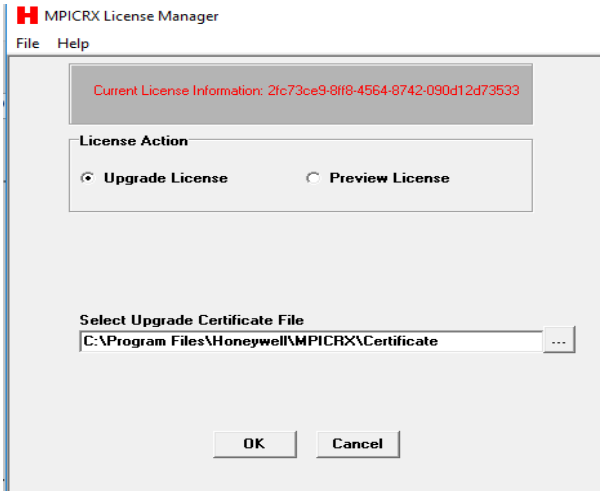
The administrator can add and delete users, assign their authority level (Administrator or Operator) and assign their initial password.

Each user can change their password by going to **Tools > Change Password**.

9.7. About License (Help > About License)

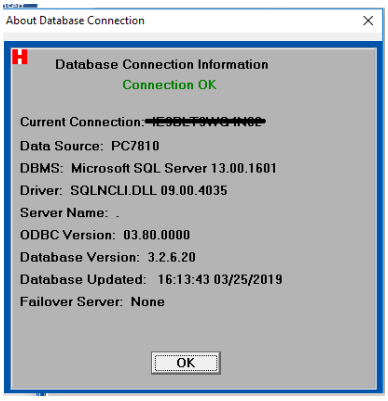
The screen displays the active license number. The **License Manager** option enables you to create a new license, upgrade an existing license, or terminate a license. You must be logged in with Admin credentials .





9.8. Database Information *(Private LAN only)*

This information screen (Help > About Database) provides an overall view of the Maxpro Receiver database configuration.



9.9. Updates

- Do not apply Windows updates immediately to the machine running the MPICRX. Automatic updates should be turned off.
- For Windows updates, Honeywell will qualify updates and send a notice. This is to maintain uptime requirements.
- However, windows updates do need to be applied in a timely fashion after Honeywell

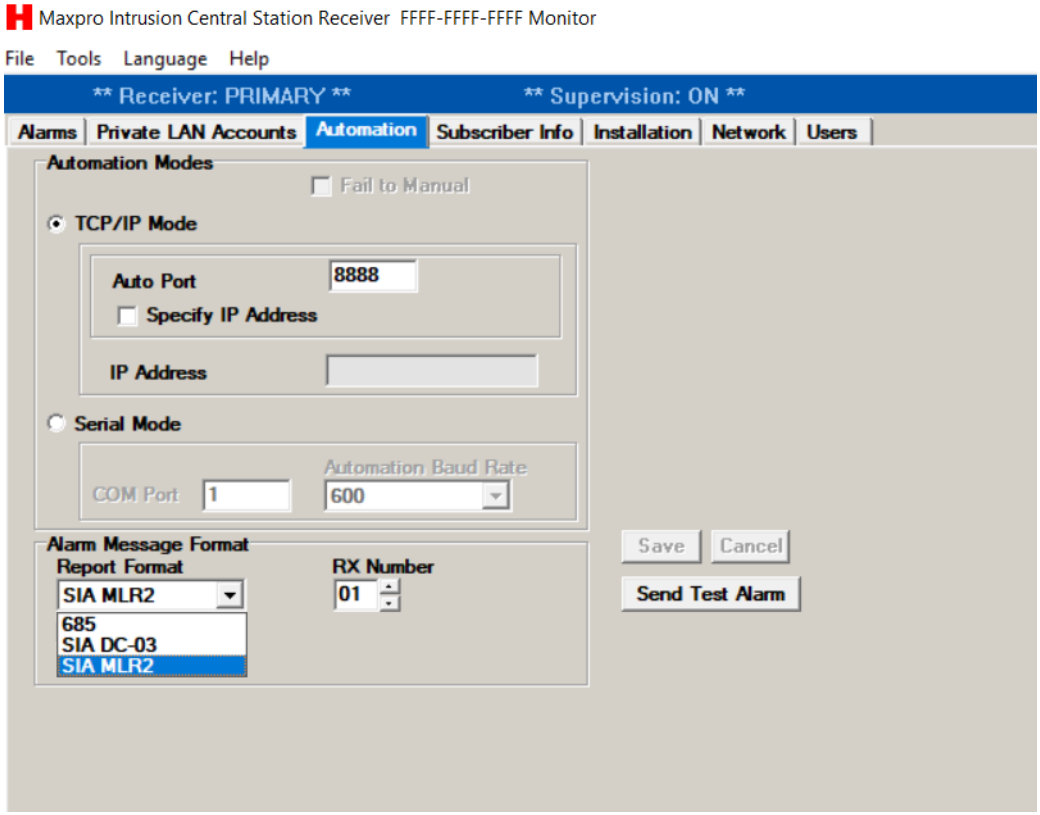
has qualified them

10. MPICRX Report Formats

MPICRX can receive messages in ISOM format and output messages in 685 (Contact ID), SIA DC-03, and SIA MLR2. This is carried through to automation with the exception of ISOM. However, the formatting of the line numbers, account numbers, and in ISOM case, the Format protocol with these messages can be tailored with reporting format choices.

Report Format Choices:

- 685 (Contact ID)
- SIA DC-03
- SIA MLR2



For all Report Formats:

- <LF>..<CR> envelop is used (<LF> = 10 <CR> = 13)\
- Expected ACK is 0x6
- The same output is sent to serial and TCPIP automation
- "\n00 OKAY @\r" sent as poll to automation for supervision purposes with Expected ACK is 0x53

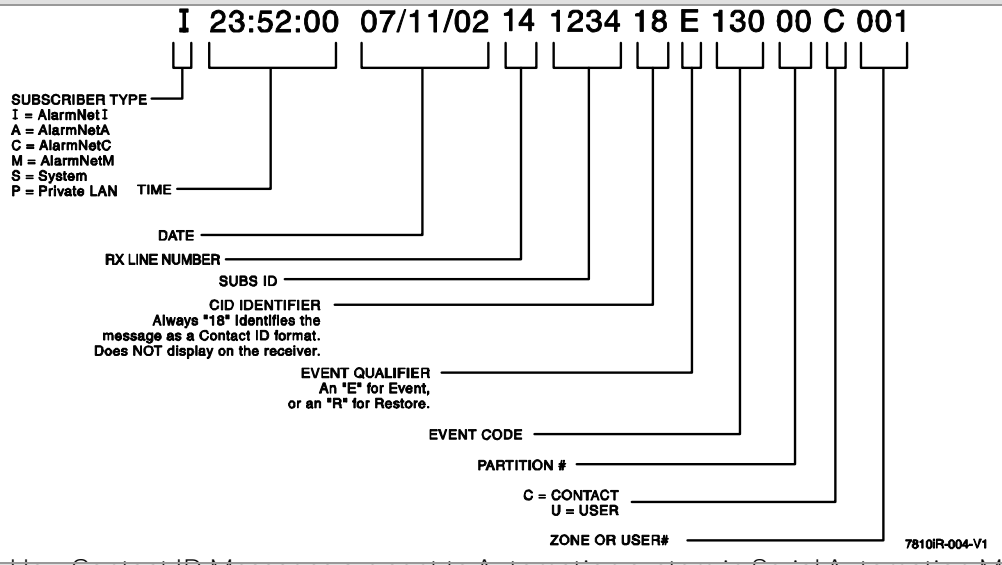
  Example for SIA DC-03
  <LF><Header Byte><Function Code><Data>< Column parity Byte><CR>
  Report Lines
  CID, Ademco HighSpeed are one line per report. SIA DC-03 can have up to 3 lines per report (3 Blocks). Each one needs to be ACKed before sending the next one.

10.1. 685 Format

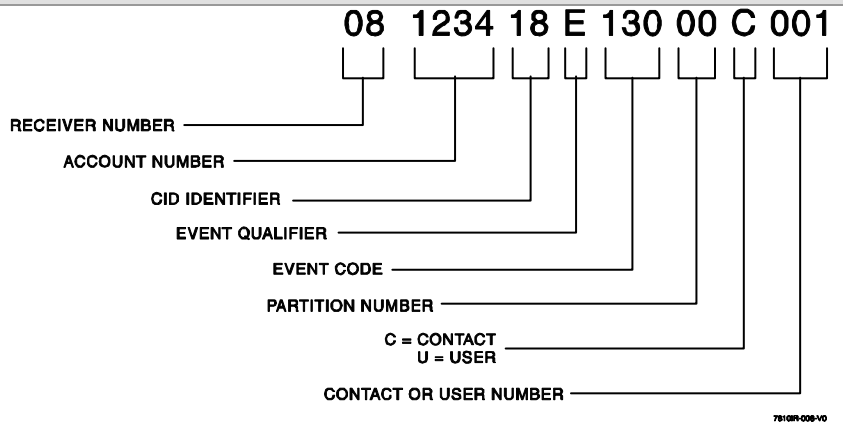
This format consists of:

- 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 Maxpro IP Alarm Receiver



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



10.2. SIA DC-03 Format

DC-03 (“SIA Format”) must have ISOM as input and has the following output

- •Line1 (required) Account Block – account number
- •Line2 (required) Data Block -report code
- •Line3 (Optional) ASCII Block – description
- •SIA level - Determines length of account number 4 or 6

<Header Byte><Function Code><Data>< Column parity Byte>

Header Byte - Reverse Channel set Disabled, Acknowledgment Request bit set Enabled Ored with Block length (Data portion) (04LL)

Function Codes - # for Account Block, N for data block, A for Ascii block

Column parity byte - will be calculated by the Maxpro Alarm receiver as follows:

a. Begin with the value 255.

b. Exclusive OR the current value with the value of the first (or next) data byte beginning with the header byte. Repeat until all bytes up to, but not including, the parity byte have been used.

10.3. SIA MLR2 Format

:SRRL[#AAAA|EMMZZZZ/MMZZZZ/MMZZZZ][DC4]

Where, S : Beginning transmission of the new SIA protocol RR : Receiver number 00-99 L : Line number 0-999 [: Beginning data delimiter # : Account ID block code AAAA : Account ID, maximum sixteen digits. | : Field separator E : Function block code MM : Event code or modifier ZZZZ : Zone code, or user code, or time/date information / : Data code packet separator] : Ending data delimiter [DC4] : Terminator, 14 Hex

Example:

S01001[#3243|Nti09:18/ri01/YK0000|A0CELL]

S01001[#0108|Nti14:48/ri01/FA0008]

SRRLLL[#AAAAAA|EMMZZZZ/MMZZZZ/MMZZZZ][DC4]

Where, S	: SIA protocol 2 identifier.
RR	: Virtual Receiver number.
LLL	: Virtual Line number.
[	: Beginning Data Delimiter.
#	: Account ID Block Code.
AAAAAA	: Account ID, maximum six digits.
|	: Field Separator.
E	: Function Block Code.
MM	: Event Code or Modifier.
ZZZZ	: Zone Code, User Code, Door or Relay.
/	: Data Code Packet Separator.
]	: Ending Data Delimiter.
[DC4]	: Terminator 14 hex.

Supervisory Heartbeat Signal Protocol for SIA MLR2 format:

1011sssssssssss@ssss[DC4]

Where, s : Space Character. @ : Supervisory Signal. [DC4] : Terminator, 14 Hex. This signal is used to supervise the communication between the receiver and the computer. It is sent to the computer about every 30 seconds, programmable on the receiver. The computer should acknowledge this signal with an [ACK]. It is recommended to have this signal running.

11. 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.

Item	Code	Description / Function
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 (Al)	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. Radiodevices 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 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 cell backup devices send zone 99 for a low battery and a zone 97 for communication failure (no response from poll). These will report as contact ID E370 (protection loop). These are signals GENERATED by the uplink to indicate STATUS of the uplink. Of course, central station will assume that the panel generated them. • Additional codes that may be sent would be for zones 81-86 which correspond to hardwire inputs 1-6. The contact ID message for these is selected by uplink when it is programmed. So, next time someone reports an unusual zone 97 or 99 being reported to their Central Station, Uplink may be the culprit. Uplink's number is 1-888-987-5465 if you need it.

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 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
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 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)
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	
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 – This code is also referred to as 'up and about'. It means 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	
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) Maxpro Receiver 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 ⅓ Day No Read Log	In the last 31.9 hours (1 and ⅓ 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.