CRX-ARMORIP

ArmorIP Internet Monitoring Application

User Manual

ICTeSecurity®

Publication Date: May 2012

Contents

Introduction 5

Document Conventions 5
Account Information 5
Data Storage and Reports 5
Encryption Support 6
Full Textual Transmission 6
Offline Account Notification 6
ArmorIP Protocols 6

Installation 8

Connection Overview 8
Computer Requirements 8
Installing the ArmorIP Internet Monitoring Application 9
Activating Your License 12
ArmorIP and Windows Firewalls 14

The ArmorIP User Interface 15

Menus 15
- File 15
- View 15
- Comms 16
- Setup 16
- Database 16
- Help 16

Toolbar 16
Tabs 17
- Accounts 17
- Events 18
- Serial 19

Status Bar 19

ArmorIP Configuration Options 20

Startup/Shutdown 20
Communication 20
- ArmorIP (UDP) 20

Accounts 21
- Poll/Grace Time 21

Online/Offline Notification 22
Encryption 23
Receiver 23
COM Port 23
Ademco 685 24
UL and ULC Configuration Requirements 25
Database Maintenance 26
ArmorIP Basics 27
Creating a new Account 27
Reviewing Account Specific Events 27
Using Account Notes 28
Removing an Account 28
Compromise Attempt Events 29
Testing Your Connection Using the RIP Utility 29
Contact 30

Introduction

The ArmorIP Internet Monitoring Application converts the ArmorIP reporting protocols used by the Protege System, PostX, and other third party products to Ademco© 685 format.

The integration process for a monitoring station is seamless and can be done in a matter of minutes allowing an immediate transition to IP reporting without the normal time consuming custom solutions:

- Converts the ICT ArmorIP reporting protocol for use in any Ademco 685 compliant monitoring station application.
- 'Live View' shows the current accounts that are online with next poll information.
- Supports AES encryption with 128, 192 and 256 Bit keys.
- Free edition for use on up to 20 accounts. Flexible licensing in 250 account blocks.

Document Conventions

This document uses the following conventions:

	Important warnings or cautionary messages to prevent equipment damage, data loss, or other similar conditions
	Notes with additional information such as an explanation, a comment, or a clarification about the subject
	Tips containing practical information that may help you solve a problem or describing actions that may save you time
	Information relating to UL and ULC compliance
[TEXT]	Bold text enclosed in brackets is used to show a section number or address of a programmable option or information on programming shortcut sequences

Account Information

Account information is presented in a 'Live View' window that shows the currently online and delinquent accounts, information includes:

- Last time the panel completed a poll and the next time the panel should poll based on the configuration parameters.
- Countdown of seconds until the next poll.
- The current IP address of the account, this allows the ability to remote access the IP device if required.
- Name of the account.

Data Storage and Reports

Information that is transmitted to the ArmorIP Internet Monitoring Application is stored in a local database; this is accessible by third party software or other applications.

Sample reports are available that extract information for a particular account or all accounts and these can be executed over a network connection.

Encryption Support

All communications can optionally be configured to use AES encryption with 128, 192, or 256 bit keys.

Full Textual Transmission

The ArmorIP protocol outputs full textual based transmission that includes the names of the objects (user, area or zone) that generated the reportable event. This information is stored in the database and can be retrieved with the appropriate ContactID data.

Offline Account Notification

The notification of an offline account is presented to the receiver by configuration of an account and appropriate CID message. This allows the monitoring station to configure the automation package in the most optimal manner for reception of alarms, by account, zone or specific account.

ArmorIP Protocols

ArmorIP (UDP)

The ArmorIP (UDP) format communicates with an ArmorIP Server using UDP as the transport layer. When using this format the account code must be set to be the same 8 digit code as is saved in the ArmorIP Server the PostX is communicating with.

Using UDP to send the messages is faster than TCP as it is a connectionless protocol, the ArmorIP (UDP) protocol includes acknowledge and retry messages to ensure that the message has been received by the server.

ArmorIP (TCP)

The ArmorIP (TCP) format communicates with an ArmorIP Server using TCP as the transport layer. When using this format the account code must be set to be the same 8 digit code as is saved in the ArmorIP Server the PostX is communicating with.

ArmorIP-E (UDP)

The ArmorIP-E (UDP) is the encrypted version of the ArmorIP protocol. It uses an AES encryption algorithm that is selectable for 128, 192 or 256 Bit encryption. If ‘Use Default Settings’ is selected, make sure that this is also selected in the ArmorIP Server, when this is selected no other details need to be entered.

If you want to increase the security use a custom key that must be entered in both the PostX and the ArmorIP Server.

ArmorIP-E (TCP)

The ArmorIP-E (TCP) is the encrypted version of the ArmorIP protocol. It uses an AES encryption algorithm that is selectable for 128, 192 or 256 Bit encryption. If ‘Use Default Settings’ is selected, make sure that this is also selected in the ArmorIP Server, when this is selected no other details need to be entered.

This format uses the TCP layer as its transport mechanism.

Contact ID (UDP)

The Contact ID (UDP) format is an ASCII based format that only contains the Contact ID message. In all instances the message will be 16 characters long with the format detailed below.

The form of the message is: ACCT MT QXYZ GG CCC S, where:

- ACCT: 4 digit account number
- MT: 2 digit message type
- Q: 1 digit event qualifier
- XYZ: 3 digit event code
- GG: 2 digit group number
- CCC: 3 digit zone number
- S: 1 digit checksum

To acknowledge this message the server must send back an identical copy of this message. TCP is used as the transport layer for this protocol.

Contact ID (TCP)

The Contact ID (TCP) format is an ASCII based format that only contains the Contact ID message. In all instances the message will be 16 characters long with the format detailed below.

The form of the message is: ACCT MT QXYZ GG CCC S, where:

- ACCT: 4 digit account number
- MT: 2 digit message type
- Q: 1 digit event qualifier
- XYZ: 3 digit event code
- GG: 2 digit group number
- CCC: 3 digit zone number
- S: 1 digit checksum

To acknowledge this message the server must send back an identical copy of this message. TCP is used as the transport layer for this protocol.

Alarm NZ

The Alarm NZ format communicates with Alarm NZ's central monitoring station alarm receivers using TCP.

Patriot LS30

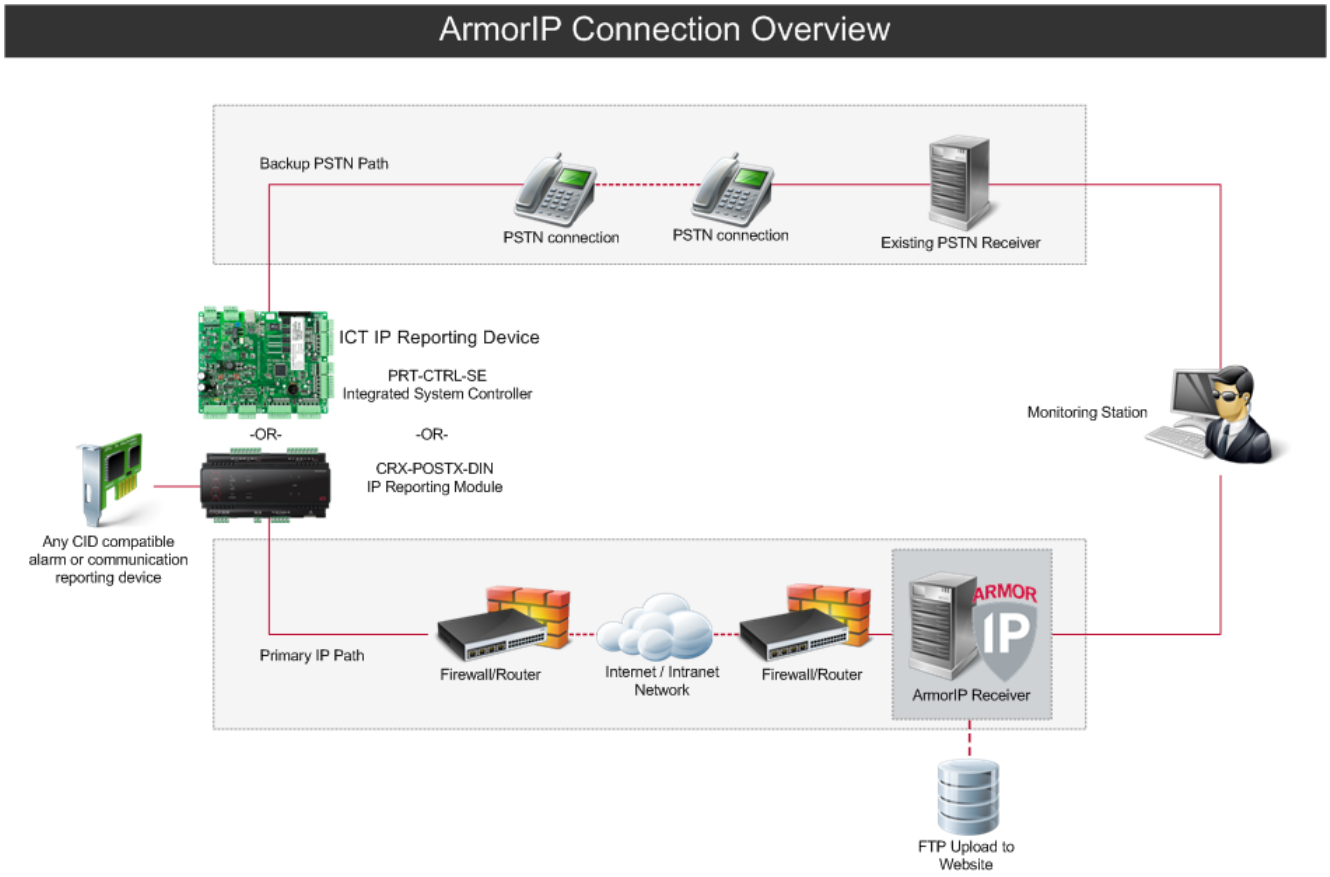
The Patriot LS30 TCP format communicates with the LS30 task in the Patriot Alarm Monitoring software.

For UL/ULC installations, **ArmorIP-E (UDP)** must be used.

Installation

Connection Overview

The following diagram provides an overview of the ArmorIP connection.



Computer Requirements

- Pentium 4 2.5GHz (Pentium 4 3GHz or higher recommended), 2GB RAM (4GB recommended), 20GB free disk space (40GB recommended).
- Windows XP Professional Edition, Windows Vista Professional (32 bit), Windows 7 Professional (32 bit), Windows 7 Professional (64 bit)
- 10/100Mbps Ethernet Card
- Serial port to be used with central station automation software computer
- Monitor supporting a resolution of at least 1024 x 768
- Keyboard
- Mouse

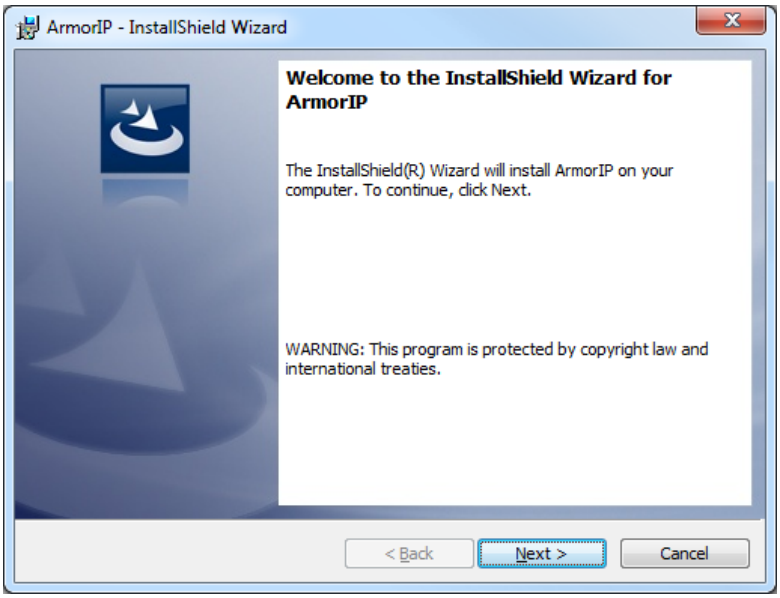
For UL/ULC installations, an ICT ArmorIP Receiver must be used. Please contact your ICT Distributor for details.

Installing the ArmorIP Internet Monitoring Application

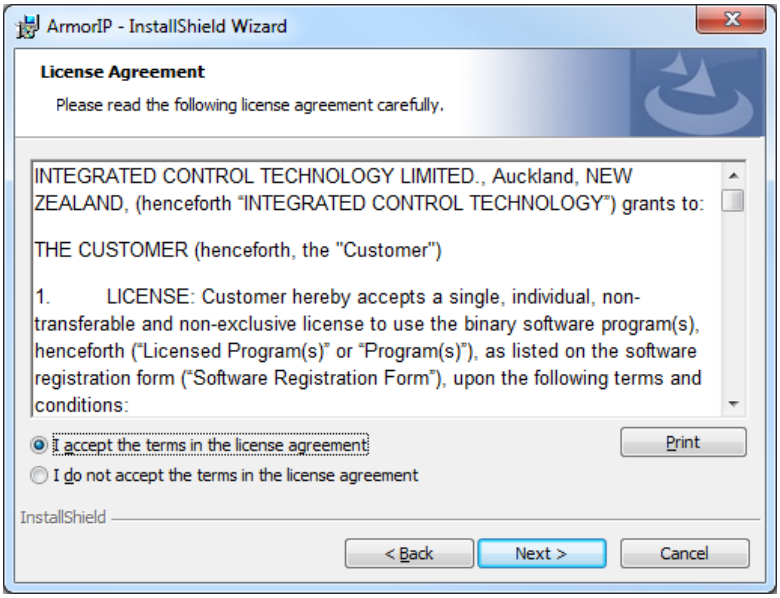
For UL/ULC installations, an ICT ArmorIP Receiver must be used. This is provided with the ArmorIP Internet Monitoring Application already installed so these steps are not required.

To Install the ArmorIP Internet Monitoring Application:

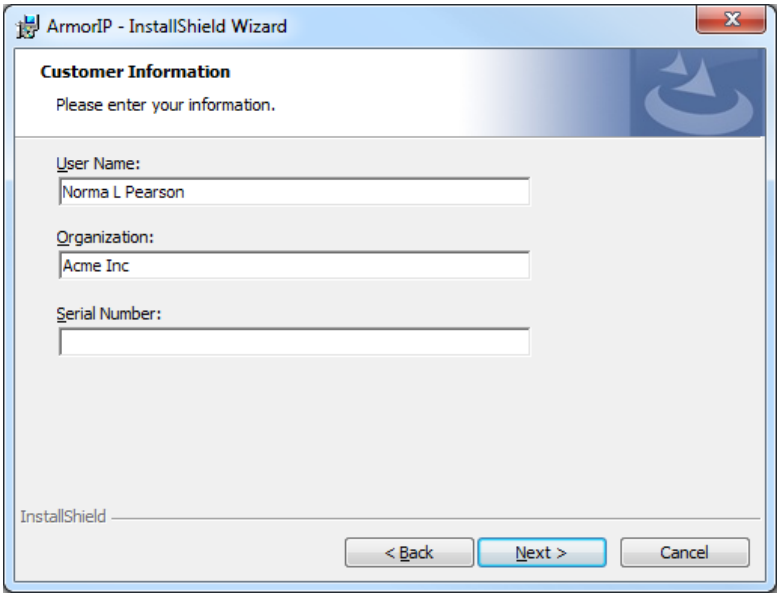
1. Run the supplied setup program. This launches the ArmorIP Install Wizard. Click **Next** to continue.



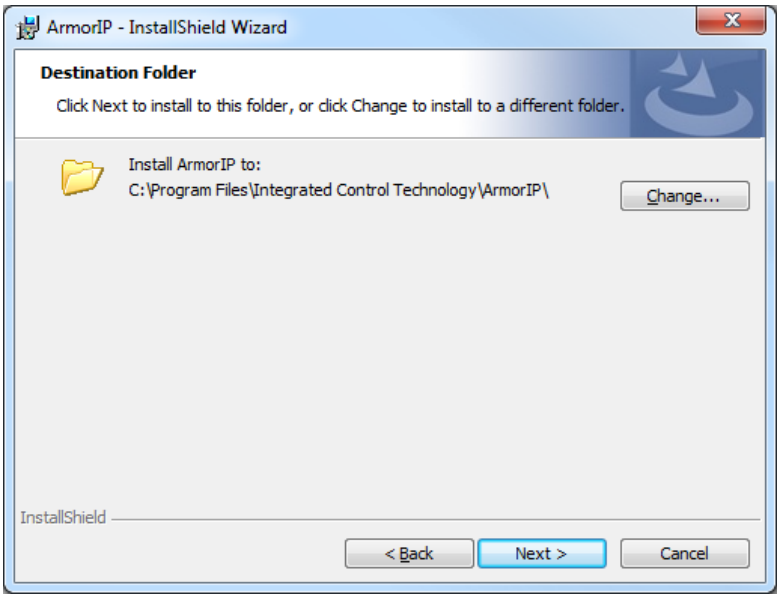
2. Read and accept the License Agreement then click **Next**.



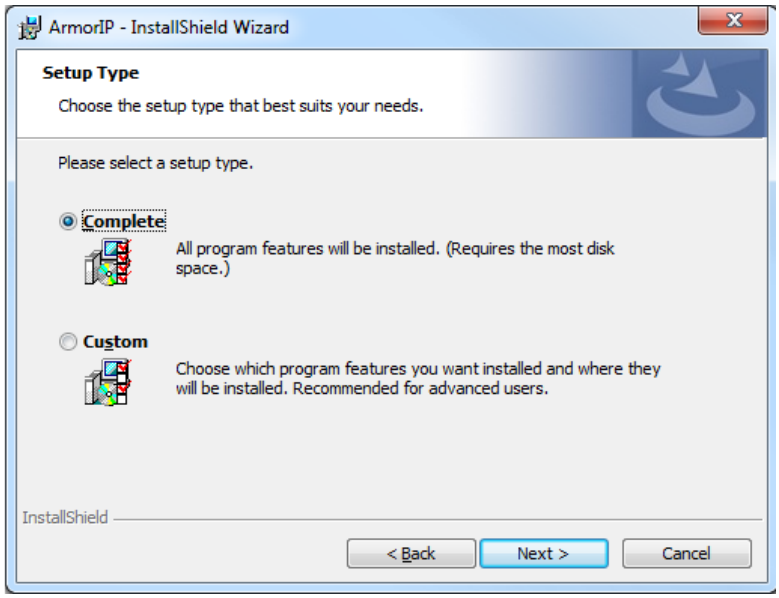
3. Enter your customer information and serial number then click **Next** to continue.



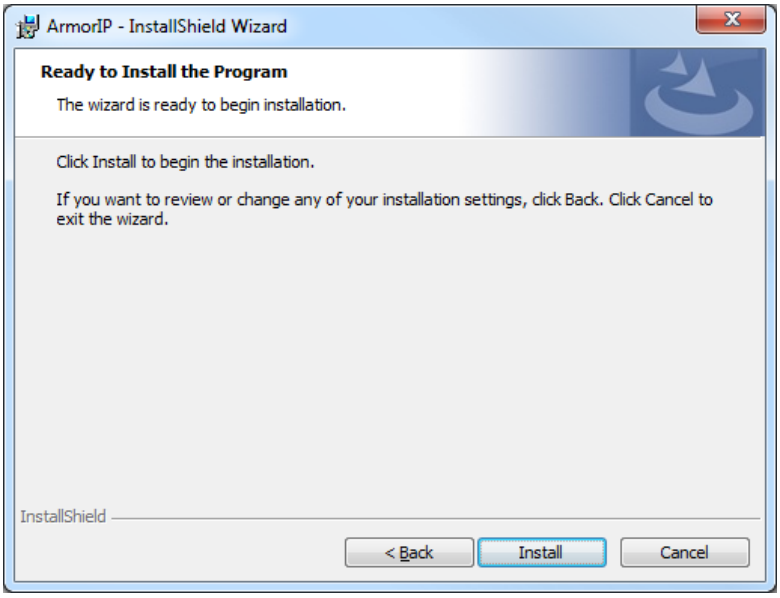
4. Click **Next** to install to the default folder or click **Change** to choose another location.



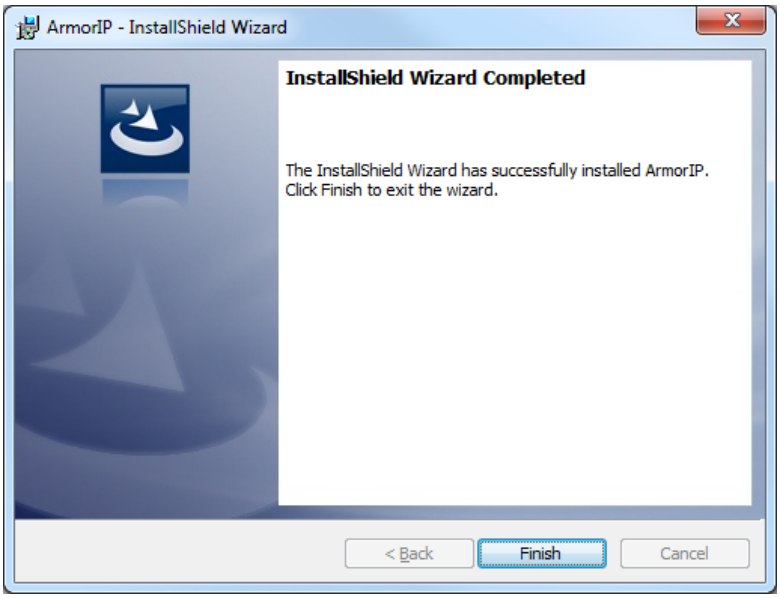
5. Select the **Complete** Setup type then click **Next**.



6. Click **Install** to begin installation.



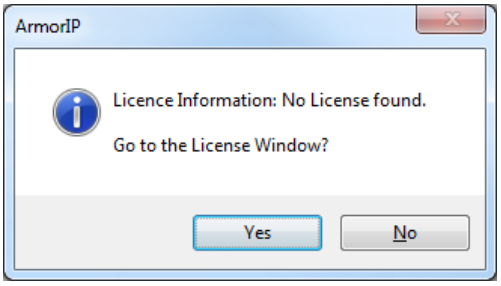
7. Click **Finish** to complete the installation and exit the Install Wizard.



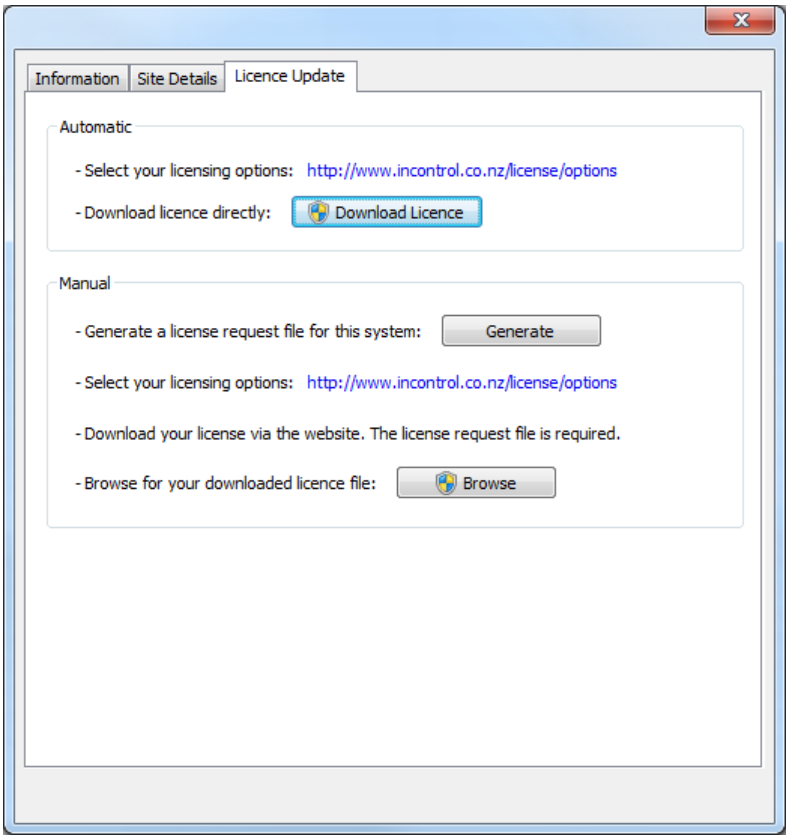
Activating Your License

Before you can begin using ArmorIP, you must register and activate your license. This is achieved using a registration service, obtaining a license file from the ICT website, and enabling the licensed features. Note that you must have local administrative privileges on the server in order to activate the license correctly.

1. Start ArmorIP. You will receive a prompt that the license information cannot be found:



2. Click **Yes** to go to the License Window.
3. Select the **License Update** tab.

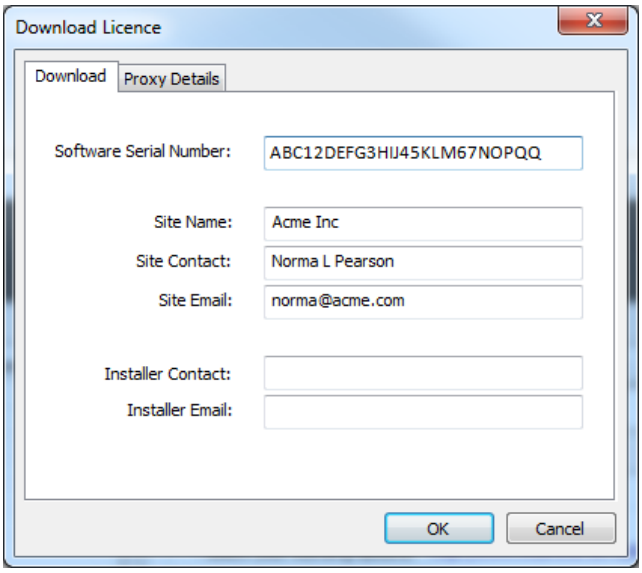


4. Select the **Automatic** or **Manual** option to download and activate your ArmorIP license.

Important: The activation process requires an Internet connection. If this is not available on the server, you will need to use the **manual** activation option, copy the license request to another machine or portable drive, and connect to the ICT website (http://www.incontrol.co.nz/license/options) from a remote machine to download the license file. The downloaded license file must then be taken back to the server, and used to complete the activation process.

Option A: To Automatically Activate Your License:

1. Click **Download License**, enter the required information and select **OK**.



2. If your internet access is via a proxy server, you will need to set this up in the *Proxy Setup* tab.
3. The ArmorIP application passes your details to the ICT web registration service, then activates your software automatically.

Option B: To Manually Activate Your License:

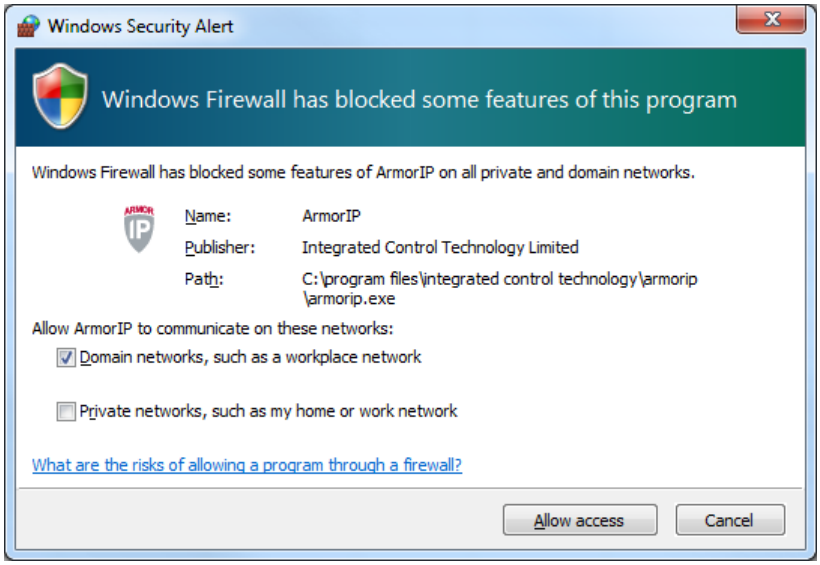
1. Click **Generate** to create a license request file. When prompted, save the **ICT_LicenceRequest.req** file to a folder on your network or a portable drive.
2. Click the link to **Select your licensing options**. This opens a webpage (http://www.incontrol.co.nz/license/options) where you will be prompted to enter your Site, Installer, and SSN details.
3. Browse to the saved **ICT_LicenceRequest.req** file and click **Submit**.
4. Your details are passed to the ICT web registration service. Once registration is complete you will be prompted to download your license (*.lic) file.
5. Click **Browse** to select the license file and activate your ArmorIP license.

Note: Steps 2 to 4 can be performed on any workstation with Internet access. Steps 1 and 5 must be performed on the server.

ArmorIP and Windows Firewalls

When enabled, Windows Firewall blocks unsolicited connections to your computer. Having the firewall turned on is good practice, however there can be occasions when Windows Firewall blocks incoming connections for legitimate programs. This can be overcome by adding an exception to the Firewall, which allows the program to run normally.

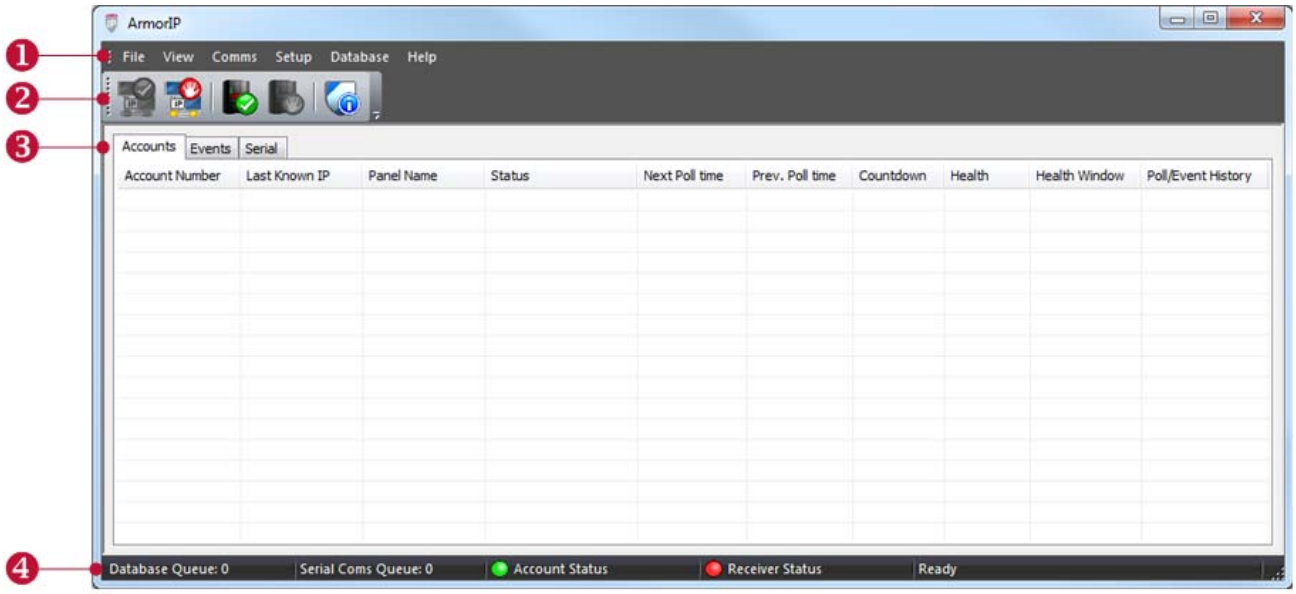
If you launch ArmorIP and Windows Firewall is turned on, the firewall blocks the connection and displays a security alert:



Select **Allow Access** to accept connections to your computer and unblock the program. This creates an exception for the program, allowing it to communicate through the firewall.

The ArmorIP User Interface

The ArmorIP application window provides a simple graphical user interface for accessing the system with ease.



The main screen consists of the following components:

1. Menus
2. Toolbar
3. Tabs
4. Status Bar

Menus

The menu bar contains a number of menus that tell ArmorIP what to do.

File

This Option:	Is Used To:
Exit	Close and Exit the ArmorIP Internet Monitoring Application

View

This Option:	Is Used To:
Status Bar	Display or hide the status bar.
Application Look	Select the application theme, enabling you to modify the color scheme of the application to suit your personal preference.
Always on Top	Select this option if you want to have the ArmorIP window always appearing in the foreground of any other window you have open.
Opacity	Select the Opacity of the ArmorIP interface. Choose from 25%, 50%, 75% or 100%. Most users would use 100%.

Comms

This Option:	Is Used To:
IP	Connect / disconnect to the IP Monitoring Service
Serial	Connect / disconnect to the Serial Receiver

Setup

This Option:	Is Used To:
Preferences	Configure the ArmorIP software

Database

This Option:	Is Used To:
Maintenance	View database status and perform maintenance tasks.

Help

This Option:	Is Used To:
License Information	View license information including SSN and site/installer details, and to update and register your ArmorIP software.
About ArmorIP...	View the application version, build and license information

Toolbar

The Toolbar provides quick access for starting and stopping communications.

This Button:	Is Used To:
	Start receiving incoming communication
	Stop receiving incoming communication
	Start serial receiver communications
	Stop serial receiver communications
	View the application version, build and license information
	Add or Remove any of the above buttons from the toolbar

Tabs

Information is displayed under one of three tabs:

This Tab:	Is Used To:
Accounts	Display an overview of all current and previous accounts ArmorIP has communicated with.
Events	Display the last 5000 events received by ArmorIP.
Serial	Display the two way communication between the Serial Receiver and ArmorIP

Accounts

The accounts view provides an overview of all current and previous accounts ArmorIP has communicated with. You can remove an account from this list by right clicking the account and selecting **Remove**.

Accounts can be in one of 4 states:

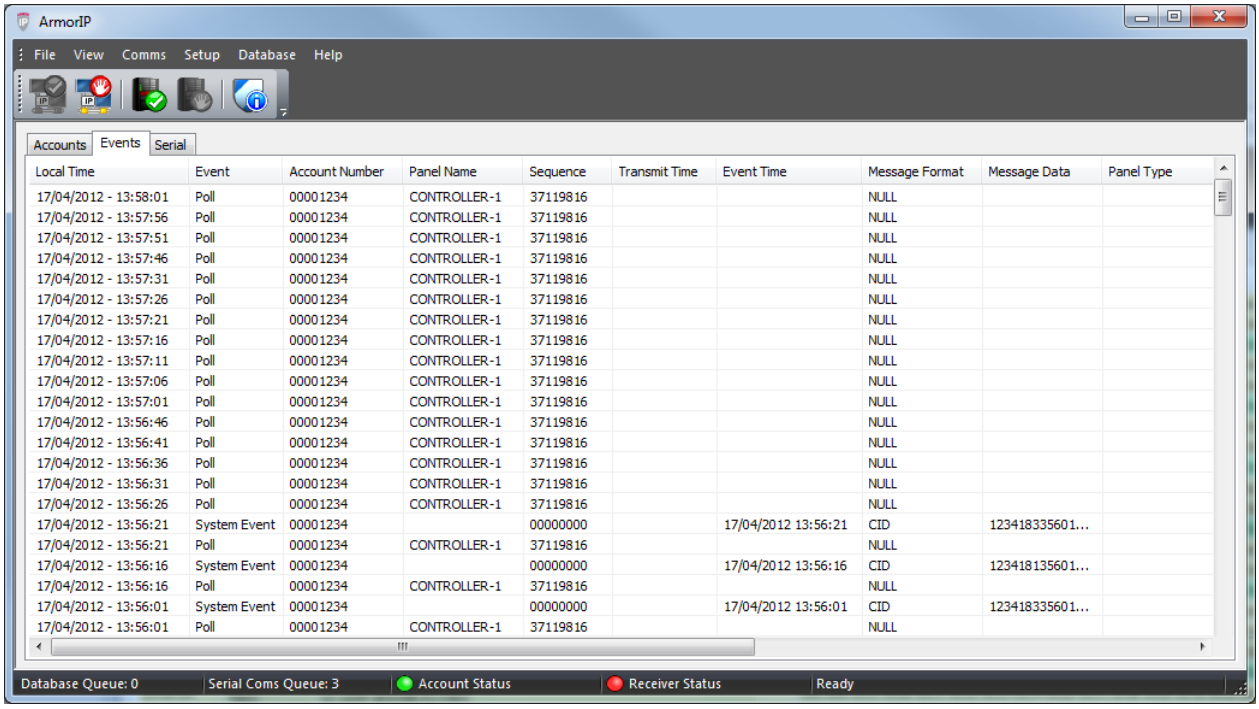
Status	Default Background Color
Online	Green
Offline	Orange
Sequence Violation	Yellow
Unknown	Gray

The accounts view displays the following information:

- **Account Number:** The account number for each panel communicating with ArmorIP (should be unique).
- **Last Known IP:** The last known IP address the account communicated from.
- **Panel Name:** The name of the panel. Panel name changes will be recorded by automatic system notes.
- **Status:** Current status of the account. Online, Offline, Sequence and Unknown.
- **Next Poll time**: Next expected poll time for this account. This is updated based on the poll time setting and when the last poll was received.
- **Prev. Poll time:** When the last poll was received.
- **Countdown:** Seconds until the next expected poll message for this account.

Events

The Events view displays the last 5000 events received by ArmorIP.



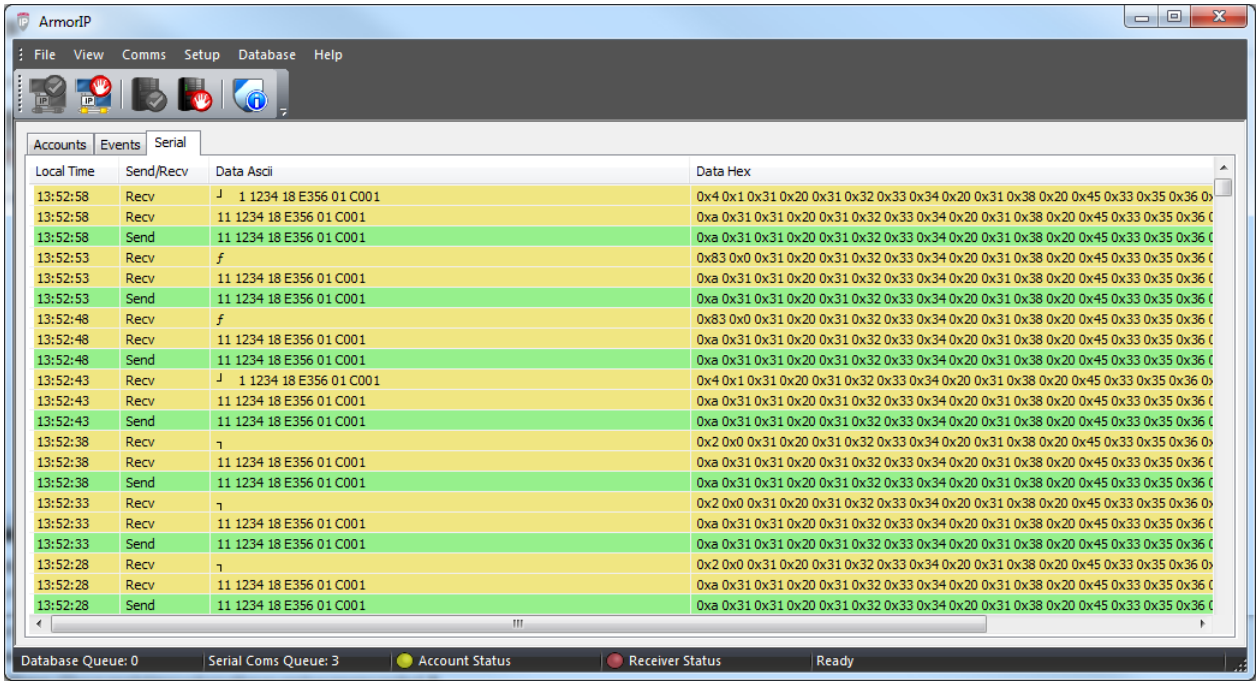
Local Time	Event	Account Number	Panel Name	Sequence	Transmit Time	Event Time	Message Format	Message Data	Panel Type
17/04/2012 - 13:58:01	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:57:56	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:57:51	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:57:46	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:57:31	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:57:26	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:57:21	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:57:16	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:57:11	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:57:06	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:57:01	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:56:46	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:56:41	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:56:36	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:56:31	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:56:26	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:56:21	System Event	00001234		00000000		17/04/2012 13:56:21	CID	123418335601...	
17/04/2012 - 13:56:21	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:56:16	System Event	00001234		00000000		17/04/2012 13:56:16	CID	123418135601...	
17/04/2012 - 13:56:16	Poll	00001234	CONTROLLER-1	37119816			NULL		
17/04/2012 - 13:56:01	System Event	00001234		00000000		17/04/2012 13:56:01	CID	123418335601...	
17/04/2012 - 13:56:01	Poll	00001234	CONTROLLER-1	37119816			NULL		

- **Local Time:** The time notification on the local computer when ArmorIP received the event.
- **Event:** The type of event received by ArmorIP.
- **Account Number:** Account that ArmorIP received the event notification from.
- **Panel Name:** Panel Name that ArmorIP received the event notification from.
- **Sequence:** After every message sent to and replied to by ArmorIP, the accounts sequence value is incremented. If a panel's next message has the same sequence, the value is incremented. If a panels next message has the same sequence value, two way communication is not successful and the panel is retrying. An account goes into sequence violation by retrying more than the number of times specified in the setup with the same sequence number.
- **Transmit Time:** The panel time when the event notification was sent.
- **Event Time:** The panel time when the event was recorded.
- **Message Format:** The format of the message received by ArmorIP.
- **Message Data:** The data contained in the message.
- **Panel Type :** When ArmorIP receives a message it can include "Panel Type" information. This is used to identify the panel.
- **Panel Serial:** The panel serial numbers.
- **Panel Version:** The firmware version of the panel.
- **Zone Name:** The zone where the event occurred.
- **Trouble Zone**: The trouble zone that caused the event.
- **User Name**: The user that caused the event.
- **Area Name**: The area where the event occurred.

Serial

The Serial tab displays the two way communication between the Serial Receiver and ArmorIP.

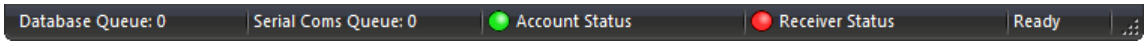
Note: In the following example there is no Serial Receiver attached, so ArmorIP is retrying the same message. This list shows the last 5000 messages.



- **Local Time:** The local time on the workstation running ArmorIP that the data was sent/received.
- **Send/Recv:** Indicates if the data was sent or received by ArmorIP.
- **Data ASCII:** The sent/received information in ASCII format.
- **Data Hex:** The sent/received information in Hex format.

Status Bar

The Status Bar is located at the bottom of the application window and indicates the current communication status.



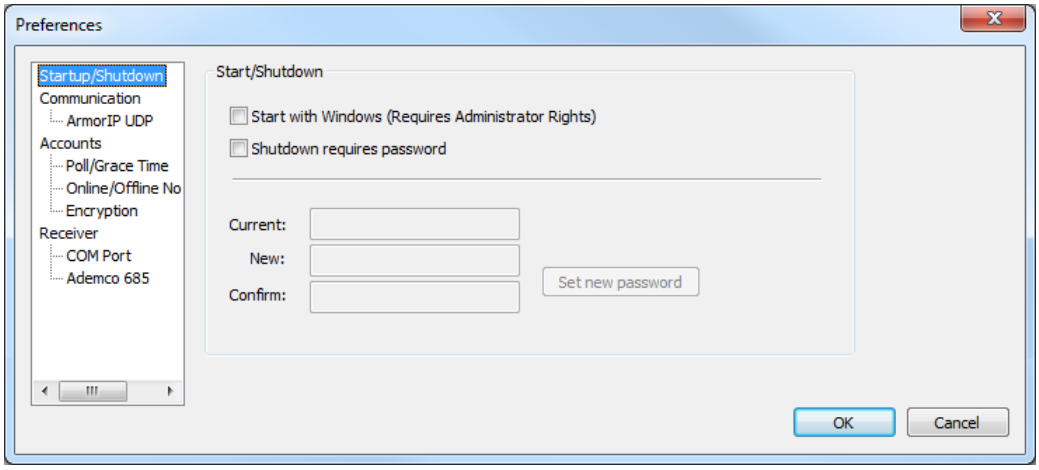
- **Database Queue:** The current number of events waiting to be transferred to the database.
- **Serial Coms Queue:** The number of messages waiting to be sent to the serial receiver.
- **Account Status:** The *overall* account status. This will only be OK (green) if ALL accounts in the list are currently online. If *any* account is in another state, this will reflect the status of that account.
  - Green: All accounts are online
  - Red: One or more accounts are offline
  - Yellow: One or more accounts are in sequence violation
  - Gray: One or more accounts are in an unknown state
- **Receiver Status:** Status of the Serial Receiver.
  - Green: OK
  - Red: Offline

ArmorIP Configuration Options

Information on how ArmorIP is configured is defined under the **Preferences** option from the Setup menu.

Startup/Shutdown

The **Startup / Shutdown** settings contain basic options for how ArmorIP will start and shutdown, and provides the option for changing the ArmorIP password.

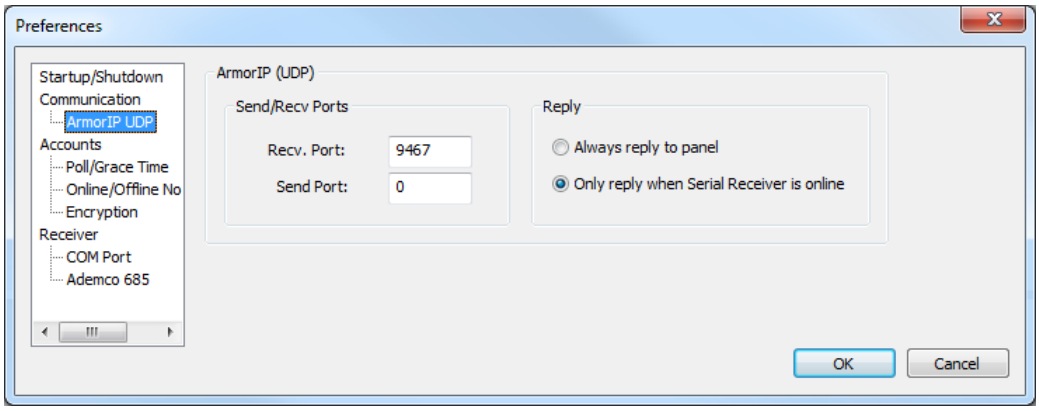


- **Start with Windows (Requires Administrator Rights)**: If enabled, ArmorIP launches automatically when Windows is started
- **Shutdown requires password**: If enabled, a valid password must be entered before the ArmorIP application can be closed.

To change the password, enter the **Current** password, the **New** password, **Confirm** the new password, then click **Set new password**.

Communication

ArmorIP (UDP)



Send/Recv Ports

- **Recv. Port**: Defines the port used by ArmorIP to receive any incoming IP based communications. The default port is 9467.
- **Send Port**: Defines the port ArmorIP uses to reply to panels.

Note: If the send port is 0, ArmorIP will reply on the same port as the incoming messages were received on.

Reply

Defines how ArmorIP will handle incoming messages. Choose either:

- **Always reply to panel**: If enabled, ArmorIP will acknowledge all valid incoming messages.
- **Only reply when Serial Receiver is online**: If enabled, ArmorIP will only reply only when it has an active connection to a Serial Receiver.

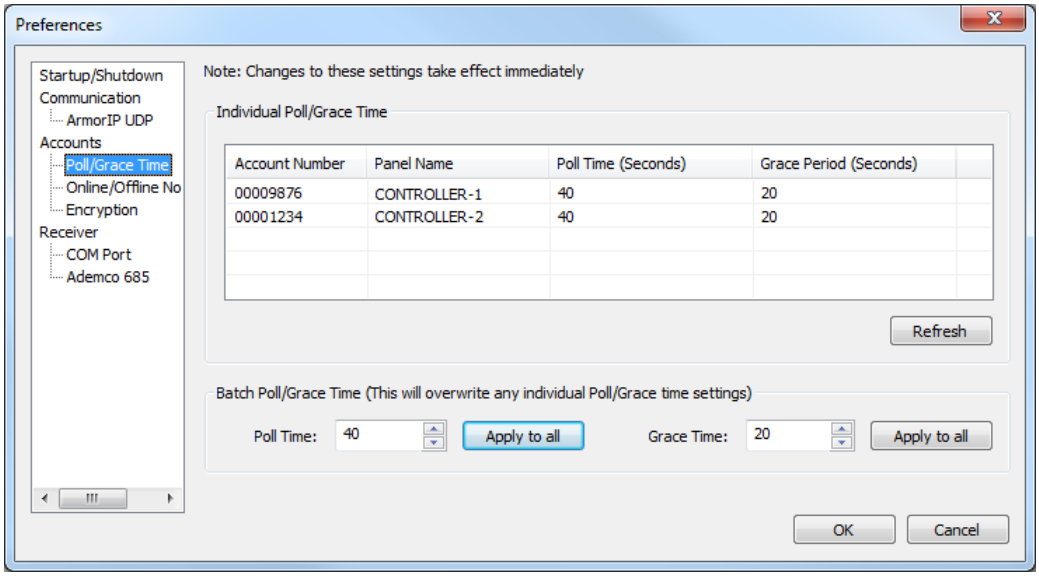
When either option is enabled, a buffering mechanism is involved to avoid loss of events. If the **always** option is selected and ArmorIP gets a valid event it is sent on to the Serial Receiver. If the receiver is not present or currently not responding, ArmorIP will buffer this event and all consecutive events until the receiver is back and successfully receiving messages. Alternatively if the **only when online** option is selected, ArmorIP will send no acknowledgements to panel messages. This causes the panels to retry a number of times. The account will then be in sequence violation and the panels themselves will buffer their own events. Once two way communication is restored, the panels will send through any events that were buffered during this time.

For UL/ULC installations, the **Only reply when Serial Receiver is online** option must be used.

Accounts

Poll/Grace Time

You can set the poll and grace time for an individual account, or use the batch options to apply to all accounts at once.



- **Poll Time**: Defines the number of seconds between consecutive poll messages from a panel.
- **Grace Time**: Defines the number of seconds in addition to the poll duration that ArmorIP will give the panel to poll before changing its status to offline and reporting through to the serial receiver.

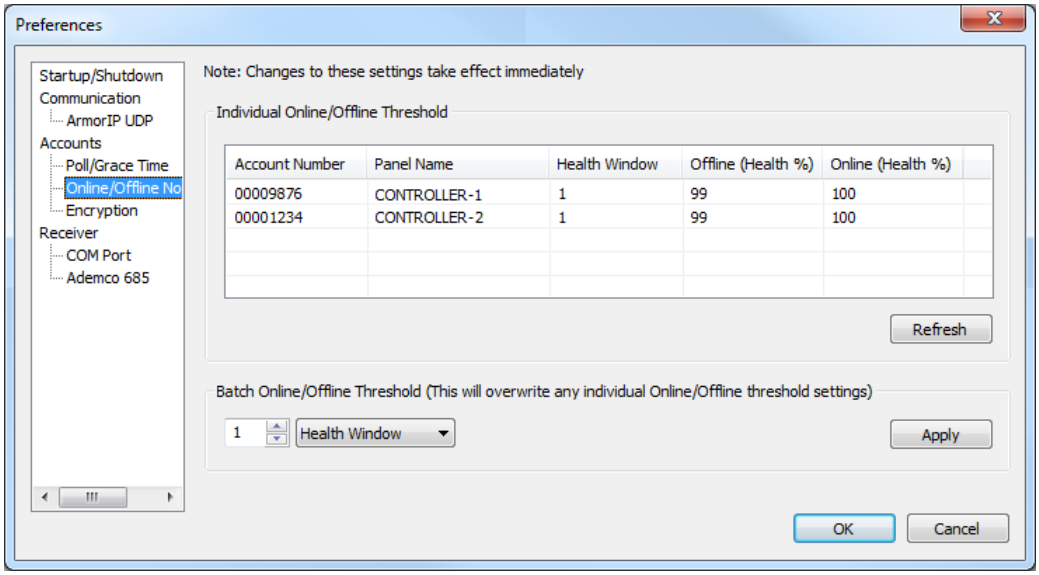
Example

A panel polls at 3:00:00pm. If the poll time is 90 seconds, the next expected poll time would be 3:01.30pm. With a grace period of 20 seconds, if a poll is not received by 3:01:50pm, the panel will go offline.

For UL and ULC installations the Poll Time must be set to **40 seconds** and the Grace Time must be set to **20 seconds**.

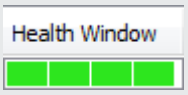
Online/Offline Notification

You can set the notification threshold for an individual account, or use the batch options to apply to all accounts at once.



- **Health Window**: Defines the number of segments / retries for the account. The health counter provides better connection stability and immunity to momentary internet connection losses. This number sets and segments the health window into equal divisions.

Example



When set to four, the health window is separated into four segments.

An account that has not received two consecutive polling/event messages within the configured poll/grace time, would then display a health window that is decremented by two segments and the health value would show as 50%.

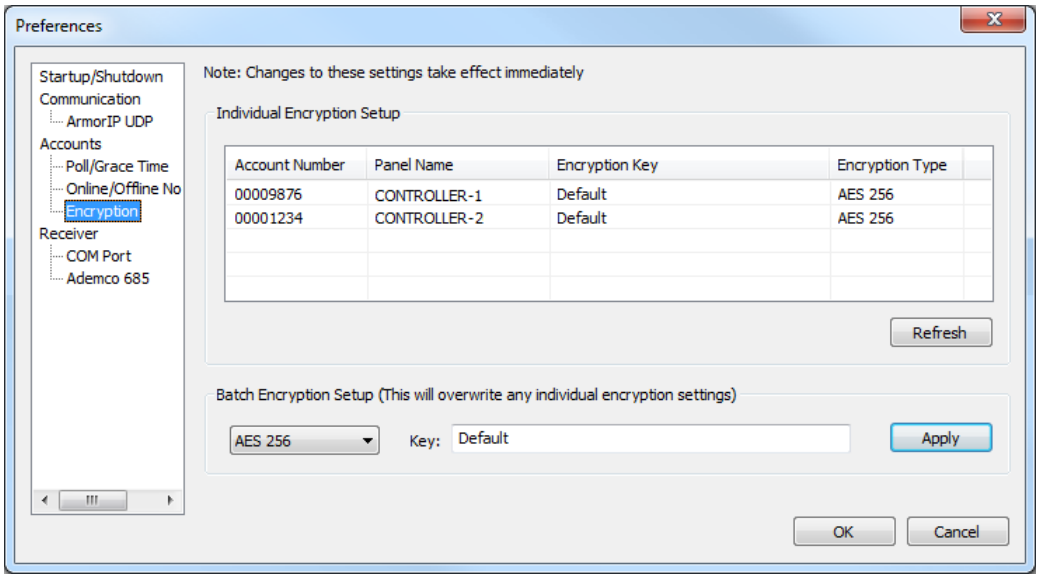
- **Offline (Health %)**: Value based on the health window indicator. When health value drops below the defined percentage, the account will go offline and an offline event will be sent to the automation software.
- **Online (Health %)**: Value based on the health window indicator. When health value goes above this Online percentage value, account will go online and an online event will be sent to the automation software.

For UL and ULC installations the **Health Window** must be set to `1`, the **Offline Health %** must be set to `99%`, and the **Online Health %** must be set to `100%`.

Encryption

The Encryption settings enable you to configure communication to be sent using AES encryption with 128, 192, or 256 bit keys.

You can set the encryption type and key for an individual account, or use the batch options to apply to all accounts at once.

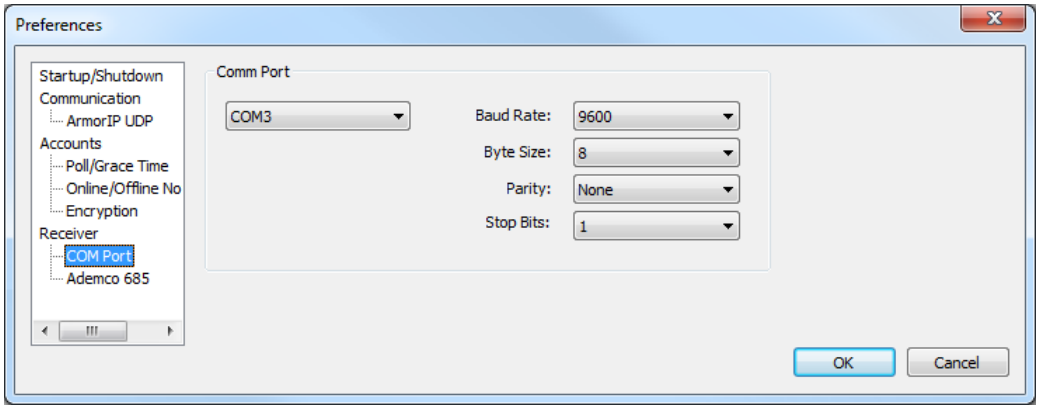


- **Encryption Key**: If an Encryption type is set, this defines the associated Key that isused. For 128 bit encryption the key should be exactly 16 characters long, for 192 bit the key should be 24 characters, and 256 bit encryption the key should be 32 characters. The key can be comprised of any combination of letters and numbers, however the key is CASE SENSITIVE meaning an AES-128 key of `1234567890abcdef` is not the equivalent of `1234567890ABCDEF`.
- **Encryption Type**: Defines the type of AES (Advanced Encryption Standard) which will be used. Choose from None, AES-128, AES-192, and AES-256.

For UL and ULC installations, the **ArmorIP-E (UDP)** protocol must be used and the **Encryption Type** must be set to `AES-256`.

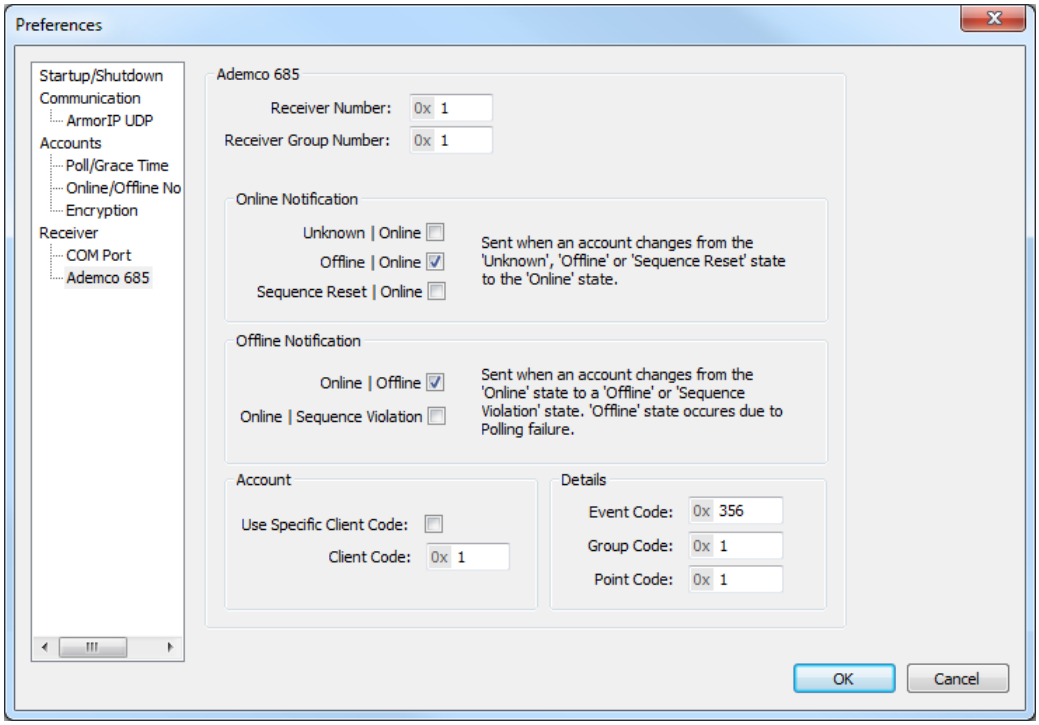
Receiver

COM Port



- **Baud Rate**: The baud rate at which communications will operate.
- **Byte Size**: The number of bits in the bytes transmitted and received.
- **Parity**: The parity scheme to be used. Choose from Even, Odd, None, Mark or Space.
- **Stop Bits**: The number of stop bits that the serial data will use.

Ademco 685



Ademco 685

- **Receiver Number**: The receiver number specified in all serial communication sent
- **Receiver Group Number**: The receiver group number specified in all serial communication sent

Online Notification

- **Unknown | Online**: When enabled, ArmorIP sends a notification to the receiver when an account changes state from unknown to online.
- **Offline | Online**: When enabled, ArmorIP sends a notification to the receiver when an account changes state from offline to online.
- **Sequence Reset | Online**: When enabled, ArmorIP sends a notification to the receiver when an account changes state from sequence reset to online.

Offline Notification

- **Online | Offline**: When enabled, ArmorIP sends a notification to the receiver when an account changes state from online to offline.
- **Online | Sequence Violation**: When enabled, ArmorIP sends a notification to the receiver when an account changes state from online to sequence violation.

Account

- **Use Specific Client Code**: When enabled, ArmorIP informs the receiver of an offline event, using the defined client code as part of the identification code.
- **Client Code**: Defines the client code to be used when sending offline events to the receiver

Details

- **Event Code**: Defines the event code to be sent when a panel goes offline
- **Group Code**: Defines the group code to be sent when a panel goes offline
- **Point Code**: Defines the point code to be sent when a panel goes offline

For UL and ULC installations the Online Notification **Sequence Reset | Online** and the Offline Notification **Online | Sequence Violation** must be turned **OFF** (disabled).

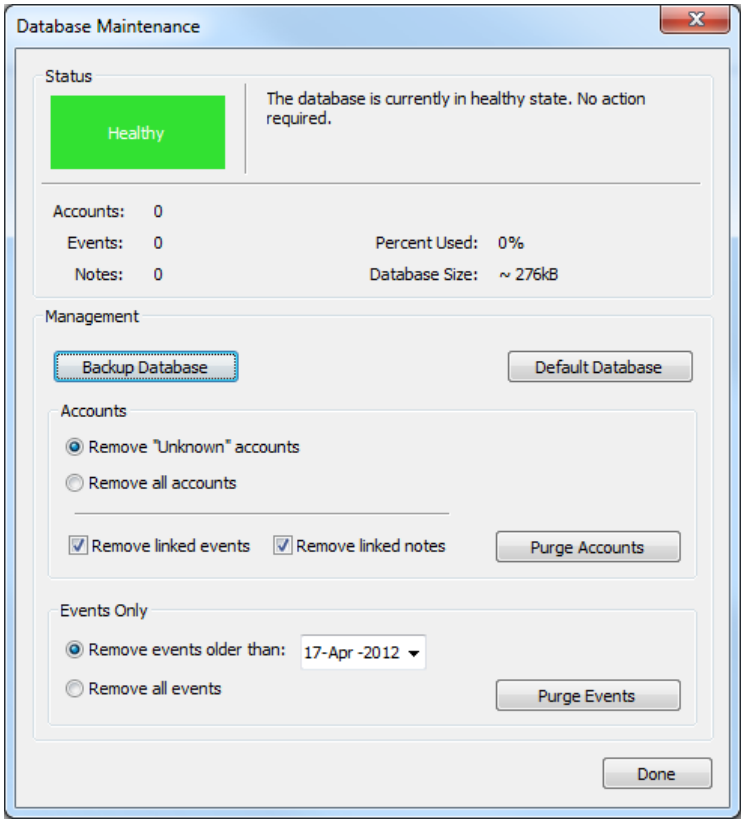
UL and ULC Configuration Requirements

To comply with UL and ULC installation requirements, the following configuration settings must be used:

- Poll time: **40 seconds**
- Grace Period: **20 seconds**
- Health Window: **1**
- Offline (Health %): **99%**
- Online (Health %): **100%**
- Encryption enabled with **AES-256**
- Online Notification option **Sequence Reset | Online** must be turned off (disabled)
- Offline Notification option **Online | Sequence Violation** must be turned off (disabled)

The reporting product (PRT-CTRL-SE Integrated System Controller or CRX-POSTX-DIN IP Reporting Module) must be configured to use the ArmorIP-E (UDP) protocol and AES-256 encryption. Please refer to the PRT-CTRL-SE or CRX-POSTX-DIN documentation and reference manual for details on how to configure the product.

Database Maintenance



Status

Displays the currents status of the database and database statistics, including the number of records and database size.

Management

- **Backup Database**: Select this option to create a backup (*.mdb file) of the ArmorIP database. You will be prompted to enter a filename and location for the file.
- **Default Database**: Select this option to remove information from the database and return it to the default state.

Accounts

- **Remove "Unknown" accounts**: Select this option to remove Unknown accounts
- **Remove all accounts**: Select this option to remove **all** the accounts.
- **Remove linked events**: Select this option to remove all linked events to accounts.
- **Remove linked notes**: Select this option to remove all linked notes to accounts.
- **Purge Accounts**: When pressed, this button will execute the options as selected in this section.

Events Only

- **Remove events older than**: Select this option to remove events older than a specified date. Use the dropdown to select the date.
- **Remove all events**: Select this option to remove all events from the database
- **Purge Events**: When pressed, this button will execute the options as selected in this section.

ArmorIP Basics

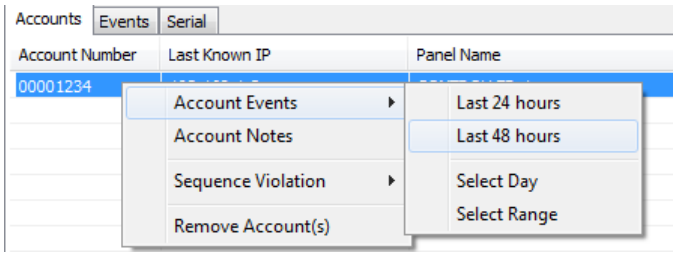
Creating a new Account

Once ArmorIP is correctly configured, all Panels setup to report to the ArmorIP server will have their accounts automatically generated. This means that panels can be brought online easily with minimal user input required.

ArmorIP automatically creates a new account when it receives a poll or event from any Panel that isn't currently in the database.

Reviewing Account Specific Events

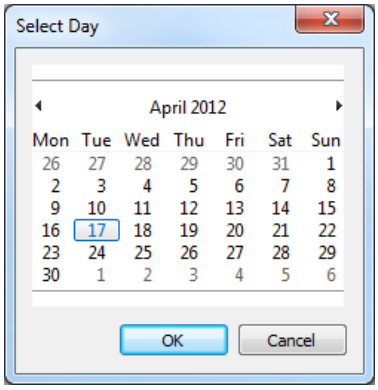
Events from a particular account may be reviewed by highlighting the desired account and selecting the **Account Events** option.

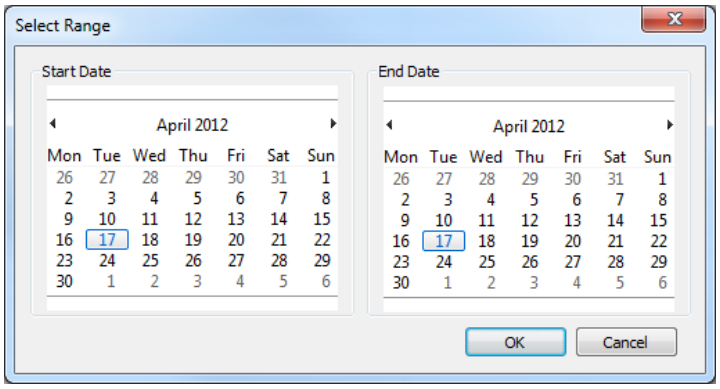


Choose the timeframe you wish to search across:

- Last 24 Hours
- Last 48 Hours
- Select Date
- Select Range

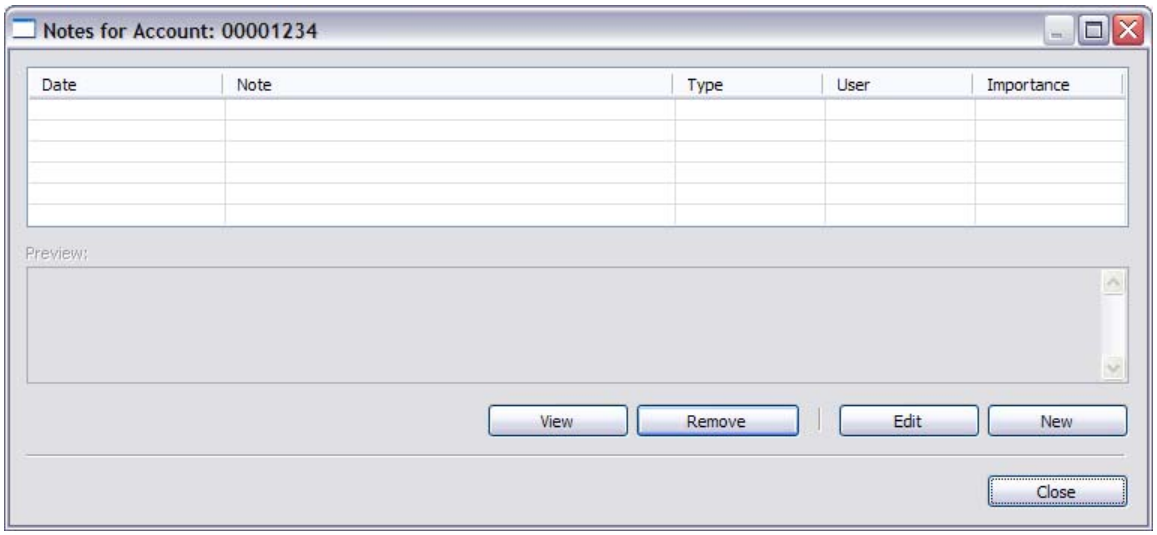
The **Select Date** and **Select Range** options give you the ability to specify specific periods for searching the event database.





Using Account Notes

Notes for a particular account may be added or reviewed by highlighting the desired account and selecting the **Account Notes** option. Notes can be useful for tracking changes and important information such as name/IP address changes.

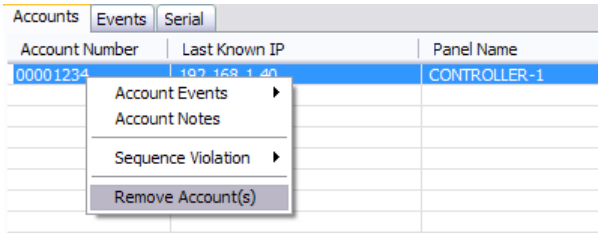


Select from the following options:

- **View**: To view the selected note in detail.
- **Remove**: To permanently remove the selected note.
- **Edit**: To edit the selected note.
- **New**: To add a new note.

Removing an Account

Accounts may be removed from ArmorIP by highlighting the Account from the main screen and selecting **Remove Account**.



This option removes an account from the list. It does not remove historic events from the database.

If an account is removed and it later sends another message to ArmorIP, ArmorIP will automatically add a new account.

Compromise Attempt Events

ArmorIP automatically detects the reception of any invalid packet on the programmed port as a potential system compromise attempt.

Each compromise attempt sends a notification to the receiver, and logs a Compromise Attempt event in the Events Tab.

The event is sent with the following details:

- Account Code as defined in the Account settings on the Ademco 685 tab (see page 24) of the Preferences Menu
- Event Code 0x163
- Group Code as defined in the Details settings on the Ademco 685 tab (see page 24) of the Preferences Menu
- Point Code as defined in the Details settings on the Ademco 685 tab (see page 24) of the Preferences Menu

For UL and ULC installations the Central Station Receiving software must have the Contact ID details as specified, programmed for the **Compromise Attempt** event.

Testing Your Connection Using the RIP Utility

The RIP utility is a command line application that enables you to test the connection between a workstation and the ArmorIP Server, and simulates the Poll events sent by an ArmorIP enabled device such as a Protege Controller or PostX Module.

You may only execute the command from the folder containing the RIP.exe file.

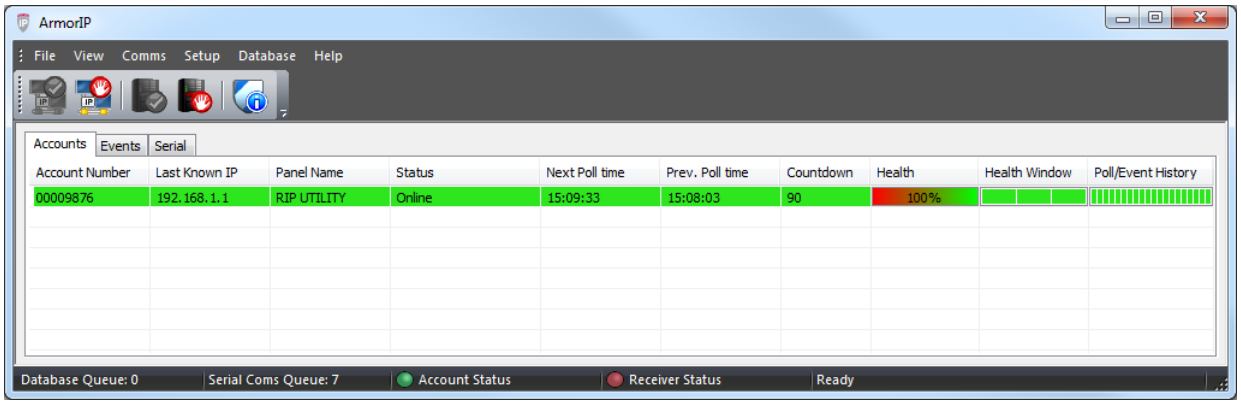
Syntax

```
RIP [IP Address] [IP Port Number] [Account Code]
```

Example:

```
rip 10.47.192.29 9467 9876
```

In the example above, the account 98764 will be created on the ArmorIP Server:



Contact

Integrated Control Technology welcomes all feedback.

Please visit our website (http://www.incontrol.co.nz) or use the contact information below.

Integrated Control Technology

P.O. Box 302-340
North Harbour Post Centre
Auckland
New Zealand

11 Canaveral Drive
Albany
North Shore City 0632
Auckland
New Zealand

Phone: +64-9-476-7124

Fax: +64-9-476-7128

Email: sales@incontrol.co.nz or support@incontrol.co.nz

Web: www.incontrol.co.nz

Integrated Control Technology Limited

11 Canaveral Drive, Albany, Auckland 0632
P.O. Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: support@incontrol.co.nz **Phone:** +64 (9) 476 7124 **Fax:** +64 (9) 476 7128
Designers & manufacturers of integrated electronic access control, security & automation products.
Designed & manufactured by Integrated Control Technology Limited.

www.incontrol.co.nz

227-5500-000 : UL Draft 22 May 2012