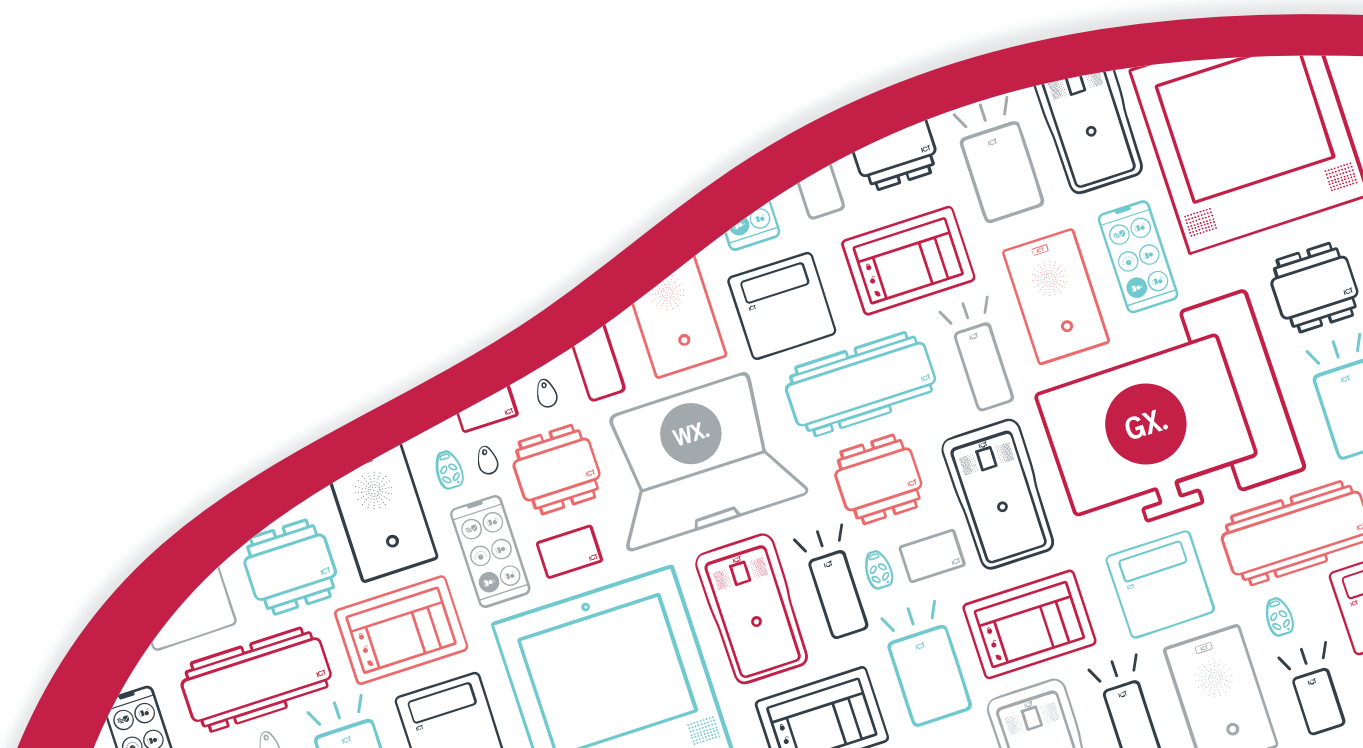
AIP-V3-CORE

ArmorIP Version 3 Internet Monitoring Application

User Manual



Last Published: 10-Nov-22 12:33 PM

Contents

Introduction

The ICT ArmorIP Internet Monitoring Application converts the ArmorIP reporting protocol used by Protege systems, PostX reporting modules and other third-party products to Ademco 685 or Surgard protocols for reporting to compliant offsite monitoring station applications.

Transmission over ethernet ensures greater data security and communication integrity, and provides faster, more reliable and more cost-effective reporting to the automation software than traditional copper line solutions.

The integration process for a monitoring station is seamless and can be completed in minutes, allowing an immediate transition to IP reporting without the usual time-consuming implementation of custom solutions.

How It Works

1. Alarms and events are generated in the Protege system.
2. The Protege reporting service sends alarms/events to the ArmorIP Internet Monitoring Application over IP.
3. The alert messages include full textual description of the event and the item that generated it, along with the appropriate Contact ID code.
4. ArmorIP receives alert messages from the Protege reporting service and attributes them to ArmorIP accounts, which represent specific areas in the Protege system, based on configured client codes.
5. ArmorIP translates the reporting service transmissions to the required reporting protocol and passes them to the third-party automation software.
6. The automation software receives the alert messages with the relevant Contact ID and account references, and full textual description of the event and the item that generated it.
7. The automation software acknowledges that it has received the transmission.

Active Communication Standards

ArmorIP is one of the only systems in the world to meet the ULC Level A4 active communications standard for burglary and fire monitoring (CAN/ULC S304). The system detects and identifies any attempt to send data in a format that cannot be decoded or has invalid data as a compromise attempt. Each compromise attempt sends a notification to the receiver and logs the event.

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 transmission which includes the name of the item (user, area or input) that generated the reportable event, making it easier for a monitoring agent to identify exactly what caused an alarm.

Each item can be individually configured in the Protege system to define the display text used to identify it. ArmorIP then reads the partition and zone/contact/user numbers from Contact ID, and uses the display text (if defined) when displaying an event. For example, instead of displaying an event as Input 8 activated, ArmorIP may display it as Warehouse SW PIR activated.

Descriptions are transmitted directly from the Protege system when the area/input goes into alarm, and updated live when any change is made to record names. This eliminates the need to supply a central station report to the monitoring station as the installer doesn't need to provide the definition for each input/area.

Account Status

Accounts allow for sectioning of the Protege system for reporting purposes. An ArmorIP account can represent a single area, a group of areas, or an entire site. This allows the monitoring station to configure the automation package in the most optimal manner for reception of alarms.

A live view displays the accounts that are online, and the notification of an offline account is presented to the receiver with the appropriate CID message.

The account status screen can be replicated to a live HTML page that can be scheduled for FTP to a remote server, allowing a control room to use this information to display the current status of accounts on a primary screen. The export can also be provided to other applications.

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 the same account that is saved in the ArmorIP server that the PostX or controller 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 the same account that is saved in the ArmorIP server that the PostX or controller 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. To increase the security, a custom key must be entered in both the PostX and the ArmorIP server.

This format uses the UDP layer as its transport mechanism.

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. To increase the security, a custom key must be entered in both the PostX and the ArmorIP server.

This format uses the TCP layer as its transport mechanism.

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

System Requirements

The following section outlines the requirements that must be met before installing ArmorIP.

For UL/ULC installations, the system shall be redundant. For up to 1000 accounts, two computers must be used. Each subsequent set of 1000 accounts requires another two computers. Each server or computer shall employ the following hardware specification and software.

Hardware Requirements

- Pentium 4 2.5GHz (Pentium 4 3GHz or higher is recommended)
- 2GB RAM (4GB recommended)
- 20GB free disk space (40GB recommended)
- 10/100 Mbps ethernet card
- Serial port to be used with central station automation software computer
- Monitor supporting a resolution of at least 1024 x 768
- An internet connection

For UL installations, this software is classified for use with listed ITE (UL60950 or UL62368) hardware that meets the hardware platform requirements specified by the software provider.

For ULC installations, this software is classified for use with COMARK Model 8580 ULC-S527-11 recognized systems.

Supported Operating Systems

The following operating systems are validated and are supported by the ArmorIP server and client application:

Operating System	Edition
Microsoft Windows Server 2022	Standard
Microsoft Windows Server 2019	Standard
Microsoft Windows Server 2016	Standard
Microsoft Windows Server 2012	Standard
Microsoft Windows Server 2008 R2 SP1	All Editions
Microsoft Windows 11	Pro, Business, Enterprise
Microsoft Windows 10	Professional, Enterprise
Microsoft Windows 8.1	Professional, Enterprise, Ultimate
Microsoft Windows 7	Professional

Supported SQL Server Versions

ArmorIP uses a non-proprietary open SQL database engine to store and share information. ArmorIP is compatible with the following versions of Microsoft SQL Server in Enterprise , Standard and Express editions:

- SQL Server 2019
- SQL Server 2016
- SQL Server 2012
- SQL Server 2008 R2

The Express edition is a scaled down, free edition of SQL Server that includes the core database engine and functionality. The Express version of SQL supports up to 10 GB.

Prerequisites

ArmorIP Licensing

The ICT ArmorIP Internet Monitoring Application is a licensed product which requires a valid subscription. The application will stop monitoring if the subscription expires.

License	Order Code	Notes
ArmorIP Version 3 Annual Subscription	AIP-V3-ANS	This subscription must be renewed periodically

ArmorIP Prerequisites

The following third-party components must be installed **before** installing ArmorIP.

Software	Version	Notes
Microsoft .NET Framework	4.0 or higher	
Microsoft SQL Server	2019	Enterprise, Standard or Express editions
	2016	
	2012	
	2008 R2	

Microsoft SQL Server Prerequisites

Note that Microsoft SQL Server has its own set of prerequisites.

Software	Notes
Microsoft ODBC Driver 11 for SQL Server	Must be installed **before** beginning installation of SQL Server

If the following components are not found when installing SQL Server you will be prompted to install them before continuing.

Software	Minimum Version
Microsoft Windows Installer	4.5
Microsoft .NET Framework	3.5 SP1
Microsoft Windows PowerShell	1.0

For UL/ULC installations, other software temporarily or permanently installed in the fire signal receiving center and systems shall not affect the operating system or site specific data.

The user shall not install software that has not been approved by ICT.

System requirements such as Windows updates and cybersecurity applications may be installed as required.

Administrative Permissions

To successfully complete installation, you must have local administrative privileges on the machine you are performing the installation on.

When installing the application, User Account Control (UAC) should automatically prompt you to run the setup as an administrator. If you don't see this prompt, right-click the setup file and choose **Run As Administrator**. If prompted for an administrator password or confirmation, type the administrator password or click **Continue**.

Installation Requirements

The monitoring application and equipment the application is installed on are to be installed in accordance with:

- The product installation instructions
- UL 681 - Installation and Classification of Burglar and Holdup Systems
- UL 827 - Central-Station Alarm Services
- UL 1610 – Central Station Burglar Alarm Units
- CAN/ULC-S301, Central and Monitoring Station Burglar Alarm Systems
- CAN/ULC-S302, Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes and Vaults
- CAN/ULC-S561, Installation and Services for Fire Signal Receiving Centres and Systems
- The National Electrical Code, ANSI/NFPA 70
- The Canadian Electrical Code, Part I, CSA C22.1
- The Local Authority Having Jurisdiction (AHJ)

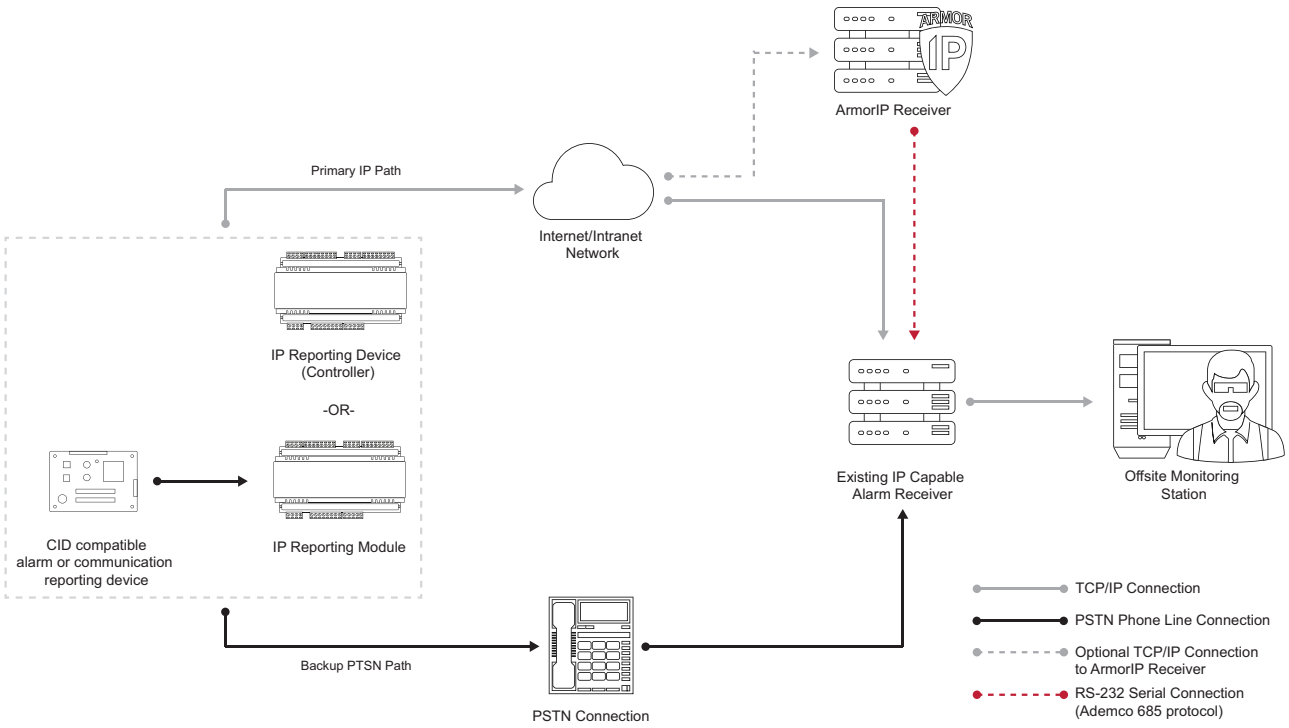
UL General Installation Requirements

1. The installation must provide supply line transient protection complying with the Standard for Transient Voltage Surge Suppressors, UL 1449, with a maximum marked rating of 330 V.
2. The installation must provide signal line transient protection complying with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B, with a maximum marked rating of 50 V.
3. The communication circuits and network components connected to the telecommunications network shall be protected by secondary protectors for communication circuits. These protectors shall comply with the Standard for Secondary Protectors For Communications Circuits, UL 497A. These protectors shall be used only in the protected side of the telecommunications network.
4. All equipment must be installed in a temperature controlled environment. A temperature controlled environment is defined as one that can be maintained between 13 - 35°C (55 - 95°F) by the HVAC system. Twenty-four hours of standby power shall be provided for the HVAC system. The standby power system for the HVAC system may be supplied by an engine driven generator alone. A standby battery is not required to be used.
5. The main power supply and secondary power supply are required to be provided at the central supervisory station, the system must be provided with an uninterruptable power supply (UPS) with sufficient capacity to operate the computer equipment for a minimum of 15 minutes. If more than 15 minutes is required for the secondary power supply to supply the UPS input power, the UPS shall be capable of providing input power for at least that amount of time.
6. Systems provided with a UPS must comply with the Standard for Uninterruptable Power Supply Equipment, UL 1778, or the Standard for Fire Protective Signaling Devices, UL 1481.
7. In order to perform maintenance and repair service, a means for disconnecting the input to the UPS while maintaining continuity of power to the automation system shall be provided.
8. The number of separate signals on a single channel shall be limited to 1000.

Installation

Connection Overview

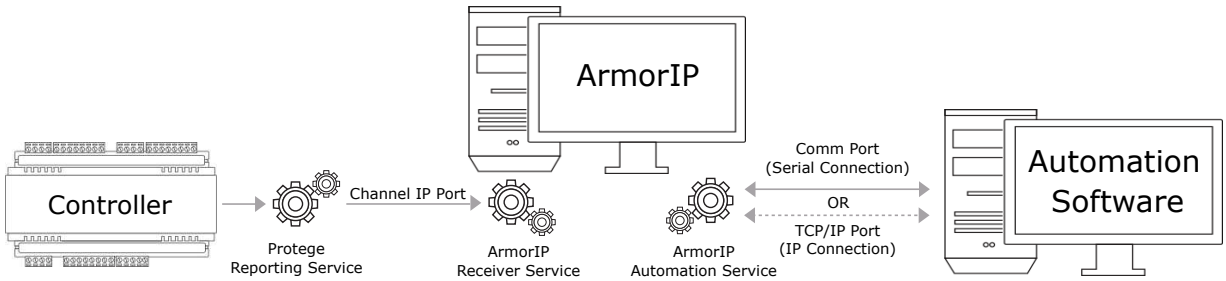
The following diagram provides an overview of the ArmorIP connection.



The ArmorIP application will typically be installed at the monitoring station, not the reporting site.

Integration Architecture

The following diagram provides an overview of the services, ports and connections that allow the ArmorIP monitoring application to receive alerts from Protege controllers and communicate with the monitoring station automation software.



Installing the Prerequisites

Before ArmorIP can be installed, you must install the prerequisite software.

Installing the Microsoft .NET 4.0 Framework

ArmorIP requires the Microsoft .NET 4.0 Framework, available from the Microsoft website.

This is likely already installed on most systems, so first check your machine. Open the control panel, and under **Programs** click **Uninstall a program**. Search or scroll down to find Microsoft .NET Framework. If there is already a version 4.0 or later then you do not need to do anything. Otherwise, follow the instructions below.

The .NET 4.0 Framework works side by side with older framework versions. Existing applications that are based on earlier versions of the framework will continue to run on the version targeted by default.

1. Download and run the **dotNetFx40_Full_setup.exe** file. This launches the Microsoft .NET Framework 4 Setup.
2. Read and accept the license agreement, then click **Install**.
3. Follow the onscreen instructions to complete the installation.

It is recommended that the machine is rebooted once the .NET Framework installation has completed. Although a reboot is not essential, additional components may be needed to complete the installation such as the Windows Image Control installation.

Installing Microsoft ODBC Driver 11 for SQL

SQL Server installation requires Microsoft ODBC Driver 11 for SQL Server, available from the Microsoft website.

If ODBC Driver 11 is not installed, installation of required SQL components will silently fail.

1. Download and run the **msodbcsql** Windows Installer Package file. This launches the Microsoft ODBC Driver 11 for SQL Server Setup.
2. Click **Next**.
3. Read and accept the license agreement, then click **Next**.
4. Follow the onscreen instructions to complete the installation.
5. When the setup is complete, click **Finish**.

It is recommended that the machine is rebooted once the ODBC driver installation has completed.

Installing Microsoft SQL Server

There are several editions of SQL Server Express, ranging from a database only installation to database, advanced services, and manageability tools installation. The following instructions are for **SQL Server 2012 R2 Express with Tools**. As well as the SQL Server Database Engine, this edition includes the SQL Server Management Studio (used for backing up and restoring databases). These instructions also apply to other SQL versions, although the exact steps may vary slightly based on the edition being installed.

Advanced settings within SQL Server, or customizing the SQL installation to a particular environment are beyond the scope of this document. If you have specific inquiries, please contact your system administrator or the ICT Technical Support team.

To Install Microsoft SQL Server:

1. Download and run the setup file to launch the SQL Server Installation Center.
2. On the **Installation** page select the **New installation or add features to an existing installation** link.
3. Read and accept the license terms, then click **Next**.
4. At the **Feature Selection**, ensure the following features are selected, then click **Next**:
   - Database Engine Services
   - SQL Server Replication
   - Management Tools – Basic
5. Set the **Named Instance** to ARMORIP then click **Next** to continue.
6. The **Server Configuration** details are displayed. Click **Next** to continue.
7. The **Database Engine Configuration** details are displayed. Click **Next** to continue.
8. Optionally, enable the error reporting option to automatically send error reports to Microsoft. Click **Next** to continue.
9. The SQL Server setup is complete. Click **Close** to exit the setup wizard.

Installing ArmorIP

The following steps guide you through the process required to install ArmorIP on your local machine.

1. Open the ArmorIP3 executable (*.exe) file. This opens the **ArmorIP3 Install Shield Wizard**.
2. Click **Next**.
3. Read and accept the terms of the **License Agreement**, then click **Next**.
4. Enter the following details into the **Customer Information** window:
   - **User Name**
   - **Organization**
   - **Serial Number**: Your serial number (SSN) is provided when you purchase an ArmorIP license.

   You will need to obtain a license before installing ArmorIP. If you install ArmorIP with an incorrect serial number you will need to uninstall the program and reinstall with the correct SSN.
5. Click **Next**.
6. In the **Setup Type** window, select **Complete** and click **Next**.
7. Enter the following details:
   - **Database Server Instance**: The SQL Server instance name. This will generally be localhost\ArmorIP.
   - **Main Database Name**: The name of the main database. This should be ArmorIP.
   - **Event Database Name**: The name of the event database. This should be ArmorIPEvents.
8. Click **Next**.
9. Read and accept the terms of the PHP License Agreement, then click **Next**.
10. Enter the following details:
    - **Time Zone**: The time zone where the server is located
    - **Website Name**: The name of your site
    - **Port to run Web Interface in IIS**: The port that the ArmorIP interface uses.
      - For HTTP connection the default is 8050. This is not recommended for a live installation.
      - When using a secure connection, select **Enable HTTPS** and enter the port number in the **Port to run Web Interface in IIS (HTTPS)** field. The default is 8060.

    ICT strongly recommends that all sites use a secure HTTPS connection for the ArmorIP interface. HTTP is an insecure protocol and is not a supported installation method for any environment.
11. Click **Next**.
12. Click **Install**.
13. Click **Finish**.

ArmorIP and Windows Firewalls

The Windows Firewall is designed to block unsolicited connections to your PC.

While it is considered good security practice to have the firewall turned on, there can be occasions when the firewall blocks incoming connections from legitimate programs. This can be overcome by adding an exception to the firewall which allows the program to run normally.

If you launch ArmorIP while the Windows Firewall is on, the firewall blocks the connection and displays a security alert. Select **Allow Access** to accept connections from ArmorIP to your computer. This creates an exception for the program, allowing it to communicate through the firewall.

IIS Management Console

The ICT ArmorIP Internet Monitoring Application requires the Windows IIS Management Console to be enabled.

Enabling the IIS Management Console

1. Enable the IIS Management Console by navigating to: **Control Panel > Programs and Feature > Turn Windows Features On or Off**.
2. In the feature list, navigate to **Internet Information Services > Web Management Tools > IIS Management Console**. Check the box to enable this feature.
3. Click **OK**.

Getting Started

Logging In

To log in to ArmorIP from a PC not running the ArmorIP service, see the instructions for Using the Secure Login on a Remote PC (see next page).

To Log In from the Server PC

1. Open a web browser and paste the following link into the URL bar:
   https://<pcname>.<domainname>:<portnumber>
   - Replace the placeholders with the relevant values.
     You can replace <pcname>.<domainname>:<portnumber> with localhost:<portnumber>
     For example: https://localhost:8060

   If you are presented with a security warning when accessing the HTTPS web page, use the advanced options to proceed to the ArmorIP web interface.
2. The login screen is displayed.
3. Enter the default operator login of admin with the password admin.

   For security reasons, this password should be changed (see page 23) before deployment.
4. Click **Login**.

Using the Secure Login on a Remote PC

The ArmorIP web interface can only be accessed securely from PCs that are running the ArmorIP service. This topic outlines the steps required to access the web interface and its functionality from additional PCs. This process involves exporting a certificate file from the PC where the ArmorIP server is installed, and importing it to the machine that you need to access the ArmorIP service from.

Exporting the ArmorIP3 Web Interface Certificate

To export the ArmorIP3 Web Interface certificate, you will need to launch IIS (Internet Information Services) on the PC where the server is installed.

1. Press the **Windows + R** keys to open the **Run** dialog box.
2. Type **inetmgr** into the search bar and press **Enter**.
3. In the IIS section, double click **Server Certificates**.
4. Right click **ArmorIP3 Web Interface** and select **View**.
5. Select the **Details** tab and click **Copy to File**.
6. This opens the Certificate Import Wizard. Click **Next** to continue.
7. Select **No, do not export the private key** and click **Next**.
8. Select the file format to export the certificate in. Click **Next**.
9. Click **Browse** and navigate to the location to export the certificate file.
10. Enter the **File name** to export the certificate as, then click **Save**.
11. Click **Next**.
12. Click **Finish**.

Importing the ArmorIP3 Web Interface Certificate to another PC

The ArmorIP3 Web Interface Certificate must now be imported to the local computer where you will be accessing the ArmorIP service.

1. Launch the Control Panel on your local PC and enter **certificate** in the search.
2. Select **Administrative Tools | Manage Computer Certificates**.
3. Expand the **Trusted Root Certification Authorities** folder.
4. Right click the **Certificates** sub folder and select **All Tasks | Import**.
5. The **Certificate Import Wizard** is displayed and **Local Machine** has been selected. Click **Next**.
6. Click **Browse** and navigate to the certificate file exported earlier (see above). Click **Next**.
7. Select **Place all certificates in the following store** and ensure that **Trusted Root Certification Authorities** is displayed. Click **Next**.
8. Click **Finish**.

Activating Your License

Before you can begin using ArmorIP, you must register and activate your license. This is achieved by obtaining a license file from the ICT website, and enabling the licensed features.

Activating Your License Automatically

1. In the ArmorIP web interface, navigate to **System | License** and select the **License Update** tab.
2. Enter the **Site Details** and **Installer Details**, then click **Save**.
3. In the **Service Status and Control** section, click **Force relicense**.
4. Wait for the status of the update service to display **Running**, then click **Refresh**.

   If an error occurs, **Dismiss** the error message that appears at the top of the page, then **Reload** the page and activate your license manually (see below).

Activating Your License Manually

If automatic licensing fails, the option to manually license ArmorIP becomes available.

1. Click **Get Request** to generate a license request file. The file may be automatically saved to your Downloads folder, or you may be prompted to save the **license_request.req** file to a folder on your network or a portable drive.
2. Open a new browser window and enter https://www.ict.co/license to open the **Manual Registration** page.
3. Enter the following details:

   Site Details
   - **Name**: The name of the site (monitoring station)
   - **Contact**: The name of the contact person for the site
   - **Email**: The email belonging to the contact person of the site

   Installer Details
   - **Contact**: The name of the installer for the site
   - **Email**: The email belonging to the installer for the site

   SSN Details
   - **SSN**: Your serial number (SSN)
   - **File**: The license request file. Click **Choose File** and browse to the **license_request.req** file generated above.
4. Click **Submit**
5. Once registration is complete, you are prompted to download and save your license (***.lic**) file. Save this file to a folder on your network or a portable drive.
6. Navigate back to the ArmorIP user interface.
7. In **Step 3** of the manual licensing process, click **Choose File** and browse to the license file downloaded from the ICT website.
8. Click **Install File**.
9. Click **Restart**.
10. Wait for the status of the update service to display **Running**, then click **Refresh**.

The ArmorIP User Interface

Dashboard

The **Dashboard** is the first page that appears after logging in to the user interface. It provides an overview of the ArmorIP system.

- The operator currently logged in is displayed at the top of the screen, along with a **Logout** option .
- **Main Menu**: Provides access to all functionality within ArmorIP via the available menus.
- **Services**: Displays the status of the automation and communication services.

  An alert will be displayed if any service is currently stopped.
- **Automation Queue**: The total number of events within the automation queue.
- **Total Events Today**: The number of events processed in the current day.
- **Total Accounts**: The total number of accounts in the system.
- **Offline**: The number of accounts that are currently offline.
- The database version and size for both the **Main Database** and **Events Database**.

You can return to the dashboard at any time by clicking on the ICT icon on the main menu.

The Main Menu

The main menu provides access to all program functions.

Accounts

The accounts menu contains the options for configuring and monitoring accounts.

Option	Description
Manage	Create and manage accounts
List | All	Lists all accounts, displaying last poll and current state
List | Offline	Lists all offline accounts
List | Online	Lists all online accounts

Events

The events menu contains the various logs for the events from the controller.

Option	Description
Live Events	Provides a real-time display of the events received
Automation Queue	Displays events received from the controller and identifies whether they have been forwarded and acknowledged
Automation Log	Displays ArmorIP automation audit messages
History	Displays the last 20 audit records
Statistics	Shows the event count in a graphical format

System

Settings that apply to system configuration are grouped under the system menu.

Option	Description
Settings	View and edit system configuration settings
Channels	Configure the inbound channels for use by the server
Operators	Create and manage the operators who can access the ArmorIP application
License	View, activate or update the ICT ArmorIP license

Toolbar

The toolbar appears below the main menu and contains buttons for working with the feature currently selected.

The available buttons will vary according to the feature you are working with. Most features include actions to **Save** and **Refresh**. Others may have options to **Add**, **Delete** and **Export**.

Configuring System Settings

System | Settings

General

- **System Name**: The name of the system as set by the user.
- **Database Version**: The version number of the current database.
- **Time Zone**: The time zone specified in the installation.

History

- **Created**: The date and time of installation.
- **Modified**: The date and time any system settings were last changed.
- **Last Modified By**: The name of the operator who last modified the system.

Settings | Automation Software

These settings relate to connection and communication with the third-party offsite monitoring station application.

Changes to these settings require the ArmorIP Receiver service to be restarted before they take effect. Once the changes have been saved, navigate to **System | Settings | Service Control** and click the green circle to stop the **Receiver service**, then click the gray circle to start.

Automation Software Interface

- **Automation Interface**: The interface used to communicate with the automation software. Options include:
  - Serial Port
  - TCP/IP
- **Automation Format**: The format required to communicate with the automation software. Formats include:
  - Ademco 685
  - Ademco 685 (XML)
  - Ademco 685 (Extended XML)
  - Surgard
  - Surgard (XML)
- **Comm Port**: The port used to communicate with the automation software, when Serial Port is selected as the automation interface. Additional comm port settings include:
  - Comm Port Speed
  - Comm Port Parity
  - Comm Port Data
  - Comm Port Stop
- **TCP/IP Port**: The port used to communicate with the automation software, when TCP/IP is selected as the automation interface.
- **Polling Timeout**: Enter the number of seconds expected between poll messages that will be received from the automation software. Polling is performed regularly by the automation software to verify the automation service's connection, and to raise an alert if connection is lost.
- **Ack Response Time**: Define the time (in seconds) allowed for the acknowledgment (ACK) response to be received from the automation software when transmissions are sent by ArmorIP.
- **Use Alphabetic Status Code For CID Data (E/R Instead of 1/3)**: Enabling this option changes the Contact ID event qualifier code represented by a 1 or 3, to E and R.

Receiver Identification

- **Receiver Account**: The receiver number specified in all serial communications sent.
- **Receiver ID**: The receiver ID for the automation software.
- **Line Number**: The line number for the automation software.
- **Account Event**: The account number specified in event communications.
- **Receiver Event**: The receiver number specified in event communications.

Interface Options

- **Log Automation Port Messages**: When enabled, the automation port messages are logged in the database.

Settings | Service Control

The ArmorIP services monitor and manage the ArmorIP system. This includes communication with Protege controllers and third-party automation software, and ArmorIP licensing requirements.

These services need to be running for ArmorIP to function. The icon is green when the service is enabled, and gray when disabled. Click the icon to disable or enable the corresponding service.

Service Control

- **Update service**: The ArmorIP update service checks and processes license activation.
- **Receiver service**: The ArmorIP receiver service receives data from Protege controllers and other devices.
- **Automation service**: The ArmorIP automation service communicates with third-party automation software.

System | Channels

These settings relate to inbound connection and communication from the Protege system and third-party offsite monitoring station applications.

Changes to these settings require the ArmorIP receiver service to be restarted before they take effect. Once the changes have been saved, navigate to **System | Settings | Service Control** and click the green circle beside the **Receiver service** to stop it, then click the gray circle to start it again.

Details

- **Name**: The name to identify the channel. This is generally the channel type followed by port number.

Channel Setup

- **Computer Name**: The name of the PC on which the server is installed and running the channel.
- **Channel IP Port**: The TCP/IP or UDP/IP port number used by ArmorIP to receive incoming communication.
- **Channel Type**: The protocol (TCP/IP or UDP/IP) used by the channel.

Channel Identification

- **Receiver ID**: The receiver ID for the automation software.
- **Line Number**: The line number for the automation software.

Format Options

- **Enable ArmorIP Format**: Enables receiving ArmorIP format communications for this channel.
- **Enable CSV Format**: Enables receiving CSV format communications for this channel.

System | Operators

Only operators with the **administrator** role assigned have access to view, add or delete other operators.

Adding an Operator

1. Navigate to **System | Operators** and click **Add**.
2. Enter the **Name** of the operator.
3. Enter the operator's **Login** and **Password**.
4. Assign the operator a **Role**, then click **Save**.

Role Permissions

The role defines the permissions for what the operator can view, modify and create within ArmorIP. Each role has a defined set of permissions, as illustrated below.

Function	Guard	Power User	Administrator
View events	✓	✓	✓
View accounts lists	✓	✓	✓
View accounts details (excluding passwords and encryption keys)		✓	✓
View system settings (excluding operators)		✓	✓
Full access to view, add, edit and delete accounts			✓
Full access to view, add, edit and delete operators			✓
Full access to view, add, edit and delete system settings			✓

Changing Operator Passwords

1. Navigate to **System | Operators** and select the operator to change the password for.
2. In the **Password** field, replace the current password with the new one.
3. Click **Save** to update the password.

Configuring and Monitoring Accounts

ArmorIP accounts are essentially a way for the monitoring station to identify who to contact in the event of an alarm. Each account represents a physical space that is reported through the ArmorIP service. An entire building may have only one account, with a single alarm response procedure, or each floor or section of the building may have its own account, with different contact details and protocols.

Each area in the Protege system is linked to an account, using Protege client codes. Through the configuration of client codes an ArmorIP account can represent a single Protege area, a group of areas, or an entire site.

Client codes can be defined in either the area or the reporting service assigned to the area. If both exist, the area setting takes priority, as illustrated in the following table.

Protege Record	Client Code	Reported Code	Notes
Reporting service	1111		The default code for reports from this service
Area 1	2222	2222	The area client code takes priority over the service
Area 2	FFFF	1111	FFFF signifies to use the reporting service client code

Multiple areas, using the same or different client codes, can report through the same service, or through multiple reporting services. ArmorIP simply links the client code attributed to an area with the account code set in ArmorIP to associate the area with the account.

Adding Accounts

While it is possible to add accounts manually, it is best to let them be created by the reporting service. When the service first makes contact and attempts to poll the receiver using the client code, it will automatically create an account for any client code that does not already have one.

Primary Accounts

A Protege area can have its own client code, and will be reported to the monitoring station accordingly. However, only the reporting service can poll the receiver, so only the account with that client code can ever be polled. This means that if the area has a different client code than the service, the receiver never receives a poll from the area's account, and it will always be offline. Monitoring, reporting and alarms will still function, but it will no longer be possible to distinguish which accounts or areas are actually offline.

To resolve this, you can set the reporting service account as the primary account for the area's account. That way, when the service polls the receiver it is recognized as also being a poll from the area's account, and it remains online. Depending on your configuration, you may need to set the reporting service account as the primary account for all other accounts.

Accounts | Manage

Manage | General

Details

- **Name**: A descriptive name for the account.
- **Account Code**: The account code links the account to the Protege area(s). Enter the Protege client code for the area(s) or reporting service the account represents. Each account code be must be unique within ArmorIP.
- **Primary Account**: If this account requires a primary account assigned, select it from the dropdown.
  For more information, see Primary Accounts (see above).

Communication

- **Remote**: The protocol, server channel port, IP address and port of the account from the last communication.
- **Last Sequence**: The last sequence number is contained in the event sent from the controller. It enables ArmorIP and the controller to identify the last message and verify that the correct message is acknowledged.
- **Last Poll**: The date and time the last message was received .

Manage | Polling

Polling times can be left at the default settings, or changed as requested by the alarm monitoring company or as dictated by local regulations.

Polling

- **Poll Time**: Defines the number of seconds expected between poll messages from a controller.
- **Poll Grace Time**: Defines the number of seconds in addition to the poll time that ArmorIP will wait for the controller to poll before changing the account status to offline and reporting to the alarm receiver.
- **Poll Count**: Obsolete. Use Poll Online and Poll Offline instead.
- **Poll Offline**: Defines the number of polls an account can miss before being considered offline. For example, if set to 3 the account can miss 2 polls and still be considered online. If it misses a third poll it becomes offline.

  This value should never be less than 1.

- **Poll Online**: Defines the number of consecutive successful polls an account must receive before it is considered to be online.

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

Polling Options

- **Log Polling Message (Caution Fills Database)**: Logs all polling messages in the database. This should only be used for setup and troubleshooting, and should be disabled during regular operation as it will create excessive numbers of database records over time.
- **Disable Account Communication Events**: Disables communication events being sent to the database.

Manage | Security

Encryption

- **Encryption**: The level of encryption for the ArmorIP service. Select from AES 128, AES 192 and AES 256.
- **Encryption Key**: The associated encryption key for the ArmorIP service. This can be comprised of any combination of letters and numbers.

  The key is any sequence of letters and numbers shared with the reporting service. The key must be 16 characters in length for AES 128 encryption, 24 characters for AES 192, and 32 characters for AES 256.

The same encryption key and method must be set in the Protege reporting service to enable communication between the Protege system and the ArmorIP Internet Monitoring Application.

For UL/ULC installations, the Encryption level must be set to **AES 256**.

CSV Account Settings

Third-party panels can communicate with the ArmorIP monitoring application using the CSV-IP protocol. This requires username/password authentication, which must also be programmed into the third-party panel.

- **CSV User**: The username for user authentication when sending via CSV format.
- **CSV Password**: The password for user authentication when sending via CSV format.

Manage | Manage

These settings create a link to a Protege system by using the port number of the controller. This allows you to log in and manage the Protege controller from the ArmorIP interface.

Management Console

- **Display Remote IP Link**: When enabled, a link is displayed to the configured Protege system.
- **Management Console Port**: The port number for the Protege system. If no port number is set, the default port 80 is used.

Removing an Account

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

To delete an account:

1. Select the account from the record list.
2. Click **Delete**.
3. Click **Yes**.

List

The list menu provides access to account lists which display the state of accounts and differentiate between the offline and online accounts for easy identification.

All Accounts

The all accounts list allows you to easily view the last poll date/time and current state for each account.

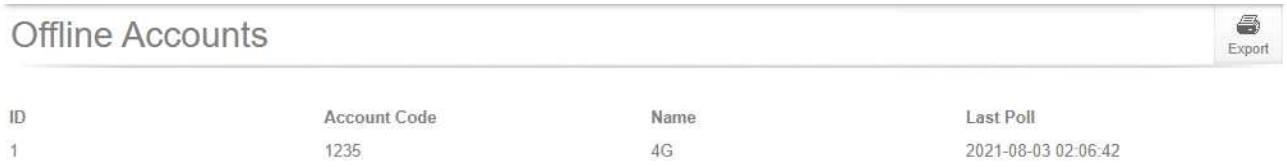
The **State** is a visual representation of the communication between the Protege system and the ArmorIP receiver service, where the first segment is the most recent poll and missed polls are displayed in red.

An account which has missed three consecutive polling/event messages within the configured poll/grace time would display a poll history that shows the first three segments colored red.

The event messages for the state can be seen in **Events | Live Events**.

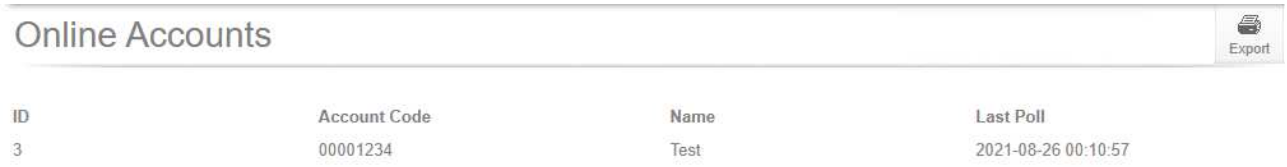
Offline Accounts

The offline accounts list displays all the accounts that could not reach the ArmorIP receiver service within the configured polling requirements.



Online Accounts

The online accounts list displays all the accounts that successfully reached the ArmorIP receiver service within the configured polling requirements.

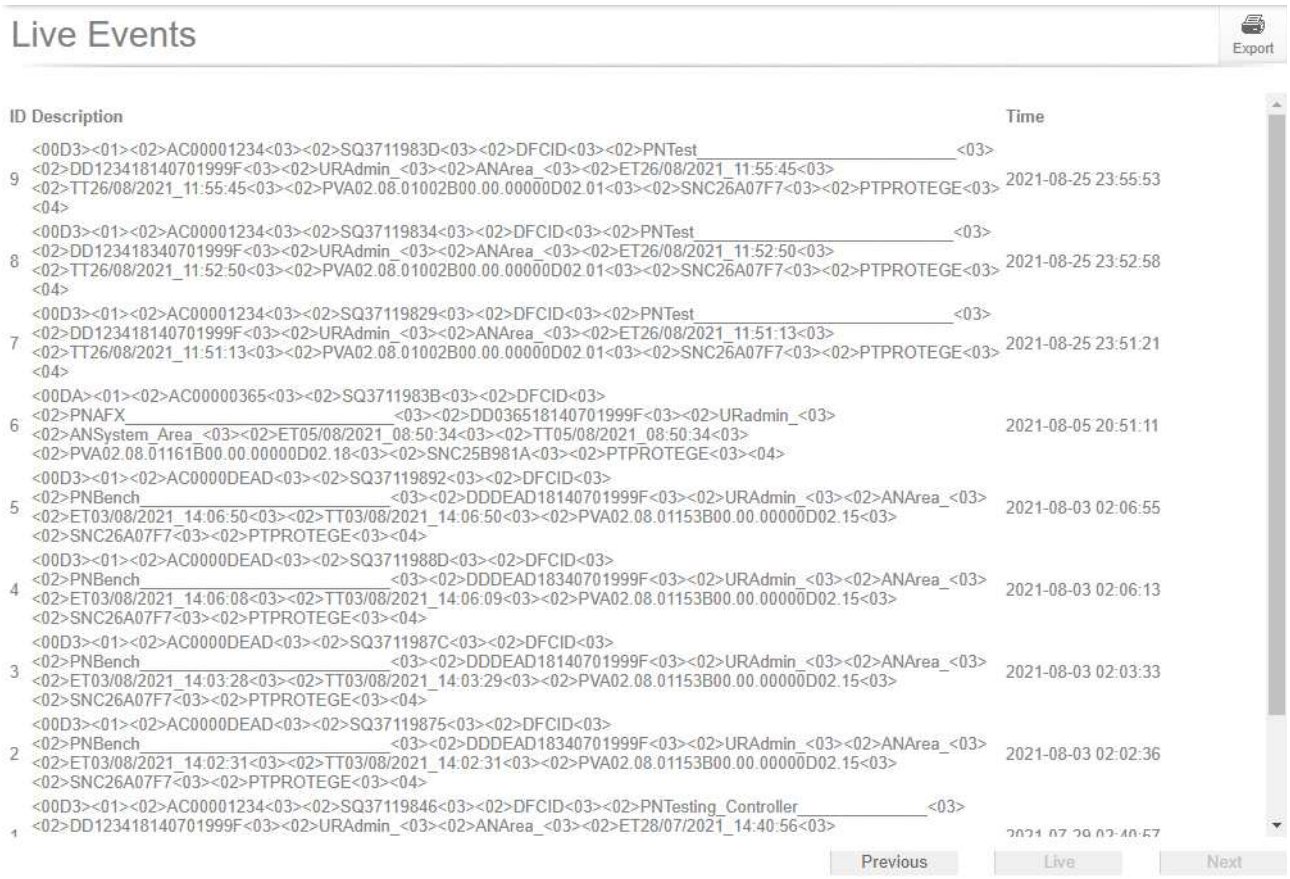


Events

If event messages are missing or a warning is displayed, you can check the Windows Events Viewer for a detailed event message. If the message states that the license limit is exceeded, please contact ICT Customer Services.

Live Events

The live events page provides a real-time display of the event messages received from the Protege system, showing a unique ID, description and time of the message.



Automation Queue

The automation queue shows the ID, description, raw data and time of the message that has been received from the controller.

ID	Description	Raw Data	Time	Ack State
11	Test Communication Restored	123418335600001F	2021-08-26 00:04:57	
10	Area Area (01) Remotely Disarmed By User Admin (999)	123418140701999F	2021-08-25 23:55:53	
9	Area Area (01) Remotely Armed By User Admin (999)	123418340701999F	2021-08-25 23:52:58	
8	Area Area (01) Remotely Disarmed By User Admin (999)	123418140701999F	2021-08-25 23:51:21	
7	Area System Area (01) Remotely Disarmed By User admin (999)	036518140701999F	2021-08-05 20:51:11	
6	Area Area (01) Remotely Disarmed By User Admin (999)	DEAD18140701999F	2021-08-03 02:06:55	
5	Area Area (01) Remotely Armed By User Admin (999)	DEAD18340701999F	2021-08-03 02:06:13	
4	Area Area (01) Remotely Disarmed By User Admin (999)	DEAD18140701999F	2021-08-03 02:03:33	
3	Area Area (01) Remotely Armed By User Admin (999)	DEAD18340701999F	2021-08-03 02:02:36	
2	Area Area (01) Remotely Disarmed By User Admin (999)	123418140701999F	2021-07-29 02:40:57	
1	Testing Controller Communication Restored	123418335600001F	2021-07-29 02:35:19	
0	Area Area (01) Remotely Armed By User Admin (999)	123418340701999F	2021-07-29 02:34:18	

Automation Log

The automation log shows the ID, server, account status and time of the polling updates.

ID	Description	Time
1	[Support-Externa] - Account Online Test Account Code [3]	2021-08-26 00:04:57
0	[Support-Externa] - Account Online Testing Controller Account Code [0]	2021-07-29 02:35:19

History

The history displays the last 20 account creation records.

ID	Description	Time
1	Accounts Record Added Account Code 00001234 By TCP 9468:49.50.247.169:52281 - Support-Externa	2021-08-25 23:55:53
0	Accounts Record Added Account Code 00001234 By TCP 9468:49.50.247.169:49344 - Support-Externa	2021-07-29 02:34:18

Statistics

The event statistics are displayed as a graph showing the number of events that have occurred for all accounts within a 24 hour period. There is also an option to export the graph as a PNG, JPEG, PDF or SVG image.

Exporting Events

1. Click the **Export** button to locate recorded events.
2. Enter the **Start/End Date** and time for each date.
3. Click **OK**.

A report is exported in CSV format for the selected period.

System Messages

System messages are sent to the automation software to monitor status messages from the ArmorIP system. Messages are sent when an account changes state, a compromise event occurs, or a sequence violation takes place. They are sent using the following generic codes. If no account is associated with an event the ArmorIP receiver will always use account code 9999.

ArmorIP System Messages		
Communication Attempt	XXXX 18 1356 0000 1F	Communication Failure
	XXXX 18 3356 0000 1F	Communication Restored
Account Offline or Online	XXXX 18 E356 00 C001	Account Offline
	XXXX 18 R356 00 C001	Account Online

When a sequence violation is reset, the account online status is also restored.

UL and ULC Installation Requirements

Only UL / ULC listed compatible products are intended to be connected to a UL / ULC listed control system.

Central Station Signal Receiver Compatibility List

- IP Receiver via Ethernet Port: ArmorIP Internet Monitoring Receiver. Internet monitoring software and interconnected with a (DAXW/C) central station automation system software and compatible receiving equipment.
- CID Receiver via Onboard Modem: Any UL and ULC listed receiver that uses the Contact ID protocol.

  Modem model only.

ULC Compliance Requirements

CAN/ULC-S304

- **Auto Arming**

  Control units that support auto arming shall provide an audible signal throughout the protected area not less than 10 min prior to the auto arming taking place. The control unit shall allow authorized users to cancel the auto arming sequence and transmit such cancelation to the signal receiving center with the identification of the authorized user that canceled the action.

  The following options must be enabled in the Protege system when using the Auto Arming feature. When the defer warning time is programmed to 10 minutes, the output group will be activated 10 minutes before the system performs the Auto Arming in the associated Area.
  - The **Defer Output or Output Group** must be programmed. Refer to the section Areas | Outputs in the Operator Reference Manual for programming instructions.
  - The **Defer Warning Time** must be programmed to not less than 10 minutes. Refer to the section Areas | Configuration in the Operator Reference Manual.
  - The **Defer Automatic Arming** option must be enabled. Refer to the section Areas | Options (2) in the Operator Reference Manual.
- **Arming Signal**

  A bell or visual indicator used as an arming acknowledgment signal must be listed to a ULC security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- **Double EOL Input Configuration**

  Only double EOL Input Configuration shall be used. Refer to the Inputs section of this manual and the section Inputs | Options in the Operator Reference Manual.
- **Multiplex System and Poll Time**

  The Protege controller is compatible with the ArmorIP Internet Monitoring Receiver. Poll Time must be set to 40 seconds and the Grace Time must be set to 20 seconds.

  In the Protege system, the reporting service must be configured to 40 seconds. The following options are required for the service selected as Report IP type:
  - The **Log Polling Message** option must be enabled. Refer to the section Report IP | Options in the Operator Reference Manual.
  - The **Poll Time** must be programmed to 40 seconds. Refer to the Report IP | General section in the Operator Reference Manual.
- **Central Station Signal Receiver**

  The common equipment of each signal receiving center control unit shall be limited to 1000 alarm systems.
- **Number of attempts**

In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

In the Protege system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The **Dial Attempts** option must be programmed. Refer to the section Contact ID | Settings in the Operator Reference Manual.

If the PRT-4G-USB cellular modem is being used as the secondary reporting option in the installation, the Report IP service assigned to the cellular modem must be programmed as above.

- **Check-In Time**

  DACT communication channel check-in time is not to exceed 24 hrs.
- **Trouble Input Service Test Report**
  - The **Test Report Time** must be programmed. Refer to the section Controllers | Configuration in the Operator Reference Manual.
  - The **Generate Input Restore on Test Input** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
  - The **Test Report Time is Periodic** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
- **Primary Communication Channel**

  The first attempt to send a status change signal shall utilize the primary communication channel.

  The Report IP and Contact ID services must be programmed and enabled within the Protege system, and the CID service must be set as the backup service.

  If the PRT-4G-USB cellular modem option is being used as the secondary reporting option in the installation, the Report IP service assigned to the cellular modem must be configured as the backup service.

  The following options are required:
  - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
  - Refer to the section Contact ID in the Operator Reference Manual.
  - The **Report IP Service** must be enabled as the primary communication channel and the **Service Mode** must be configured to start with the operating system. The **Reporting Protocol** must be set to ArmorIP, and the **Backup Service** must be configured to use the Contact ID Service.

    If the PRT-4G-USB cellular modem option is being used as the secondary reporting option in the installation, the **Backup Service** must be configured to use the Report IP service assigned to the cellular modem.
  - Refer to the section Report IP in the Operator Reference Manual.
  - All ULC S304 P3 applications must transmit signals simultaneously over both the primary communications channel and the Backup Service. This will occur automatically with the above programming.
- **Status Change Signal**

  An attempt to send a status change signal shall utilize both primary and secondary communication channels.
- **Local Annunciation if Signal Reporting Failure**

  Failure of the primary communication channel or secondary communication channel shall result in a trouble signal being transmitted to the signal receiving center within 240 seconds of the detection of the fault. Failure of either communication channel shall be annunciated locally within 180 seconds of the fault.

  The following options must be enabled in the Protege system:
  - The **Ethernet Link Failure** trouble input must be programmed.
  - The **Trouble Input Area** must be armed. Refer to the section Trouble Inputs | Areas and Input Types in the Operator Reference Manual.
  - The **Log Modem Events to Event Buffer** option must be selected in the backup reporting service.
- **Network and Domain Access**

Neither the subscriber control unit nor the signal receiving center receiver shall be susceptible to security breaches in general-purpose operating systems.

Network access policies should be set to restrict unauthorized network access and "spoofing" or "denial of service" attacks.

- **Ethernet Connections**

  All ethernet network connections shall be installed within the same room as the equipment.

- **Encryption**

  For active communications channel security, encryption shall be enabled at all times.

  The ArmorIP-E (UDP) protocol must be used and the Encryption Type must be set to AES-256.

  The following options must be enabled for the Report IP service in the Protege system.

  - The **Reporting Protocol** must be set to ArmorIP (UDP) Encrypted. The AES key must be set as specified by monitoring station.
  - Refer to the section Report IP | General in the Operator Reference Manual.

- **Server Configuration**

  Where a server is employed for control over network addressing, encryption or re-transmission, such shall be designed to remain in the "on state" at all times.

  Communicators are not suitable for active communication channel security and medium or high risk applications unless such can be "online" at all times, have a minimum 128 bit encryption scheme, have encryption enabled, network and domain security implemented.

  Network access policies shall be set to restrict unauthorized network access and "spoofing" or "denial of service" attacks.

- **Internet Service Provider (ISP)**

  The Internet Service Provider (ISP) providing service shall meet the following requirements:

  - redundant servers/systems
  - back-up power
  - routers with firewalls enabled and
  - methods to identify and protect against "Denial of Service" attacks (i.e. via "spoofing")

- **Information Technology Equipment, Products or Components of Products**

  Products or components of products, which perform communications functions only, shall comply with the requirements applicable to communications equipment as specified in CAN/CSA-C22.2 No. 62368-1, Audio/video, information and communication technology equipment - Part 1: Safety requirements. Where network interfaces, such as the following, are internal to the subscriber control unit or receiver, compliance to CAN/CSA-C22.2 No. 62368-1 is adequate. Such components include, but are not limited to:

  - A) Hubs;
  - B) Routers;
  - C) Network interface devices;
  - D) Third-party communications service providers;
  - E) Digital subscriber line (DSL) modems; and
  - F) Cable modems.

- **Backup Power Requirements**

  Power for network equipment such as hubs, switchers, routers, servers, modems, etc., shall be backed up or powered by an uninterruptible power supply (UPS), stand-by battery or the control unit, capable of facilitating 24h standby, compliant with Clauses 16.1.2 and 16.4.1 of CAN/ULC-S304.

  For communications equipment employed at the protected premises or signal receiving center and intended to facilitate packet switched communications, as defined in CAN/ULC-S304, 24h back-up power is required.

- **Compromise Attempt Events**

  ArmorIP 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 under the Live Panel Events.

  The event is sent with the following details:

- **Account Code** as defined in the Serial Receiver settings
- **Event Code** 0x163
- **Group Code** as defined in the Serial Receiver settings
- **Point Code** as defined in the Serial Receiver settings

Refer to the section Global Settings | Serial Receiver in the ArmorIP Version 3 Internet Monitoring Application User Manual.

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

- **Power Supply Mains Power Connection**

  If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.

  The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

CAN/ULC-S559

- **Signal Reporting**

  Any fault of an active communication system shall be annunciated and recorded at the signal receiving center within 180 s of the occurrence of the fault.

  The Report IP and Contact ID services must be programmed and enabled within the Protege system. The following options are required:

  - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
  - Refer to the section Contact ID in the Operator Reference Manual.
  - The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
  - Refer to the section Report IP in the Operator Reference Manual.
  - The **Trouble Area** must be armed. Refer to the section Trouble Inputs | Areas and Input Types in the Operator Reference Manual.

  In the ArmorIP Internet Monitoring Software the **Poll Time** must be set to 40 seconds and the **Grace Time** must be set to 20 seconds. Refer to the section Poll/Grace Time in the ArmorIP Version 3 Internet Monitoring Application User Manual.

- **Central Station Signal Receiver**

  The maximum number of signal transmitting units connected to any transmission channel shall conform to the manufacturer's recommendations. The ArmorIP Receiver supports up to 10000 simultaneous connections.

  Refer to the section Internet Connections Requirements in the ArmorIP Receiver Installation Manual for further details.

- **Number of attempts**

  In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

  In the Protege system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The **Dialing Attempts** option must be programmed. Refer to the section Contact ID | Settings in the Operator Reference Manual.

  If the PRT-4G-USB cellular modem is being used as the secondary reporting option in the installation, the Report IP service assigned to the cellular modem must be programmed as above.

- **Check-In Time**

  DACT communication channel check-in time is not to exceed 24 hrs.

- **Trouble Input Service Test Report**
  - The **Test Report Time** must be programmed. Refer to the section Controllers | Configuration in the Operator Reference Manual.

- The **Generate Input Restore on Test Input** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
- The **Test Report Time is Periodic** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.

- **Ethernet Connections**

  All ethernet network connections shall be installed within the same room as the equipment.
- **External Wiring**

  All wiring extending outside of the enclosure must be protected by conduit.
- **Power Supply Mains Power Connection**

  If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.

  The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.
- **Arming Signal**

  A bell or visual indicator used as an arming acknowledgment signal must be listed to a ULC security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- **Keypad Wiring**

  The RS-485 connection to the keypad must be wired such that the shorts and other faults on the RS-485 line connection of the keypad will not cause the controller to malfunction.
- **Fire Areas**

  Fire areas shall be separated from burglar areas through area partitioning.

  NOTE: Any available dry relay contact on the Protege controller or output expander may be used for the FACP system, provided the selected output is programmed as the Report OK output.

UL Compliance Requirements

UL1610

For Security Grade 4 installations, two forms of reporting are required. This can be satisfied using the onboard 2400bps modem included with the modem controller model, or through the incorporation of the PRT-4G-USB cellular modem module into the installation with the non-modem controller model.

- A local alarm sounding device, alarm housing, and control unit shall comply with the mercantile requirements in the Standard for Police Station Connected Burglar Alarm Units and Systems, UL365.
- A bell or visual indicator used as an arming acknowledgement signal must be listed to a UL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Exit and entry delay must not exceed 60 seconds. To program the entry and exit delay time, refer to the section Areas | Configuration in the Operator Reference Manual.
- All ethernet network connections shall be installed within the same room as the equipment.
- Signals between the premises control unit and the receiving equipment, when not carried by wireless means, shall be protected by the following method:
  - Onboard modem telco connection must be dedicated to the Protege controller.

    Modem model only.
  - Ethernet connection to the Internet Service Provider (ISP) with a fixed IP Address must be dedicated to the Protege controller.
- To comply with the dual signal line transmission system requirement, both transmission lines (onboard modem and IP reporting) must be enabled. Signals shall be sent simultaneously to both the primary communications channel and the Backup Service.

  The Report IP and Contact ID services must be programmed and enabled within the Protege system. The following options are required:
  - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.

- Refer to the section Contact ID in the Operator Reference Manual.
- The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
- Refer to the section Report IP in the Operator Reference Manual.

- When more than one means of signal transmission is used, loss of communication with the receiving system shall be annunciated at the receiver within 200 seconds. If a fault is detected on any of the signal transmission means, at least one of the signal transmission channels shall send a signal to the central-station to report the fault within 200 seconds.

  The Report IP and Contact ID services must be programmed and enabled within the Protege system.

  The Protege controller is compatible with the ArmorIP Internet Monitoring Receiver. Poll Time must be set to 40 seconds and the Grace Time must be set to 20 seconds.

  In the Protege system, the reporting service must be configured to 40 seconds. The following options are required for the service selected as Report IP type:
  - The **Poll Time** must be programmed to 40 seconds. Refer to the Report IP | General section in the Operator Reference Manual
  - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
  - Refer to the section Contact ID in the Operator Reference Manual
  - The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
  - Refer to the section Report IP in the Operator Reference Manual.
  - The **Trouble Input Area** must be armed in 24h mode. Refer to the section Trouble Inputs | Areas and Input Types in the Operator Reference Manual.

  In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

  In the Protege system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The following options are required:
  - The **Dial Attempts** option must be programmed. Refer to the section Contact ID | Settings in the Operator Reference Manual.
- DACT communication channel check-in time is not to exceed 24 hrs.
- Trouble Zone Service Test Report
  - The **Test Report Time** must be programmed. Refer to the section Controllers | Configuration in the Operator Reference Manual.
  - The **Generate Input Restore on Test Input** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
  - The **Test Report Time is Periodic** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
  - ArmorIP 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 under the Live Panel Events.

    The event is sent with the following details:
    - **Account Code** as defined in the Serial Receiver settings
    - **Event Code** 0x163
    - **Group Code** as defined in the Serial Receiver settings
    - **Point Code** as defined in the Serial Receiver settings

    Refer to the section Global Settings | Serial Receiver in the ArmorIP Version 3 Internet Monitoring Application User Manual.

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

- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

Disclaimer and Warranty

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.

For warranty information, see our Standard Product Warranty.

Submitted to UL 10-Nov-22

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.