ROSSLARE
Secure Access Solutions

AxTraxPro™

Access Control Management Software Desktop Client V28.0.1.7

User Guide



© 2022 Rosslare Enterprises Ltd. All rights reserved.

This manual and the information contained herein are proprietary to ROSSLARE ENTERPRISES LIMITED and/or its related companies and/or subsidiaries' (hereafter: "ROSSLARE"). Only ROSSLARE and its customers have the right to use the information.

No part of this manual may be re-produced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of ROSSLARE.

ROSSLARE owns patents and patent applications, trademarks, copyrights, or other intellectual property rights covering the subject matter in this manual.

TEXTS, IMAGES, AND ILLUSTRATIONS INCLUDING THEIR ARRANGEMENT IN THIS DOCUMENT ARE SUBJECT TO THE PROTECTION OF COPYRIGHT LAWS AND OTHER LEGAL RIGHTS WORLDWIDE. THEIR USE, REPRODUCTION, AND TRANSMITTAL TO THIRD PARTIES WITHOUT EXPRESS WRITTEN PERMISSION MAY RESULT IN LEGAL PROCEEDINGS.

The furnishing of this manual to any party does not give that party or any third party any license to these patents, trademarks, copyrights, or other intellectual property rights, except as expressly provided in any written agreement of ROSSLARE.

ROSSLARE reserves the right to revise and change this document at any time, without being obliged to announce such revisions or changes beforehand or after the fact.

Notice and Disclaimer

This manual's sole purpose is to assist installers and/or users in the safe and efficient installation and usage of the system and/or product, and/or software described herein.



Before attempting to install and/or use the system, the installer and the user must read this manual and become familiar with all safety requirements and operating procedures.

- The system must not be used for purposes other than those for which it was designed.
- The use of the software associated with the system and/or product, if applicable, is subject to the terms of the license provided as part of the purchase documents.
- This manual describes the maximum configuration of the system with the maximum number of functions, including future options. Therefore, not all functions described in this manual may be available in the specific system and/or product configuration you purchased.
- Incorrect operation or installation, or failure of the user to effectively maintain the system, relieves the manufacturer (and seller) from all or any responsibility for consequent noncompliance, damage, or injury.
- The text, images and graphics contained in the manual are for the purpose of illustration and reference only.
- All data contained herein subject to change without prior notice.
- In no event shall manufacturer be liable for any special, direct, indirect, incidental, consequential, exemplary, or punitive damages (including, without limitation, any and all damages from business interruption, loss of profits or revenue, cost of capital or loss of use of any property or capital or injury).
- All graphics in this manual are for reference only, some deviation between the image(s) and the actual product may occur.
- All wiring diagrams are intended for reference only, the photograph of the PCB(s) are intended for clearer illustration and understanding of the product and may differ from the actual PCB(s).

Contents

1. Overview **8**
2. Scope **8**
3. Specifications and Requirements **9**
3.1. AxTraxPro Server and Client 9
3.2. System Capabilities 10
3.3. System Requirements 12
3.3.1. AxTraxPro Server and Client Requirements 12
3.3.2. Microsoft Framework 12
4. Installation **12**
4.1. Downloading the AxTraxPro Installation File 12
4.2. Beginning the Installation 13
4.3. Installing AxTraxPro Client 17
4.4. Installing AxTraxPro Web Server 19
4.5. AxTraxPro Configuration Tool 21
4.6. Installing AxTraxPro Server Software 23
4.7. SQL Server Setup 24
4.7.1. Default Setup 24
4.7.2. Custom Setup 27
4.8. Firewall Settings 30
4.9. SQL Server Settings 30
5. Starting AxTraxPro **30**
5.1. Configuring the AxTraxPro host 30
5.2. Configuring the AxTraxPro client 31
5.3. Configuring the AxTraxPro web server 32
5.4. Starting AxTraxPro 36
6. Getting to Know the Interface **38**
7. Defining Time Frames **39**
7.1. Adding Time Zones 39
7.2. Adding Holidays 41
8. Configuring a Site **42**
8.1. Adding a Network for AC-215x, AC-225x, and AC-425x Panels 43
8.2. Adding an Access Control Panel to an Existing Network 47
8.3. Searching for Existing Access Control Panels 47
8.4. Adding a Network for an AC-825IP Panel 49
8.5. Configuring a Panel 50
8.6. Configuring an AC-825IP Panel 55
8.6.1. OSDP-SC Tab 60

8.6.2. Inventory Tab 65
8.6.3. Interlock Groups 65
8.7. Adding an Expansion Board 66
8.7.1. AC-225x and AC-425x 66
8.7.2. AC-825IP 68
8.8. Deleting a Panel 69
8.9. Configuring a Reader 69
8.9.1. General Tab 69
8.9.2. Options Tab 73
8.9.3. Access Event 74
8.9.4. OSDP-SC Tab 74
8.10. Adding a Biometric Terminal 75
8.10.1. On a Local Network 76
8.10.2. From a Remote Network 77
8.10.3. Configuring a Biometric Terminal 79
8.10.4. Mapping a Biometric Terminal to a Reader 81
8.10.5. Terminal Firmware Update 82
8.11. Configuring the Doors 82
8.12. Adding Panel Links 85
8.12.1. Global Triggering of Output Groups 90
8.13. Configuring the Inputs 91
8.14. Controlling Outputs Manually 92
9. Managing Groups 94
9.1. Adding Access Groups 94
9.2. Adding Access Areas 95
9.3. Adding Output Groups 97
9.4. Adding Input Groups 98
9.5. Adding Global Antipassback Rules 100
9.6. Managing Lockdowns 102
9.6.1. Adding Lockdown Groups 102
9.6.2. Using Lockdown Groups 112
9.7. Defining Card + Card Groups 120
9.7.1. Adding a Card + Card Group 120
9.7.2. Adding Users to a Card + Card Group 121
9.8. Vehicle Access Groups 121
9.9. Adding Car Parking 121
10. Managing Users 125
10.1. Adding Departments 125
10.2. Adding a Batch of Users and Cards 125
10.3. Viewing Users 128
10.4. Adding an Individual User 129
10.4.1. General 130

10.4.2. Credentials Tab 135
10.4.3. Details Tab 137
10.5. Managing Cards 138
10.5.1. Associating a User to a Card 142
10.5.2. Card Design (Photo ID) 145
10.5.3. Setting Card Automation 154
10.6. Adding Vehicle Types 155
10.7. Using the User Filter to Search for Users 157
11. Adding Operators 159
12. Managing Visitors 161
13. Integrating Video Systems 163
14. Configuring Access Levels 164
15. Creating Status Maps 168
15.1. Manually Opening a Door from Status Map 172
16. Viewing Events 173
17. Viewing Reports 174
17.1. Generating a Report 175
17.2. Scheduling a Report 176
17.3. Previewing a Report 178
18. Viewing the Guard Screen 180
19. Updating Firmware 180
19.1. AC-215x, AC-225x, and AC-425x Panels 180
19.2. AC-825IP Panel 182
Appendix A. Administrator Operations 186
A.1 Setting the Time and Date 186
A.2 Testing User Counters 186
A.3 Maintaining the Database 188
A.4 AxTraxPro Options and Preferences 190
A.4.1 General Tab 190
A.4.2 User Custom Fields 192
A.4.3 Custom Operations 193
A.4.4 Email Notifications 194
A.4.5 Company Details 195
A.5 Importing/Exporting User Data 196
A.6 Notification Settings 198
A.7 Conversion Tables 199
Appendix B. Configuring a Network 202
B.1 TCP/IP Connection 202
Appendix C. Configuring User Counters 204
C.1 Resetting Counter on Panel Re-enable 204
Appendix D. Controlling the Door Manually 206

Appendix E. Enrolling a Face from a Terminal **208**
Appendix F. Enrolling a License Plate **210**
Appendix G. Enrolling a User's Fingerprint **211**
Appendix H. Help Menu **214**
H.1 About 214
H.2 User Manual 214
H.3 AxTraxPro Product Activation 215
19.2.1. General Information about AxTraxPro and the License Agreement 215
19.2.2. Activating AxTraxPro Desktop Client 218
H.4 Feedback 220
Appendix I. Opening a Program in Windows' Firewall **221**
Appendix J. WAN Connection Troubleshooting **224**
J.1 Server is Down or Wrong IP and Port Configuration 225
J.2 Server is Down or Network Failure between AxTraxPro Client and AxTraxPro Server 226
J.3 IP + Port Setting are Fine but Client Does Not Start 226

1. Overview

The Rosslare Enterprises Ltd. AxTraxPro Desktop Client software is a web-based software management system for use with Rosslare Enterprises Ltd. access control panels. The AxTraxPro access control system is user-friendly, intuitive, and rich in functionality. Using AxTraxPro, you can configure door functionality based on areas and time frames for different types of personnel and for varying alarm situations. This manual is compatible with AxTraxPro software Version V28.0.1.7.

User Types

In the AxTraxPro Desktop Client software the users are divided into four categories. Each category has a different type of access to the system.

An administrator has full system access by default. An operator can view and/or modify only the specified system components that they are given. Operators may also be given antipassback, interlock, or lockdown immunity.



Only a specified operator can administer and control a lockdown.

Users and visitors are only given access to specified access areas. But they may also be given antipassback and interlock immunity.

2. Scope

This document contains the procedures to use the Rosslare Enterprises Ltd. AxTraxPro Desktop Client software. The document includes the following for normal setup and operation and optional functions and additional setup procedures in the appendices:

Normal Setup and Operation Procedures

- A list of the system requirements for the AxTraxProDesktop Client, see System Requirements.
- Gives the procedure to install the AxTraxProDesktop Client, see Installation.
- Shows the structure of the AxTraxProDesktop Client software, see Getting to Know the Interface.
- Gives the procedure to define time frames, see Defining Time Frames.
- Gives the procedure to configure a site, see Configuring a Site.
- Gives the procedures to add groups, Managing Groups.

- Gives the procedure to add operators, see Adding Operators.
- Gives the procedure to add users, see Managing Users.
- Gives the procedure to add visitors, see Managing Visitors.
- Gives the procedure to integrate video systems, see Integrating Video Systems.
- Gives the procedure on how to view access levels, see Configuring Access Levels.
- Gives the procedure to create status maps, see Creating Status Maps.
- Gives the procedure on how to view reports, see Viewing Reports.
- Gives the procedure on how to see the guard screen, see Viewing the Guard Screen.

Optional Functions and Additional Setup Procedures

- Lists administrator operations, see Administrator Operations.
- Gives the procedure to configure a network, see Configuring a Network.
- Gives the procedure to configure user counters, see Configuring User Counters.
- Gives the procedure to control a door manually, see Controlling the Door Manually.
- Gives the procedure to enrolling a face, see Enrolling a Face from a Terminal.
- Gives the procedure to enroll a license plate, see Enrolling a License Plate.
- Gives the procedure to enroll a fingerprint, see Enrolling a User's Fingerprint.
- To see the Help menu options, see Help Menu.
- Gives the procedure to open a program in Windows firewall, see Opening a Program in Windows' Firewall.
- Gives the procedure to troubleshoot a WAN connection problem, see WAN Connection Troubleshooting.

3. Specifications and Requirements

3.1. AxTraxPro Server and Client

The AxTraxPro system includes both the AxTraxPro Server and the AxTraxPro Client software applications separately.

Install the AxTraxPro Server on the computer that controls the access control panels and manages the database.

The computer should be a dedicated PC for the AxTraxPro server with no SQL entity or any non-Windows service existing or installed on the PC.

It is highly recommended that the AxTraxPro Server will be online 24 hours per day.

Install the AxTraxPro client software on any PC from which you wish to access the system. One AxTraxPro server can serve an unlimited number of AxTraxPro clients.

AxTraxPro is based on a standard Client-Server architecture:

- Only the server connects to the database; the clients gather the information from the server
- Panels are connected to the server using a serial (RS-485) or LAN/WAN communication
- The server runs as a Windows service by default

3.2. System Capabilities

General	
Software Architecture	Client-Server
Database Type	SQL Server Express 2019
Max. Number of Credentials	• 30,000 per panel (AC-215IP, AC-215B, AC-225, AC-425) • 5000 (AC-215) • 100,000 (AC-825IP)
Max. Access Groups	Based on the maximum number of users, 30,000 x the number of panels
Max. Number of Time Zones	128 (256 with AC-825IP)
Max. Credentials per User	16
Max. Access Control Panels and Expansions	1023
Antipassback	• Timed • Door • Global – across the entire facility
International Holiday Support	Up to 64 holidays

Networks	
Max. Number of Networks	Up to 1023 (depending on network topology)
Supported Access Control Panel Models	• AC-215B, AC-215IP-B • AC-225B, AC-225IP-B • AC-225B, AC-225IP-B with MD-IO84B • AC-225B, AC-225IP-B with MD-D02B • AC-425B, AC-425IP-B • AC-425B, AC-425IP-B with MD-IO84B • AC-425B, AC-425IP-B with MD-D04B • AC-825IP R805, S-805, D-805, P-805 • Legacy: AC-215, AC-215 (SPV), AC-215IP • Legacy: AC-225, AC-225IP • Legacy: AC-225, AC-225IP • Legacy: AC-225, AC-225IP with MD-IO84 • Legacy: AC-225, AC-225IP with MD-D02 • Legacy: AC-425, AC-425IP • Legacy: AC-425, AC-425IP with MD-IO84 • Legacy: AC-425, AC-425IP with MD-D04
Panel Networks Communication Interface	• Serial (RS-232/485) • TCP-IP AC-825IP has TCP/IP only
Communication Speed	9600, 19200, 57600, and 115200 bps

3.3. System Requirements

3.3.1. AxTraxPro Server and Client Requirements

Operating System	Windows 8.1, 64-bit Windows 10
CPU	Minimum: Intel core i5, 2.4 GHz or faster processor Recommended: Intel core i7, 4 cores or more, 2.4 GHz or faster processor
Memory	Minimum: 8 GB RAM Recommended: 16 GB RAM
Network	LAN card required for TCP/IP networking
Hard Disk Space	Minimum 4 GB free space, SSD strongly recommended

3.3.2. Microsoft Framework

You must have Microsoft .NET Framework 4.0 or above installed on your PC.

4. Installation

The AxTraxPro installation setup file consists of the following four main components:

- AxTraxPro Client
- SQL Server
- AxTraxPro Server



The AxTraxPro Client is only needed on the main computer; however, it can be installed on additional computers.

- (Optional) ViTrax software – Enables video integration

4.1. Downloading the AxTraxPro Installation File

Install the AxTraxPro access control software on the computer that connects to the access control panels and manages the database.

To download the AxTraxPro installation file:

1. Go to http://www.rosslaresecurity.com.
2. Log in to your account.
3. Click **Download Center** in the Quick Links section.
4. In **Product**, select the latest Access Control Management Software version.
5. In **Document Types**, select Software and click **Search**.

   In the search results, you'll see **AxTraxPro software**.
6. Click the Download icon on the right.

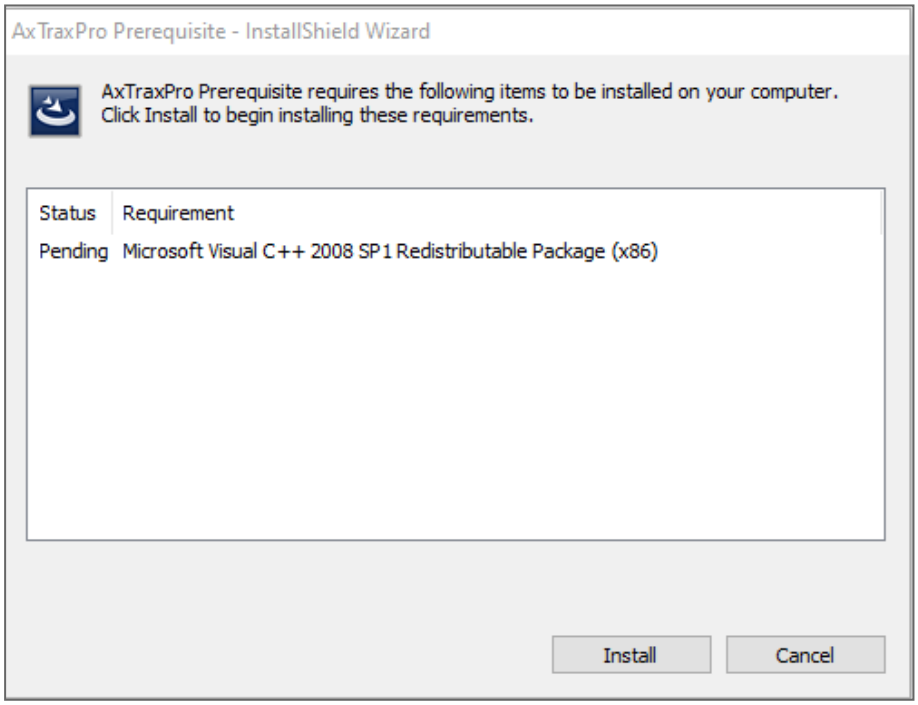
   The installation file is downloaded to your computer.

4.2. Beginning the Installation

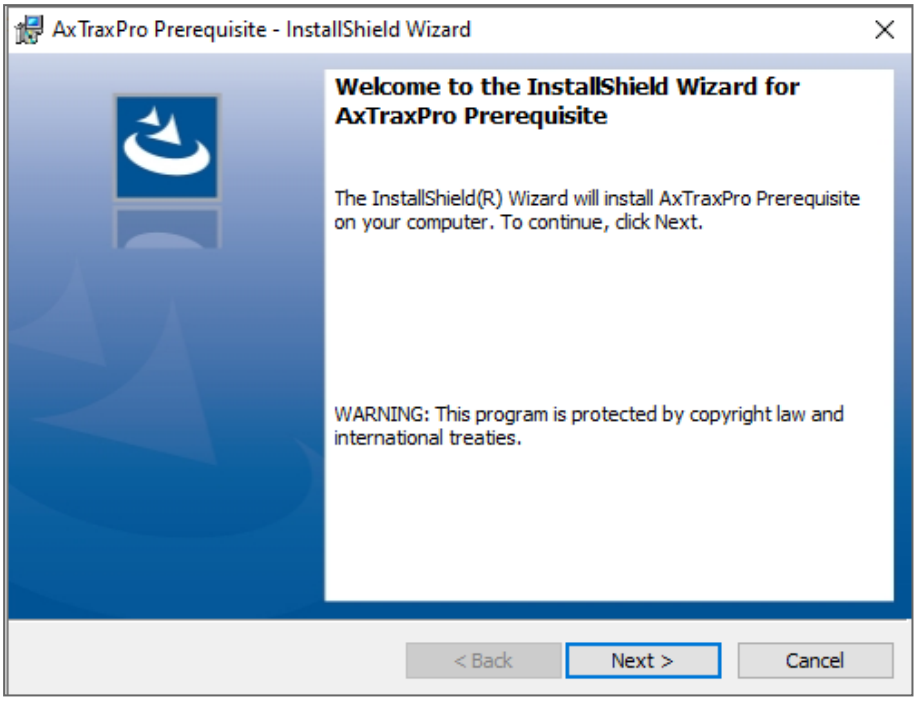
Once you have downloaded the installation file, you can begin the installation.

To begin the installation:

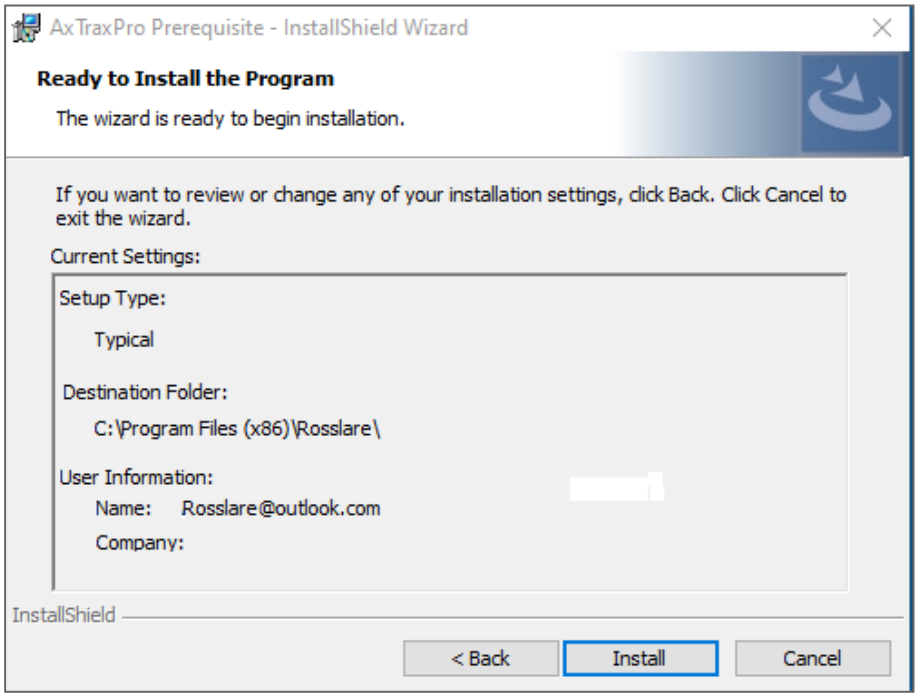
1. Browse to the downloaded file and double-click it.
2. Click **Install** after the necessary files are extracted.



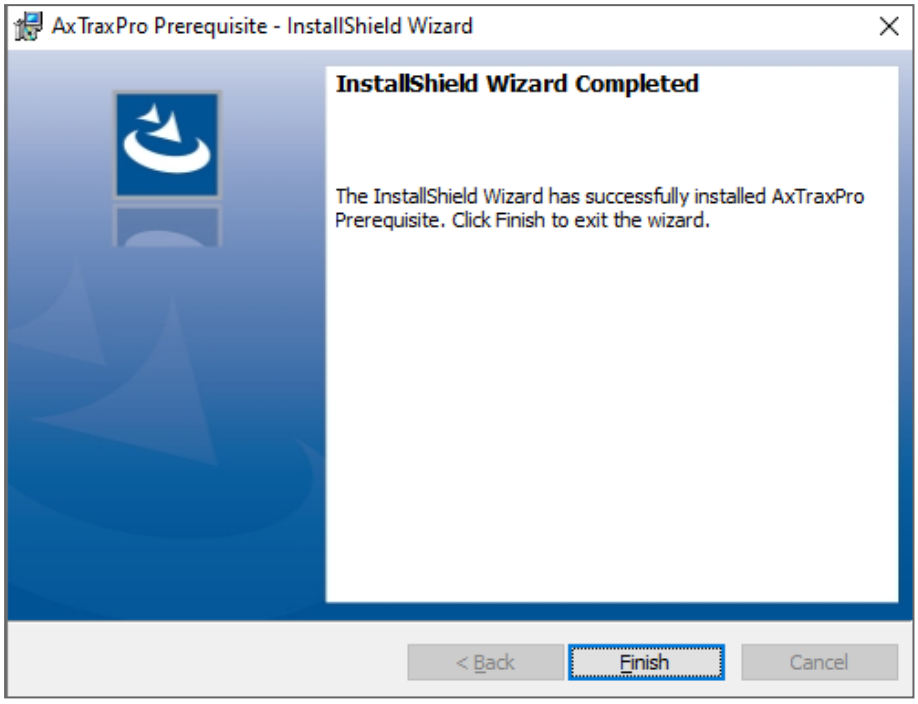
3. Click **Next**



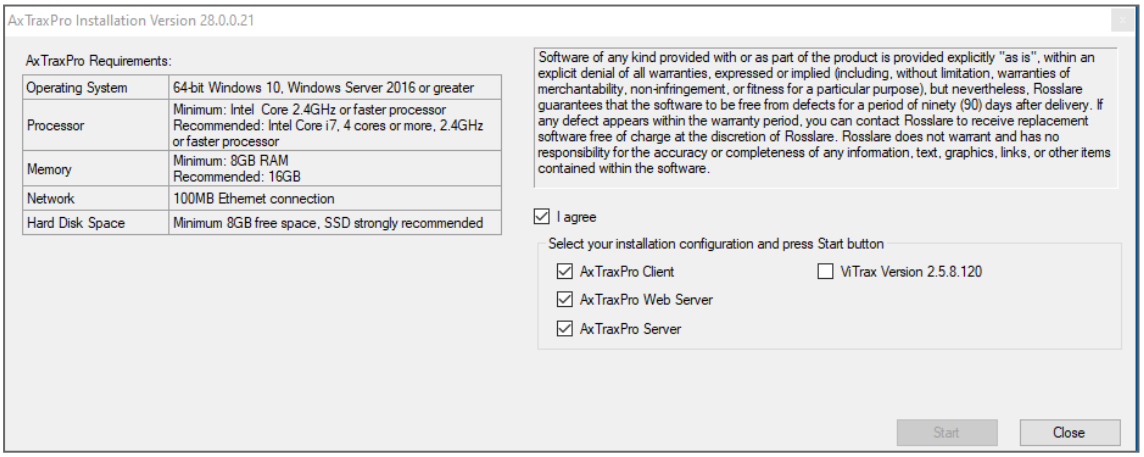
4. Click **Install**.



5. Click **Finish**.



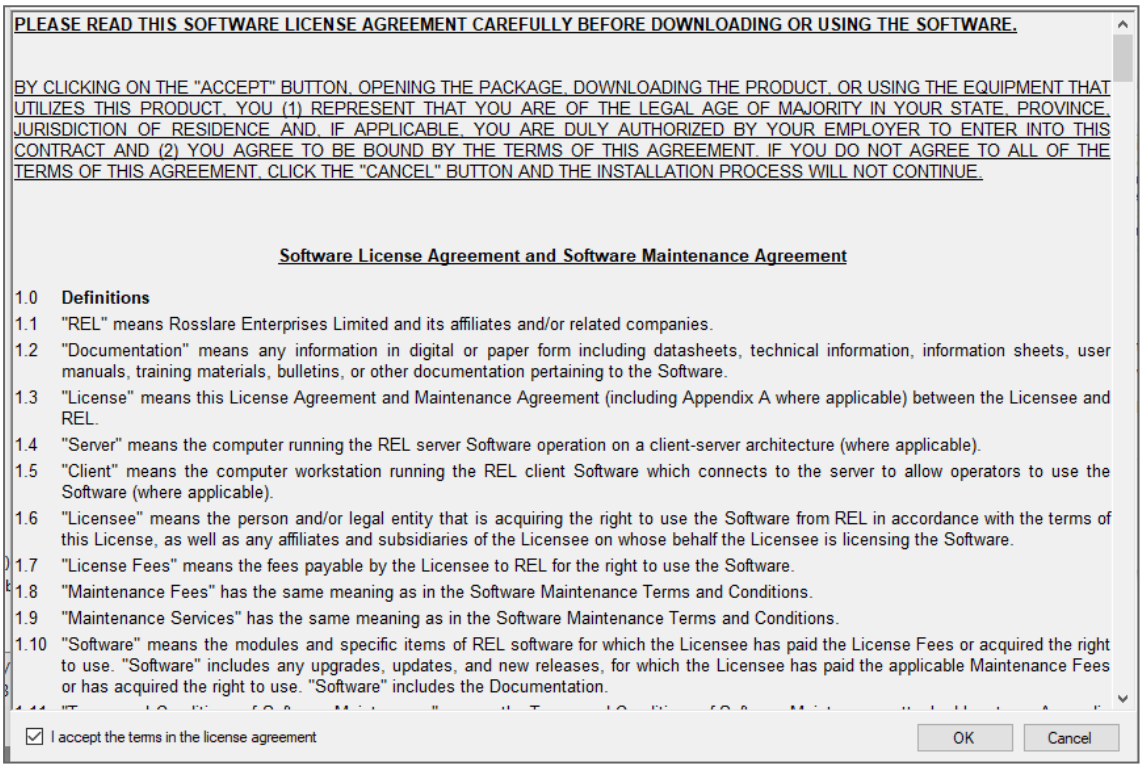
6. Select the **I agree** check box and select which packages to install.



7. Click **Start**.

> This screen remains open in the background as various elements of the software are installed.

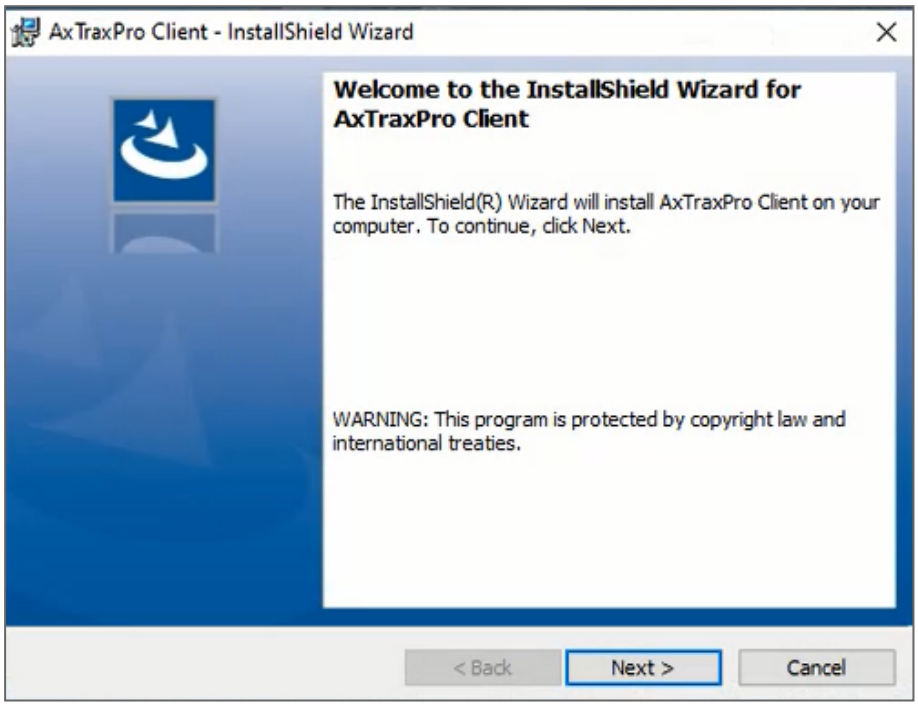
8. Select **I accept the terms in the licensing agreement** and click **OK**.



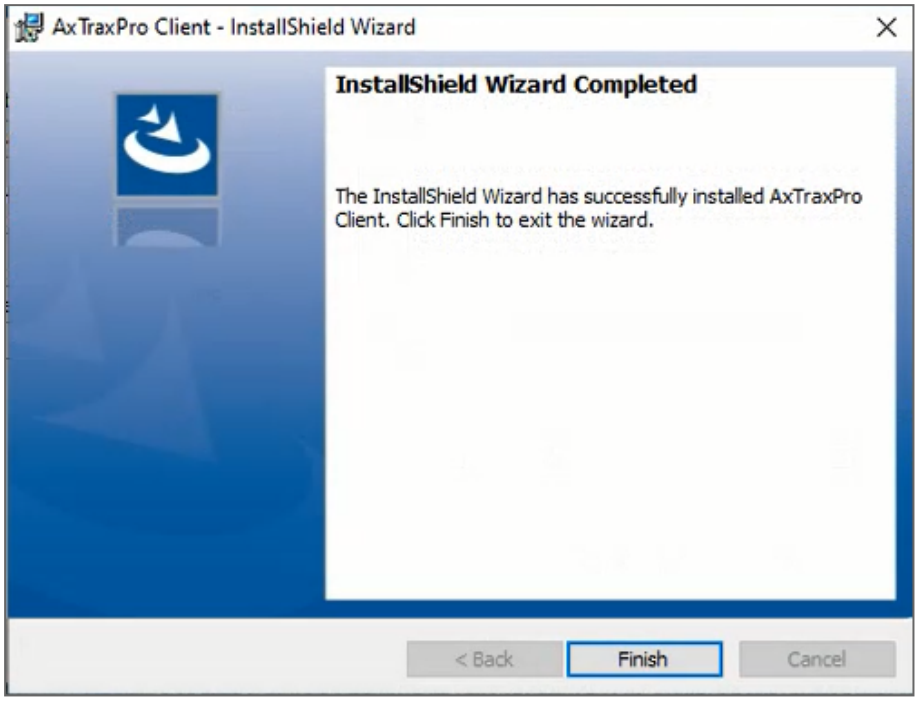
4.3. Installing AxTraxPro Client

To install the AxTraxPro Client application:

1. Click **Next** to begin the AxTraxPro Client installation process.



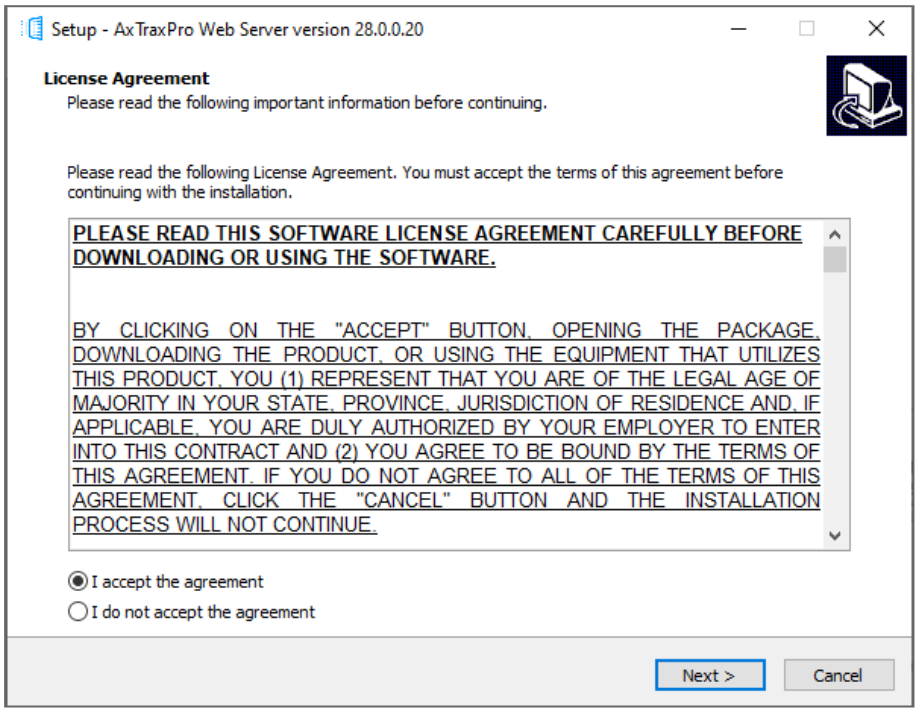
2. Click **Finish** to complete installing the AxTraxPro Client.



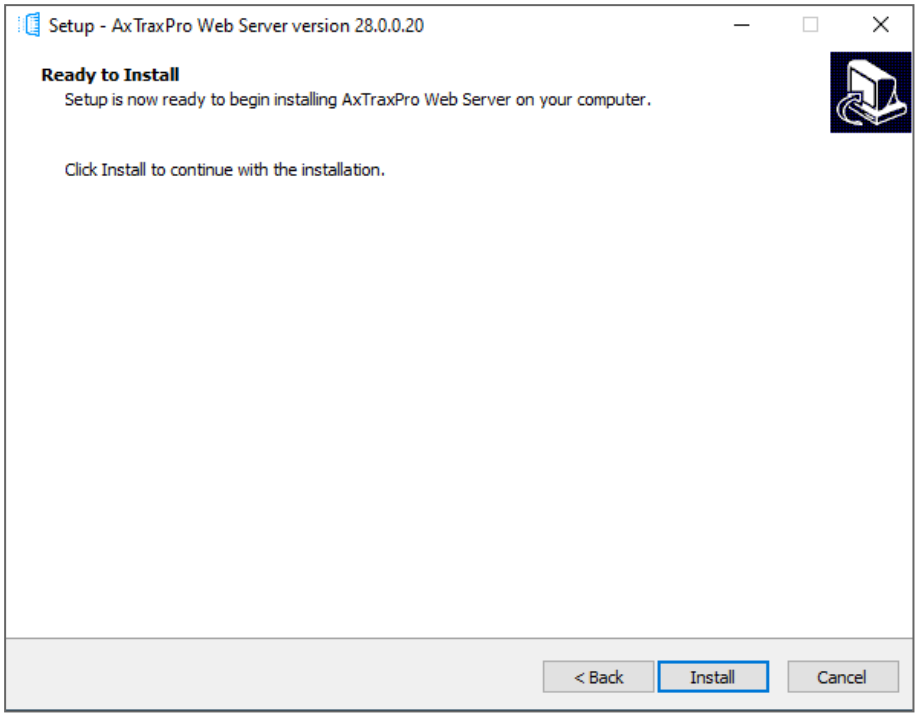
4.4. Installing AxTraxPro Web Server

To install the AxTraxPro Web Server:

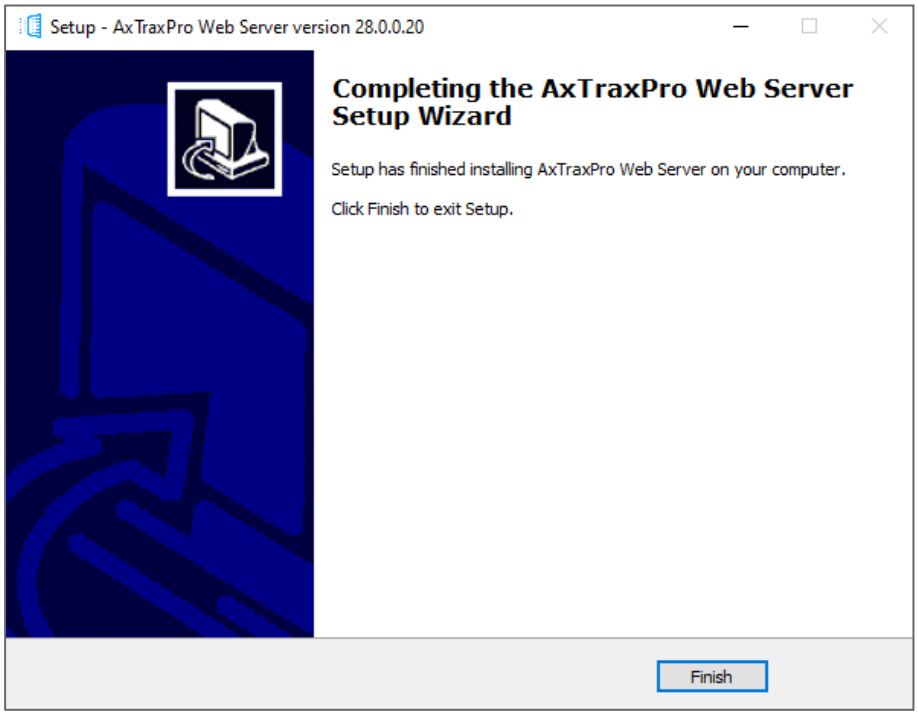
1. Select **I accept the terms in the licensing agreement** and click **Next**.



2. Click **Install**.



3. Click **Finish**.

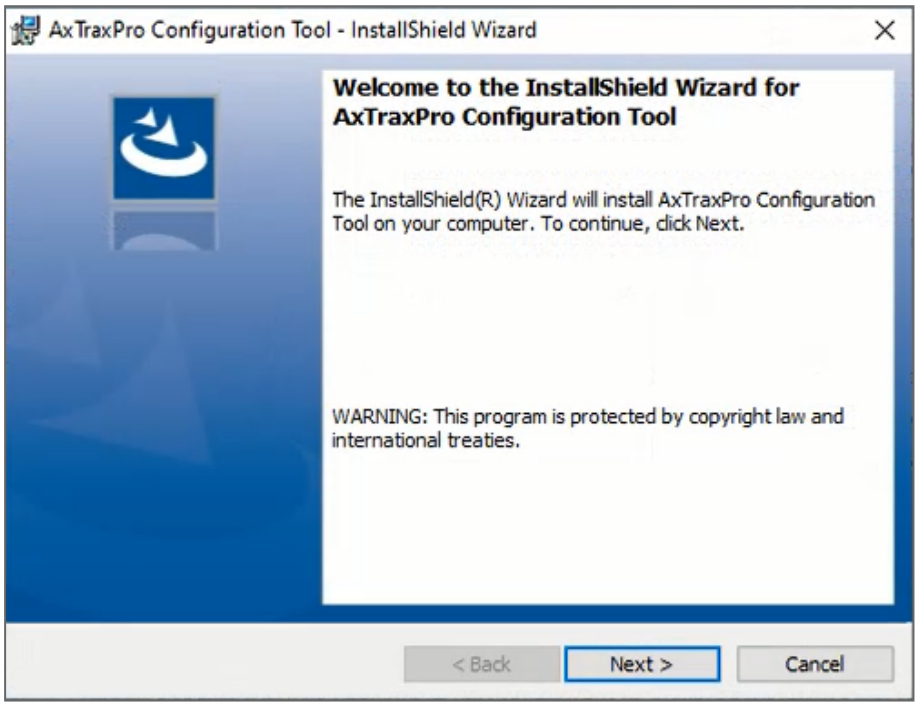


4.5. AxTraxPro Configuration Tool

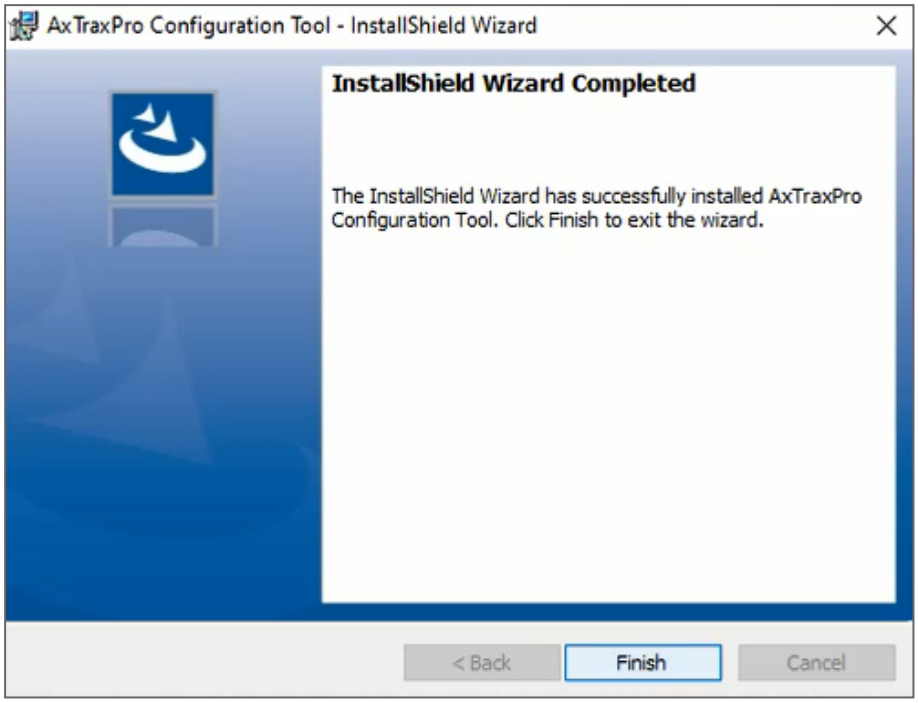
Following the AxTraxPro Client installation, a window opens to install the AxTraxPro Configuration Tool.

To install the AxTraxPro configuration tool:

1. Click **Next** to begin the AxTraxPro Configuration Tool installation process.



2. Click **Finish** to complete installing the AxTraxPro Configuration Tool.

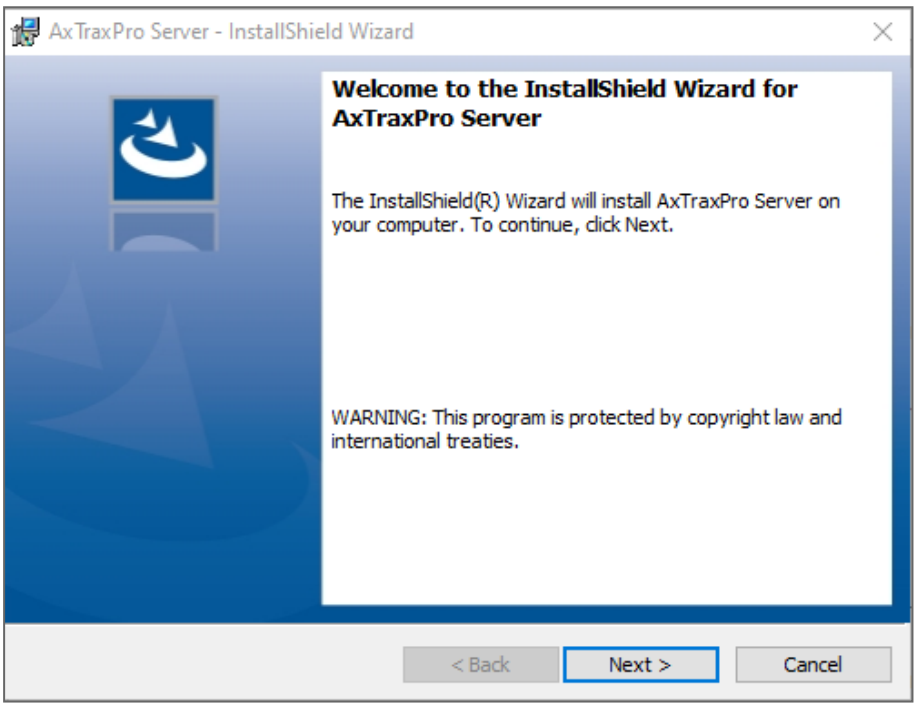


4.6. Installing AxTraxPro Server Software

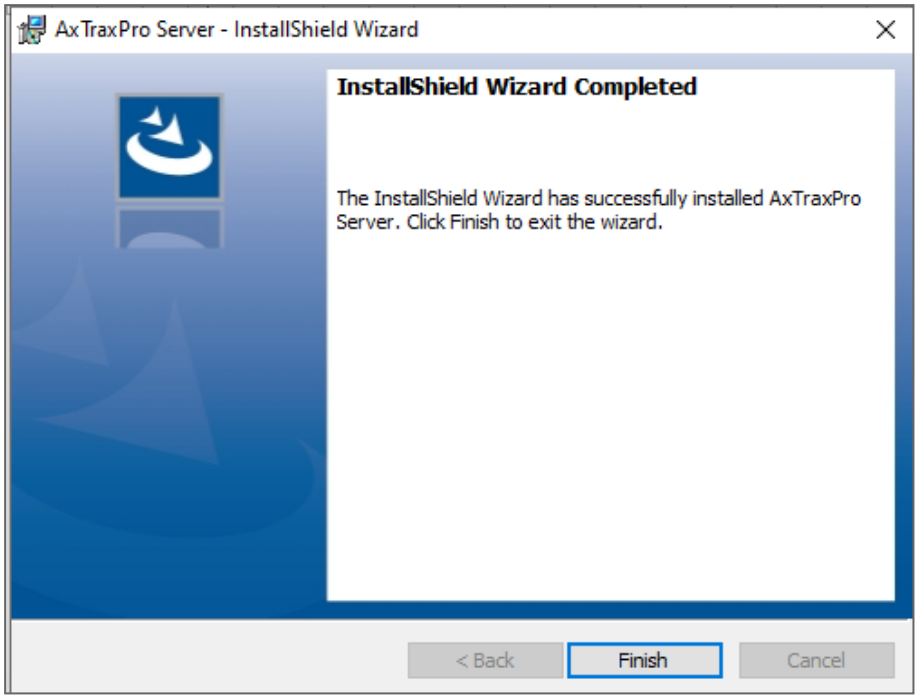
Following the AxTraxPro configuration tool installation, the AxTraxPro Install Shield Wizard for the AxTraxPro Server software installation appears.

To install the AxTraxPro Server:

1. Click **Next**.



2. Click **Finish** to complete installing the AxTraxPro Server installation.



4.7. SQL Server Setup

Following the AxTraxPro Configuration Tool installation, a window opens to install the SQL Server.

The AxTraxPro Server operates using an SQL server 2019 database. There are three options to install the SQL server:

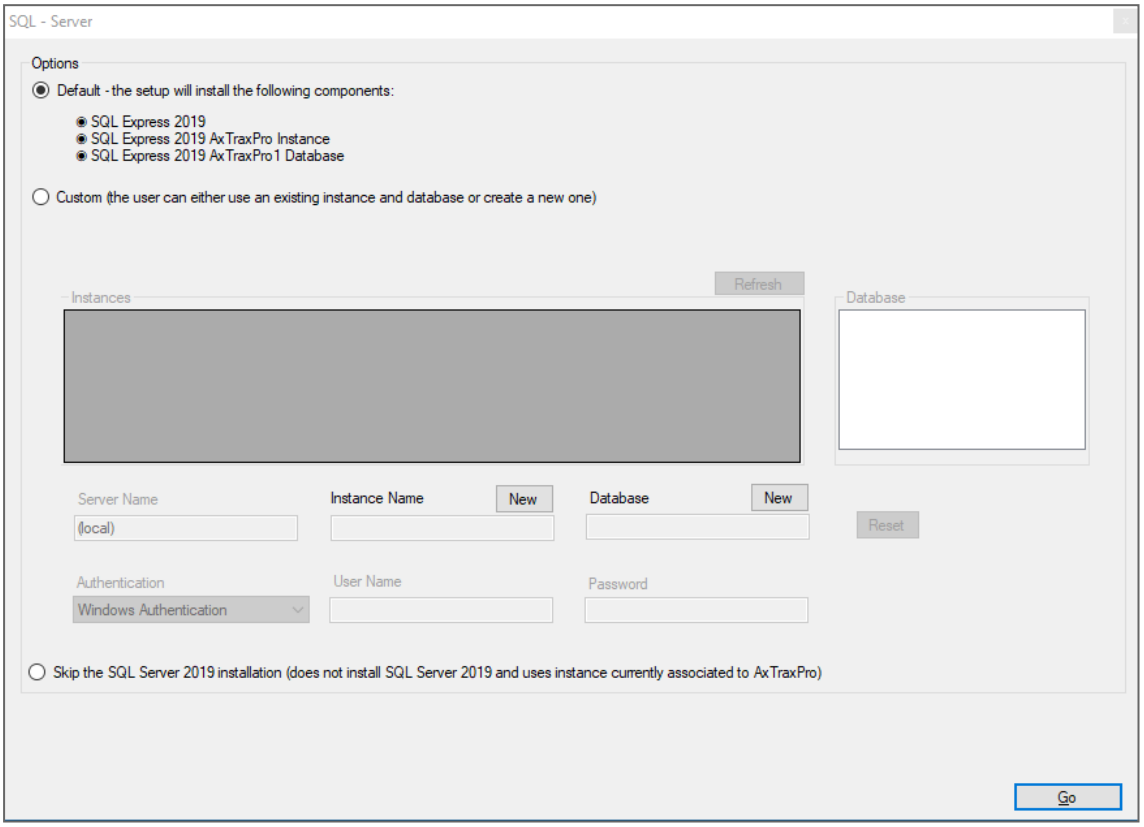
1. Select **Default** to install Microsoft SQL Server Express 2019.
2. Select **Custom** to use an existing instance of the SQL 2019 server available on your computer network with your SQL login credentials.
3. Select **Skip** to use the current AxTraxPro SQL Server instance.

4.7.1. Default Setup

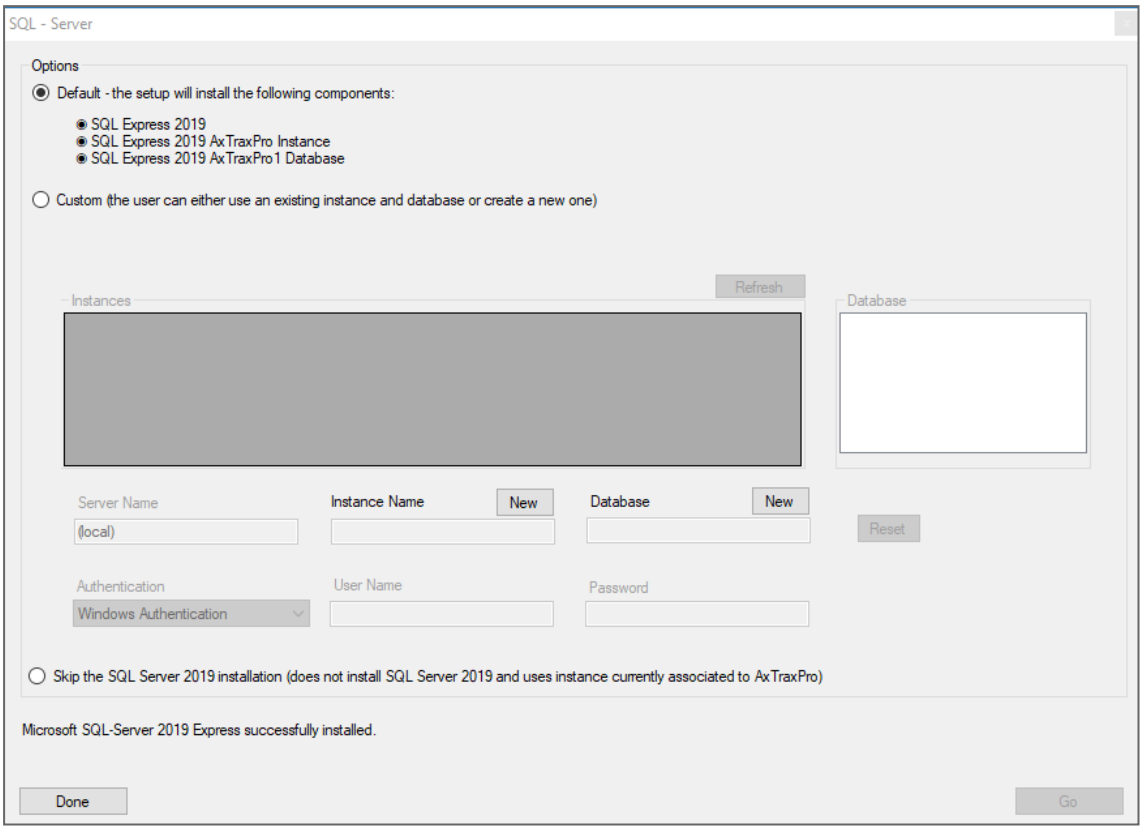
Do not install the SQL server when installing additional AxTraxPro clients that connect to the AxTraxPro Server database.

To install the default SQL Server application:

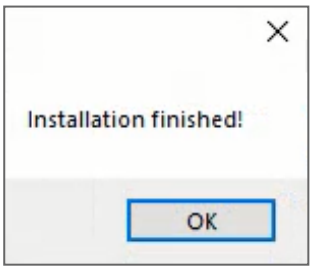
1. Select **Default** and click **Go**.



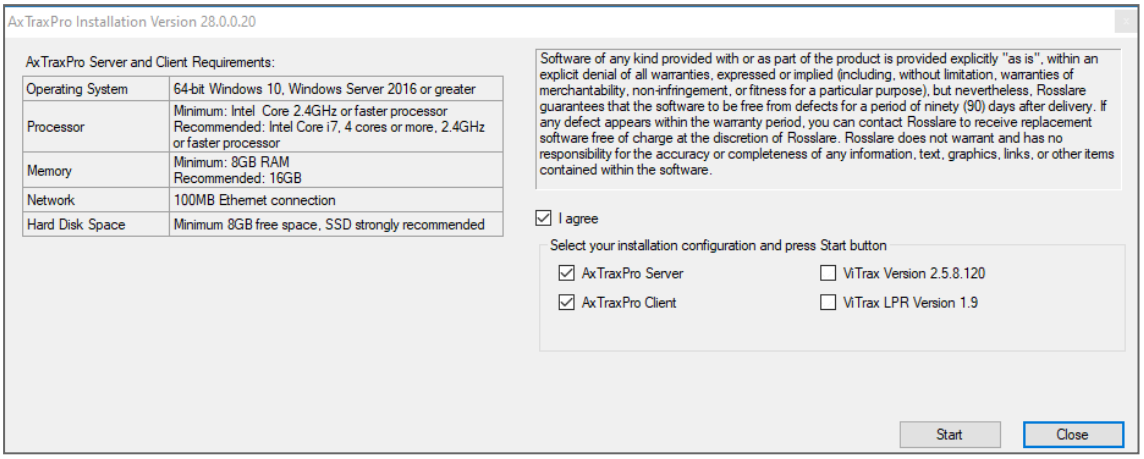
2. A confirmation sentence appears on the lower part of the screen when the process finishes. Click **Done**.



3. Click **OK**.



4. Click **Close**.



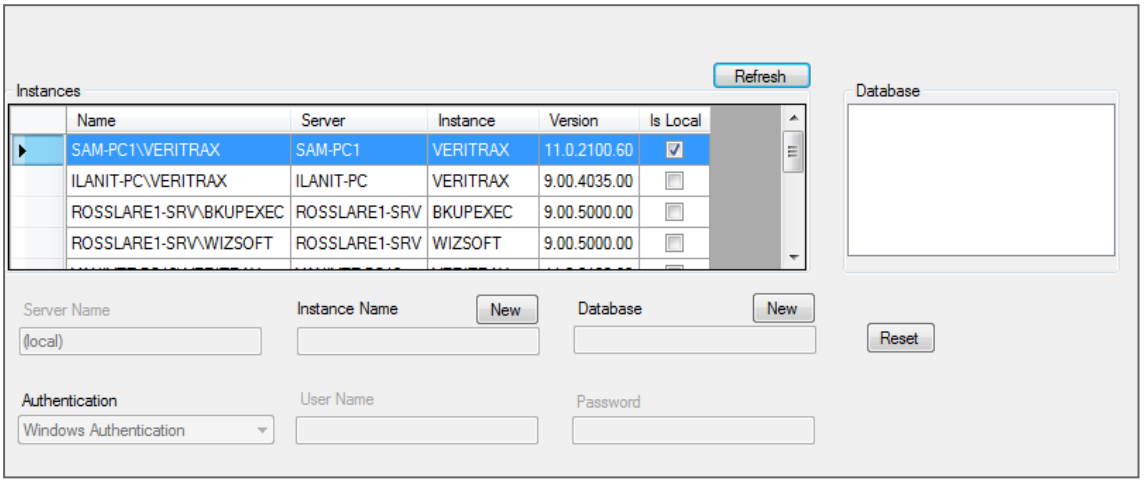
4.7.2. Custom Setup

Select **Custom** to use an existing instance of the SQL 2019 server available on your computer network with your SQL login credentials.

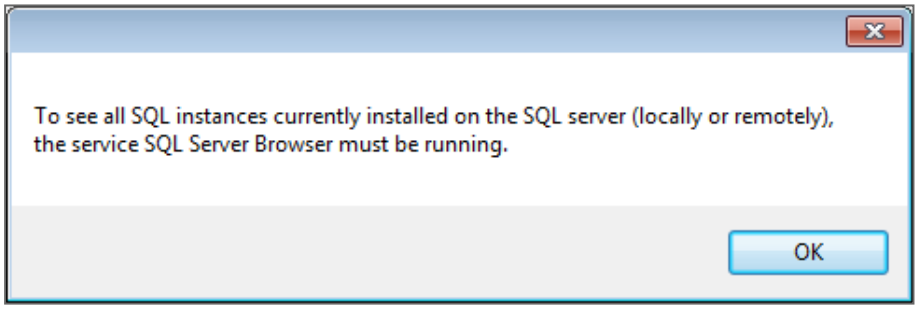
To install an existing instance of the SQL Server application:

1. Select **Custom**.

   A list of existing SQL instances is in the table.



   If you do not see the table, you receive the following message instead:



   You need to enable the SQL Server Browser service and start it, and then click **Refresh**.

2. Select the instance from the table that you wish to use.
3. Enter all field information as needed.

   A setup wizard for the SQL Server 2019 Express opens.

The password must meet the Microsoft SQL Server Strong Password requirements:

- Does not contain all or part of the user's account name
- Is more than eight characters in length
- Contains characters from at least three of the following categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example: !, $, #, %)

- If installed SQL server instance has SQL Server Authentication, installing a new instance with Windows Authentication is impossible.
- When creating a new instance, be sure that the instance name is different than the existing instance name.
- The new instance is created with System Administrator rights (User 'SA'). To create an instance with limited rights, please ask your DB Administrator.

4. Click **Go**.

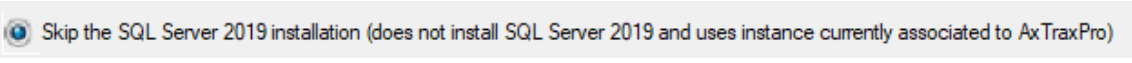
A setup wizard for the SQL Server 2019 Express opens.

4.7.2.1. Using Current SQL Server

Select Cancel to use the current SQL Server instance.

To use the current instance of the SQL Server application:

1. Select **Skip the SQL Server 2019 installation**.



2. Click **Go**.

The installation continues.

4.8. Firewall Settings

Internal firewall settings may prevent the AxTraxPro Server from connecting to the SQL database or to panel control units using TCP/IP and remote Server-Client connection.

Contact your system administrator or Rosslare Technical Support for further guidance.

4.9. SQL Server Settings

After installing AxTraxPro, verify that the SQL server service on the computer is running and set to the required installation.

For more information on SQL server settings, see Appendix Opening a Program in Windows' Firewall.



If SQL Express 2019 is being installed (part of the installation package), the installation must be on the same Windows user account that is being used for AxTraxPro.

5. Starting AxTraxPro

AxTraxPro is based on WCF technology. After AxTraxPro is installed on a host PC, the AxTraxPro client is run via a WAN (Internet) connection.

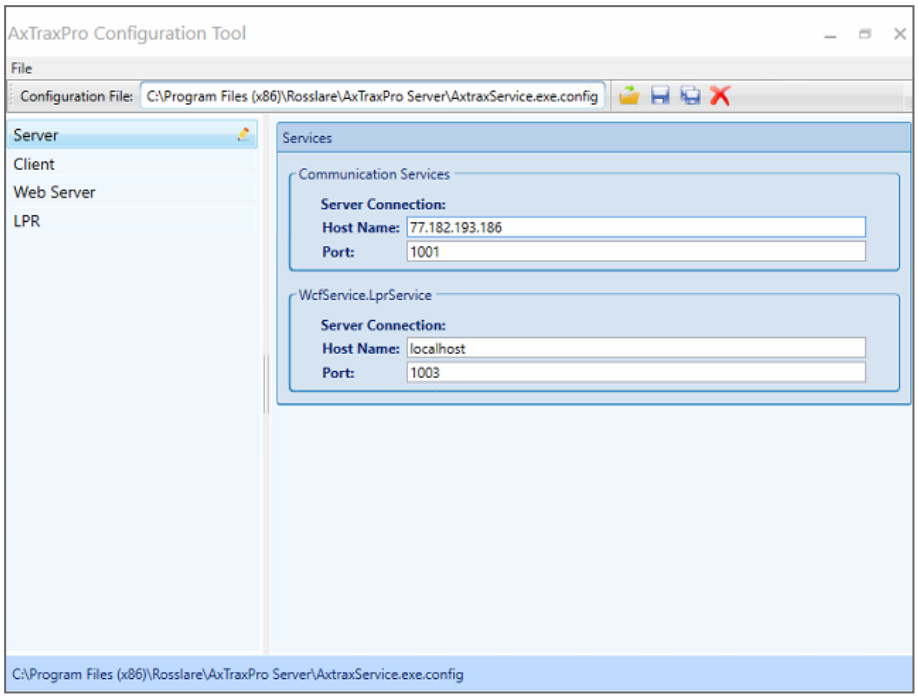
To run the AxTraxPro client you must define the server and client connections using the AxTraxPro Configuration Tool.

5.1. Configuring the AxTraxPro host

To set the Host Name for the AxTraxPro host PC:

1. On the AxTraxPro host PC, go to **C:\Program Files (x86)\Rosslare\AxTraxPro Configuration Tool**.
2. Run the **AxTraxConfigTool** as **Administrator**.
3. Select the **Server** tab.

4. In the **Host Name** field for the **Server Connection** in the **Communication Services** section enter the IP address of the host PC.



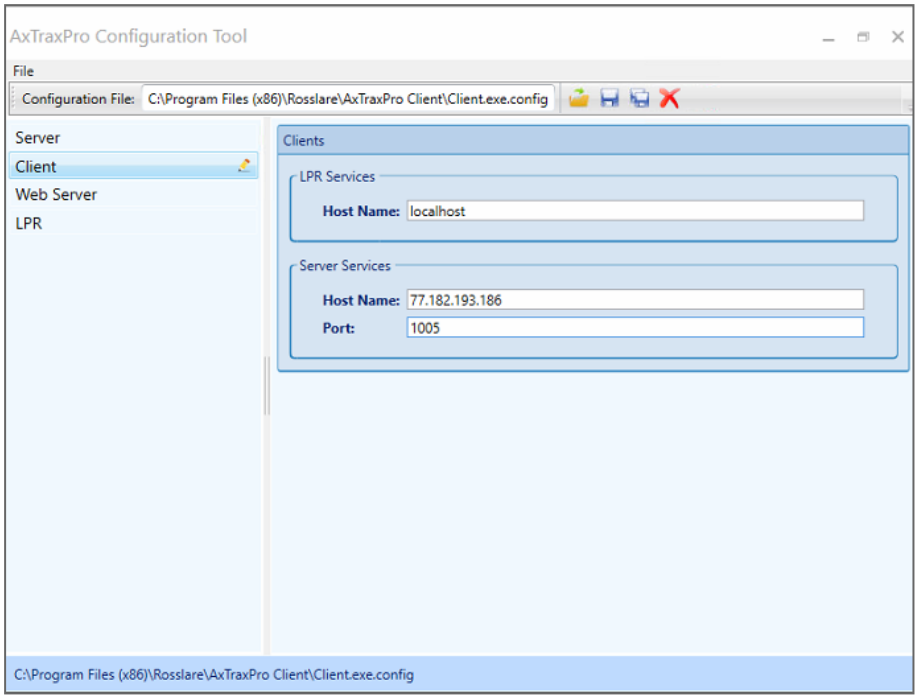
5. Click **Save**
6. Restart the AxTraxPro services.

5.2. Configuring the AxTraxPro client

To set the Host Name in the AxTraxPro PC client:

1. On the AxTraxPro client PC, go to **C:\Program Files (x86)\Rosslare\AxTraxPro Configuration Tool**.
2. Run the **AxTraxConfigTool** as **Administrator**.
3. Select the **Client** tab.

4. In the **Host Name** field for the **Server Services** enter the IP address of the host PC.



5. Enter a **Port** number.
6. Click **Save**.

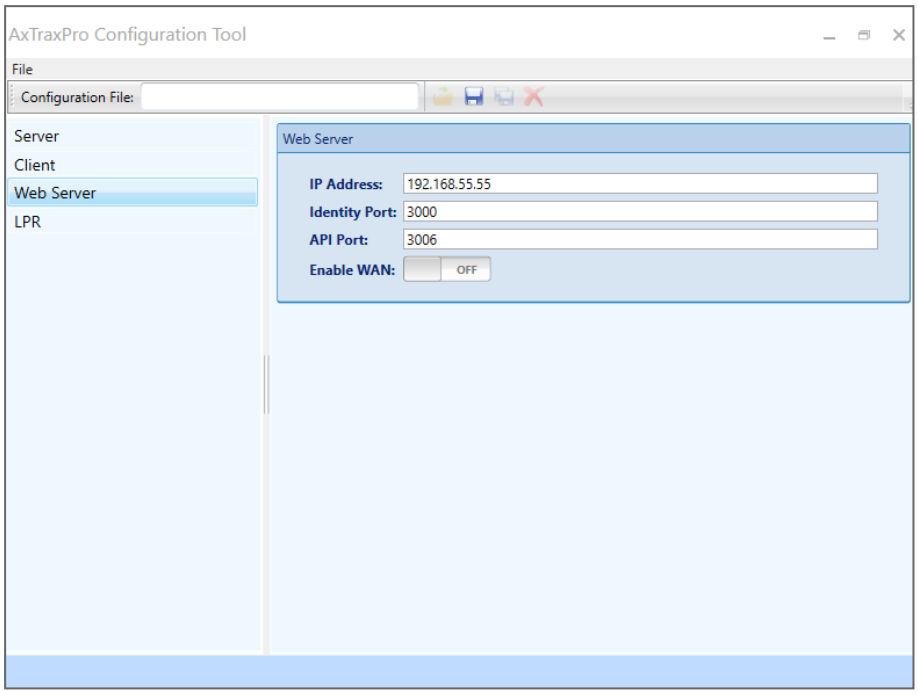
5.3. Configuring the AxTraxPro web server

The following procedure configures the AxTraxPro web server to support multiple connections.

To set the IP Address in the Web Server:

1. On the AxTraxPro client PC, go to **C:\Program Files (x86)\Rosslare\AxTraxPro Configuration Tool**.
2. Run the **AxTraxConfigTool** as **Administrator**.
3. Select the **Web Server** tab.

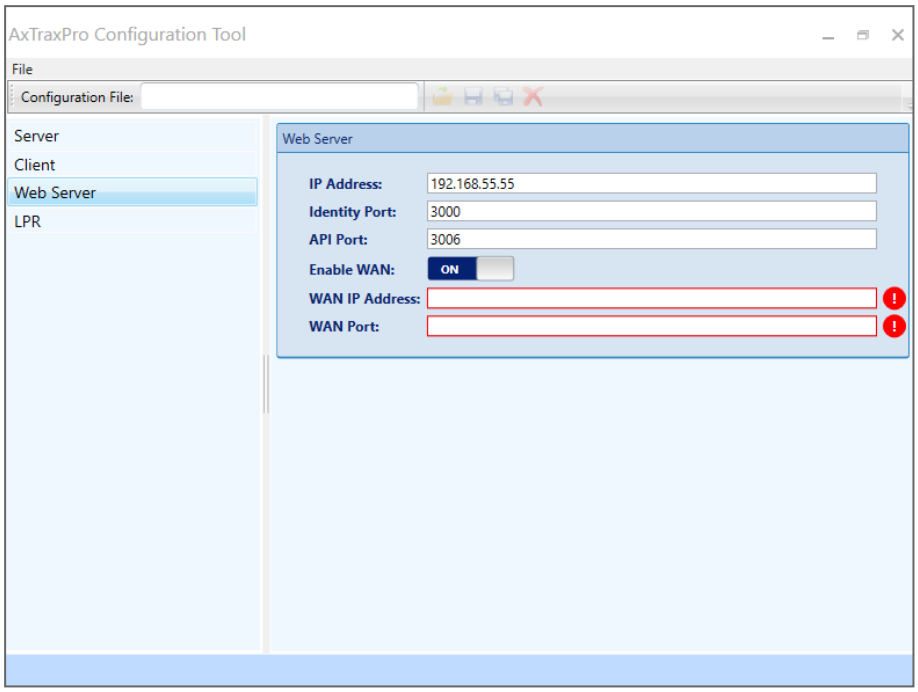
4. In the **IP Address** field enter the IP address of the host PC.



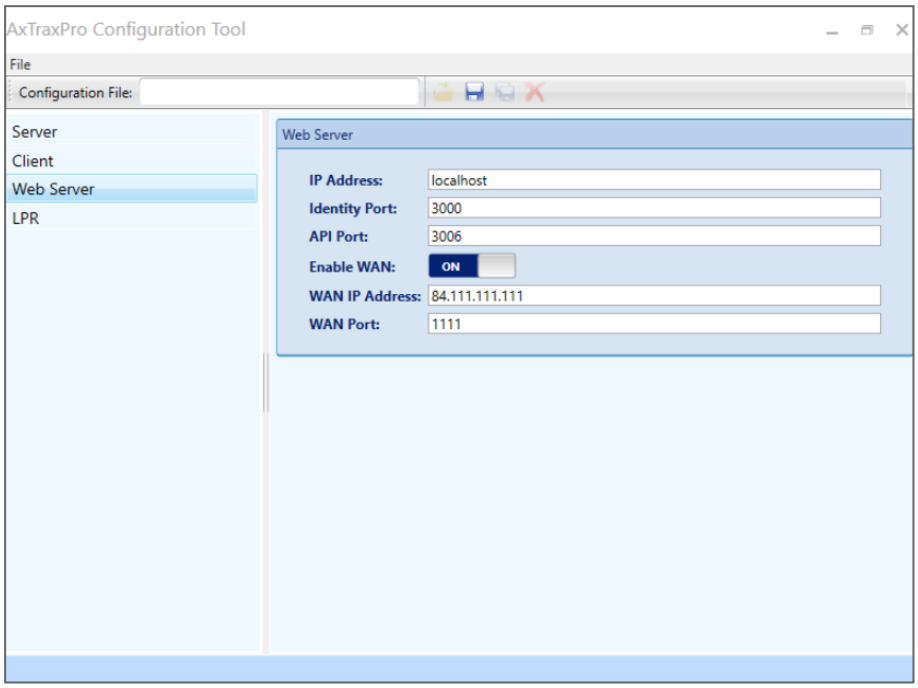
Make sure the **Identity Port** number is 3000.

Make sure the **API Port** number is 3006.

5. To use the web server in a wide area network (WAN), select the toggle.



6. Enter the following:
   a. **WAN IP Address** of the public router.
   b. **WAN Port** of the router.



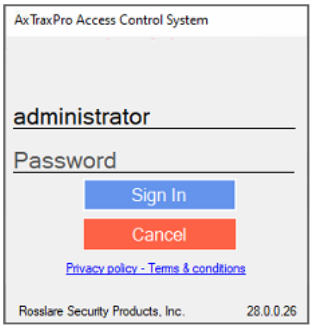
7. Click **Save**.

5.4. Starting AxTraxPro

This section explains how to start the AxTraxPro Access Control System and to **Sign In**.

To start the AxTraxPro:

1. Double-click the AxTraxPro Client icon ( ) on the desktop or select the program from the Rosslare Enterprises Ltd. folder in the Start menu.



2. Enter an **Operator name**.

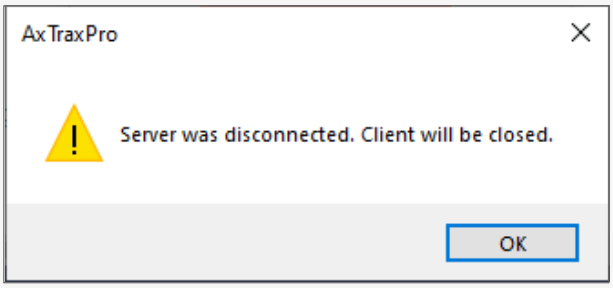
> The default **Operator name** is **administrator**.

3. Enter a **Password**.

> The default **Password** is **admin**.

4. Click **OK**.

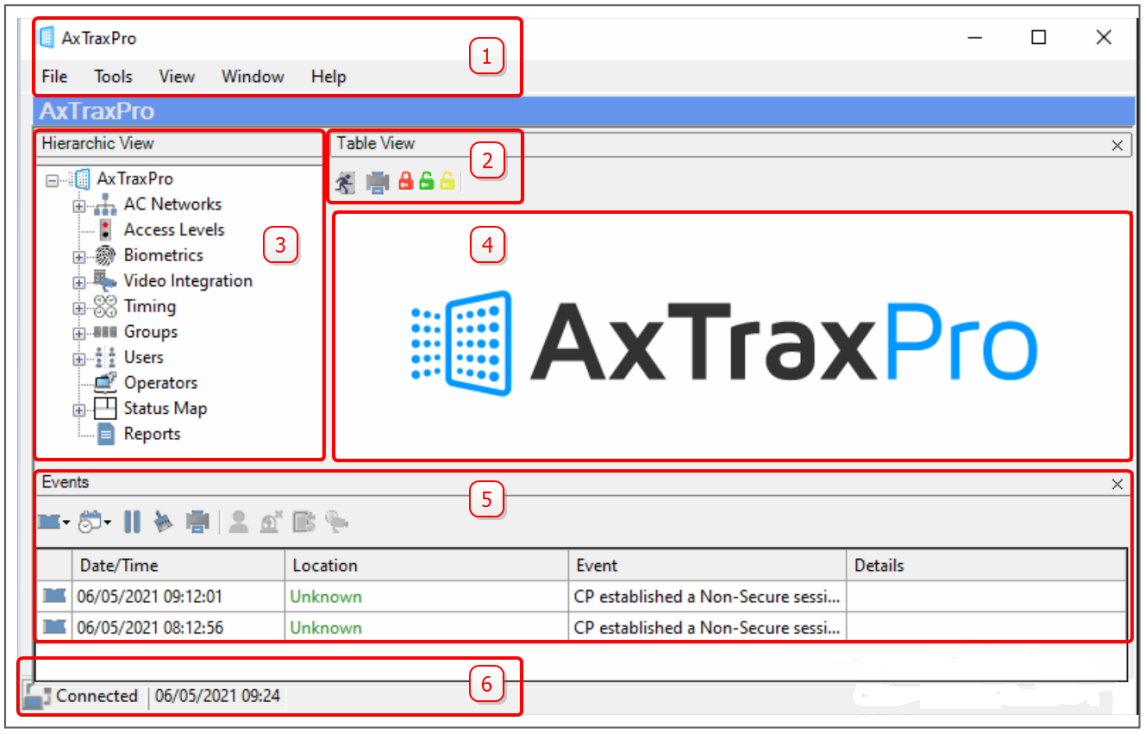
If the AxTraxPro server is disconnected, the following image is shown. To connect to the AxTraxPro server, see Configuring the AxTraxPro web server.



6. Getting to Know the Interface

The Rosslare AxTraxPro Desktop Client is a web browser interface to manage Rosslare Enterprises Ltd. access control panels.

The following image and table describe the Rosslare AxTraxPro main window.



#	Item	Description
1	Menu Bar	The Menu Bar controls the software's general operation and setup.
2	Toolbar	The main toolbar consists of icons for the key tasks required in managing access control across a facility. The available icons change according to the view selected. Lockdown shortcuts are available in all table views, see Using Lockdown Groups for the different lockdown group operations.
3	Hierarchic View	The Hierarchic View or tree view allows users to configure, monitor, and control every aspect of access control.

#	Item	Description
4	Display Area	The Display Area displays all items within the selected Tree View element. It also provides options to add, edit, or delete* items manually without opening the detailed element windows. In addition, the Display Area provides various system updates.
5	Event Log	The Event Log displays a detailed log of every time access was granted or denied for every door on the site, as well as when inputs and output are opened or closed. The event log toolbar consists of icons allowing the user to monitor potential door tamper or forced entry attempts. These warnings are logged and displayed as internal system warnings.
6	Status Bar	The Status Bar displays server connection status and the server time.

*To delete an item, select it in the Display Area and click the icon on the Toolbar. The **Delete** key on the keyboard is not supported for all items.

7. Defining Time Frames

The AxTraxPro software can manage an access control system that is located in a geographic area different than for the server. Time frames can be specified for the system.

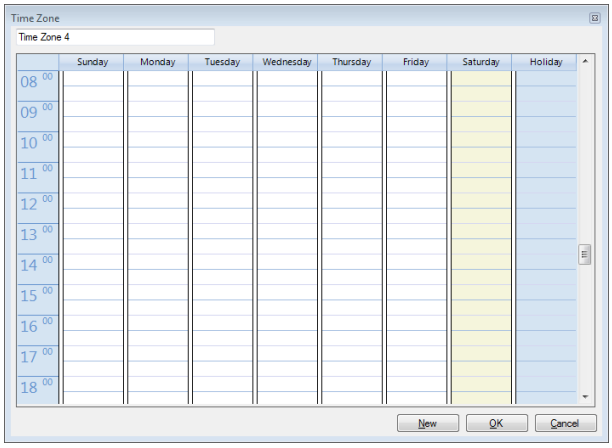
7.1. Adding Time Zones

A time zone is a group of periods within a week. Door access rights, as well as alarms and input and output behavior, can all be set to behave differently for each time zone. Many operations can be automatically enabled or disabled within a selected time zone.

The **Time Zone Properties** window displays the selected periods for each day of the week.

To add a new time zone:

1. In the Tree View, select **Timing > Time Zone**.
2. On the toolbar, click the  icon.



3. Enter a name for the time zone.
4. Click and drag the mouse down a day column to select a time interval.
5. Right-click the selected area and select **Create**.
6. Right-click the selected area again and select **Properties** to fine tune the time frame and then click **OK**.
7. Repeat Steps 4 to 6 for each day. Up to 16 intervals can be added per day.

> You can move a defined time zone to a different day and time using drag and drop.

8. Click **OK** when all of the time zones are defined.

> AC-215A control panel can support up to 8 time intervals for each day.

7.2. Adding Holidays

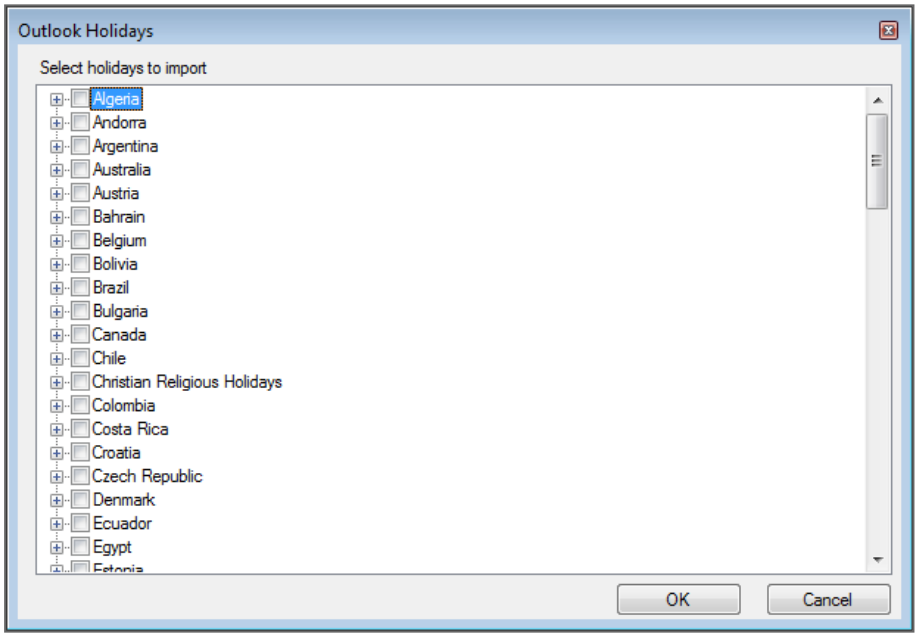
You can add and define annual holiday dates on which it is then possible to set special access behaviors.

There are two ways to add holidays:

- Add a known national holiday(s)
- Add a new holiday

To add a national holiday:

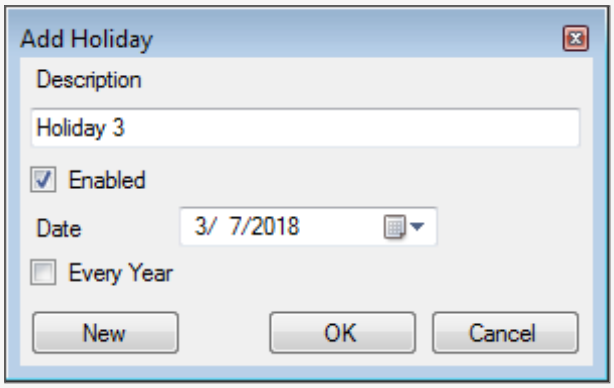
1. In the Tree View, select **Timing > Holidays**.
2. On the toolbar, click the  icon.



3. From the list, find the relevant country and either:
   a. Select the main check box to select all holidays for that country.
   b. Expand the check box and select which holidays to add.
4. Click **OK**.

To add a new holiday:

1. In the Tree View, select **Timing > Holiday**.
2. On the toolbar, click the icon.



3. In **Description**, enter a name for the holiday.
4. Select **Enabled** to enable the holiday.
5. Use the **Date** drop down to select the holiday's date.
6. Select **Every Year** to repeat the date yearly.
7. Click **OK**.

8. Configuring a Site

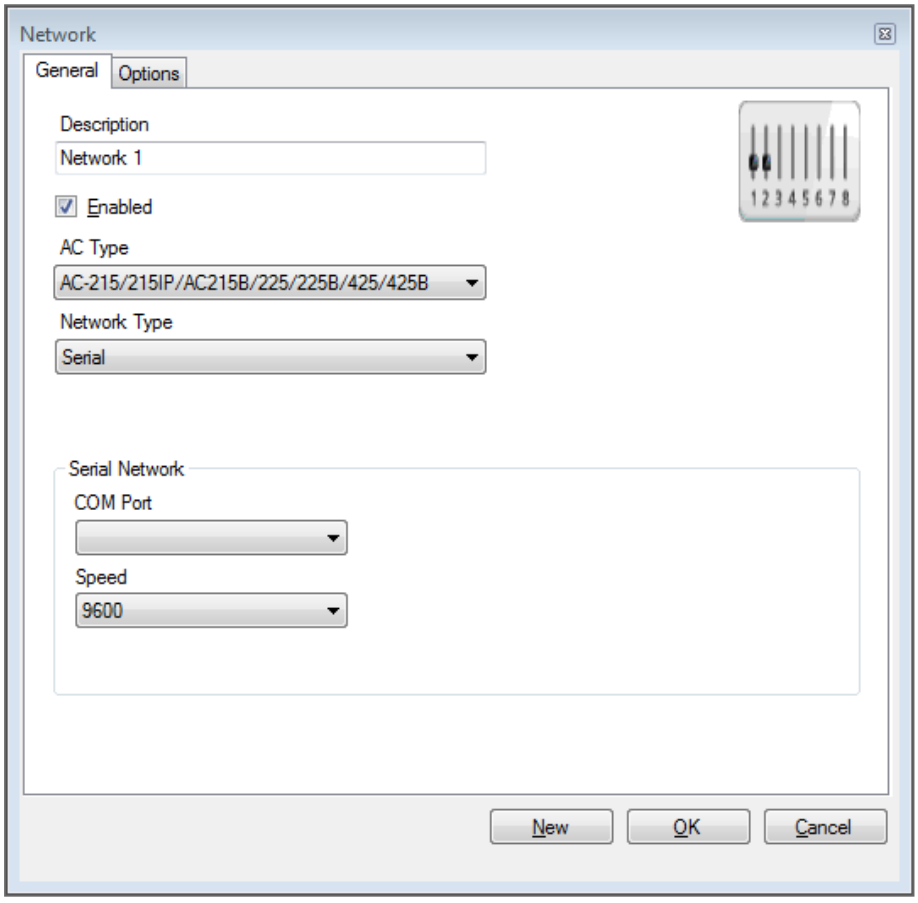
The access control site includes one or more access control networks. An access control network can contain one or more access control panels, The AxTraxPro PC client communicates with each access control panel in the network.

When adding a network, you must select the type of access panels that are in the network.

8.1. Adding a Network for AC-215x, AC-225x, and AC-425x Panels

To add a network for AC-215x, AC-225x, and AC-425x panels:

1. In the Tree view, select **AC Networks**.
2. On the toolbar, click the icon.



3. In **Description**, enter a name for the network.
4. Select **Enabled**.

> If **Enabled** is not selected, communication to panels on the network is halted.

5. In **AC Type**, select **AC-215/215IP/215B/225/225B/425/425B**.

6. In **Network Type**, select the network type and set the connection settings:
   a. For serial, select the correct COM port and speed.
   b. For a TCP/IP network, enter the IP address, select the port and speed, and select whether the network is WAN or LAN.
7. If you do not know the connection settings:
   a. For a TCP/IP connection, click **Configuration** to locate the hardware on the local network.

   See Configuring a Network for the procedure to configure an access control network. Check with your system administrator for more information or contact Rosslare technical support.



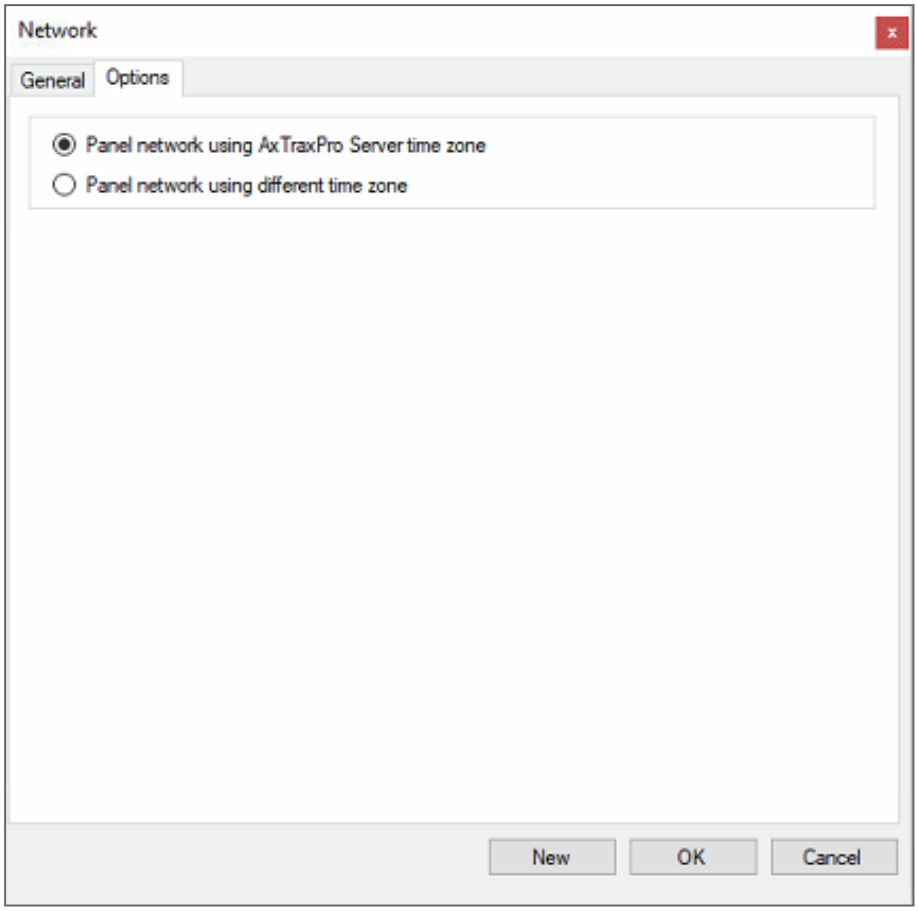
Access control panels connect to a TCP/IP network via an MD-N32 Serial to Ethernet Gateway or by using the onboard module in the AC-225IP or AC-425IP. Refer to the relevant hardware installation guides for more details.

8. For all types of networks, set the DIP switch on the access control panel hardware to match the diagram at the top of the screen.



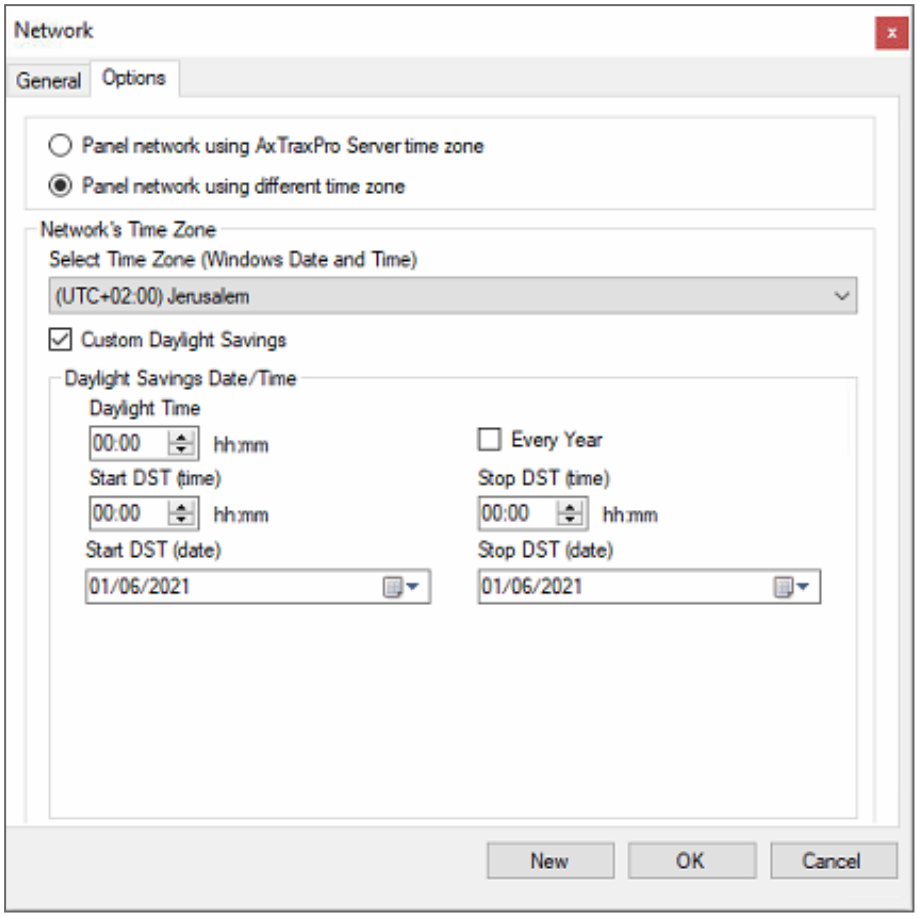
After changing the DIP switch, make sure to power down and then power up the panels.

9. In the **Network** window, select the **Options** tab.



10. To use the time zone of the AxTraxPro Server for the panel network, select **Panel network using AxTraxPro Server time zone** (default), and then continue to Step 13.

11. To select a different time zone for the panel network, select **Panel network using different time zone**.



12. Set the Daylight Saving Time definitions according to the field descriptions in the following table:

Field	Description
Daylight Time	Select the new hour at the time that daylight saving time begins.
Start DST (time)	Select the hour that daylight saving time begins.
Stop DST (time)	Select the hour that daylight saving time ends.
Every year	Select **Every year** to set a day in one of the weeks of a defined month to automatically begin and end daylight saving time every year. Clear **Every year** to set a date for one-time setting of the beginning and end of daylight saving time. In this case, a new date must be set each year.
Start DST (date)	If **Every year** is not selected, select the commence date for daylight saving time.
Stop DST (date)	If **Every year** is not selected, select the end date for daylight saving time.

13. To save this network/panel and to add another panel, click **New**.

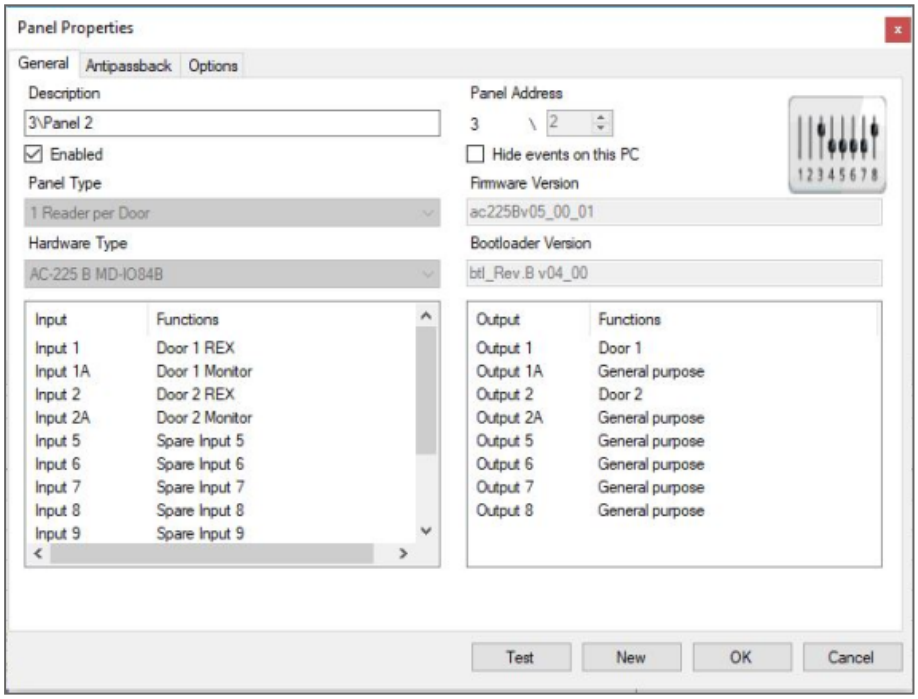
14. To save this network/panel and exit **OK**.

8.2. Adding an Access Control Panel to an Existing Network

You can add an individual panel using the **Tree View**.

To add an individual panel:

1. In the **Tree View**, click **AC Networks**.
2. Select an available network.
3. On the toolbar, click the  icon.



4. To add the panel and to configure it at another time, select **OK**.
5. To add the panel and to configure it at this time, select **New** (see Configuring a Panel for the panel configuration procedure).

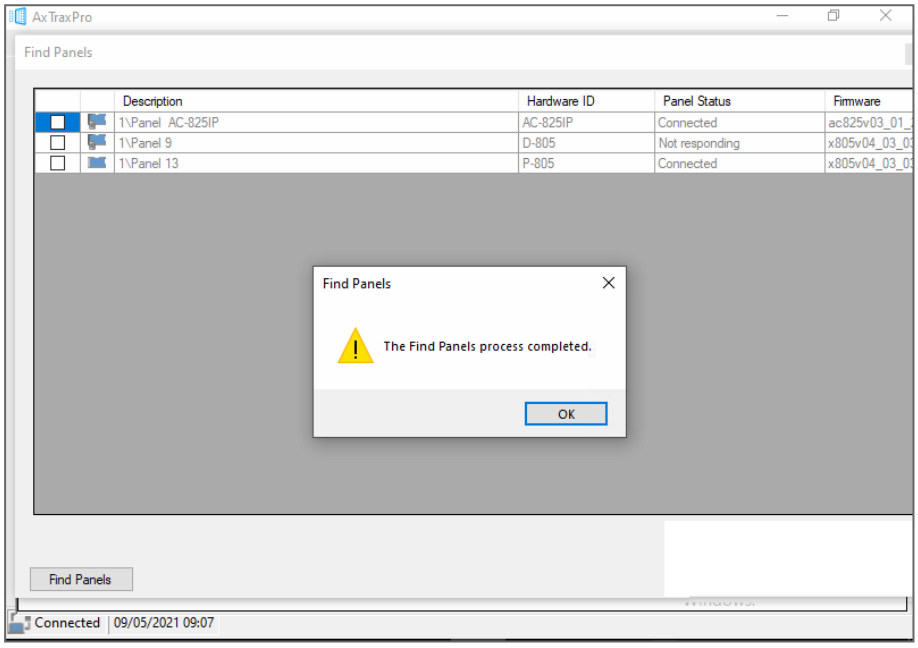
8.3. Searching for Existing Access Control Panels

It is possible to search for panels over the access control network using the **Find Panels** option. AxTraxPro finds all connected panels in the network and checks them. Panels can then be quickly

activated and updated.

To search for existing panel on the network:

1. In the Tree View, expand the **AC Networks** element and select a network.
2. On the toolbar, click the  icon.



Once the detection process is complete (this may take a few minutes), the display shows all of the detected panels and their corresponding information.

3. Select the panels that you wish to add and click **Add Panels**.

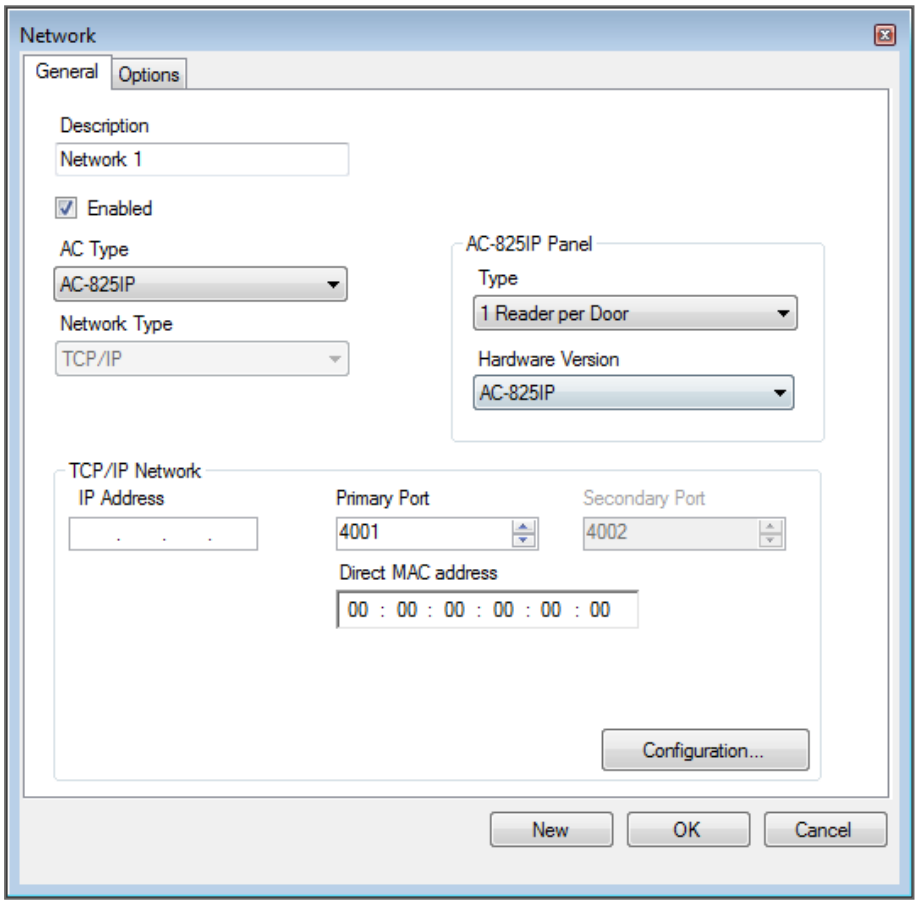
   The selected panels then appear in the Tree View under current network.

To configure the panel see Configuring a Panel for the panel configuration procedure.

8.4. Adding a Network for an AC-825IP Panel

To add a network for an AC-825IP panel:

1. In the Tree view, select **AC Networks**.
2. On the toolbar, click the  icon.
3. In **Description**, enter a name for the network.
4. Select **Enabled**.
5. In **AC Type**, select **AC-825IP**.



6. In the **AC-825 Panel** area:
   a. From **Type**, select if the panel is 1 or 2 readers per door.
   b. From **Hardware Version**, select whether this is an AC-825IP panel or one of its expansions (R/S/D/P-805).



Once these parameters are chosen, they cannot be changed.

7. Enter the IP address, the primary port, MAC address.
8. If you do not know the connection settings, click **Configuration** to automatically locate the hardware on the local network.

   For more information on how to configure a TCP/IP connection, see TCP/IP Connection. Check with your system administrator for more information or contact Rosslare technical support. Clear **Enabled** if you want to halt communication to panels on the network.



Access control panels connect to a TCP/IP network using the onboard module in the AC-825IP. Refer to the **AC-825IP Hardware Installation and User Manual** for more details.

9. Click **OK**.

There can be only one AC-825IP panel in a network. However, you can add one expansion board to the AC-825IP panel (see AC-825IP for the procedure to add an x-805 expansion board) or up to 12 extensions using RS-485.

8.5. Configuring a Panel

Every network is a cluster of access control panels. In its standard form, each access control panel can be configured as either one or two readers per door. Each of the AC-215x and AC-225x panels has two readers and can be configured as a one or two-door panel. Each AC-425x panel has four readers and can be configured as a two or four-door panel.

When using an optional MD-D02 (supported by AC-225x) or MD-D04 (supported by the AC-425x) reader expansion board, each panel has four or eight readers and is configurable as such.

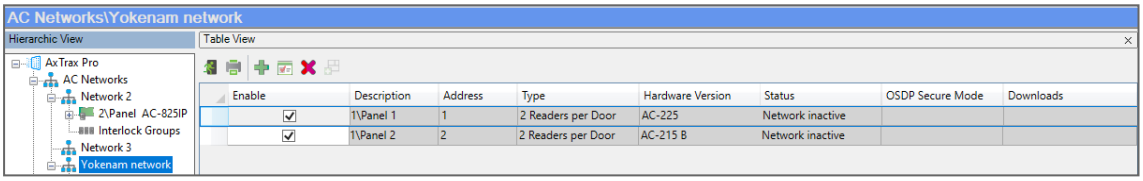
Use two readers per door when one door acts as both the entrance and exit to an area of the site. When only an entry reader is required, use one reader per door.

For example:

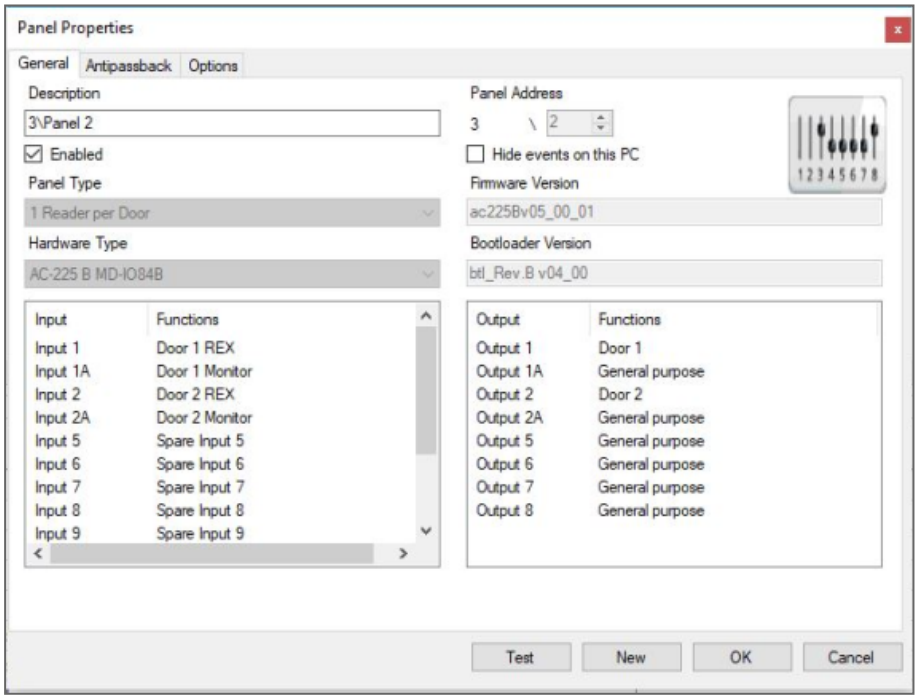
- Use configuration with two readers per door set to IN and OUT to produce attendance reports.
- Use one reader per door configuration to control two doors with an IN reader only (premises will be exited using a Request-to-Exit (REX) switch or a mechanical door handle only).

When there is communication with the panel, the Tx and Rx LEDs flash.

1. In the Tree View, expand the AC Networks element and select a network.
2. Select the row for a panel



3. On the toolbar, click the icon.
4. In the **Panel Properties** window, select the **General** tab.



5. Configure the panel according to the fields described below.

Field	Description
Description	Type a description for the panel
Panel Address	Type an address number for the panel The network's address appears to the left of the panel address. Valid entries are 1–32.
Enabled	Select to activate this panel Clear if the panel is not connected
Hide events on this PC	Select to hide events originating from this PC
Panel Type	Select one or two readers per door
Hardware Type	Select the appropriate panel hardware type
Firmware Version	Upon selection of the hardware version, the field displays the current firmware version
Bootloader Version	Upon selection of the hardware version, the field displays the current bootloader version
Inputs	Displays the input connections for the panel
Outputs	Displays the output connections for the panel
Test	Click to test if that the panel is correctly connected to the server. The Test Panel window displays hardware details, including hardware type, firmware, and bootloader versions, and indicates whether a reader or I/O expansion board is installed on the panel.



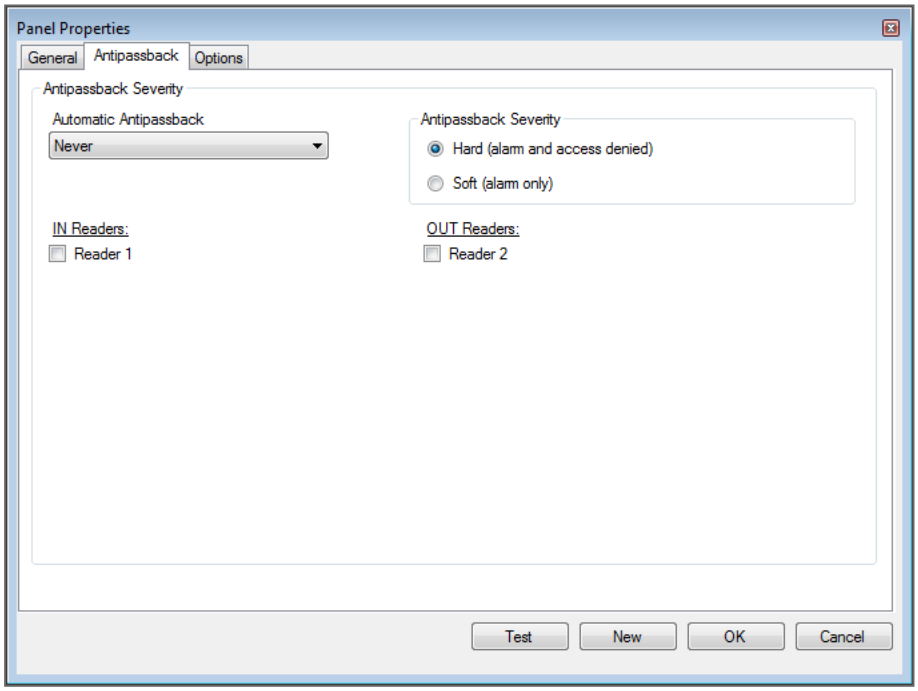
Make sure that the DIP Switch 3 position on the panel corresponds with its position demonstrated in the **Panel properties** window.

6. Click **Test**.



If an expansion board is connected to the access control panel, it appears under “Board”, and an **Add Board** button is visible (see Adding an Expansion Board).

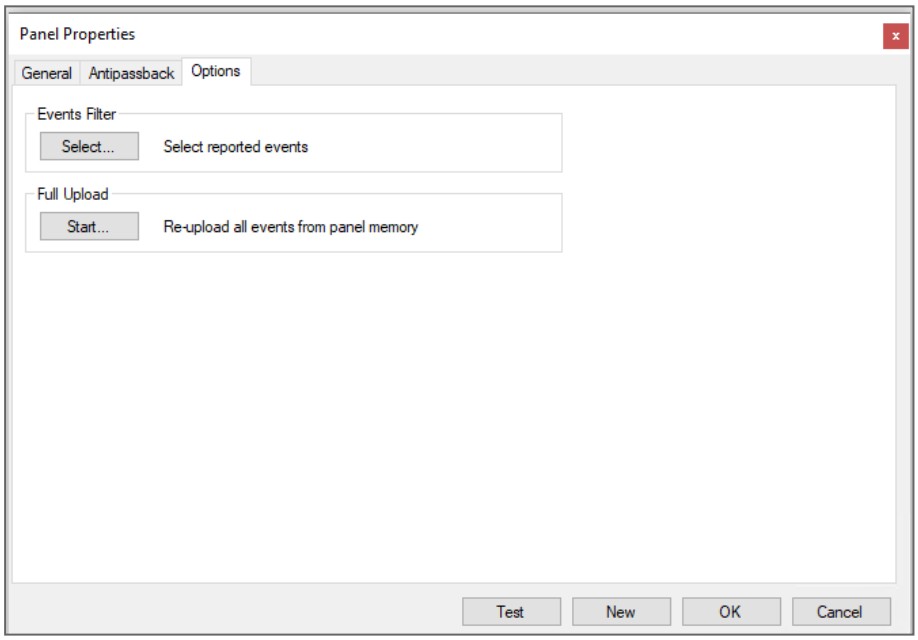
7. Click **Close**.
8. In the **Panel Properties** window, select the **Antipassback** tab.



9. Set the Antipassback behavior according to the field descriptions below.

Field	Description
Automatic Antipassback	From the Automatic Antipassback dropdown, select the time zone for door antipassback rules to apply.
Antipassback Severity	• **Hard** – An event is generated and the door does not open • **Soft** – An event is generated and the door opens
In/Out Reader List	From the IN/OUT readers list, select the checkboxes to apply antipassback restrictions to the readers as needed. The reader antipassback is enabled when the checkbox is selected.

10. In the **Panel Properties** window, select the **Options** tab.



11. Set the recording events behavior according to the field descriptions below.

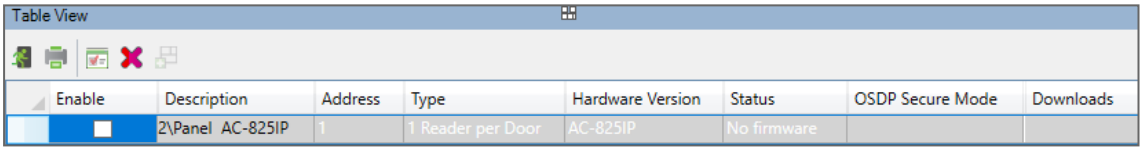
Field	Description
Events Filter	Click **Select** to open the Events Filter and select the events that this panel should record. Set the filter's operation method: In the default configuration, some events are filtered and may not be seen in the Events view.

Field	Description
Full Upload	Click **Start** to re-upload all events from panel memory. Use the option only after consulting Rosslare's Technical Support. A full upload can take up to 3 hours.

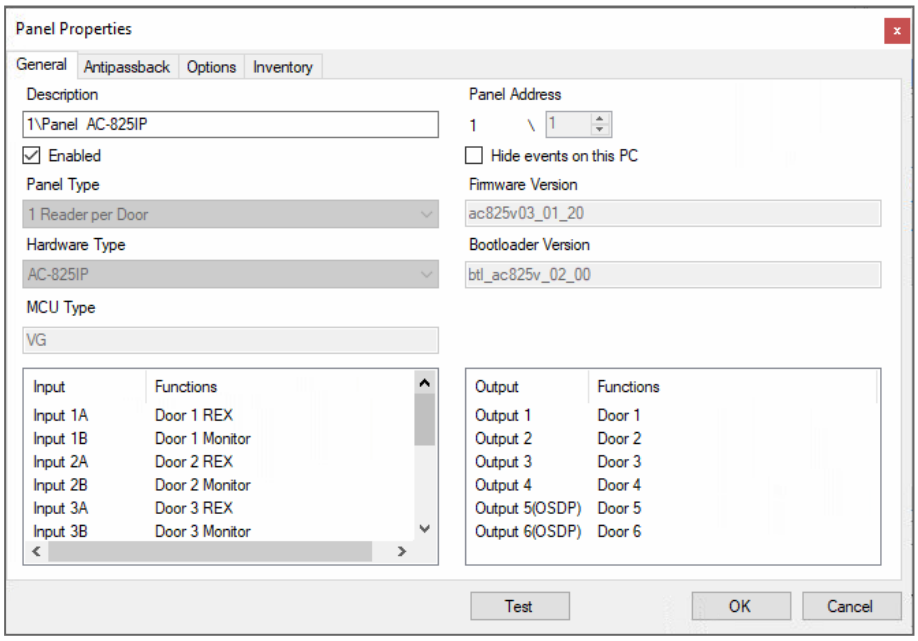
12. Click **OK**.

8.6. Configuring an AC-825IP Panel

1. In the Tree View, expand the AC Networks element and select a network.
2. Select the row for the 825IP panel



3. On the toolbar, click the icon.
4. In the **Panel Properties** window, select the **General** tab.



5. Configure the panel according to the fields described below.

Field	Description
Description	Type a description for the panel
Enabled	Select to activate this panel Clear if the panel is not connected
Hide events on this PC	Select to hide events originating from this PC
Hardware Type	Select the appropriate panel hardware type
Firmware Version	Upon selection of the hardware version, the field displays the current firmware version
Bootloader Version	Upon selection of the hardware version, the field displays the current bootloader version
Inputs	Displays the input connections for the panel
Outputs	Displays the output connections for the panel
Test	Click to test if that the panel is correctly connected to the server. The Test Panel window displays hardware details, including hardware type, firmware, and bootloader versions, and indicates whether a reader or I/O expansion board is installed on the panel.

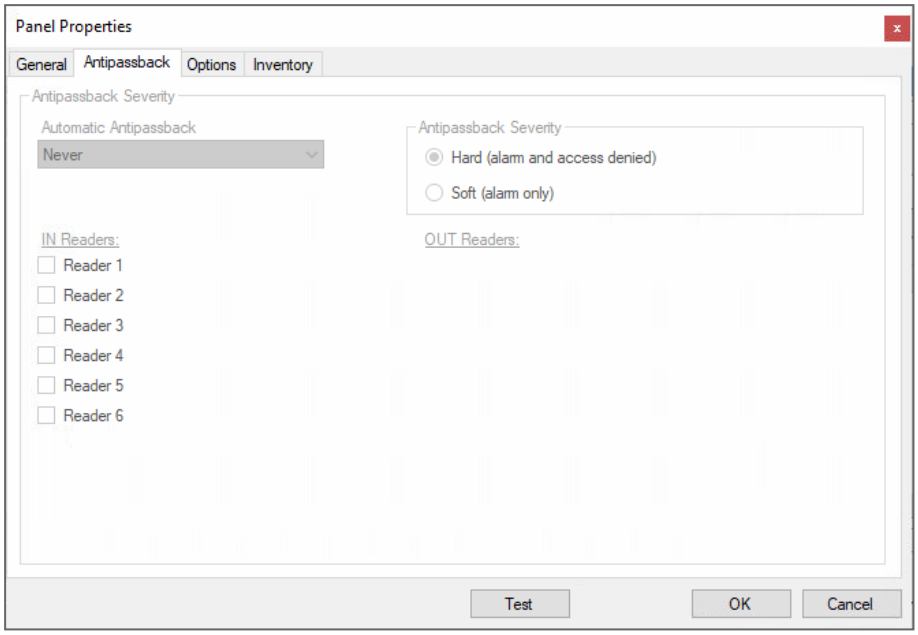
6. Click **Test**.



If an expansion board is connected to the access control panel, it appears under “Board”, and an **Add Board** button is visible (see Adding an Expansion Board).

7. Click **Close**.

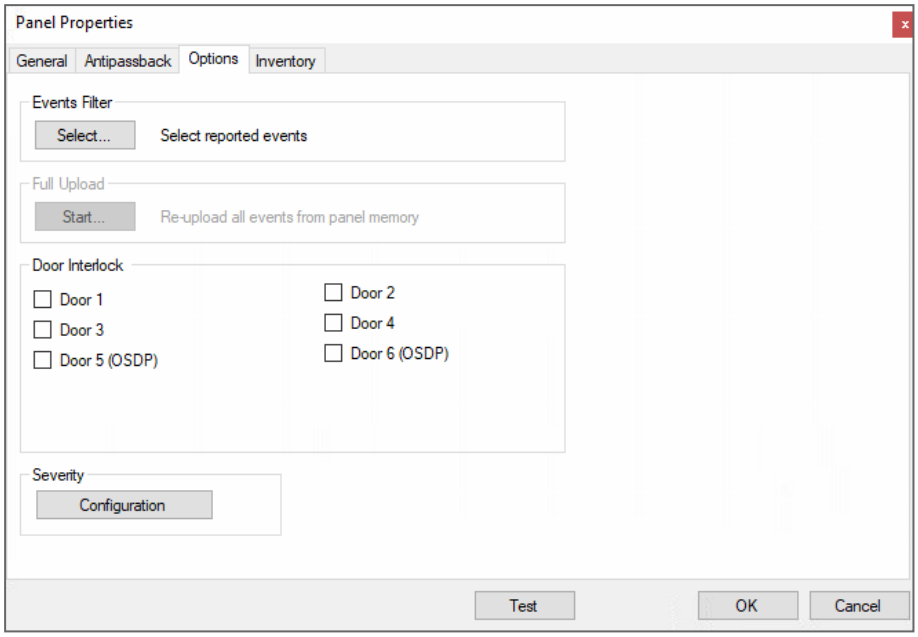
8. In the **Panel Properties** window, select the **Antipassback** tab.



9. Set the Antipassback behavior according to the field descriptions below.

Field	Description
Automatic Antipassback	From the Automatic Antipassback drop down, select the time zone for door antipassback rules to apply.
Antipassback Severity	• **Hard** – An event is generated and the door does not open • **Soft** – An event is generated and the door opens
In/Out Reader List	From the IN/OUT readers list, select the check boxes to apply antipassback restrictions to the readers as needed. The reader antipassback is enabled when the check box is selected.

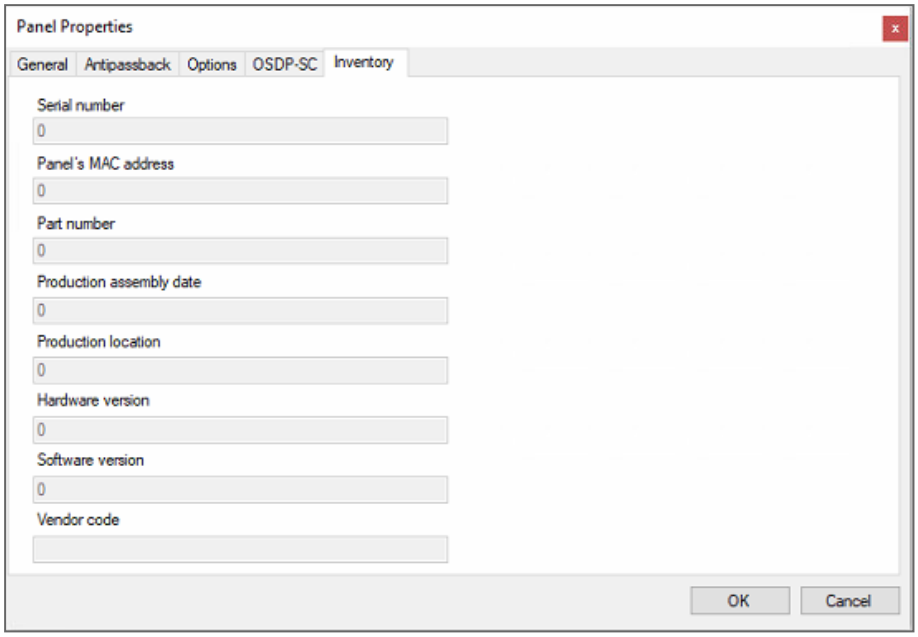
10. In the **Panel Properties** window, select the **Options** tab.



11. Set the recording events behavior according to the field descriptions below.

Field	Description
Events Filter	Click **Select** to open the Events Filter and select the events that this panel should record. Set the filter's operation method: In the default configuration, some events are filtered and may not be seen in the Events view.
Door Interlock	This option is only visible when the panel is configured with at least two doors. Select the check boxes to apply the Door Interlock rule to the relevant doors. A maximum of 10 readers can be defined with a door interlock rule when a D-805 extension is connected to an AC-825IP panel's expansion slot. When using a rule, be sure that it does not conflict with an existing interlock group (see Interlock Groups). If you are configuring both antipassback and door interlock features, you must configure the antipassback feature first. If reader was set in Card+Card mode, this function does not work in an AC-225 or an AC-425 panel.
Severity	Click **Configuration** to set the severity type of the configuration log.

12. In the **Panel Properties** window, select the **Inventory** tab.



Field	Description
Unique board number	Serial number
Panel's MAC address	MAC address
Card type - App can identify card type	Part number
Production assembly date	Production assembly date
Production location	Production location
Hardware change	Hardware version
Software version	Software version
Vendor code	For OSDP use

13. Click **OK**.

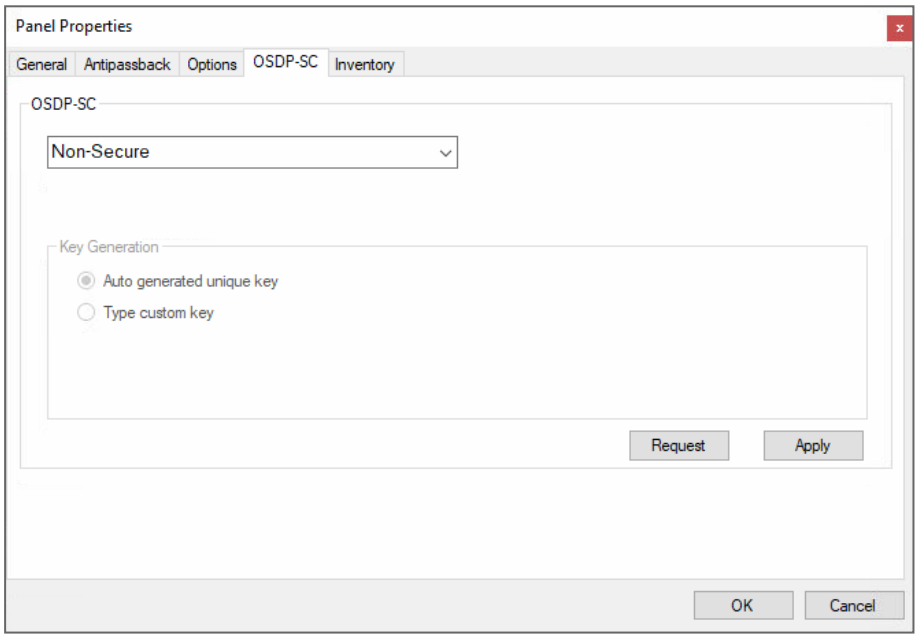
8.6.1. OSDP-SC Tab

This procedure is for peripheral devices with Open Supervised Device Protocol (OSDP). AC-825IP control panels support OSDP communication with x-805 expansions units (R/S/D/P) and 3 OSDP readers.

An AC-825IP control panel can use two peripheral devices connected to the OSDP bus. The addressees for the readers must be set to 13 and 14.

The installer key (default) is used to start the OSDP-Secure Channel security configuration procedure.

1. In the **Panel Properties** window, select the **OSDP-SC** tab.
2. Select a security mode in the list box.

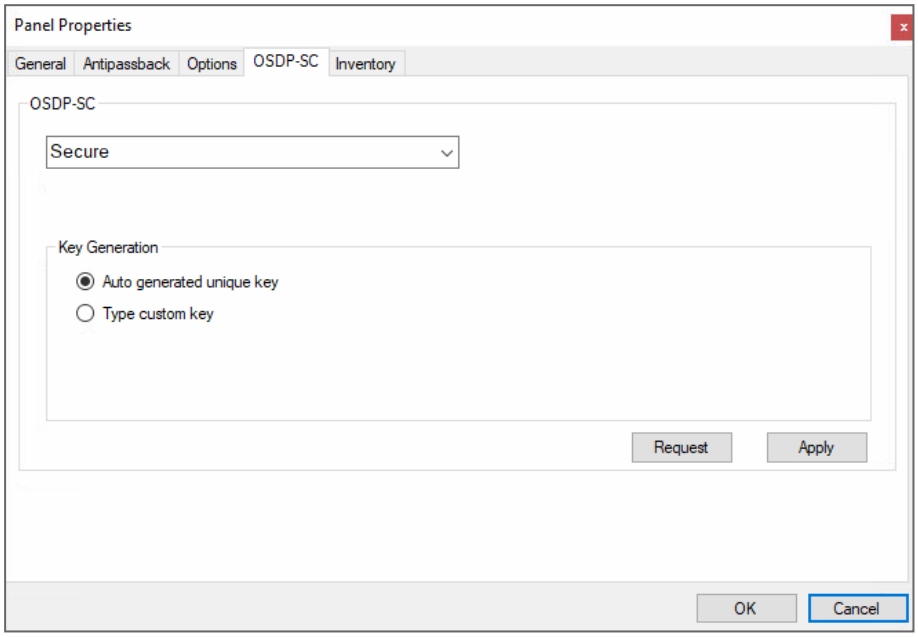


The available security modes are:

- Non-Secure: used where no authentication is necessary
- Secure: used for OSDP-Secure Channel
- Default key - Installation mode: used to start with the secure channel communication

Method 1: Auto Generated Unique Key:

1. Select **Auto generated unique key** for a **Key Generation** method.



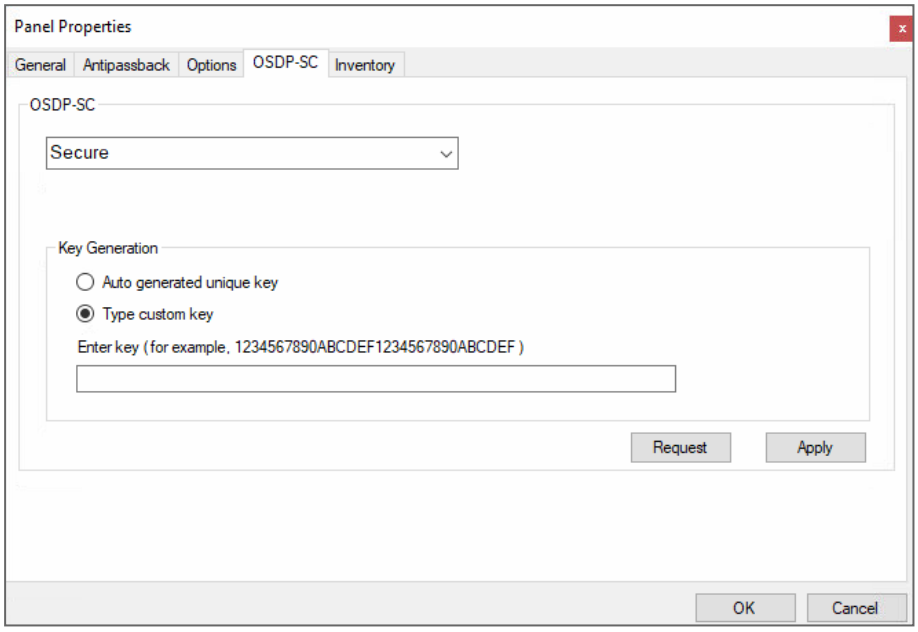
A random and unique key is generated each time this procedure is done.

It is recommended to copy and paste the key to a secure location

2. Click **Apply**.

Method 2: User Provided Custom Key:

1. Select **Type custom key** for **Key Generation** method, type the key in the **Enter key** box.



Make sure to enter a 128-bit key as hexadecimal number.

2. Click **Apply**.

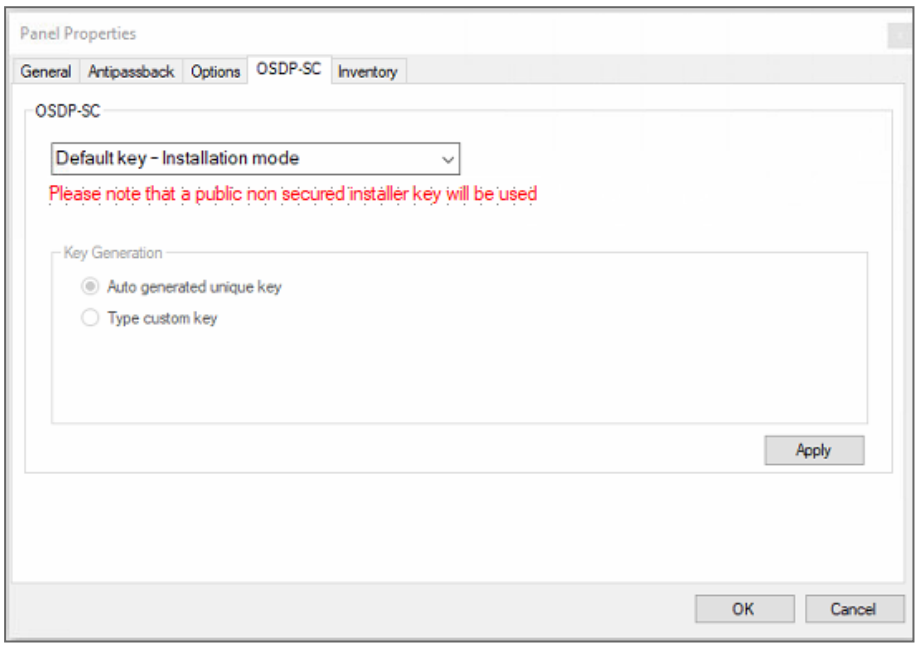
Installation Mode to Start Secure Channel Communication

When it is necessary to reconfigure a reader use the **Secure - default key (Installation mode)** to reset the reader.

When the **Default key - Installation mode** is selected all applicable hardware must be set to installation mode.

1. Select **Default key - Installation mode** for a **Security** method.

> After selecting a default key the communication is not secure. This is because the default key is a public non secured installer key.



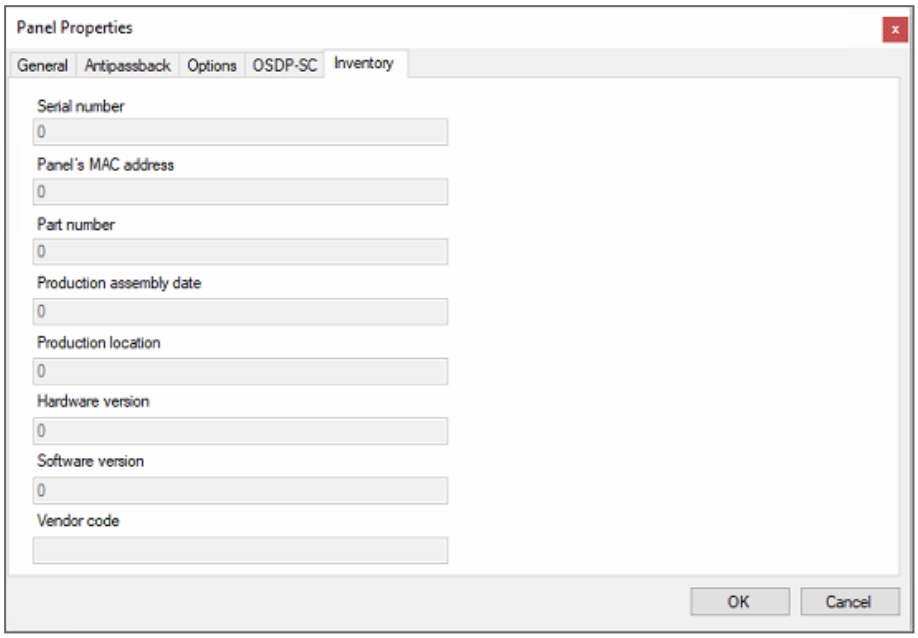
2. Click **Request**.
3. Click **Apply**.
4. Set OSDP with Method 1: Auto Generated Unique Key:.

   or

5. Set OSDP with Method 2: User Provided Custom Key:.

8.6.2. Inventory Tab

1. In the **Panel** window, select the **Inventory** tab.



Field	Description
Serial number	Serial number
Panel's MAC address	MAC address
Part number	Part number
Production assembly date	Production assembly date
Production location	Production location
Hardware change	Hardware version
Software version	Software version
Vendor code	For OSDP use

2. Click **OK**.

8.6.3. Interlock Groups

For AC-825IP panels, interlock groups can be defined. A group of doors can be selected to be activated in the interlock method, meaning only one door can be opened at a time.

A maximum of 5 doors can be defined per group.

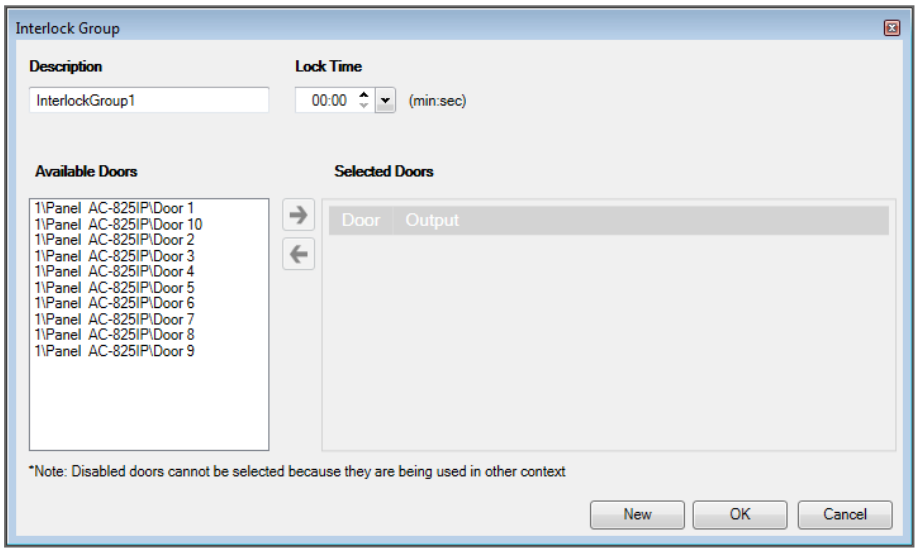
A door can be selected to up to 5 different interlock groups.

A timer can be defined in case that interlock mode has been activated following door closing. All doors of the group are disabled for that period of time.

When defining an interlock group, be sure that it does not conflict with an existing interlock rule, see Door Interlock.

To add an interlock group:

1. In the Tree view, expand an AC-825IP network.
2. Select **Interlock Groups**.
3. On the toolbar, click the icon.



4. Select and move the desired doors from **Available Door** to **Selected Doors** using the arrows.
5. Click **OK**.

The window closes and the new interlock group appears in the Display Area.

8.7. Adding an Expansion Board

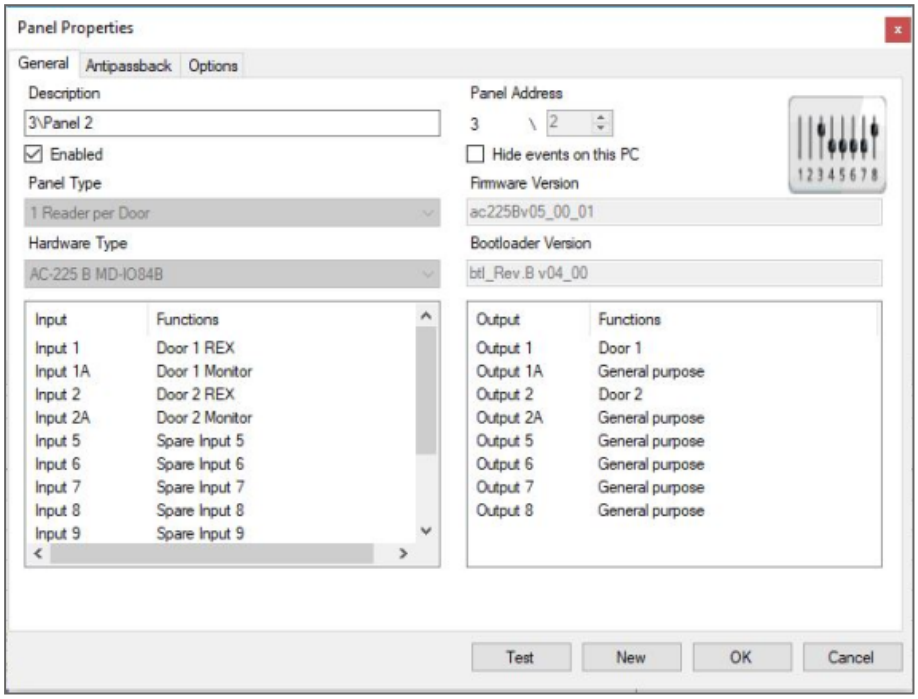
8.7.1. AC-225x and AC-425x

For the AC-225x panels, you can add one MD-D02 or MD-IO84 expansion board per access control panel.
For the AC-425x panels, you can add one MD-D04 or MD-IO84 expansion board per access control panel.

To add an expansion board:

1. Power down the panel.

2. Plug the expansion board into the panel and repower the board supply.
3. In the **Tree View**, expand the **AC Networks** element and select a network.
4. On the toolbar, click the  icon.

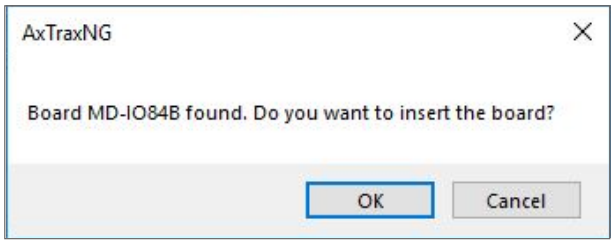


5. Click **Test**.



6. Click **Add Board**.

   After a few moments, the following confirmation appears.



7. Click **OK**.

The window closes and the new panel appears in the Display Area.

To remove a board from a panel, you must delete the panel from the database.

8.7.2. AC-825IP

For the AC-825IP panel, you can add an x-805 expansion board.

Only one expansion board can be added per access control panel.

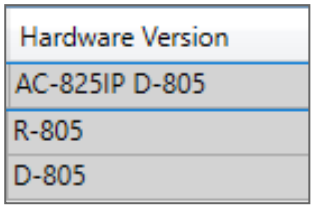
To add an expansion board:

1. Power down the panel.
2. Plug the expansion board into the panel and repower the board supply.

   To add an AC-825 with D-805 expansion board in a daisy chain topology, it is necessary to specify the **AC-825IP D-805** configuration. This configuration will not be added automatically.

   Once the AC-825IP panel is connected, you will see in the Hardware Version column in the Tree View

that the expansion board was installed.



To remove a board from a panel, you must delete the panel from the database.

8.8. Deleting a Panel

To delete a peripheral device:

1. In the Tree View, expand the **AC Networks** element.
2. Expand a network and expand a panel
3. Select the row for the panel to delete.
4. Click .
5. Click **Yes**.

The Events log, will show **Succeed** for the panel that was deleted.

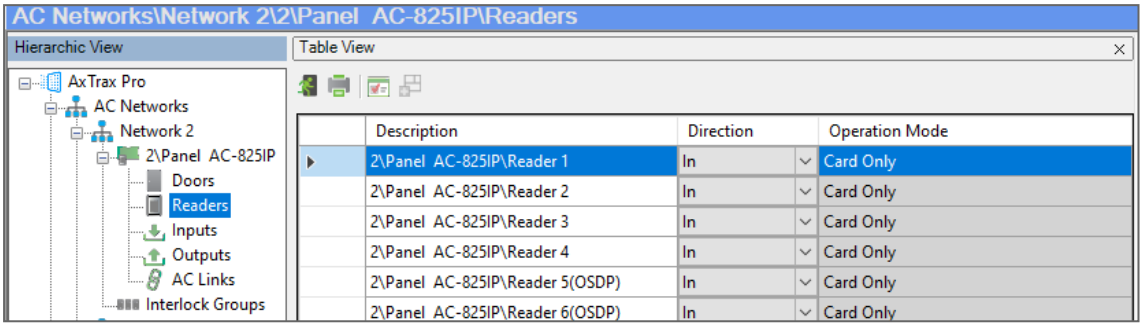
8.9. Configuring a Reader

A panel can be connected to two, four, or eight readers, when the MD-D02 or MD-04 extension boards are connected.

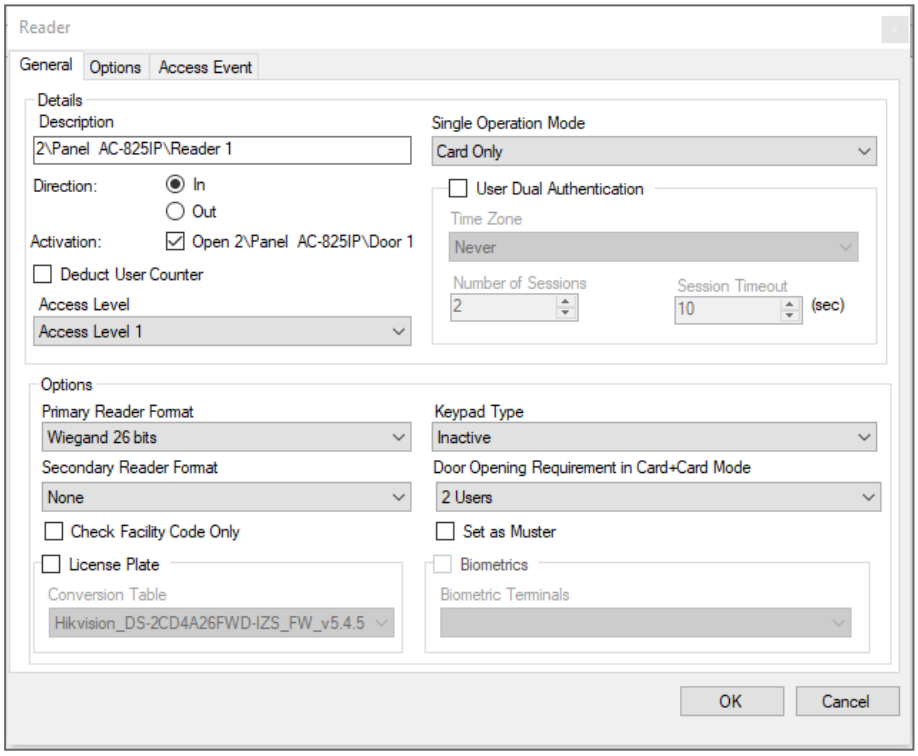
8.9.1. General Tab

1. In the Tree View, expand the AC Networks element and select a network.
2. Select a panel and select a reader.

3. Select the row for a reader.



4. On the toolbar, click the  icon.
5. In the **Reader** window, select the **General** tab.



6. Set the reader properties according to the field descriptions in the following table:

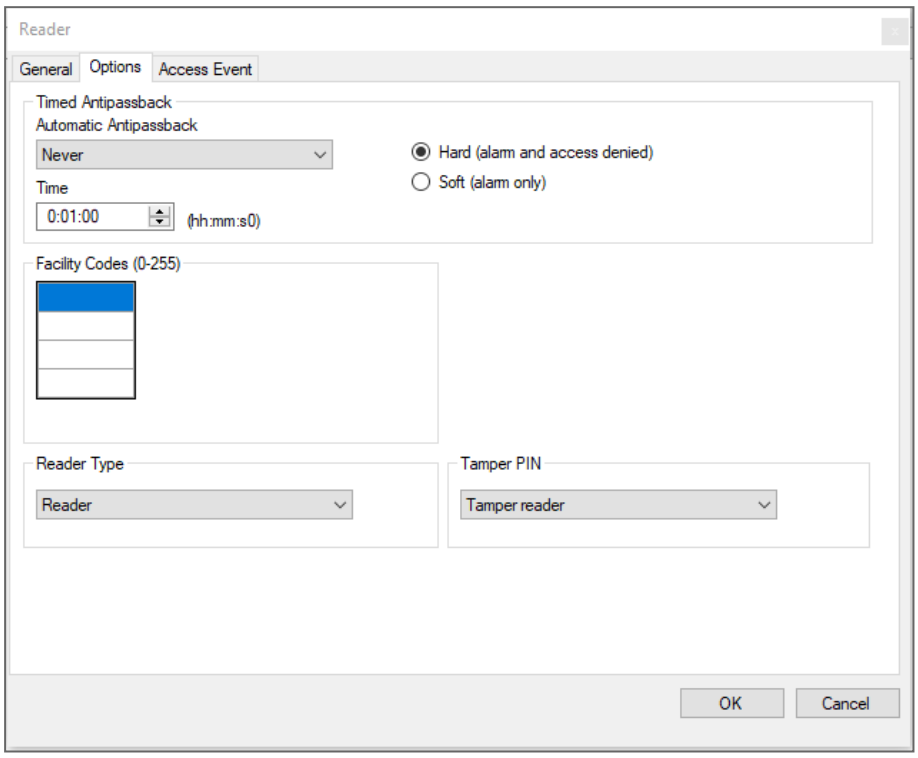
Field	Description
Details > Description	Enter the name of the reader

Field	Description
Details > Direction	Select whether the reader is allowing entry into the area or exit out of the area
Details > Activation	Select to allow the reader to unlock the door. If selected, the door output is active while a valid user is present. If cleared, access logged events are received online and appear in the Events toolbar.
Details > Deduct User Counter	Select to record this entry against the user's entry allowance counter.
Details > Access Level	Select the access level
Details > Single Operation Mode	Select how the reader operates: • **Inactive:** The reader is not in use • **Card Only:** The reader uses RFID cards only • **PIN Only:** The reader uses PIN inputs only • **Card or PIN:** The reader uses both cards and PIN codes • **Desktop:** The reader is inactive, but is being used to record new cards on the computer • **No Access:** The reader does not grant access to any users • **Card + Card:** The reader grants access only when two separate users present their cards
User Dual Authentication	Select to activate the dual authentication mode, which enforces 2 credentials per user per access  A maximum of 10 readers in a network can be set with dual authentication.
User Dual Authentication > Time Zone	Select the time zone in which dual authentication is active • Always (default) • Never • Any previously defined time zone(s) in the system

Field	Description
User Dual Authentication > Number of Sessions	Select to define the number of sessions available A session is the time during which 2 credentials per user for single access are presented. • 1 (default) • 2 (for AC-825IP panels only)
User Dual Authentication > Session Timeout	The length in seconds of each session Range is 5 to 255, default is 10)
Options > Primary Reader Format	Select the data transmission type for the primary reader hardware
Options > Secondary Reader Format	Select the data transmission type for the secondary reader hardware.  This field is used when 2 different types of cards are used.
Options > Keypad Type	Select the data transmission type for the type of keypad hardware
Options > Door opening requirement in Card + Card mode	Select 2 or 3 users needed to open the door in Card + Card mode.  In AC-215A this function is disabled.
Options > Check Facility Code Only	Select to allow access to any user assigned to a facility listed in the selected list of facilities. The list of facilities is defined on the **Options** tab.  This option is only available for certain formats.
License Plate	Select to allow using a customized conversion table.
License Plate > Conversion Table	Select the relevant conversion table.
Options > Set as Muster	Select to allow tracing the personnel that presented their credentials to it.
Biometrics	Select the check box to select from the drop down to map a reader to a terminal (see From a Remote Network).

8.9.2. Options Tab

1. In the **Reader** window, select the **Options** tab.

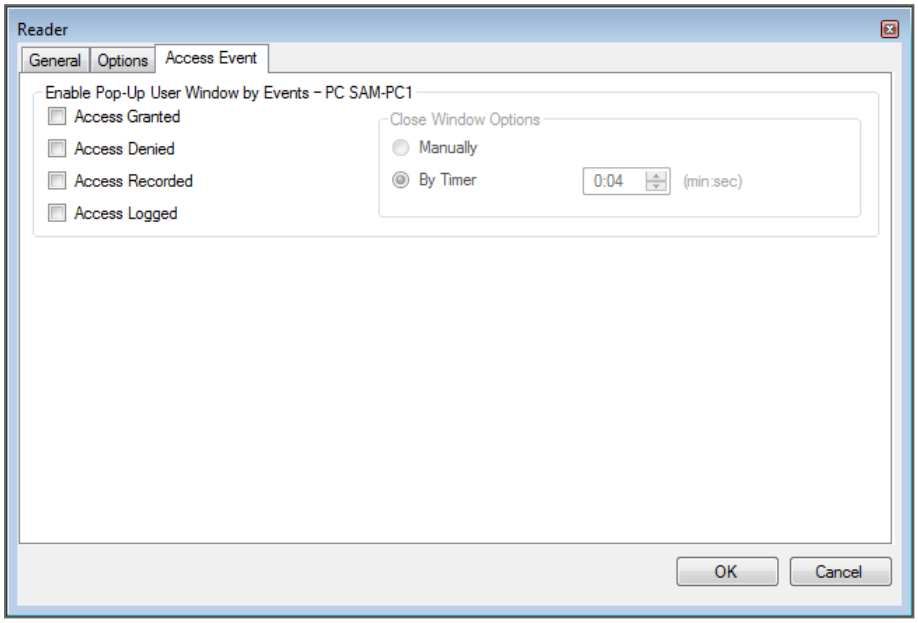


2. Set the properties according to the field descriptions in the following table:

Field	Description
Automatic Antipassback	Select whether to apply antipassback rules. To set Time Zones, see Adding Time Zones.
Hard	When hard antipassback is selected, an event is generated and the door does not open.
Soft	When soft antipassback is selected, the door opens but an event is generated.
Time	Set the number of minutes before a user can re-enter using this reader.
Facility Codes	Click and type the Facility code (between 0–255). Up to four different Facility codes can be entered.
Reader type	Select the reader type.
Tamper PIN	Select the Tamper PIN type.

8.9.3. Access Event

1. In the **Reader** window, select the **Access Event** tab.



2. Set the properties according to the field descriptions in the following table:

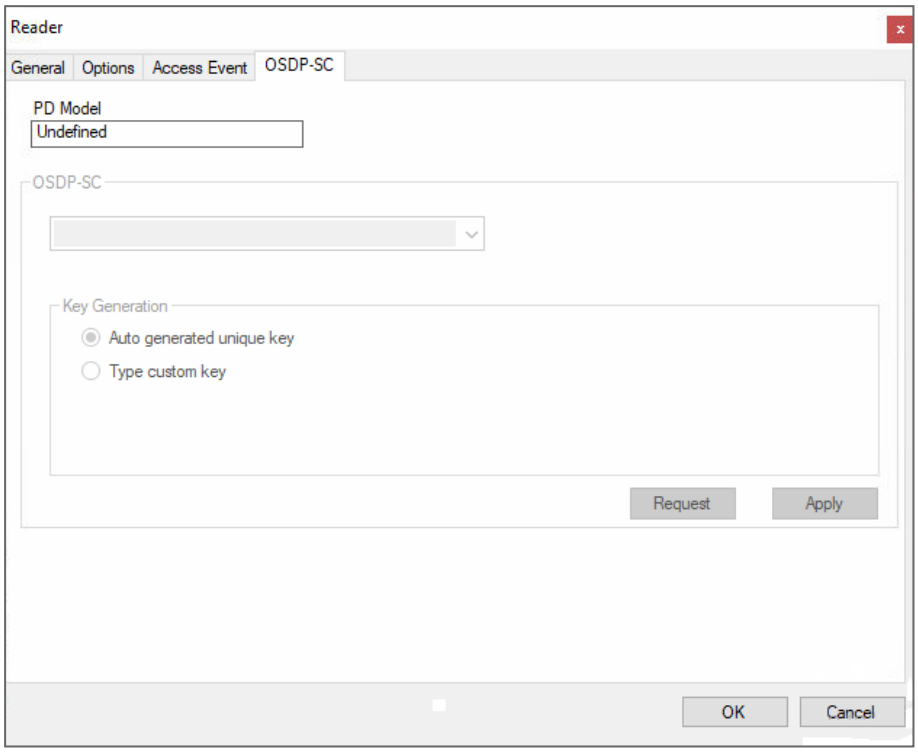
Field	Description
Access Granted	Select to enable a pop-up window for Access Granted event type alerts.
Access Denied	Select to enable a pop-up window for Access Denied event type alerts.
Access Recorded	Select to enable a pop-up window for Access Recorded event type alerts.
Access Logged	Select to enable a pop-up window for Access Logged event type alerts.
Close window Options	Once a pop-up is enabled, the close window options are available. Select one of two options: • **Manually:** The operator is required to manually close the pop-up window. • **By timer:** The pop-up window closes automatically based on the predefined timer.

8.9.4. OSDP-SC Tab

This procedure is for readers with Open Supervised Device Protocol (OSDP).

The addressees for the readers must be set to 13 and 14.

1. In the **Reader** window, select the **OSDP-SC** tab.
2. Select a **PD Model** in the list box.



3. Click **Apply**.

Installation to Reconfigure a Reader

When it is necessary to reconfigure a reader, the follow the procedure given in Configuring an AC-825IP Panel.

8.10. Adding a Biometric Terminal

You can add a biometric terminal to a network using the **Biometrics** element.

A biometric terminal can be used to read and transmit credentials or enroll new credentials (fingerprint and cards).

The terminals support both TCP/IP and Wiegand protocols.

Adding a biometric terminal can be done both on a local network and from a remote network.

8.10.1. On a Local Network

To add a biometric terminal on a local network:

1. In the Tree View, expand the **Biometrics** element and select **Terminals**.
2. On the toolbar, click the icon.



3. In **Description**, enter a name for the new terminal.
4. Select **Enabled** to enable the terminal.
5. In **Model Number**, select the reader model.
6. In the **TCP/IP Network** area, enter the MAC address, IP address, and the port.

For models AY-B9250BT and AY-B9350, an additional **Enable camera snapshot** check box appears. If selected, the terminal takes a snapshot of the terminal view.

For Bio9000 series there is an option of Live Fingerprint detection.

Once enable this option, expect to get longer time for recognition and lower recognition rate.

7. Click **OK**.

   The window closes and the new terminal appears in the Display Area.

If you do not know the connection settings click **Configuration** to locate the hardware on the local network. Refer to Configuring a Biometric Terminal for how to search for a biometric terminal and configure it.

8.10.2. From a Remote Network

To add a biometric terminal from remote network, you must first receive an exported file from the remote network that contains all the terminal's configuration settings. Once you receive this file, you can then add the biometric terminal by importing this file.

8.10.2.1. Exporting a Terminal File

To export a terminal file:

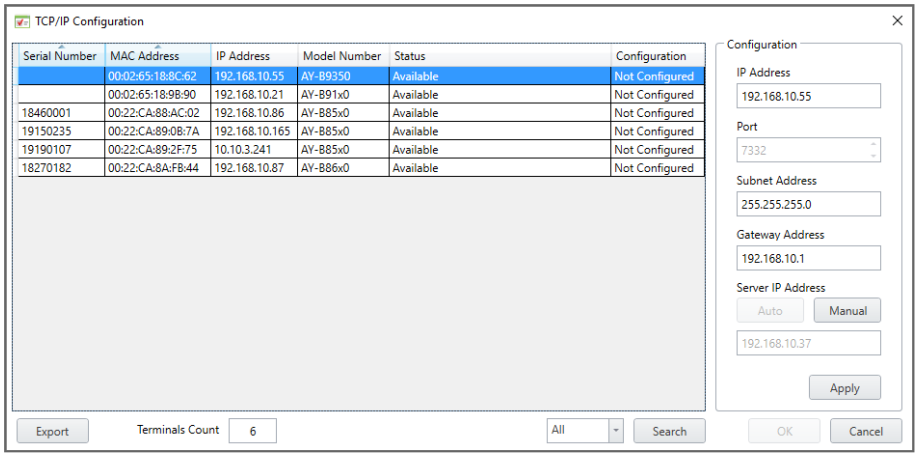
1. In the Tree View, expand the **Biometrics** element and select **Terminals**.

2. On the toolbar, click the icon.



3. Click **Configuration**.

4. The **TCP/IP Configuration** window opens and automatically searches for any terminals connected to the network.



5. Click **Export**.
6. In the **Save as** window, type a file name and save the file (xxx.axbio) on your PC where it can be easily accessed.

The Export function adds “axbio” to the end of file name of the exported file. The Import function executes only with a file that contains this string at the end of the file name.

8.10.2.2. Importing a Terminal File

To import a terminal file:

1. In the Tree View, expand the **Biometrics** element and select **Terminals**.
2. On the toolbar, click the  icon.

   The **Import Terminal** window opens.
3. Browse to the previously exported xxx.axbio file and double-click it.

The window closes and the terminal appears in the Display Area.

8.10.3. Configuring a Biometric Terminal

The AxTraxPro server communicates with a biometric terminal in two ways: TCP/IP (either LAN or WAN) and Wiegand protocols.

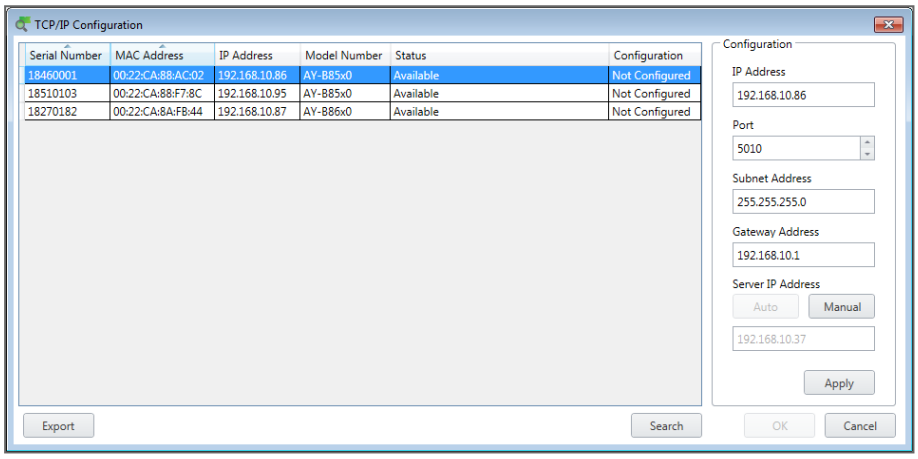
Each terminal has a unique MAC address and appears separately in the system.

The AxTraxPro server supports multiple terminals per access control network.

To search for the biometric terminal to configure:

1. In the Tree View, expand the **Biometrics** element and select **Terminals**.
2. On the toolbar, click the  icon.
3. Click **Configuration**.

   The **TCP/IP Configuration** window opens and automatically searches for any terminals connected to the network.



   The main window lists all terminals connected to the local network and indicates if they have been previously assigned to a terminal or not.

For a biometric terminal that has not yet been configured:

1. Select the appropriate terminal.

   The terminal's parameters are displayed in the **Configuration** area on the right.
2. Click **Apply**.

   Wait for the list to refresh and see that the terminal's status is now **Configured**.
3. Select the terminal from the list again.
4. Click **OK**.

   The window closes and the new terminal appears in the Display Area.

8.10.4. Mapping a Biometric Terminal to a Reader

Once you have added a biometric terminal to the system, you must map it to a specific reader in order for the system to recognize the terminal.

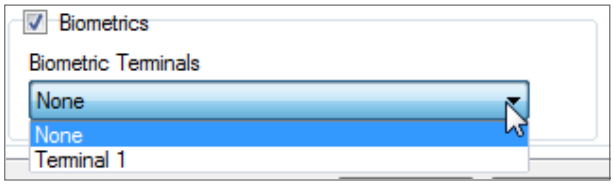
To map a biometric terminal:

1. In the Tree View, expand the **AC Networks** element.
2. Expand a network and expand a panel.
3. Select **Readers**.

   The available readers are listed in the Display Area.
4. Select a reader in the Display Area.
5. On the toolbar, click the  icon.

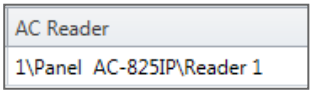
   The **Reader Properties** window opens to the **General** tab.
6. Select the **Biometric** check box and select the relevant terminal from the drop down.





7. Click **OK** to accept the changes.

   When you select the **Terminal** element, you can now see to which reader the terminal is mapped in the Display Area.

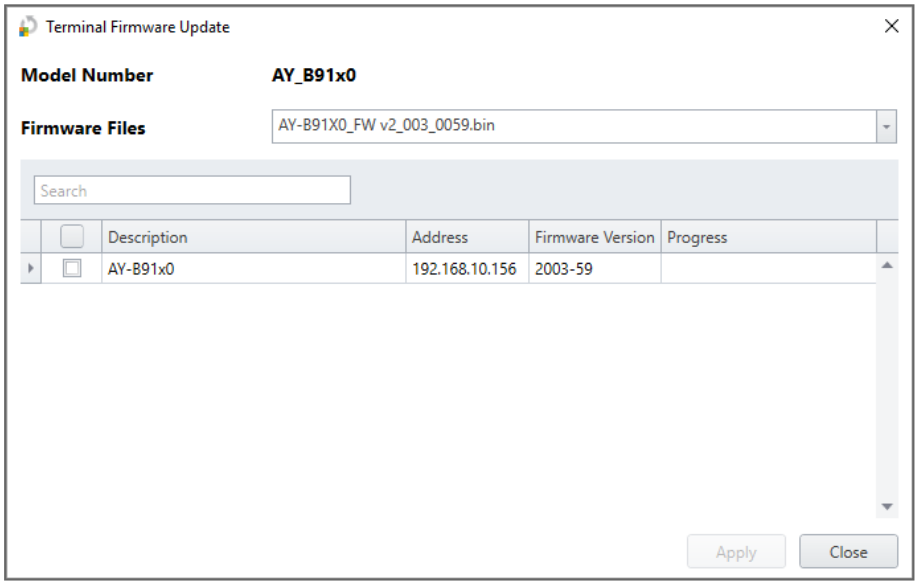


8.10.5. Terminal Firmware Update

To update the firmware:

> This function is available only for the 9000 Biometric series

1. In the tree view expand the **Biometrics > Terminals.**
2. Select a terminal.
3. On the toolbar click icon.



4. Check the terminal(s) from the list
5. Click **Apply**.
6. Wait till the process will finish and click **Close**.

8.11. Configuring the Doors

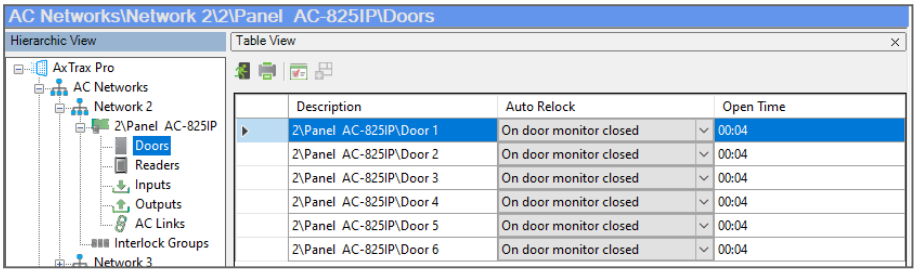
Each panel controls one to eight doors. Each door can be configured individually.

The **Door** window displays the following:

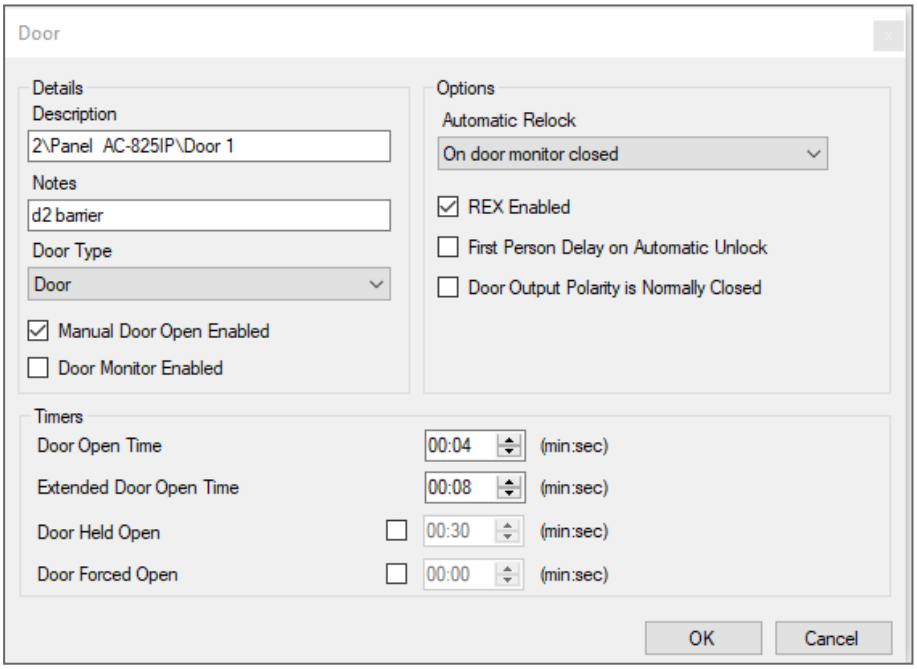
- The settings for unlocking and relocking
- The time available before the door relocks or records alarm events

To edit door properties:

1. In the Tree View, expand the **AC Networks** element.
2. Expand a network and expand a panel.
3. Select **Doors**.
4. Select a door in the Display Area.



5. On the toolbar, click the  icon.



6. Configure the door according to the fields described in the following table:

Field	Description
Description	Type a name for the door.
Notes	Type notes.
Door Type	Select the door type.
Automatic Relock	Select the event that causes the door to relock automatically.
REX Enabled	A Request-to-Exit unlocks the door for a user-defined duration. Select to allow REX for this door. The location of the door REX input depends on panel configurations; it can be seen in the Panel properties window.
First Person Delay on Automatic Unlock	Sets the door's behavior during an automatic unlock time zone. Select to require that during the selected time zone, the door remains locked until the first user opens it. The automatic unlock time zone is selected in Panel Links by selecting the output corresponding to that door (see Adding Panel Links).
Door Output Polarity is Normal Closed	Select to ensure Fail Safe door opening if the Fail Safe door lock device power fails. Once enabled, the door output relay is activated when the door is closed and is deactivated when the door is open. In this configuration, the Fail Safe lock device should be wired to the door relay N.O. (Normal Open) and COM (Common) terminals.
Manual Door Open Enabled	Select to allow operators to adjust the door manually (see Adding Panel Links).
Door Monitor Enabled	Select to monitor the door.
Door open time	Set the duration for which the door stays unlocked.
Extended door open time	Set the duration for which the door stays unlocked for users with Extended door open rights.
Door Held Open	Set the duration for which the door can be held open without raising an alarm event. Select to use this timer. For the Server application, the Pop-up and Snapshot section opens.  If this feature is enabled, then the Activity start delay (see Adding a Biometric Terminal) feature for that door must be set to 0.

Field	Description
Door Forced Open	Set the duration after which when the door is forced open, an event occurs. Select to use this timer. For the Server application, the Pop-up and Snapshot section opens. If this feature is enabled, then the Activity start delay (see Adding a Biometric Terminal) feature for that door must be set to 0.

7. Configure the door as required.
8. Click **OK**.

8.12. Adding Panel Links

Panel links are rules defining how the system should behave when events occur in the access control panel.

Numerous events and links can be defined. It is the operators' responsibility to avoid conflicting or non-logical definitions. Not all events that appear in the **Link** window are enabled in the panel; this too is the operator's responsibility to verify. Link condition operations should be checked after making any changes in the links definitions.

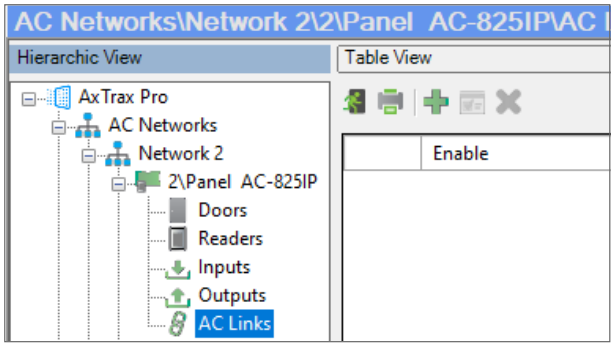
The **Link** window displays the following:

- An event on a panel and the panel component to which the link response applies
- The required input or output response
- Any alarm message to display on the current AxTraxPro Client computer

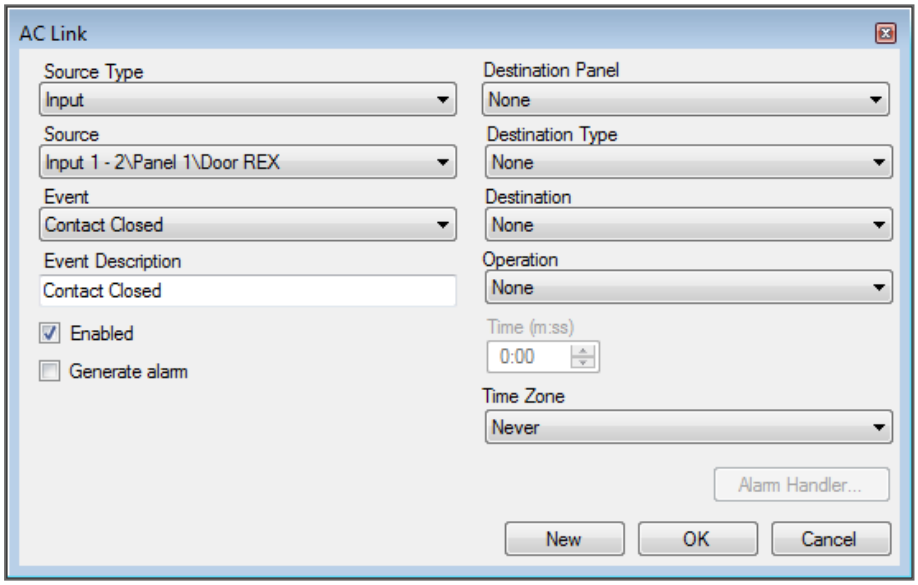
To create a panel link:

1. In the Tree View, expand the **AC Networks** element.
2. Expand a network and expand a panel.

3. Select **AC Links**.



4. On the toolbar, click the  icon.



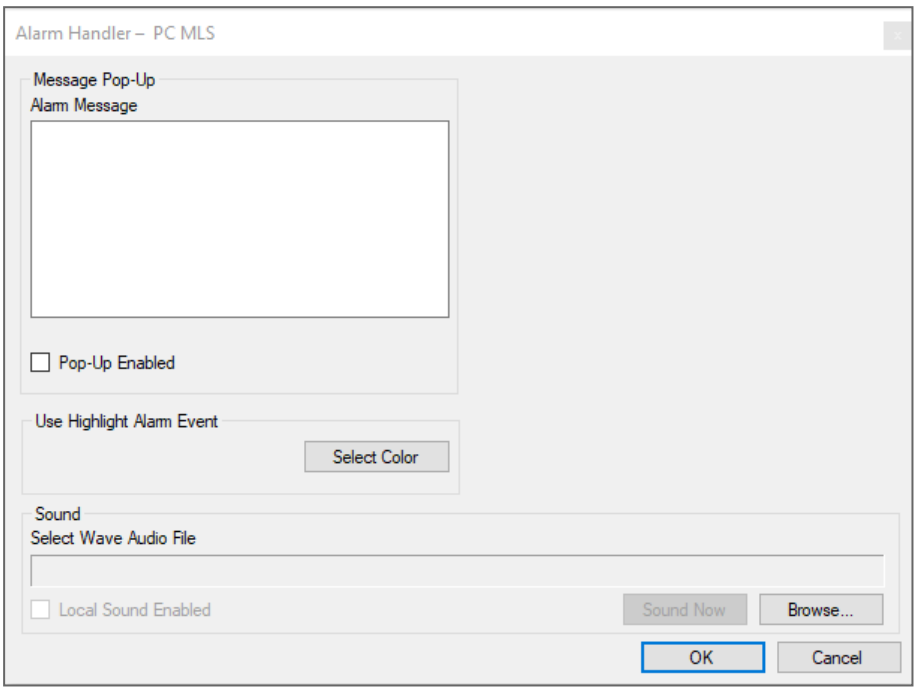
5. Configure the link rule as required according to the field descriptions in the following table:

Field	Description
Source Type	Select the panel component type which is the event source: • Input • Output • Reader • Door • Panel • Car parking
Source	Select the specific panel component that raises the event based on the source type selected. Up to 8 links can be created for each source type in the AC-225, AC-425, and AC-825IP panels. Up to 2 links can be created for each source type in an AC-215 panel.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Event</td><td>Select the event type for the panel component.
<table>
<tr><th>Input</th><th>Output</th><th>Reader</th><th>Door</th><th>Panel</th></tr>
<tr>
<td>• Contact Closed
• Contact Open
• Input Trouble
• Automatic Operation</td>
<td>• Output Active
• Output Idle
• Automatic Operation</td>
<td>• Access Granted - any user
• Access Denied - any code
• Bell Button
• Reader Tamper
• Access Denied - selected user
• Handicap
• Access Granted - selected user
• Output Group selected by user
• Timed Antipassback
• Door Antipassback
• Global Antipassback
• Duress Code
• Card + Card Mode</td>
<td>• Door forced open
• Door held open</td>
<td>• AC power fail
• Low Battery
• Case Tamper
• Battery not charging</td>
</tr>
</table></td></tr>
<tr><td>Event Description</td><td>Type the link or event description</td></tr>
<tr><td>Enabled</td><td>Select to enable the link rule</td></tr>
<tr><td>Generate alarm</td><td>Select to generate an alarm event in addition to the link rule activity</td></tr>
<tr><td>Destination Panel</td><td>From the network, select the board to be activated by the link rule trigger event</td></tr>
<tr><td>Destination Type</td><td>Select the panel component type, which is to be activated by the link rule trigger event</td></tr>
<tr><td>Destination</td><td>Select the specific panel component, which is to be activated by the link rule trigger event</td></tr>
<tr><td>Operation</td><td>Select the operation performed by the destination panel component</td></tr>
</table>

Field	Description
Time	Define a duration time frame for the operation. This box is only available when a time-bound operation is selected
Delay for the Target Operation	Select the delay time (in seconds) for the operation. This appears when **Destination Type** is specified.
Time Zone	Select the time zone for which the link rule applies
Alarm Handler	The Alarm Handler function is only enabled when **Generate Alarm** is selected. The Alarm Handler configuration window contains the following fields: • **Alarm Message:** Type a personalized message to be displayed on the screen as an alarm message when the selected event occurs • **Pop up Enabled:** Select to enable an alarm pop-up message • **Select Color button:** A color selection window opens allowing a color selection for the alarm message • **Browse… button:** Find and upload an audio wav file to be sounded when the selected event occurs • **Sound Now button:** After uploading the audio file click to button to hear the audio file • **Local Sound Enabled:** Select to enable sound for the alarm • **Fire Input Alarm:** Select to open all outputs, usually relevant for fire alarms In addition, when a camera is linked to a panel, the following fields appear in the window: • **Camera**: List of available cameras • **Options**: Which alarm is activated • **Opus Enabled**: Activates a pop-up to appear on the user's screen when alarm is triggered • **Close window options**: Can select **By timer** and specify the time, or Manually

6. [Optional] Set a general alarm:
   a. Select **Generate Alarm** to activate the **Alarm Handler** button.
   b. Click **Alarm Handler**.



   c. Configure the alarm handler as required.
   d. Click **OK** to return to the **Link** window.
7. Click **OK**.

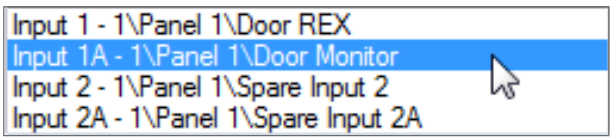
8.12.1. Global Triggering of Output Groups

Global triggering is used for cross panel activations. For example, in case of a fire alarm, all doors in the system are opened from a single input.

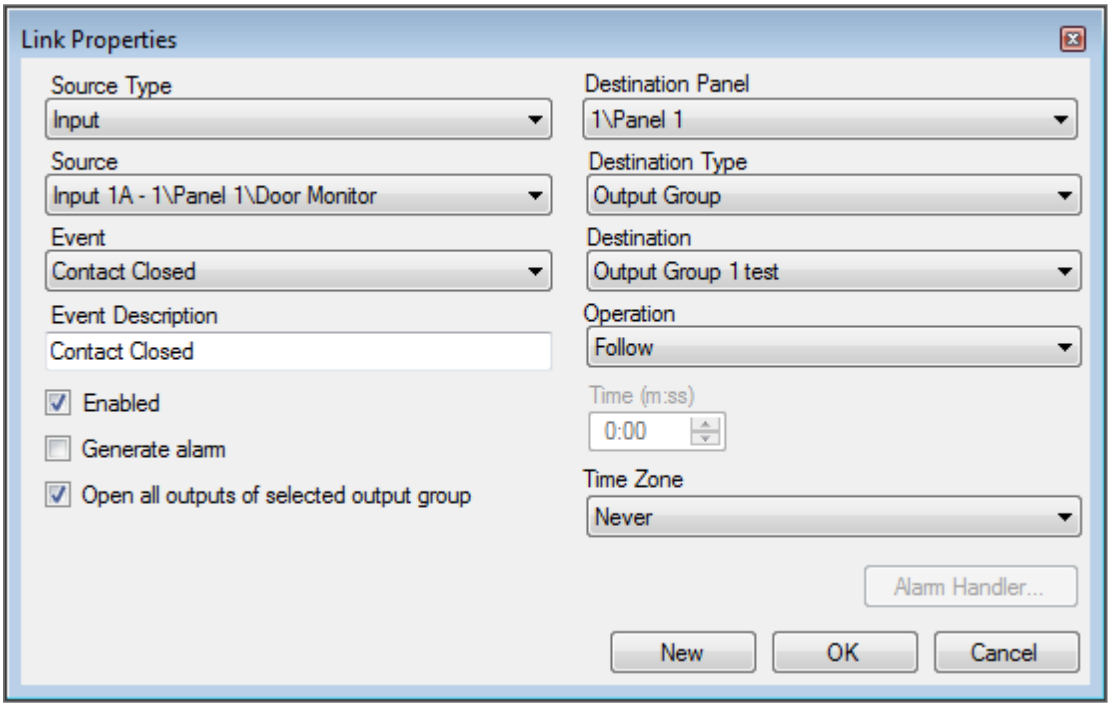
To create global triggering of output groups:

1. In the Tree View, expand the **AC Networks** element.
2. Expand a network and expand a panel.
3. Select **AC Links**.
4. On the toolbar, click the  icon.

5. Configure the link as follows:
   a. In **Source Type**, select **Input**.
   b. In **Source**, select either a Door Monitor or a Spare input.



   c. In **Destination Panel**, select the relevant panel.
   d. In **Destination Type**, select **Output Group**.
   e. Select **Open all outputs of selected output group**, which is now visible.



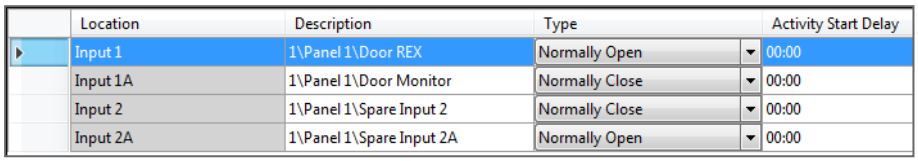
8.13. Configuring the Inputs

Each panel has four inputs. Using the MD-IO84 expansion board adds an additional eight inputs (a total of 12 inputs). Using the MD-D02 or MD-D04 expansion board adds four inputs (a total of 8 inputs). Some inputs are dedicated and have default functionality and some are for general purpose.

The table window displays the settings for each input. Input type is programmed individually, regardless of whether it is a dedicated input or for general purpose use.

To configure an input:

1. In the **Tree View**, expand the **AC Networks** element.
2. Expand a network and expand a panel.
3. Select **Inputs**.



	Location	Description	Type	Activity Start Delay
▶	Input 1	1\Panel 1\Door REX	Normally Open	00:00
	Input 1A	1\Panel 1\Door Monitor	Normally Close	00:00
	Input 2	1\Panel 1\Spare Input 2	Normally Close	00:00
	Input 2A	1\Panel 1\Spare Input 2A	Normally Open	00:00

4. Set the properties according to the field descriptions in the following table:
5. Select the type of input to be monitored as shown below.

Field	Description
Type	Select the type of input to be monitored. • **Normally Open/Close:** An input either in an open or closed state • **Normally Open/Close 1 Resistor:** An input in an open, closed, or trouble state. This option is only available for supervised inputs. • **Normally Open/Close 2 Resistors:** An input in an open, closed, or trouble state, with additional checks for short-circuit and open-circuit tampering. This option is only available for supervised inputs. For more information, refer to the access control panel's hardware manual.

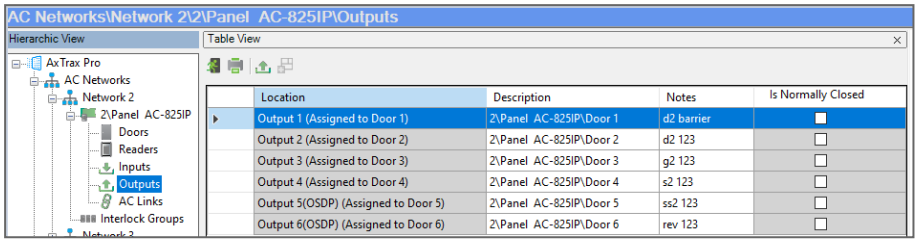
8.14. Controlling Outputs Manually

The Manual Output Operation window allows an operator to open or close a selected group of outputs on a panel directly.

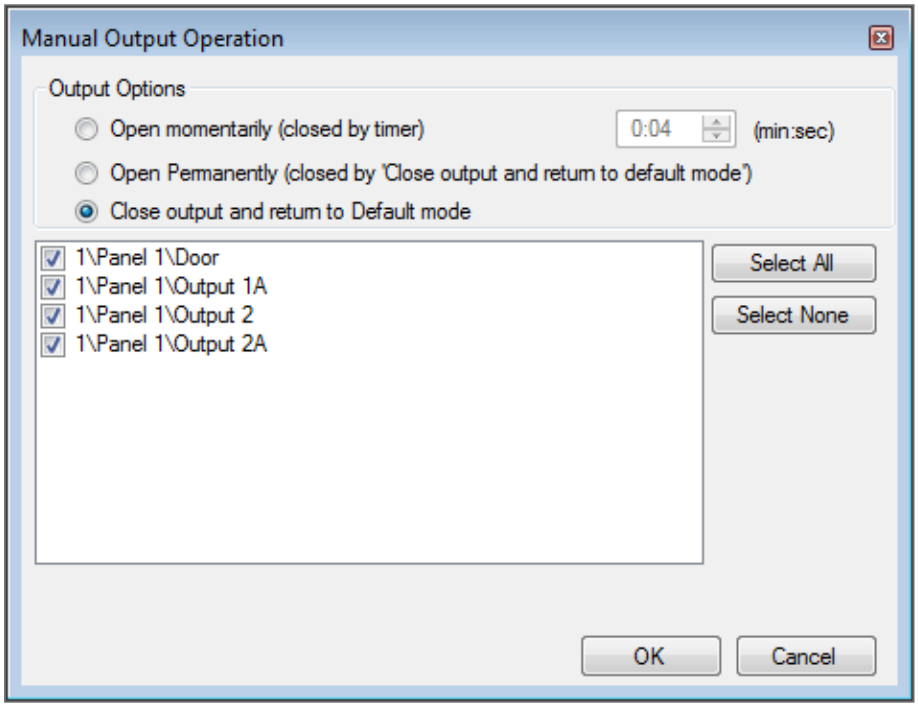
To manually open or close an output:

1. In the **Tree View**, expand the **AC Networks** element and expand a selected network.

2. Select a panel.



3. On the toolbar, click the  icon.



4. Select an option:
   - **Open momentarily** – Opens all selected outputs for the time set in the timer box.
   - **Open permanently** – Opens all selected outputs.
   - **Close output and return to default mode** – Closes the selected outputs and returns control to default.
5. Select the check boxes of the outputs to which to apply the operation.
6. Click **OK**.

9. Managing Groups

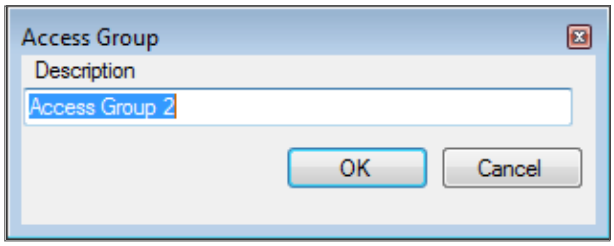
You can create access groups and areas, as well as input and output groups to be used by the system to create automated rules.

9.1. Adding Access Groups

An access group includes a list of door readers and the time zones during which each of those door readers are available for access. Every user is assigned to an access group.

To add an access group:

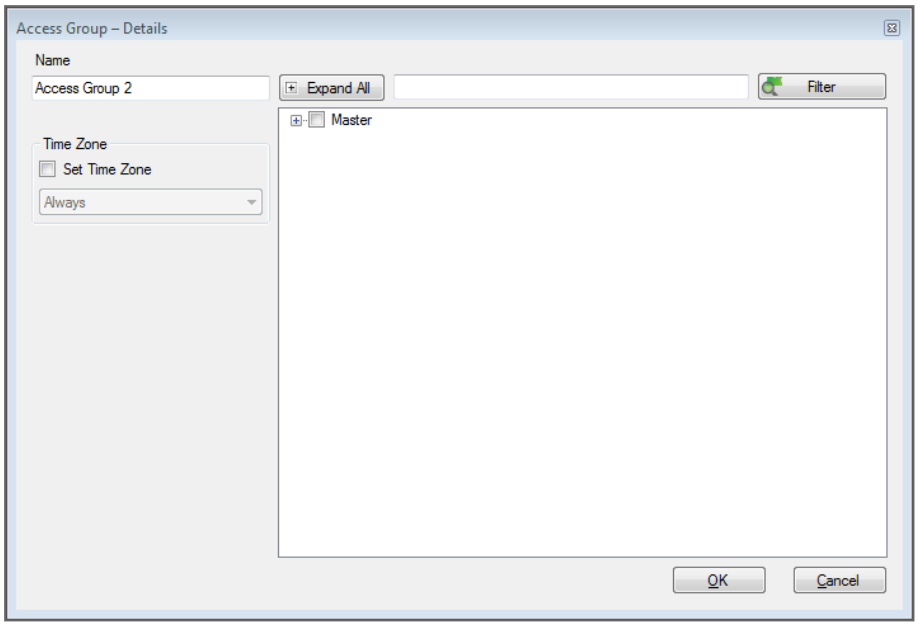
1. In the Tree View, expand the **Groups** element.
2. Select **Access Groups**.
3. On the toolbar, click the  icon.



4. In the **Description** field, enter a name for the access group and click **OK**.

   The new access group appears in the **View Tree**.

5. Select the access group from the View Tree and click the icon.



6. Select the **Set Time Zone** check box.

   From the **Time Zone** drop down, select a time.
7. Expand the list and select the desired readers.
8. Click **OK**.

   The window closes and the new access group appears in the Display Area.

9.2. Adding Access Areas

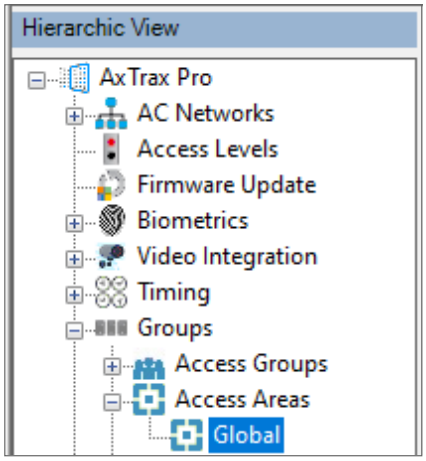
A large site can be divided into several smaller, more manageable access areas. Reports can be produced individually for each area. In addition, global Antipassback rules can be applied for each access area. When global Antipassback rules are in effect, users cannot re-enter an access area until they have left it.

Use the **Access Area** window to add entry and exit door readers to and from an area within the facility.

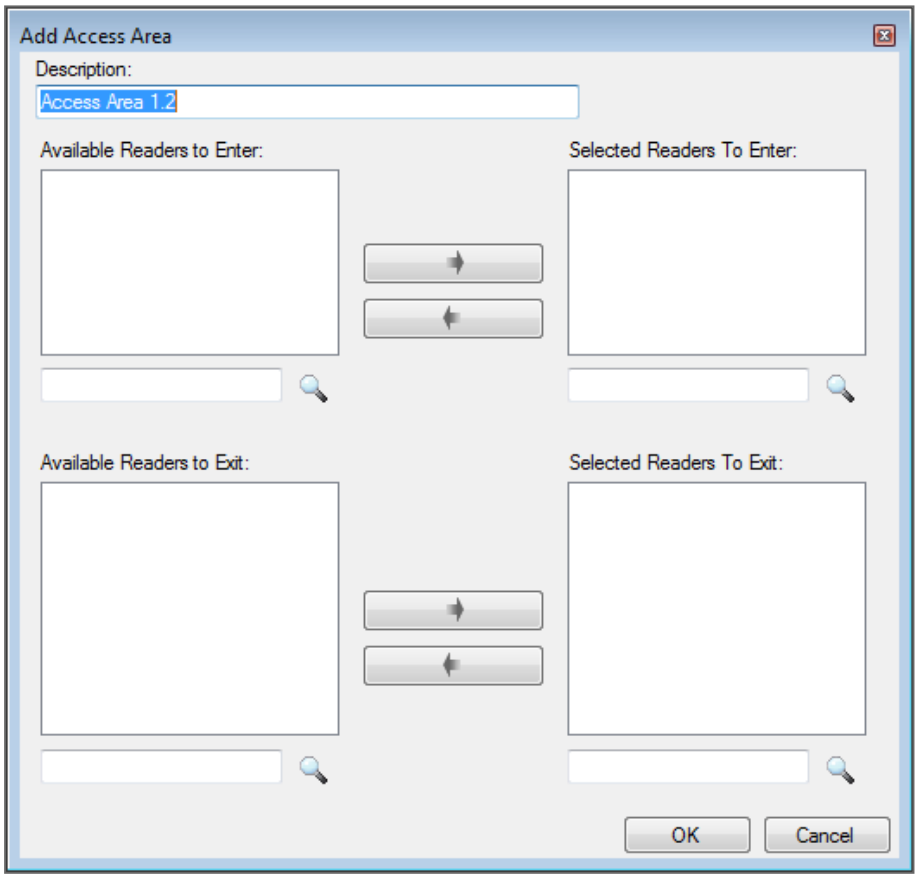
To add an access area:

1. In the **Tree View**, expand the **Groups** element.

2. Expand the **Access Areas** element and click **Global**.



3. On the toolbar, click the  icon.



4. In the **Description** field, enter a name for the access area.
5. Select and move the desired readers from **Available Readers to Enter** to **Selected Readers to Enter** using the arrows.
6. Select and move the desired readers from **Available Readers to Exit** to **Selected Readers to Exit** using the arrows.
7. Click **OK**.

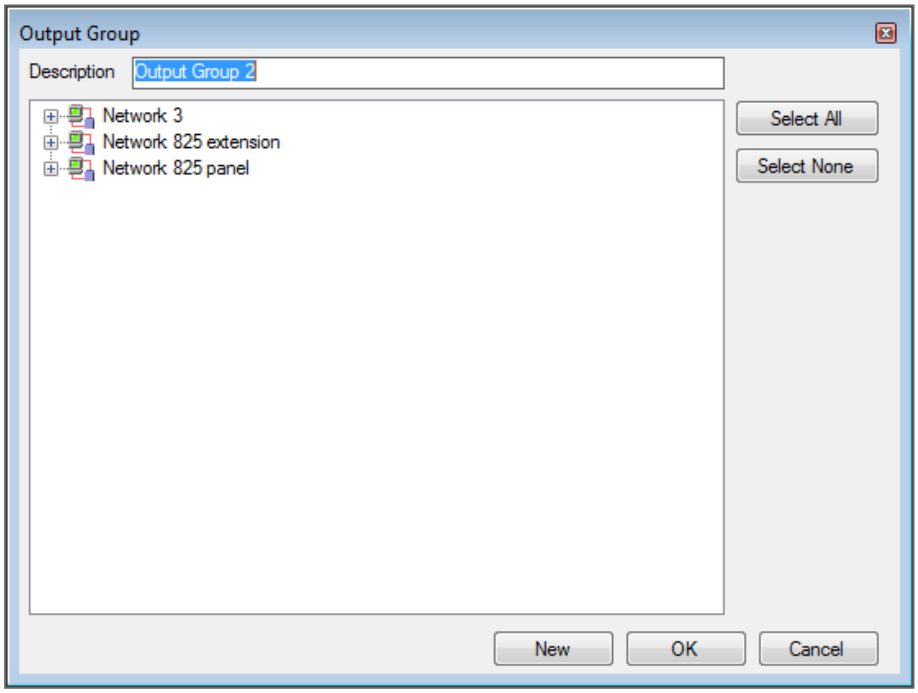
   The window closes and the new access areas appear in the **Display Area**.

9.3. Adding Output Groups

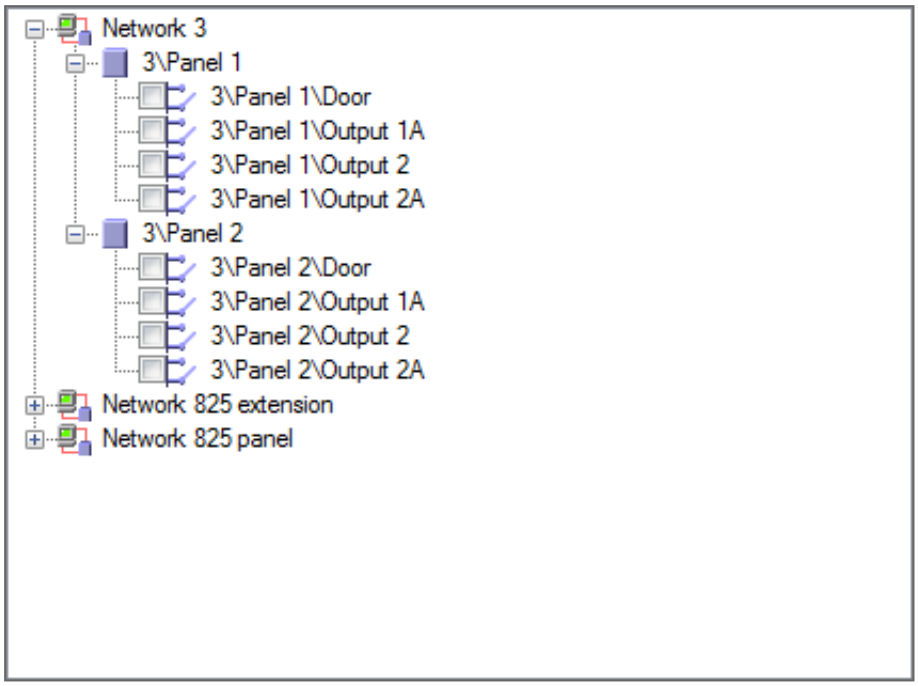
Output groups are a collection of outputs from panel that can be used in panel links to perform advanced operations, such as elevator control.

To add an output group:

1. In the Tree View pane, expand the **Groups** element.
2. Select **Outputs Groups**.
3. On the toolbar, click the  icon.



4. In the **Description** field, enter a name for the input group.
5. Expand a network to see its panels.



6. Select the check boxes of all relevant outputs. You can also use **Select All**.
7. Click **OK**.

   The window closes and the new output group appears in the Display Area.

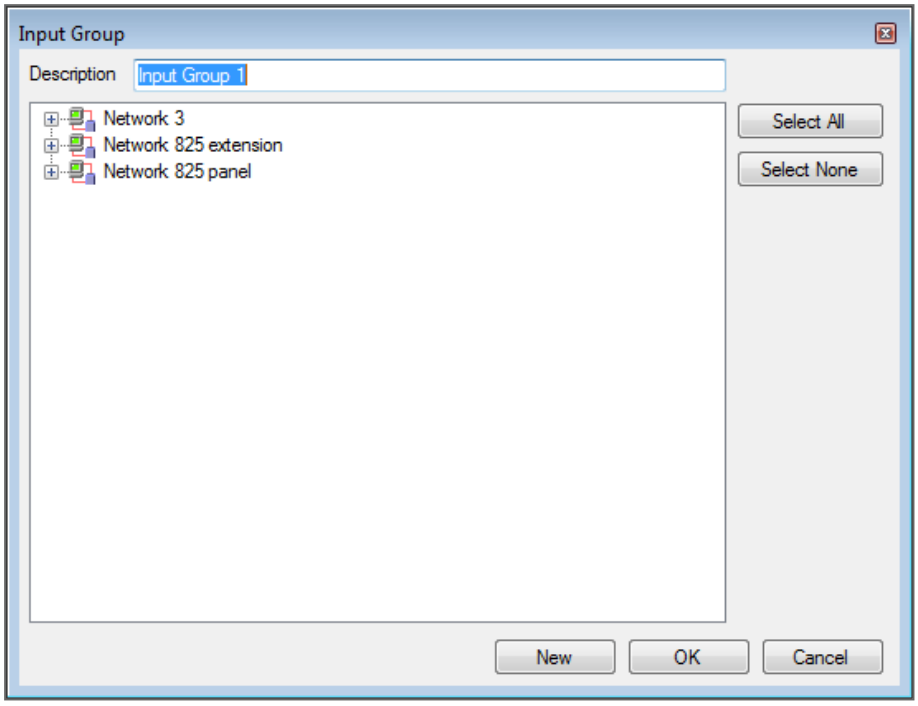
9.4. Adding Input Groups

Input groups are a collection of inputs from one or more panels that can be used in panel links to perform advanced operations.

To create an input group:

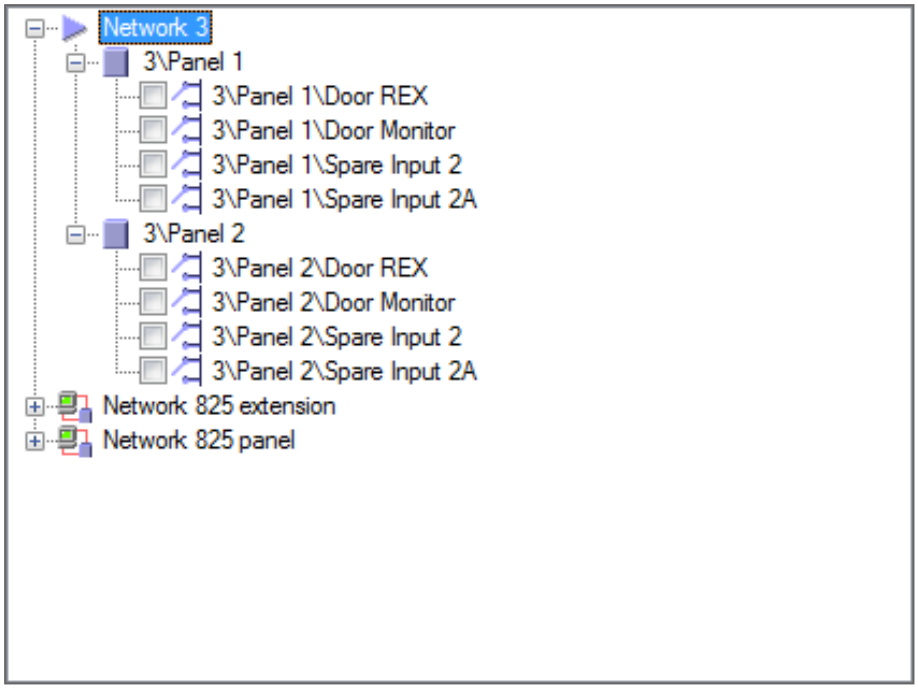
1. In the Tree View, expand the **Groups** element.
2. Select **Inputs Groups**.

3. On the toolbar, click the icon.



4. In the **Description** field, enter a name for the input group.

5. Expand a network to see its panels.



6. Select the check boxes of all relevant inputs. You can also use **Select All**.
7. Click **OK**.

   The window closes and the new input group appears in the Display Area.

9.5. Adding Global Antipassback Rules

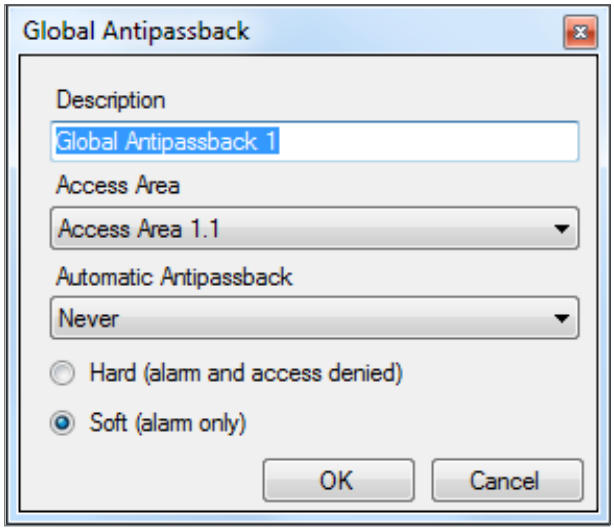
Global antipassback functionality is only enforced when the AxTraxPro Server is connected and monitoring the entire access control system.

A global antipassback rule can only be added if an access area has previously been defined (see Adding Access Areas).

To create antipassback rules:

1. In the Tree View, click **Global Antipassback**.

2. On the toolbar, click the icon.



3. In the **Description** field, enter a name for the antipassback rule.
4. From the **Access Area** drop down, select the access area.
5. From the **Automatic Antipassback** drop down, select the time zone for which the global antipassback applies.
6. Select either the **Hard** or the **Soft** Antipassback option.
7. Click **OK**.

   The window closes and the global antipassback rule appears in the Display Area.

Global Antipassback applies an Antipassback event only on "Enter" readers to the defined "Area".

To implement Antipassback on Exit readers as well, you must define a new area with opposite reader directions:

Readers defined "Enter" in the first area need to be defined again in the new area as "Exit" readers, and "Exit" readers in the first area should be defined as "Enter" readers in the second area.

9.6. Managing Lockdowns

9.6.1. Adding Lockdown Groups

A lockdown group includes a list of doors which will be locked and the operators who administer and control the lockdown.

During a lockdown, the doors in the lockdown group can only be opened by immuned users.

A lockdown can only occur when the AxTraxPro server is connected and monitoring the entire access control system.

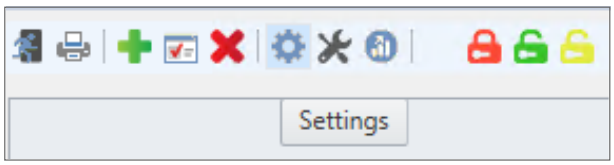
A lockdown operation can only be used with AC-825IP panels.

The AC-825IP network must be specified before a lockdown group can be added.

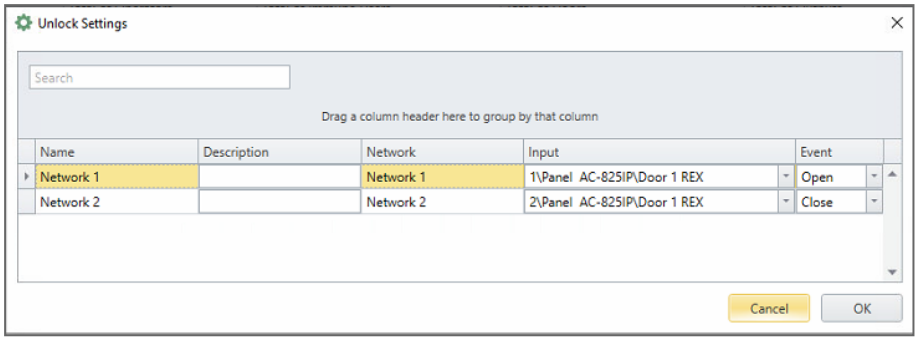
Setting AC-825IP Network Input:

Each AC-825IP network on the lock down must have a specified input for manual override of an active lockdown.

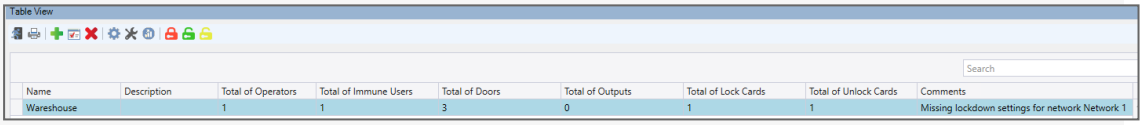
1. From the Table view, select the Settings icon from the toolbar.



2. Select the **Network**, **Input**, and **Event** for physical unlock settings.

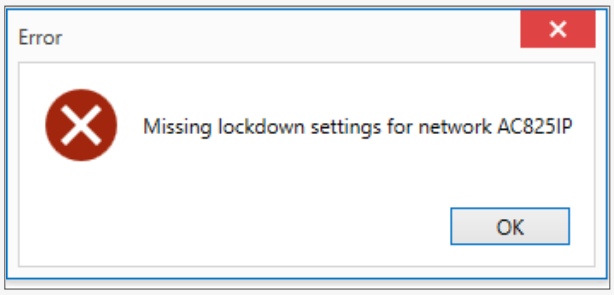


An input must be selected before you can configure the lockdown group. If an input is not selected, the group cannot be activated.



3. Click **OK**.

The following message is shown if the AC-825IP network settings have not been configured.

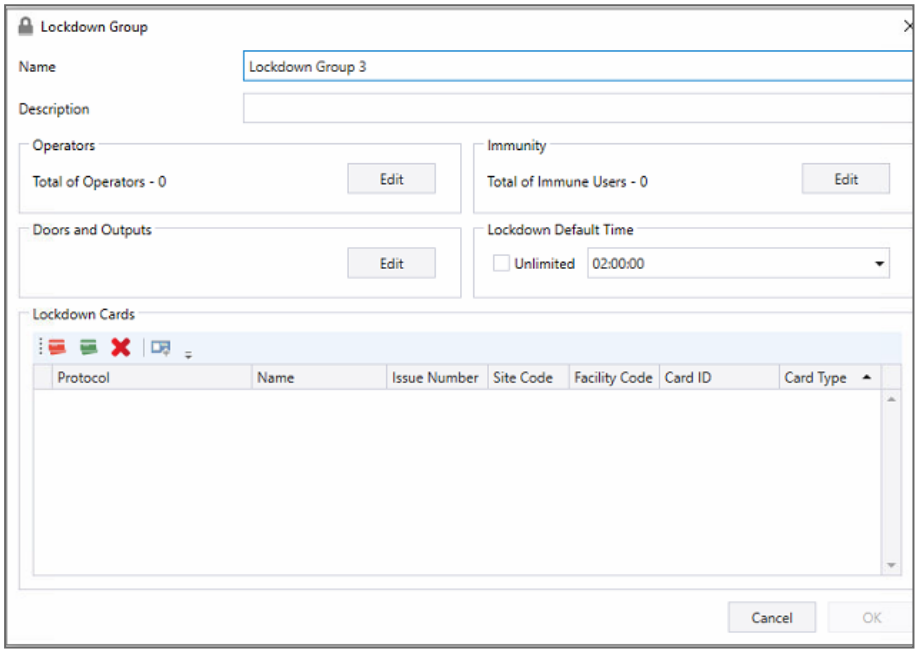


During a lockdown if a communication failure occurs the lockdown can be canceled from a manual override. An example of a manual override is a button.

9.6.1.1. Adding a Lockdown Group to a Tree

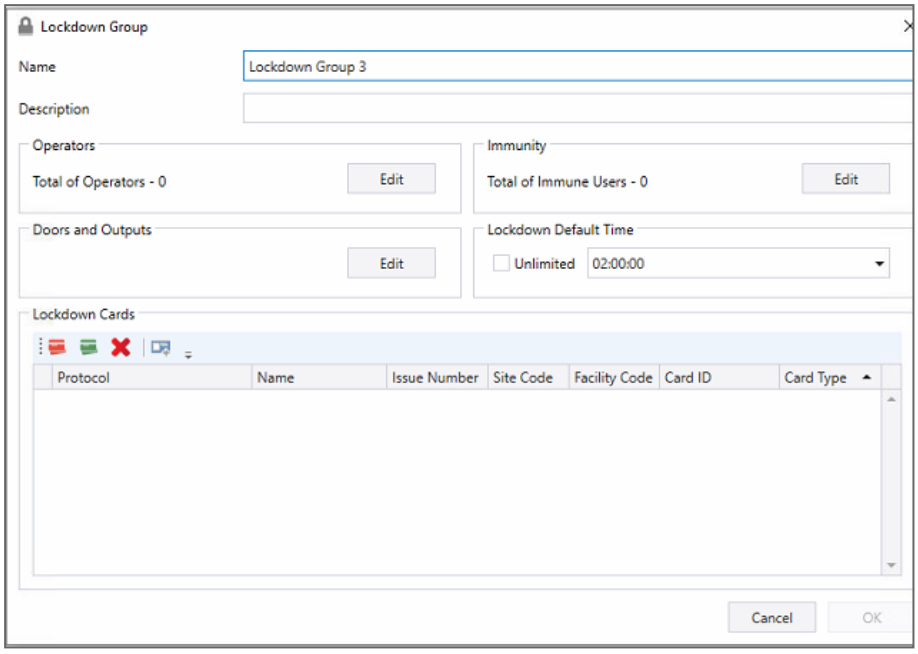
To add a lockdown group:

1. In the Tree View, expand the **Groups** element.
2. Select **Lockdown Groups**.
3. On the toolbar, click the icon.



4. Type a name and description for Lockdown group in the appropriate fields.
5. To add operators to group, see Add/Edit Operators within Lockdown Group.
6. To add doors and outputs to group, see Add/Edit Doors and Outputs within Lockdown Group.
7. To add immune users to group, see Add/Edit Immunity Users within Lockdown Group.
8. To add a new lockdown card to group, see Add New Lock or Release Card to Lockdown Group.
9. To add an existing lockdown card to group, see Add Existing Lockdown Card to Lockdown Group.

10. To add lockdown time, type or select the time in **Lockdown Default Time**.



The default lockdown parameters are:

- Operators - 0
- Immune users - 0
- Lockdown default time - 2:00 hours

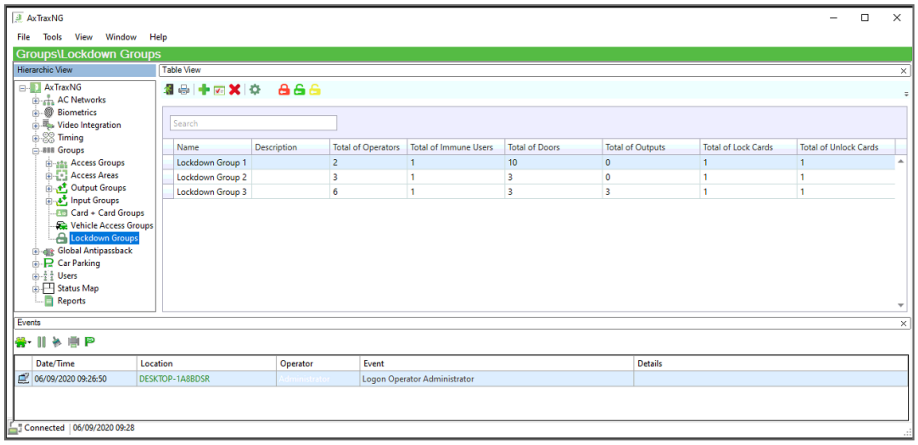
11. Click **OK**.

    The new lockdown group appears in the Table View.

9.6.1.2. Edit Lockdown Group Properties

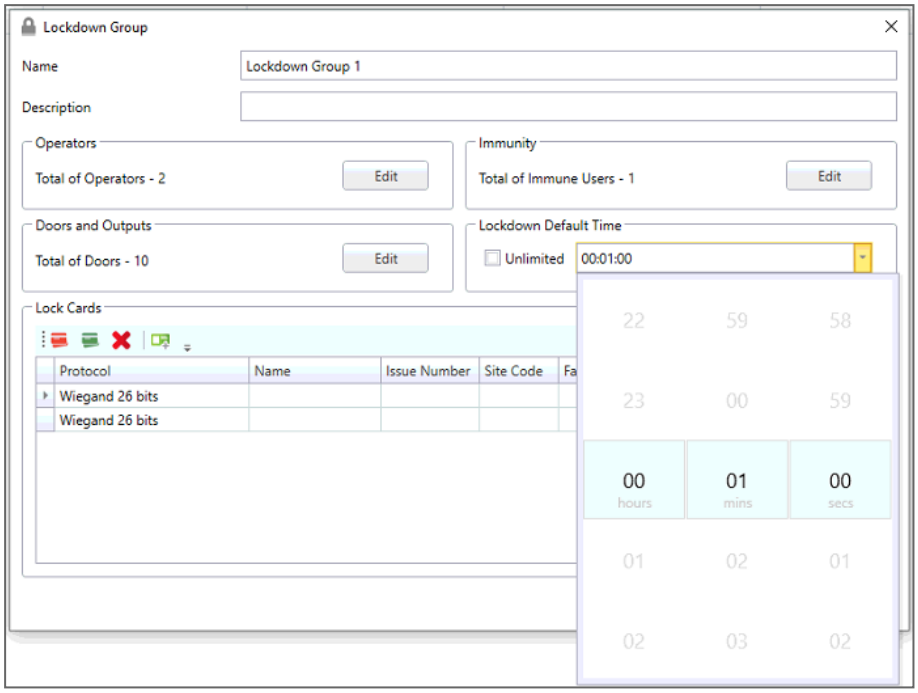
To edit lockdown group properties:

1. In Table View, select the lockdown group to be edited.



2. Select  (edit group) from menu bar.
3. If required, edit the group **Name** or **Description**.
4. The number of operators defined in the group is shown. To change, click **Edit** (see Add/Edit Operators within Lockdown Group).
5. The number of doors and outputs defined in the group is shown. To change, click **Edit** (Add/Edit Doors and Outputs within Lockdown Group).
6. The number of immune users defined in the group is shown. To change, click **Edit** (see Add/Edit Immunity Users within Lockdown Group).
7. The lock cards defined in the group is shown. To add new lockdown card to group, see Add New Lock or Release Card to Lockdown Group.
8. To add an existing lockdown card to group, see Add Existing Lockdown Card to Lockdown Group.

9. To change the lockdown time, type or select the time in **Lockdown Default Time**.



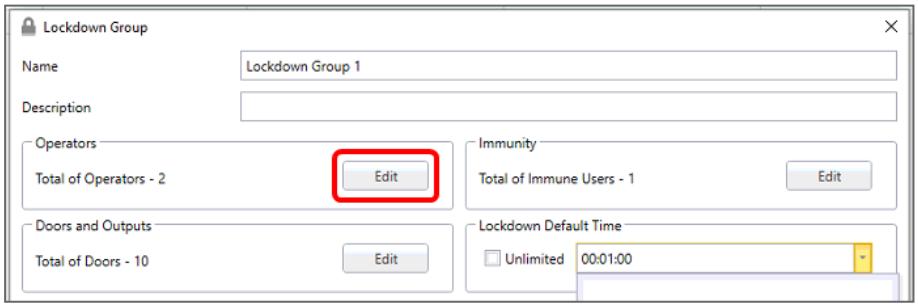
10. Click **OK.**

9.6.1.3. Add/Edit Operators within Lockdown Group

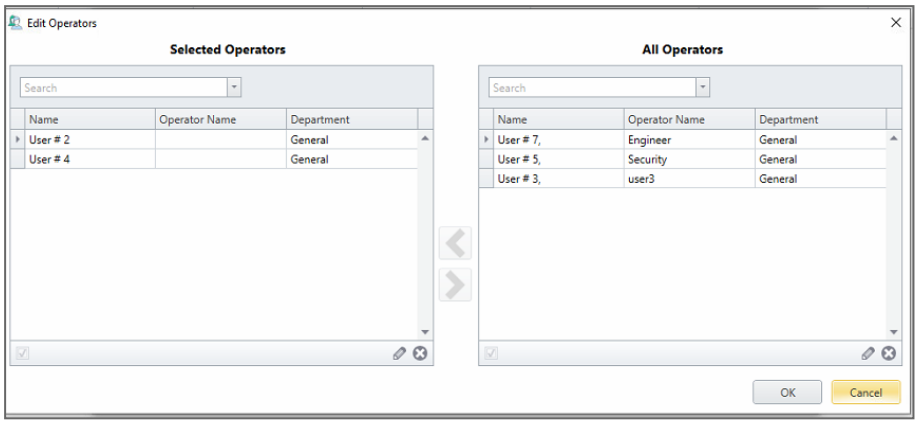
To add/edit operators within a lockdown group:

Only operators with read/ modify rights to lockdown can be added.

1. In group properties window, click **Edit** near **Operators**.



2. To add operators to the group, select the required operators in the right table and click the upper arrow to move them to the list of the left. To remove operators, do the reverse.

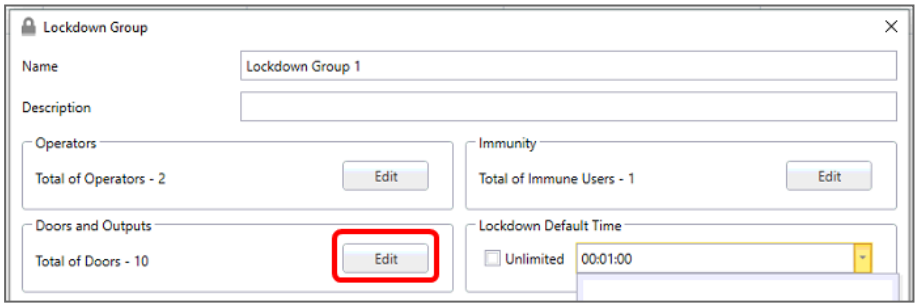


3. After completing all changes, click **OK**.

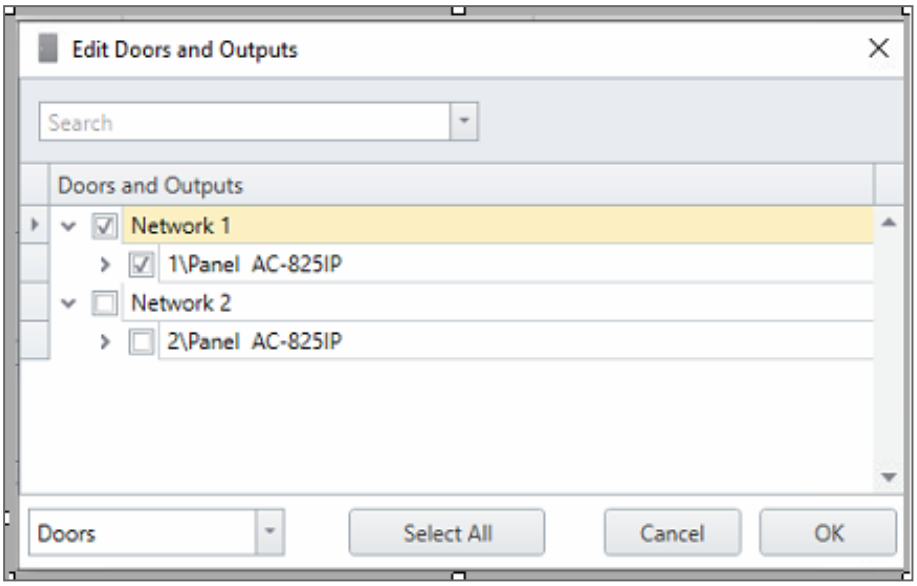
9.6.1.4. Add/Edit Doors and Outputs within Lockdown Group

To add/edit Doors and Outputs within a lockdown group:

1. In group properties window, click **Edit** near **Doors and Outputs**.



2. To change doors selection, select **Doors**. To change output selection, select **Outputs**. Check/uncheck doors or outputs to be added/removed from group.



3. After completing all changes, click **OK**.

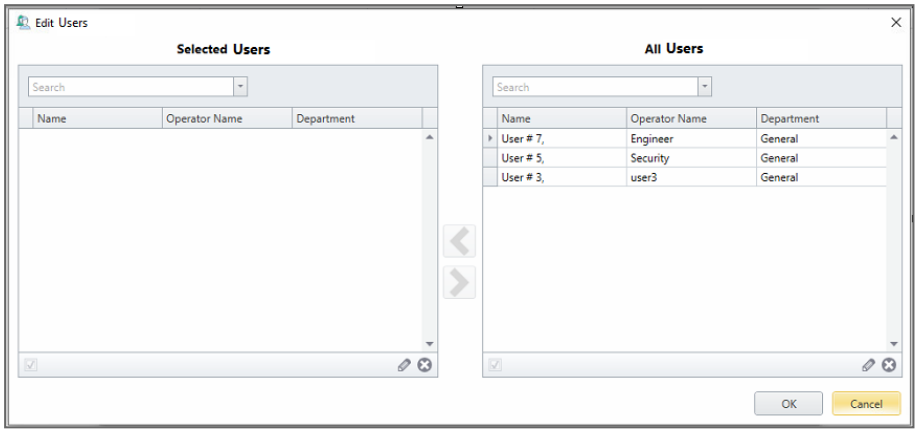
9.6.1.5. Add/Edit Immunity Users within Lockdown Group

Immune users are the users that can open doors during a lockdown.

A list of immune users must be selected for each lockdown group independently. There is no global user immunity for lockdown groups.

To add/edit immune users within a lockdown group:

1. In group properties window, click **Edit** near **Immunity**.



2. To add immune users, select the required users in the right table and click the upper arrow to move them to list on the left. To remove users, do the reverse.
3. After completing all changes, click **OK**.

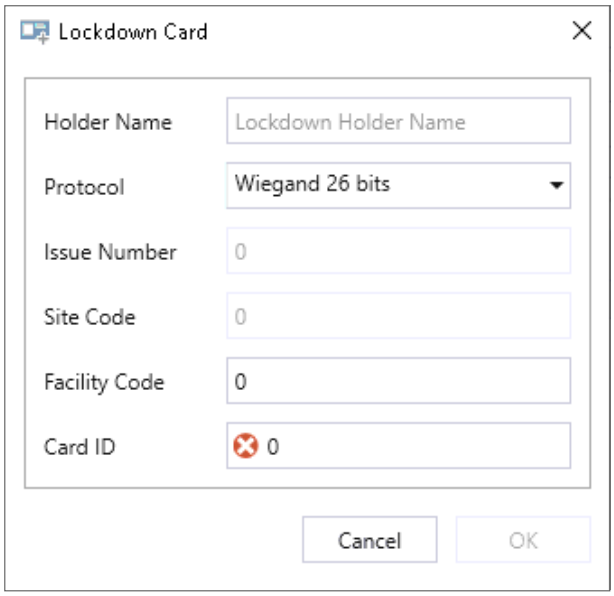
9.6.1.6. Add New Lock or Release Card to Lockdown Group

You must define at least two lockdown cards. One lockdown card will initiate a lockdown and the other lockdown card will release a lockdown. The cards should be stored in a safe location to be used in emergencies. A lockdown card can be shared between different users.

To add a new lockdown card to a lockdown group:

You cannot use an existing card in the system to make a new lockdown/release card.

1. To add new lockdown cards to the group, select for a lock card or for an unlock card.



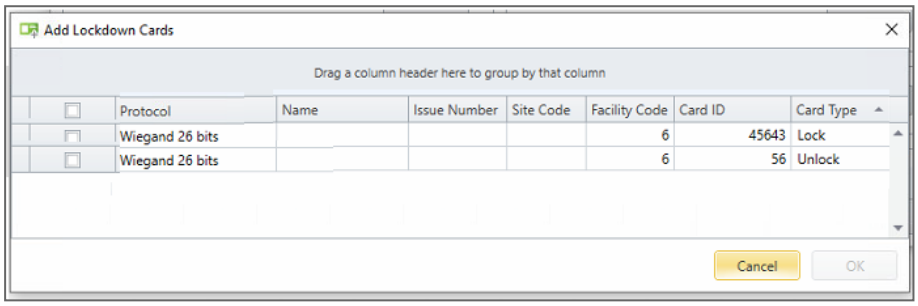
2. For each new lockdown card to be added, enter the required configuration for the card in the following fields:
   - Name
   - Protocol
   - Issue Number
   - Site Code
   - Facility Code
   - Card ID
3. After completing all changes, click **OK**.

9.6.1.7. Add Existing Lockdown Card to Lockdown Group

To add an existing lockdown card to lockdown group:

1. To add an existing lockdown card to the group, click  in the toolbar.

   The *Add Lockdown Card* window displays the existing cards.



2. Select the cards to be added to the Lockdown group and click **OK**.

9.6.2. Using Lockdown Groups

Lockdown group operations can be controlled in the following ways:

1. Using specially configured access cards to initiate or release a lockdown.

> A lockdown can be initiated with a lockdown card or with the AxTraxPro Management Software client on all readers in the system.

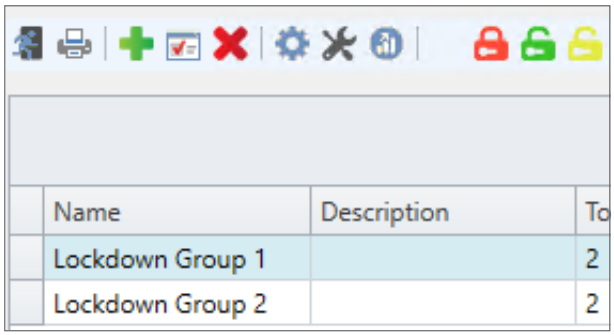
> Each time a lockdown card initiates a lockdown, the lockdown timer will reset and start to count again. The default lockdown time is 2 hours.

> During a lockdown, the specified doors and outputs set in the lockdown can only be opened by immuned users, from a lockdown bypass, or by an authorized operator.

1. Using AxTraxPro Management Software.

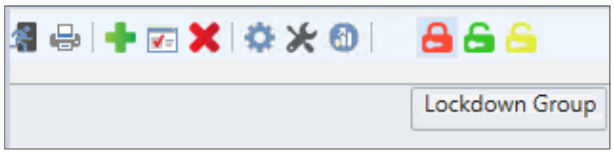
To manually initiate lockdown with the AxTraxPro Management Software:

1. From the Table view, select the desired lockdown group.

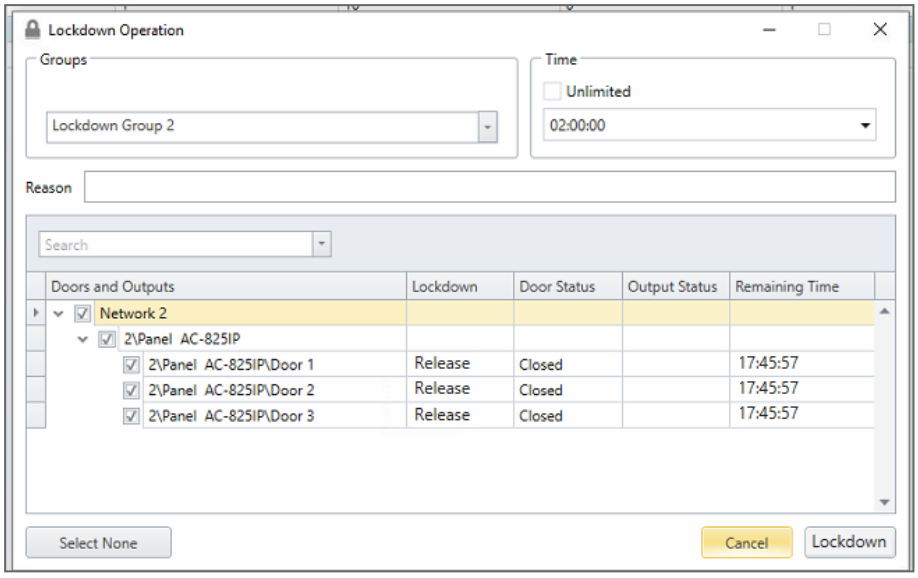


When a lockdown group is not shown in a color the lockdown group is open.

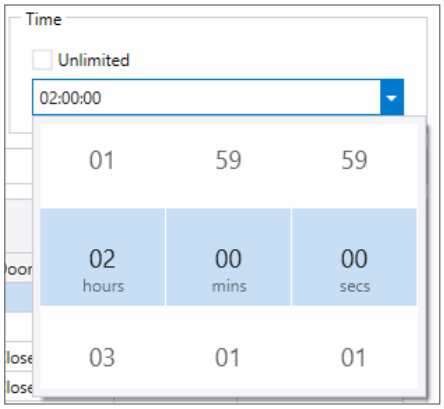
2. Click the **Lockdown Group** icon.



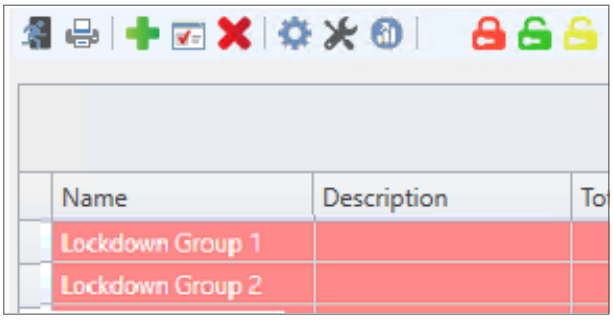
3. Check/uncheck the doors to be locked.



4. To set the lockdown time, clear the **Time** check mark next to **Unlimited** andselect the time.



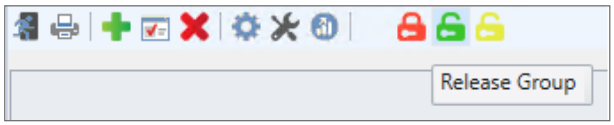
5. Click **Lockdown**.



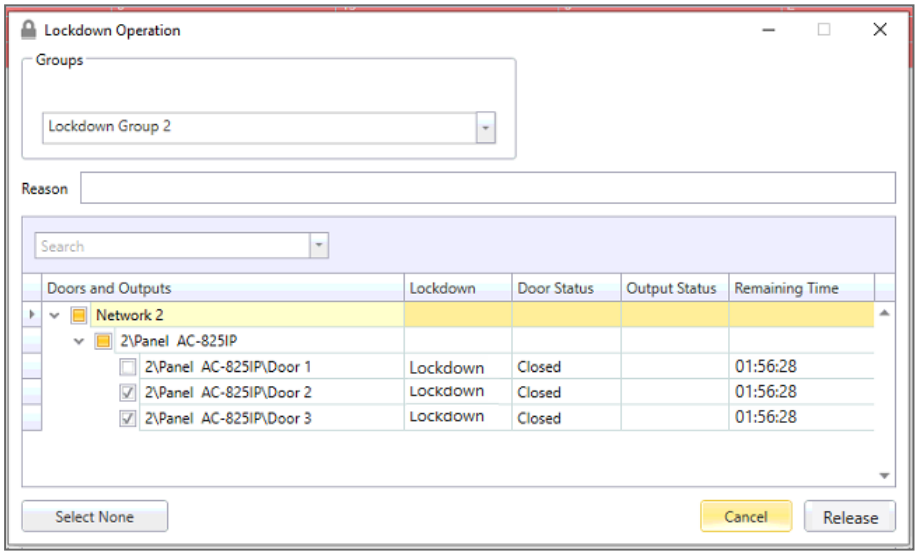
When a lockdown group is highlighted in red all doors all of the lockdown group are locked.

To disable a lockdown and release specified door(s) with the AxTraxPro Management Software:

1. From the Table view, select the desired lockdown group and click the **Release Group** icon.



2. Check/uncheck the doors to be open.

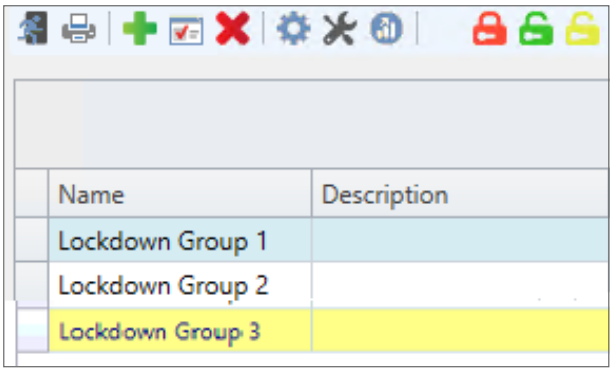


3. Click **Release**.
4. Click **Yes** to release the lockdown



or

5. Click **No** to cancel the lockdown release.

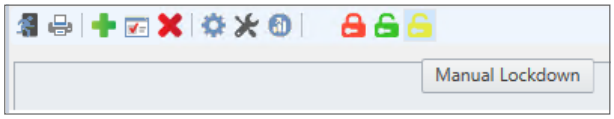


When a lockdown group is highlighted in yellow only a some of the doors in the lockdown group are locked.

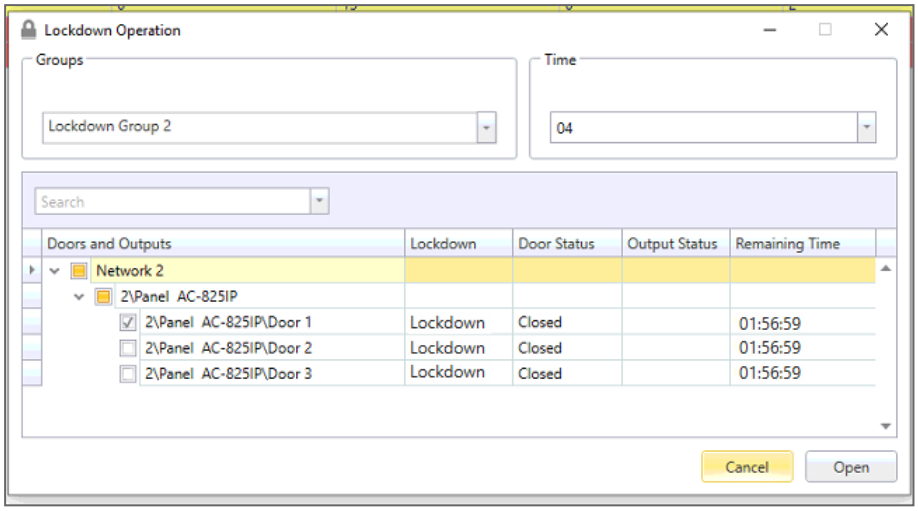
To manually bypass a lockdown for a specified time period and for only one specified door with the AxTraxPro Management Software:

This step will let users with authorized access permission to open a door and exit.

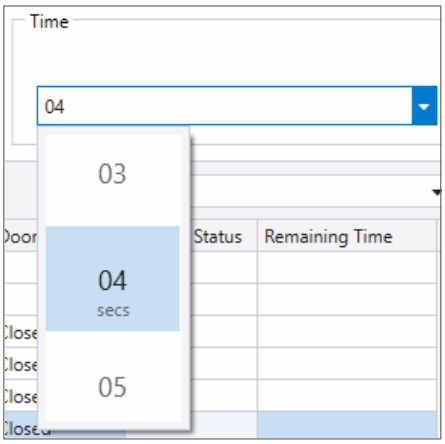
1. From the Table view, select the desired lockdown group and click the **Manual Lockdown** icon.



2. Check/uncheck the door to be open.



3. Type or select the time.

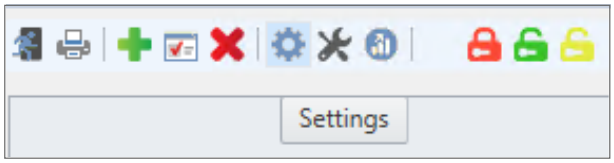


The time value is in seconds.

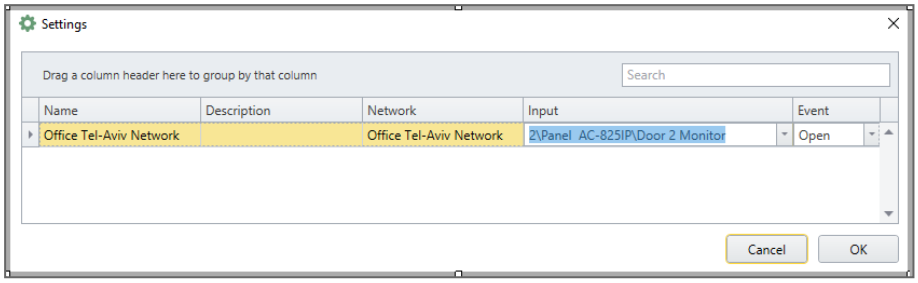
4. Click **Open**.

To define an event that automatically initiates lockdown:

1. From the Table view, select the desired lockdown group and click the Settings icon from the toolbar.



2. Select the **Input** and **Event** that will initiate lockdown for that group.

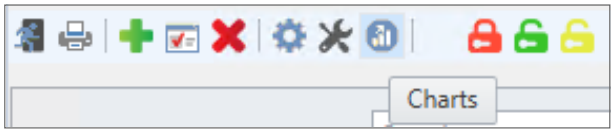


3. Click **OK**.

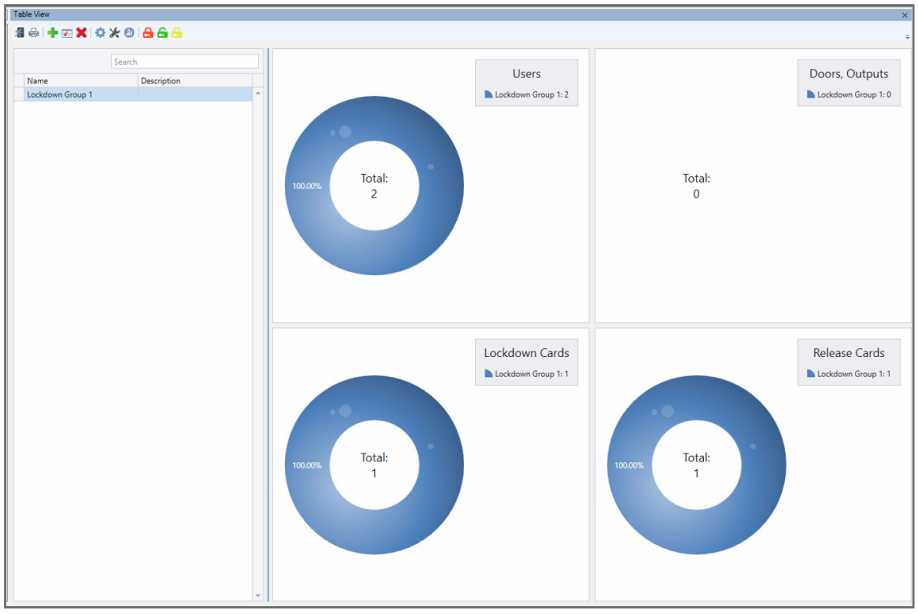
Each AC-825IP network must have specified lockdown **Inputs**.

To see a chart of the lockdown:

1. Click the **Charts** icon.

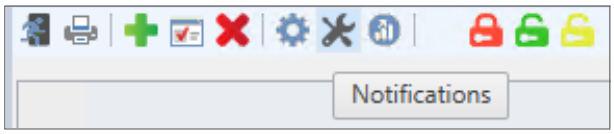


2. To close the chart, click the icon.

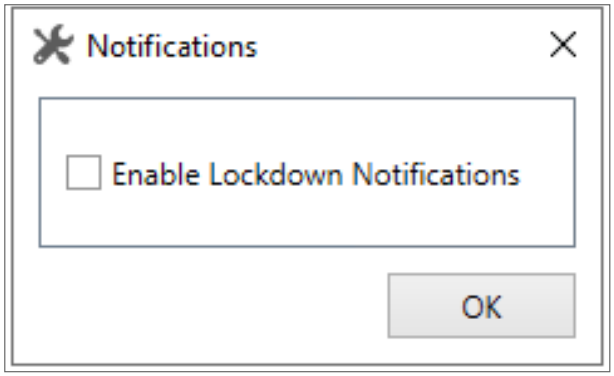


To receive a notification about a lockdown:

1. Click the **Notification** icon.



2. Select the **Enable Lockdown Notifications** check box.



3. Click **OK**.

9.7. Defining Card + Card Groups

Card + Card mode is a secure mode that requires two card holders (users) to grant access to a particular reader.

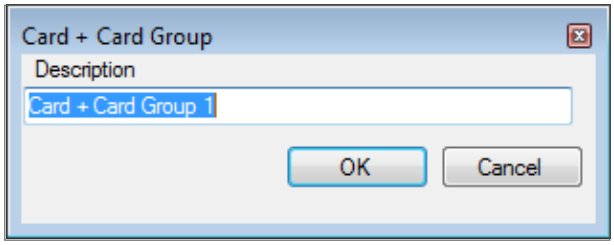
This feature is not available for AC-215 access control panels.

9.7.1. Adding a Card + Card Group

First, you must add a Card + Card group.

To add a Card + Card group:

1. In the Tree View pane, expand the **Groups** element.
2. Select **Card + Card Groups**.
3. On the toolbar, click the icon.



4. In the **Description** field, enter a name for the input group.
5. Click **OK**.

The window closes and the new Card + Card group appears in the Display Area.

9.7.2. Adding Users to a Card + Card Group

Once a Card + Card group is created, you must add users to it.

To add users to a Card + Card group:

1. In the Tree View, expand the **Departments/Users** element and select a department that contains the users you wish to add to the Card + Card group.
2. Select a user in the Display Area.
3. On the toolbar, click the  icon.
4. On the **General** tab of the **User Properties** window, select the Card + Card group from the **Card + Card Group** drop down.
5. Click **OK**.
6. Repeat this process for each user you wish to add to a particular Card + Card group.

9.8. Vehicle Access Groups

The Vehicle Access Group is used for defining cars for LPR.

The functionality will be discussed in future versions of the manual.

9.9. Adding Car Parking

The Car Parking management option allows you set up groups that have limited number of users who can access a particular area. For example, a parking lot that serves several companies and each company has a specified number of parking spots. With this option, we can set up each company's limit and when the limit is reached, access is no longer granted. This feature is counter based that keeps track of the number of users in a specified area.



This feature is not available to AC-215 access control panels.

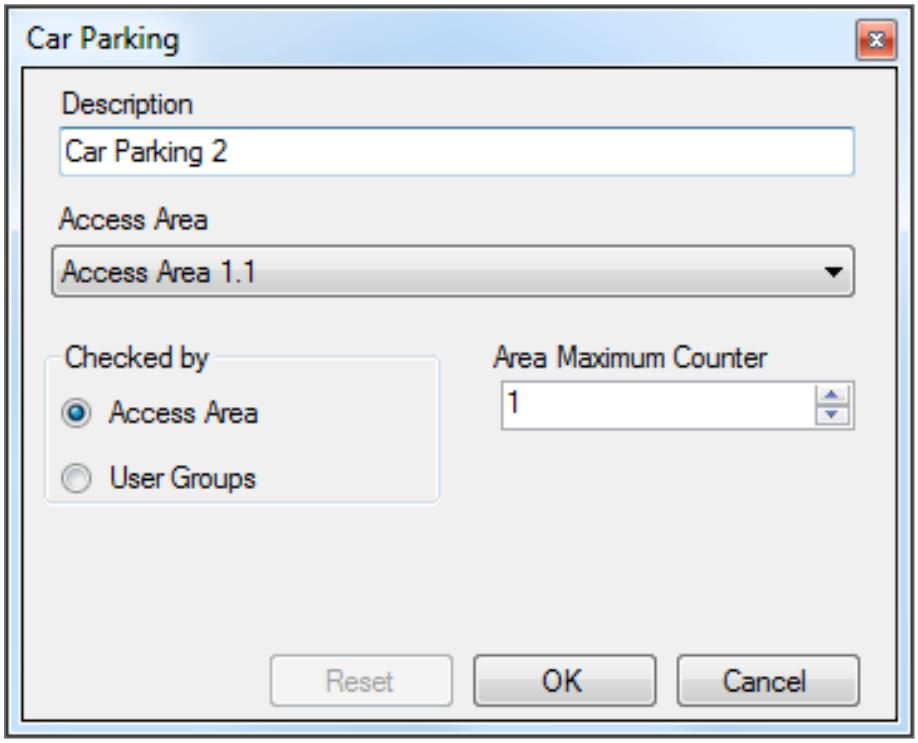


Only one car park area can be added per panel.

A car parking area can only be added if an access area has previously been defined (see Adding Access Areas).

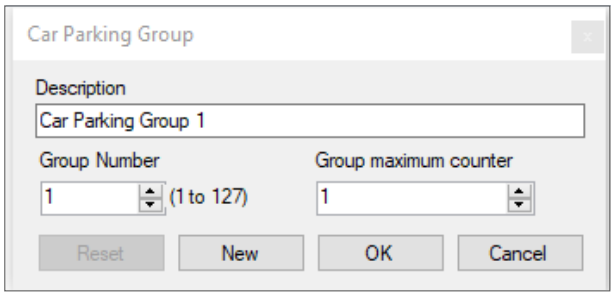
To define a car parking area:

1. Create an access area with Enter and Exit readers (see Adding Access Areas).
2. In the Tree View, click **Car Parking**.
3. On the toolbar, click the icon.



4. In **Description**, enter a name of the car parking area.
5. In **Access Area**, select the relevant access area that you defined in Adding Access Areas.

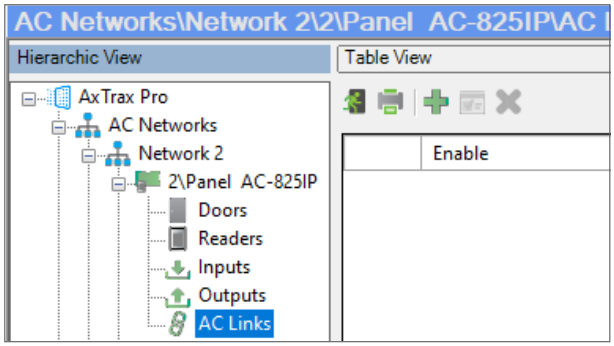
6. In the **Checked by** area, perform one of the following:
   a. Select **Access Area**.
      i. In **Area maximum counter**, select the number of parking spots available in that access area.
      ii. Click **OK**.
   b. Select **User Groups**.
      i. Click **OK**.
      ii. In the Tree View, expand the **Car Parking** element and select the car parking area you just created.
      iii. On the toolbar, click the  icon.



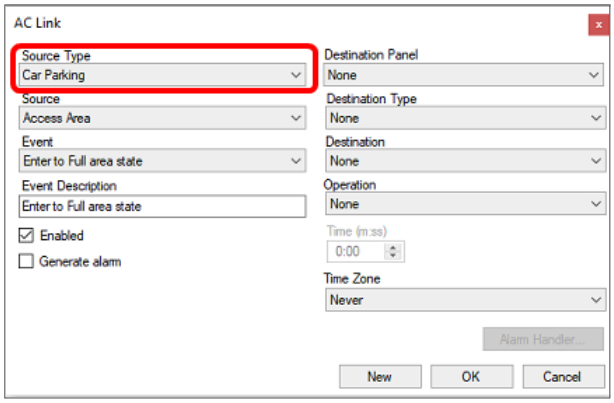
      iv. In **Description**, enter a name of the car parking sub-group.
      v. In **Group maximum counter**, select the number of parking spots available for the parking group.
      vi. Click **OK**.
      vii. In the **Tree View**, expand the **Departments/Users** element and select a department that contains the users you wish to add to the Car Parking sub-group.
      viii. Select a user in the Display Area.
      ix. On the toolbar, click the  icon.
      x. On the **General** tab of the **User Properties** window, select the **Car Parking** sub-group from the **Car Parking Group** drop down.
      xi. Click **OK**.

      The window closes and the new car parking group appears in the Display Area.
      xii. Repeat Steps *vi* to *xi* for each user you wish to add to a Car Parking Group.

7. Select **AC Links**.



8. On the toolbar, click the  icon.
9. In the **Source Type** list, select **Car Parking**.



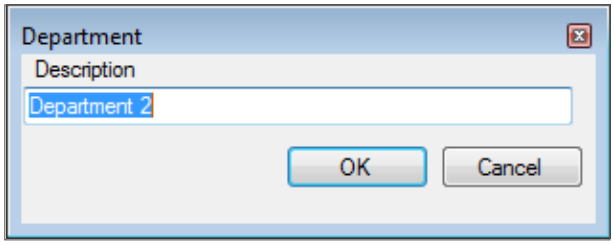
10. Managing Users

Every user is associated with a department. For each user, AxTraxPro stores contact details, associated card details, and access rights.

10.1. Adding Departments

To add a department:

1. In the Tree View, expand the **Users** element and click the **Departments/Users** element.
2. On the toolbar, click the  icon.



3. In the **Description** field, enter a name for the department and click **OK**.
   The window closes and the new department appears in the Display Area.

10.2. Adding a Batch of Users and Cards

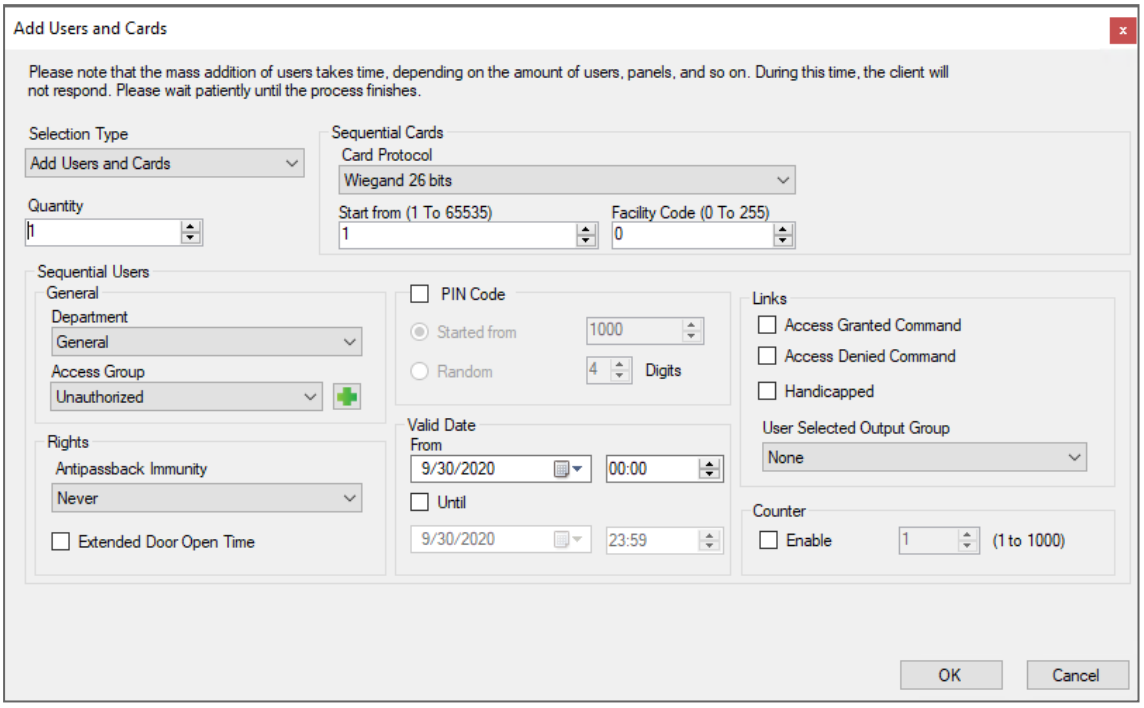
One can also add a batch of users and cards at one time and define the following:

- The type of reader needed to read the card
- The number of cards to create
- Whether or not a user should be created for each new card

To add users and cards:

1. In the Tree View, select the **Users** element.

2. On the toolbar, click the  icon.



3. Configure the card properties as required according to the field descriptions in the following table:

Field	Description
Selection Type	Select what will be added: Users and cards, Users only, or Cards only
Quantity	Type or select the number of cards/users to add
Sequential Cards	Define the card properties: • **Reader Type:** Select the type of reader appropriate for the new cards being added • **Start from:** Type the number of the first card in the set • **Facility code:** Type the site code for these cards. This field is not available for all reader types

Field	Description
Sequential Users > General	Define the user's general properties: • **Department:** Associate to the new user(s) created to a department • **Access Group:** Associate to the new user(s) created to an Access group Click  to add the user to a custom access group within all available readers.
Sequential Users > Rights	Define the user's right properties: • **Antipassback Immunity:** Select how to override any antipassback restrictions: Never, Always, according to time zone • **Extended Door Open Time:** Select to activate the extended door option defined for each door
Sequential Users > PIN Code	Select to define automatic pin codes, select between: • **Start from:** Sequential pin code starting from a predefined number based on a defined number of digits • **Random:** Random pin codes where the only definition is the number of PIN code digits
Sequential Users > Valid date	Define the access right validity: • **From:** Define the date and time to begin allowing access • **Until:** Select to define an end date for the access right validity, then define the date and time
Sequential Users > Links	Select to define associated link commands: • **Access Granted check box:** Activate a user-defined set of inputs or outputs for access granted events • **Access Denied check box:** Activate a user-defined set of inputs or outputs for access denied events • **Handicapped check box:** Activate a dedicated output a short time after the door is unlocked. The outputs are set in the Links window. • **User selected Output group:** Select an output group for this user. The outputs are triggered every time the user accesses a door. The operations, inputs, and outputs are defined in the Links window (see Adding Panel Links).
Sequential Users > Counter	Select Enable to use the counter option then type or select the counter number to be used for the first user

4. Click **OK** to close the window.

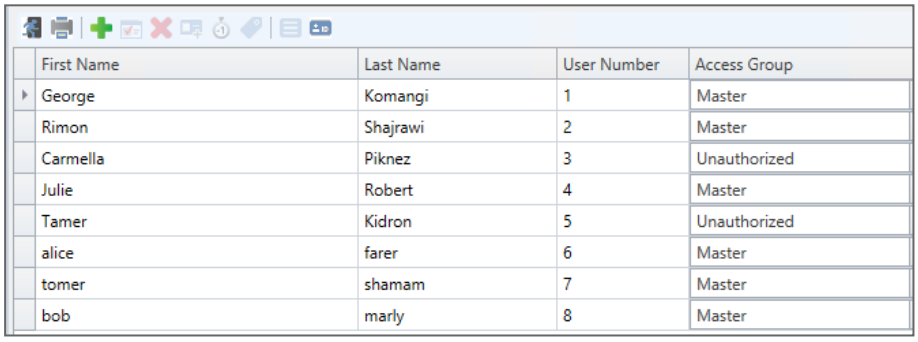
The process may take a few minutes after which a dialog reports that the operation has been completed.

10.3. Viewing Users

Users can be seen in a list or as a group of cards.

To see the users in a list:

1. In the tree view, select the department for the users to see.
2. Click the **List** icon.

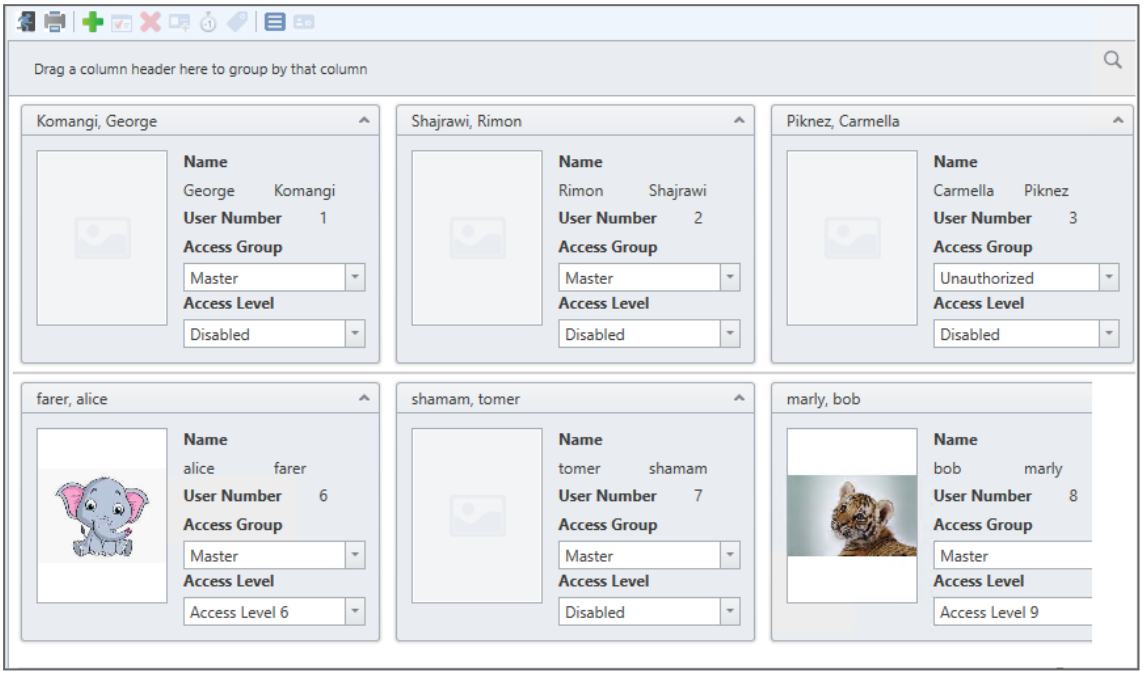


First Name	Last Name	User Number	Access Group
George	Komangi	1	Master
Rimon	Shajrawi	2	Master
Carmella	Piknez	3	Unauthorized
Julie	Robert	4	Master
Tamer	Kidron	5	Unauthorized
alice	farer	6	Master
tomer	shamam	7	Master
bob	marly	8	Master

To see the users as group of cards:

1. In the tree view, select the department for the users to see.

2. Click the **Card** icon.



10.4. Adding an Individual User

To add an individual user:

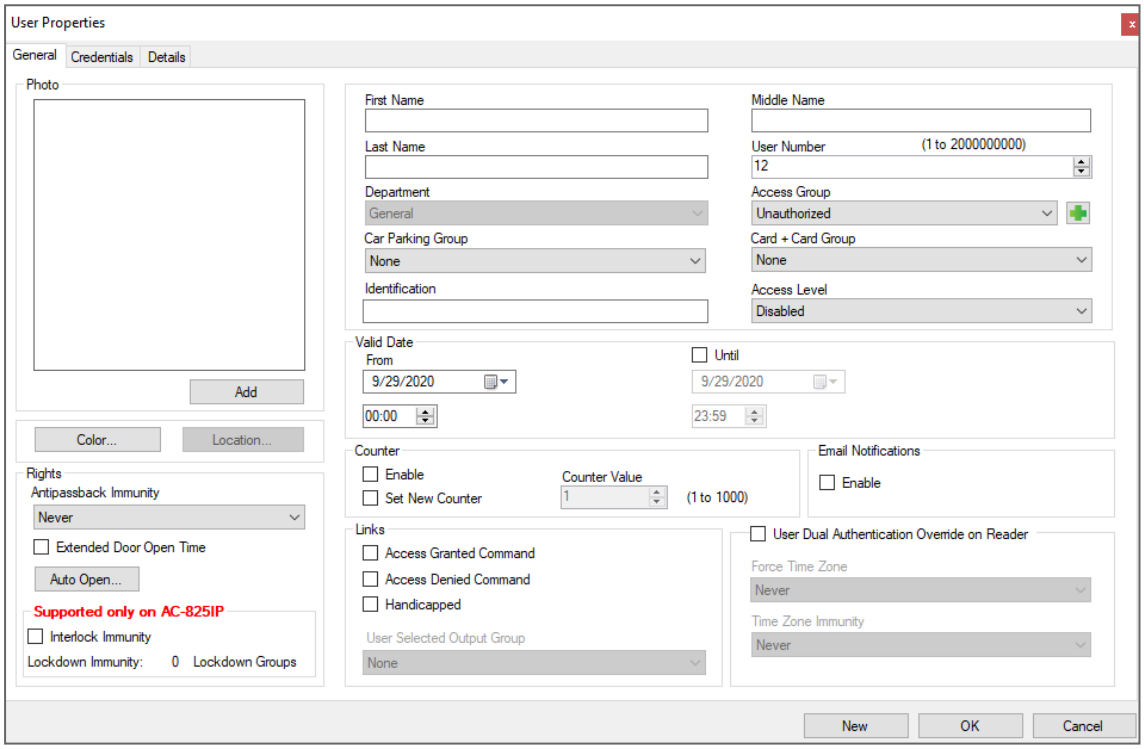
1. In the Tree View, expand the **Users** element.
2. Expand the **Departments/Users** element and select a department for the new user.
3. On the toolbar, click the icon.
4. Enter the user details as needed using the tabs described in the subsections below.
5. Click **OK**.

   The window closes and the new user appears in the Display Area.

10.4.1. General

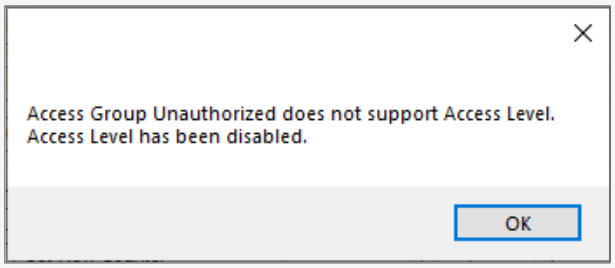
The **General** tab displays:

- User identification information
- User validity settings
- Access rights for the user



The **General** tab fields are described in the following table:

Field	Description
Photo > Add	Click to add a photo of the user, or to remove an existing photo. The selected photo aspect ratio should be 1.25 H x 1.00 L; otherwise, the photo may be distorted. Be sure that the photo is rotated properly before adding it.
First Name	Type the user's first name.
Middle Name	Type the user's middle name.
Last Name	Type the user's last name.

Field	Description
User Number	Type a unique user number to identify the user.
Department	Select the user's associated department.
Access Group	Select the user's access group. Default: Unauthorized Click  to add the user to a custom access group within all available readers and mapped terminals.
Car Parking Group	Select to add a user to a defined Car Parking group.
Card + Card Group	Select to add a user to a defined Car + Card group.
Identification	Add text that identifies the user
Access Level	Select the access level An access level cannot be selected for a user in an Access Group Unauthorized. 
Color	Click to select which color to use to highlight this user when the user generates access events. User highlighting must be activated in **Tools > Options > General** tab.
Location	Click to display a log of doors accessed by this user.
Valid Date > From	Select the date/time from when the user's access rights begin.
Valid Date > Until	Select the date/time on which the user's access rights end. This field is only available when the check box is selected. For AC-215 panels, only the date is recognized; the time entered is not recognized. Also, the Until date is not part of the valid range.
Counter > Enable	Select to set an access rights countdown counter for this user (see Configuring User Counters). When the counter reaches zero, the user's access rights end.

Field	Description
Counter > Set new counter	Select to set a new countdown counter value for this user (see Configuring User Counters).
Counter > Counter Value	Select a new countdown counter value for this user. This field is only enabled when the **Set new counter** check box is selected.
Email Notifications > Enable	Select to enable email notifications to be sent to the user's email, which is defined in the **Details** tab (see Details Tab)
Rights > Antipassback Immunity	Select to override any Antipassback restrictions for this user. • **Never** • **Always** • **User-defined time zone** For an AC-215 access control panels, only Always will work.
Rights > Extended Door Open Time	Select to entitle this user to an extended unlocked door duration. The extended duration is set for each door (see AC-825IP).
Rights > Auto Open	When defining user properties, you can define certain output groups to be active automatically (see Auto Opening for Output Groups).
Rights > Interlock Immunity	Allows the user to open doors within the relevant access group regardless of the interlock status This feature works only for AC-825IP.
Links > Access Granted Command	Select to activate a link rule initiated by access granted commands for this user (see Adding Panel Links).
Links > Access Denied Command	Select to activate a link rule initiated by access denied commands for this user (see Adding Panel Links).
Links > Handicapped	Select to activate a dedicated output a short time after the door is unlocked (see Adding Panel Links).
Links > User Selected Output Group	Select an output group for this user. The outputs are triggered every time the user accesses a door, as specified in the **Links** window (see Adding Panel Links).

Field	Description
User Dual Authentication Override on Reader	Select to override the dual authentication defined by the system. • **Force Time Zone**: The user must present two credentials, even though the reader does not require it. For this feature to be active, the Dual Authentication Mode check box in the Reader window. • **Time Zone Immunity**: User is granted access per one credential and not per two credentials, even though the reader might be in "User Dual Authentication" mode.

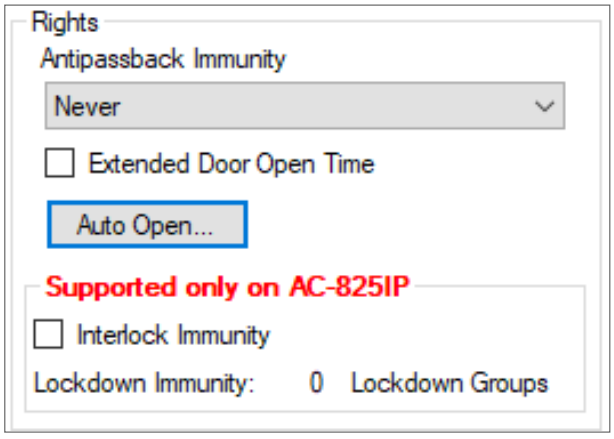
10.4.1.1. Auto Opening for Output Groups

When defining user properties, you can define certain output groups to be active automatically.

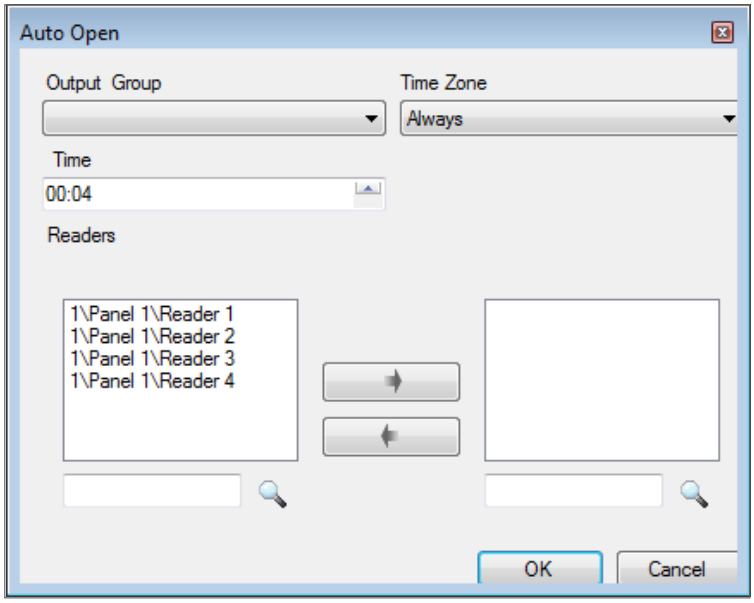
Output that needs to active this function must be always in Active state in the "Event Filter" (Panel properties > Options).

To define Auto Open for output groups:

1. In the Rights section, click **Auto Open**.



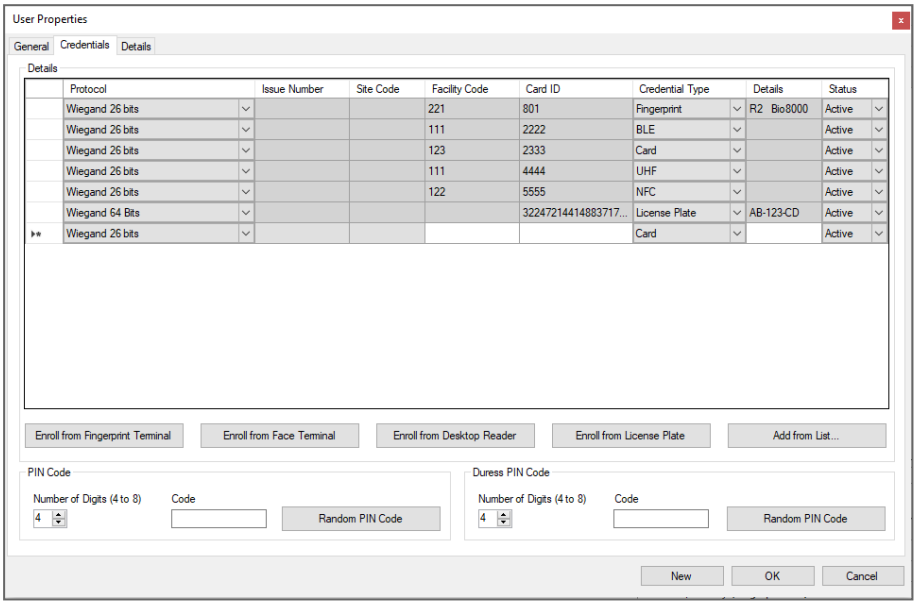
2. For each output group selected in the **Output Group** drop down:
   a. From the **Time Zone** drop down, select a time zone.
   b. From the **Time** box, select a duration time of the activation.
   c. Select and move the desired readers using the arrows.



3. Click **OK**.

10.4.2. Credentials Tab

Use the **Credentials** tab to associate up to 16 cards with each user, as well as to assign a user's PIN codes.



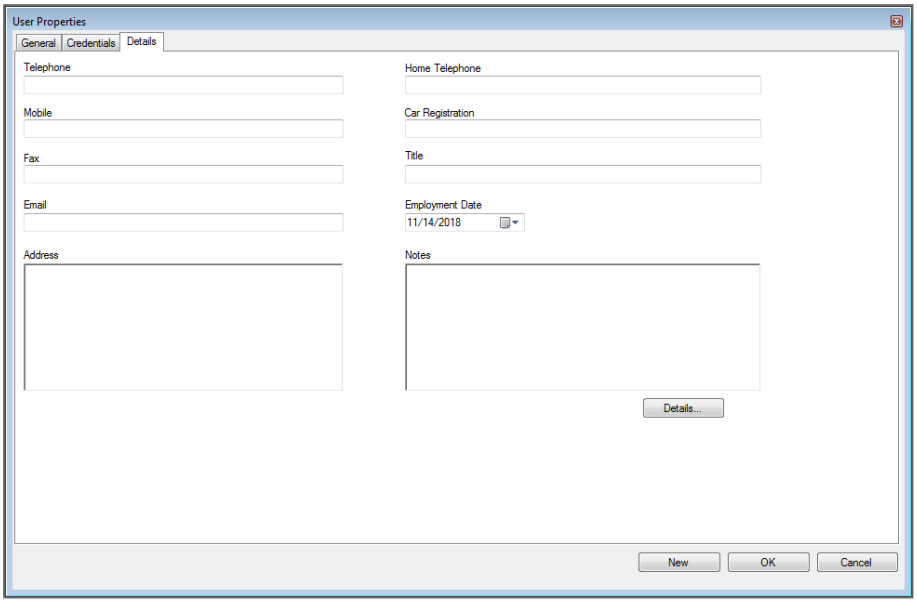
The **Credentials** tab fields are described in the following table:

Field	Description
Details	Displays the various properties of the credential added to the system for the user The Issue Number and Site Code fields are only available if the Protocol selected is "Rosslare 38-Bit (Rosslare Proprietary)".
Details > Enroll from Fingerprint Reader	Click to enroll a user's fingerprint (see Enrolling a User's Fingerprint).
Details > Enroll License Plate	Click to enroll a license plate (see Enrolling a License Plate).
Details > Enroll Face from Terminal	Click to enroll a face from a terminal (see Enrolling a Face from a Terminal).
Details > Enroll from Desktop Reader	Click to enroll credentials using a desktop reader (see Enrolling a License Plate)

Field	Description
Details > Add from List	Click to associate a user to a card or multiple cards (see Associating a User to a Card).  Before you can associate a user to a card, you must be sure that the card has been added to the system (see Auto Opening for Output Groups). All cards within the user's specified Facility code are listed
PIN/Duress PIN Code	Define PIN and Duress PIN code options: • **Number of digits:** Select the length of the PIN for this user • **Code:** The 4- to 8-digit PIN and/or Duress PIN code • **Random PIN Code**: Click to automatically generate a random PIN

10.4.3. Details Tab

The **Details** tab contains detailed contact and identification details about the user.



The **Details** tab fields are described in the following table:

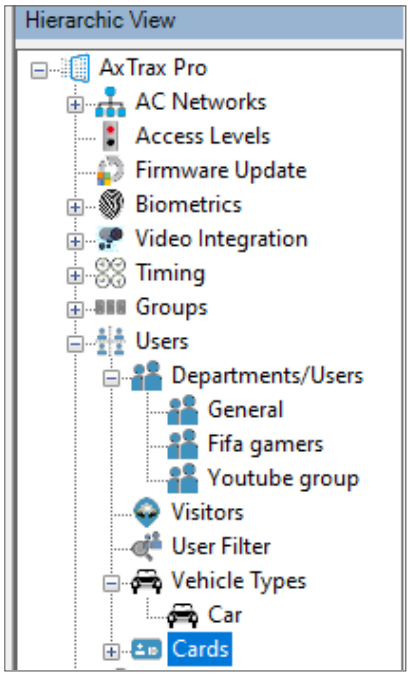
Field	Description
Telephone	Type an office telephone number for the user.
Mobile	Type a cell phone number for the user.
Fax	Type a fax number for the user.
Email	Type an email address for the user (up to 100 characters)
Address	Type a postal address for the user.
Home telephone	Type a home telephone number for the user.
Car registration	Type the user's license plate number.
Title	Type the user's title (e.g. "Mr.").
Employment Date	Enter the date that the user joined the firm.
Notes	Type any additional information.
Details	Click to open the user's additional details folder.

10.5. Managing Cards

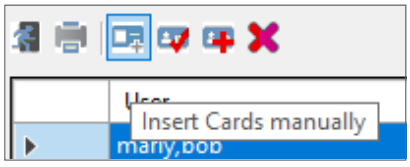
Access cards are added to the system manually. The enrollment for a card is done from a desktop reader or from a UHF reader. Once a card has been added to the system, it can be associated to a user.

To add cards manually

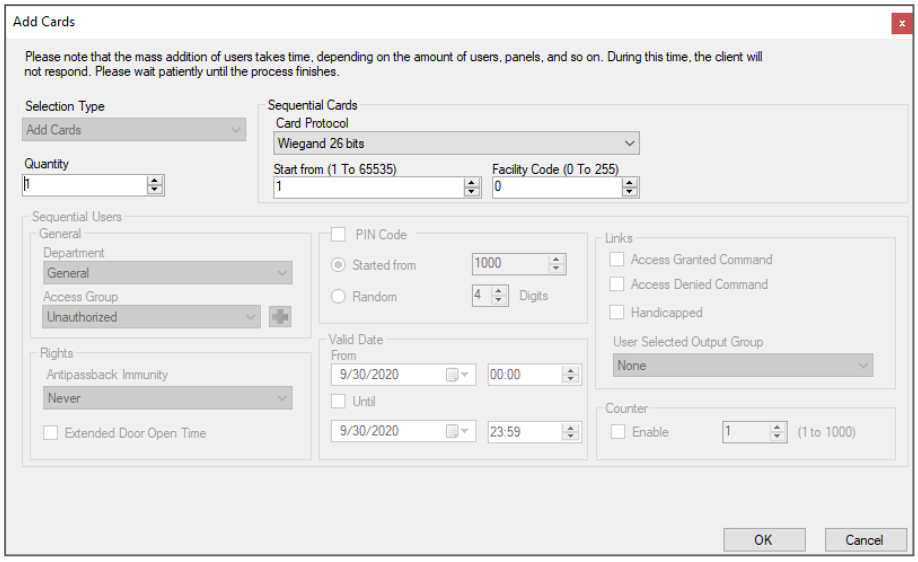
1. In the **Users** tree view, select **Cards**.



2. Click the **Insert Cards manually** icon.



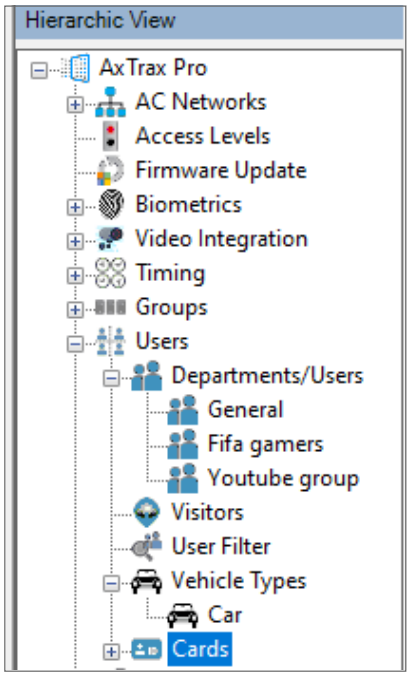
3. Type or select the **Quantity**, the number for the first card, and the **Facility Code** in the applicable box.



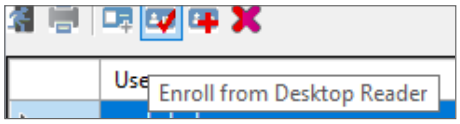
4. Click **OK**.

To enroll cards from a desktop reader:

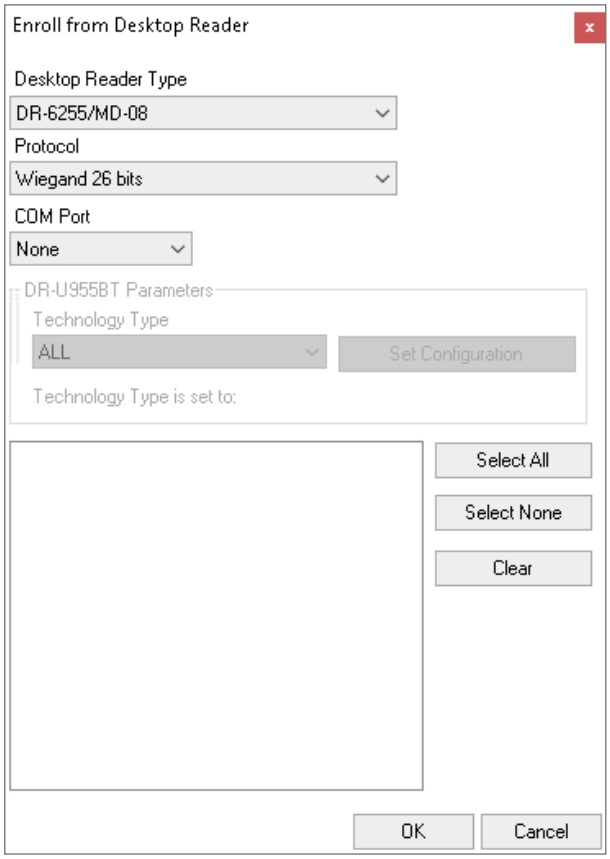
1. In the **Users** tree view, select **Cards**.



2. Click the **Enroll from Desktop Reader** icon.

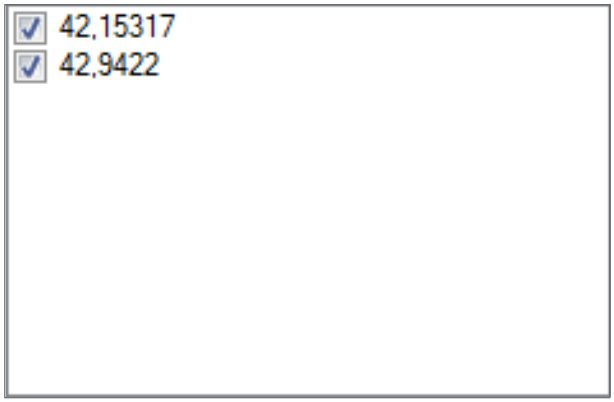


3. Select the **Desktop Reader Type**, **Protocol**, and **COM Port** from the applicable list.



4. If the DR-U955BT is selected in **Desktop Reader Type**, then you must also select the technology type from the drop down and click **Set Configuration**.

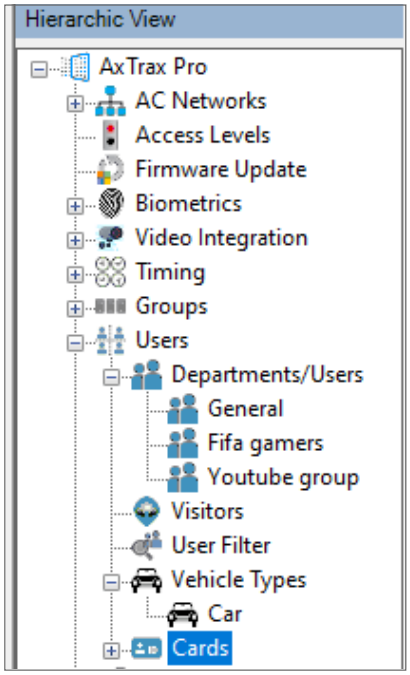
5. Enroll a card by presenting it to the reader. Each card enrolled appears in the screen.



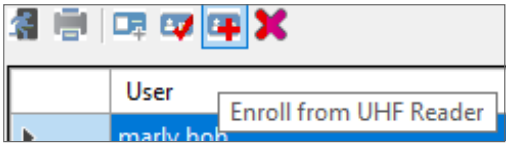
6. Select the cards to add (added cards are selected by default).
7. Click **OK**.

To enroll cards from an UHF reader:

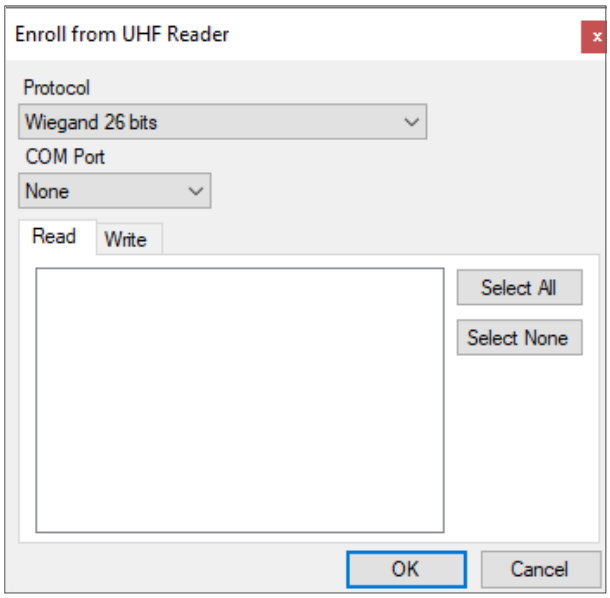
1. In the **Users** tree view, select **Cards**.



2. Click the **Enroll from UHF Reader** icon.



3. Select the **Protocol** and **COM Port** from the applicable list.



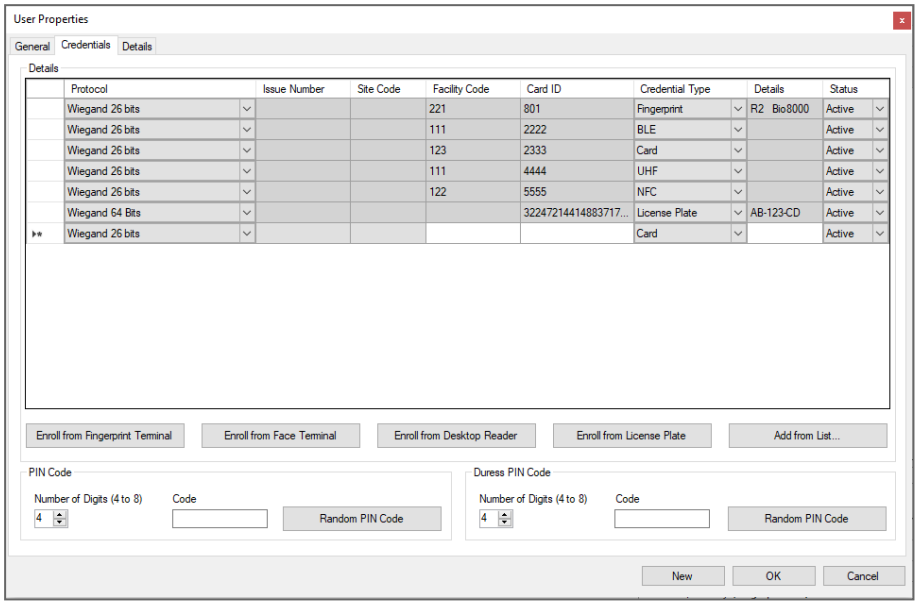
4. Click **OK**.

10.5.1. Associating a User to a Card

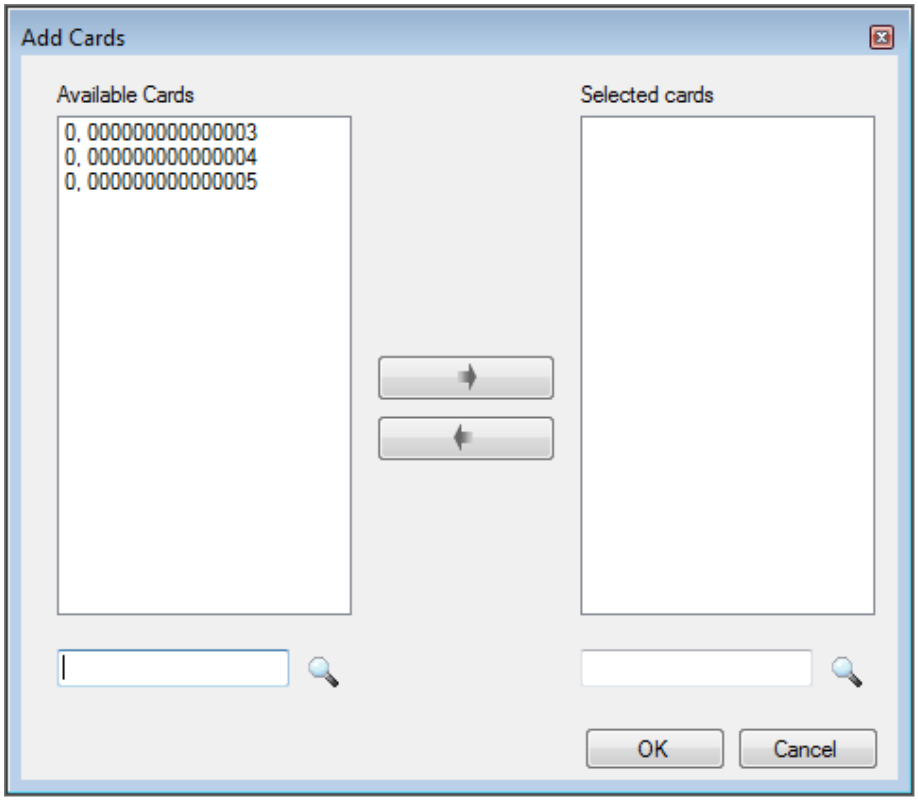
Once users and cards have been added to the system, you must associate each user to a card.

To associate a user to a card:

1. While in the **User Properties** window, click the **Credentials** tab.



2. Click **Add from List**.



3. Select the card(s) from the Available Cards list you wish to associate with the user and move them to the right panel using the arrows.

   If a card has already been associated to this user, it appears in the Selected Cards list.

4. Click **OK**.

   Alternatively, you can open the **Add Cards** window using the **Tree View**.

5. In the Tree View, expand the **Users** element and expand the **Departments/Users** element.
6. Select a department that contains the users you wish to associate with a card and select a user from the table.
7. Click the icon.

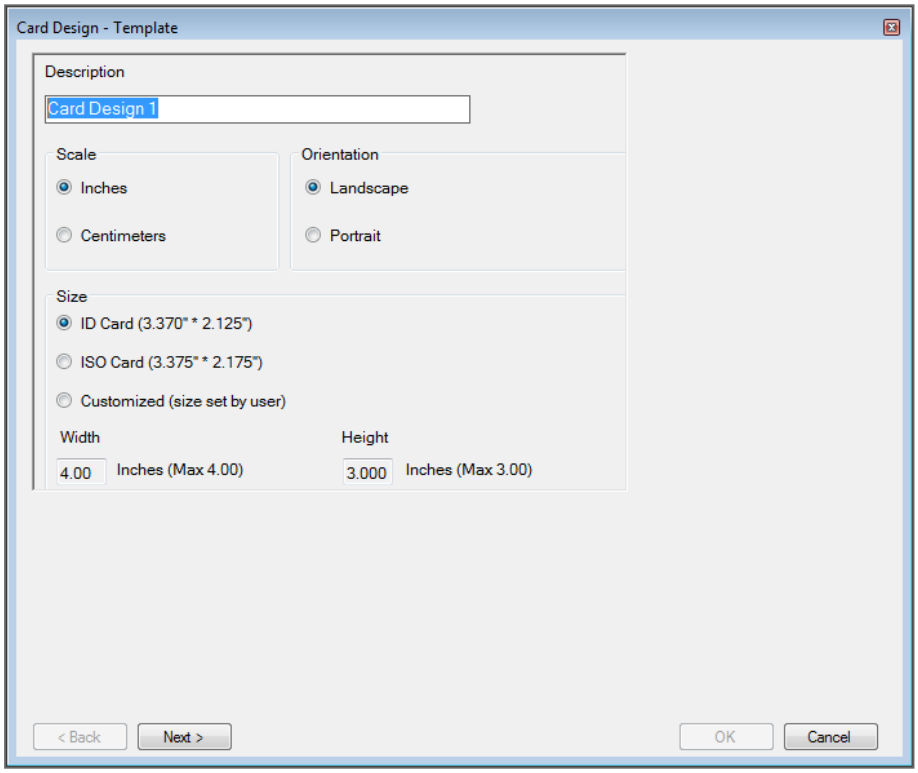
10.5.2. Card Design (Photo ID)

AxTraxPro allows you to design badges for mass printing and supports connectivity with digital cameras for image capture.

10.5.2.1. Creating a Card Template

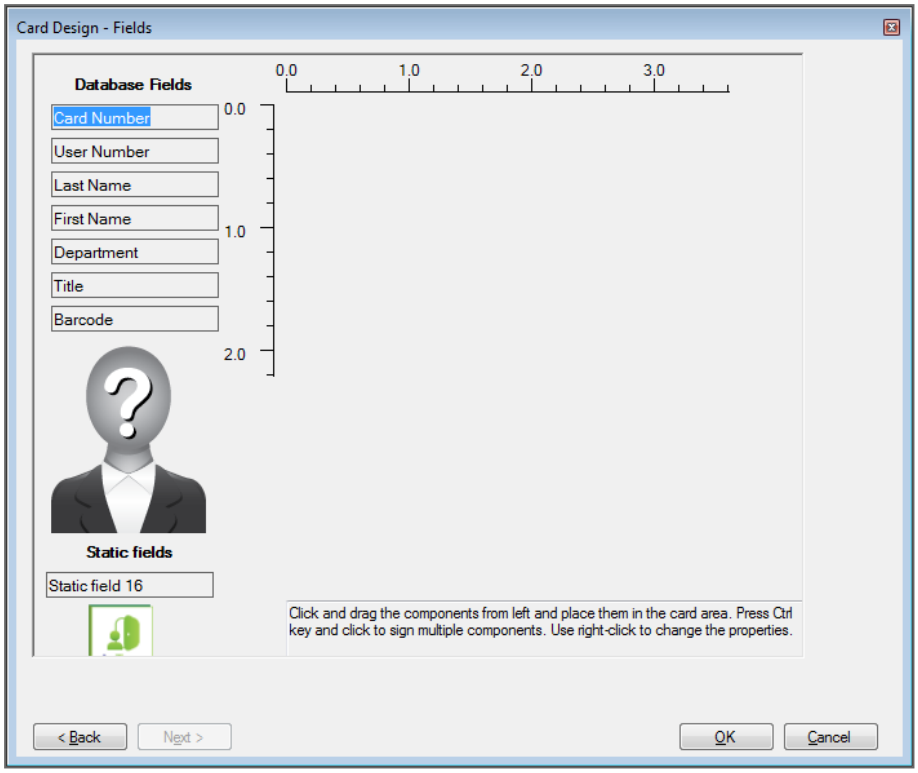
To create a card template:

1. In the **Tree View**, expand the **Users** element.
2. Expand the **Cards** element and click **Card Design**.
3. On the toolbar, click the  icon.

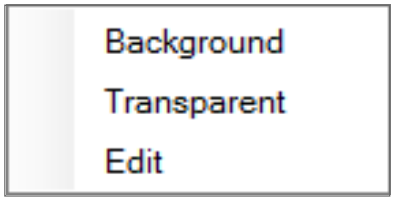


4. Enter a description for the template and define the scale, orientation, and size.

5. Click **Next**.

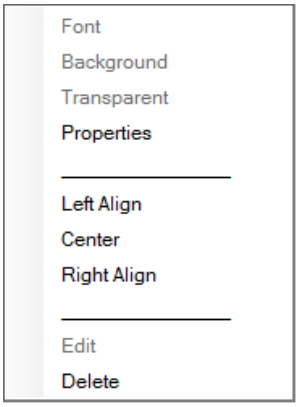


6. Right-click the card area background to set the background color or to select a file to use as the background.

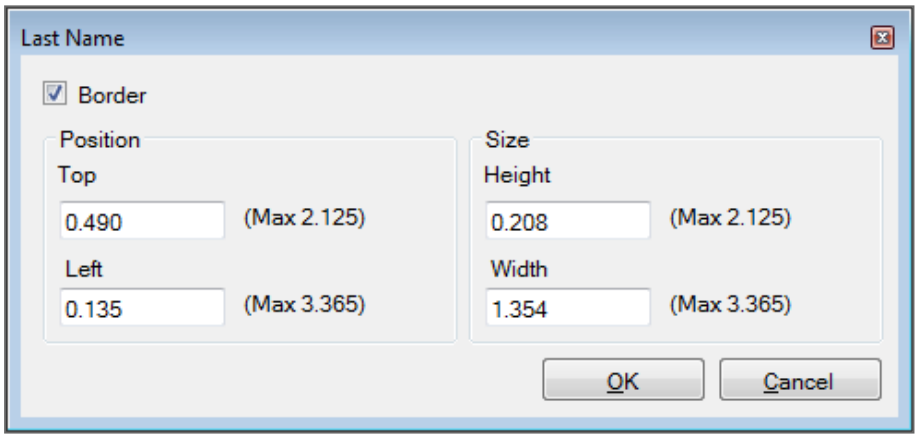


7. As desired, drag the fields on the left into the card area to create the layout of the card.

8. Right-click on any field appearing in the card area to show the following menu options:



9. Click **Properties** to remove the border and change the field size.



10. Click **OK** to return to the **Card Design - Fields** screen.
11. Click **OK** to save the card template.

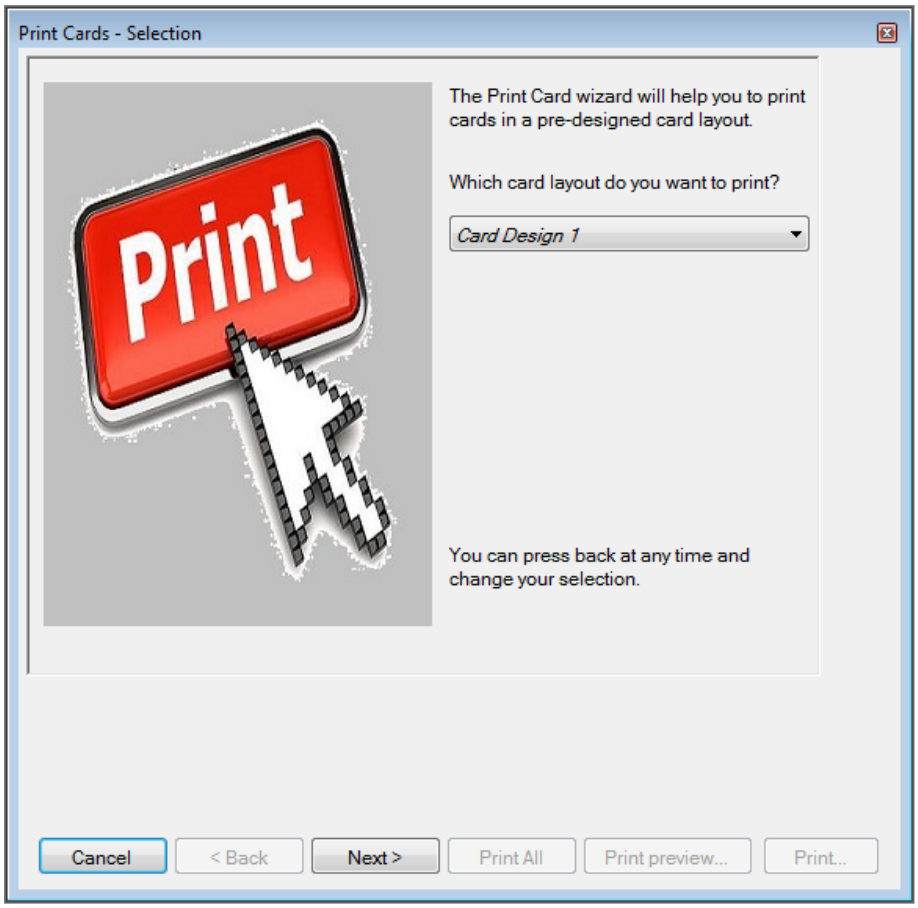
10.5.2.2. Printing a Card

Once you have saved a card template, you can print cards using the template.

For best printing results, it is strongly recommended to use 300 dot per inch (dpi) and a high screen resolution (at least 1280x1024 for a portrait card or 1600x900 for a landscape card). A resolution of 1920x1080 is recommended.

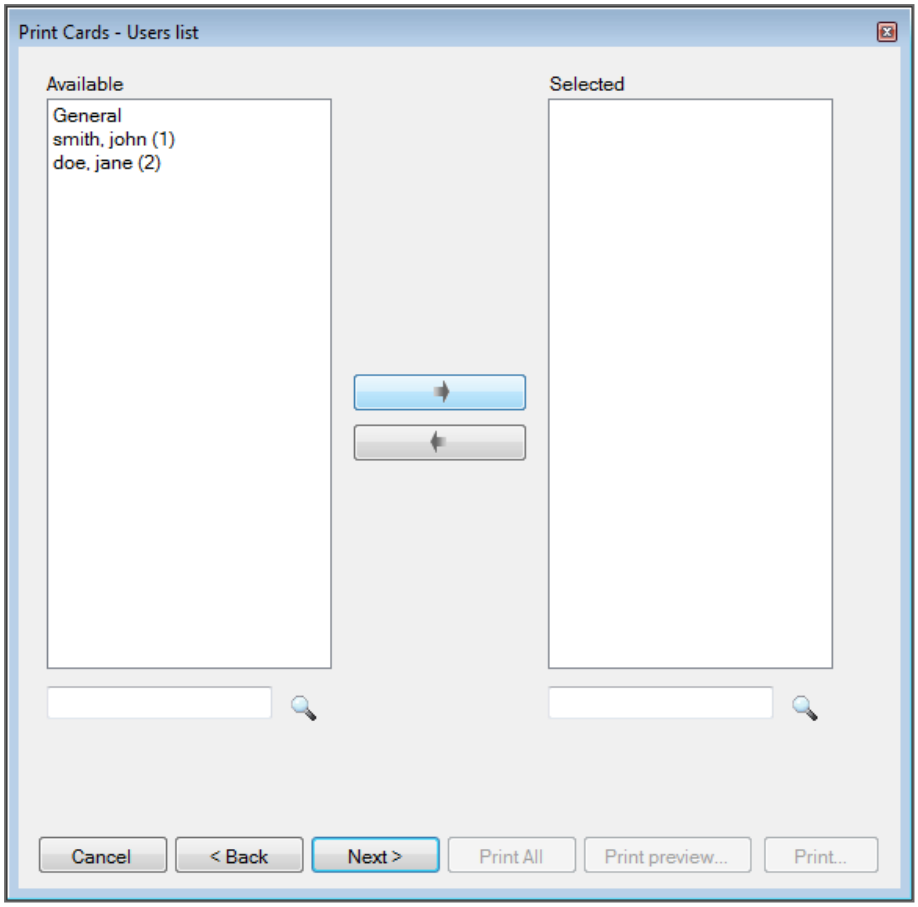
To print a card:

1. From the card template list in the Display Area, select the template you wish to use and click the  icon.



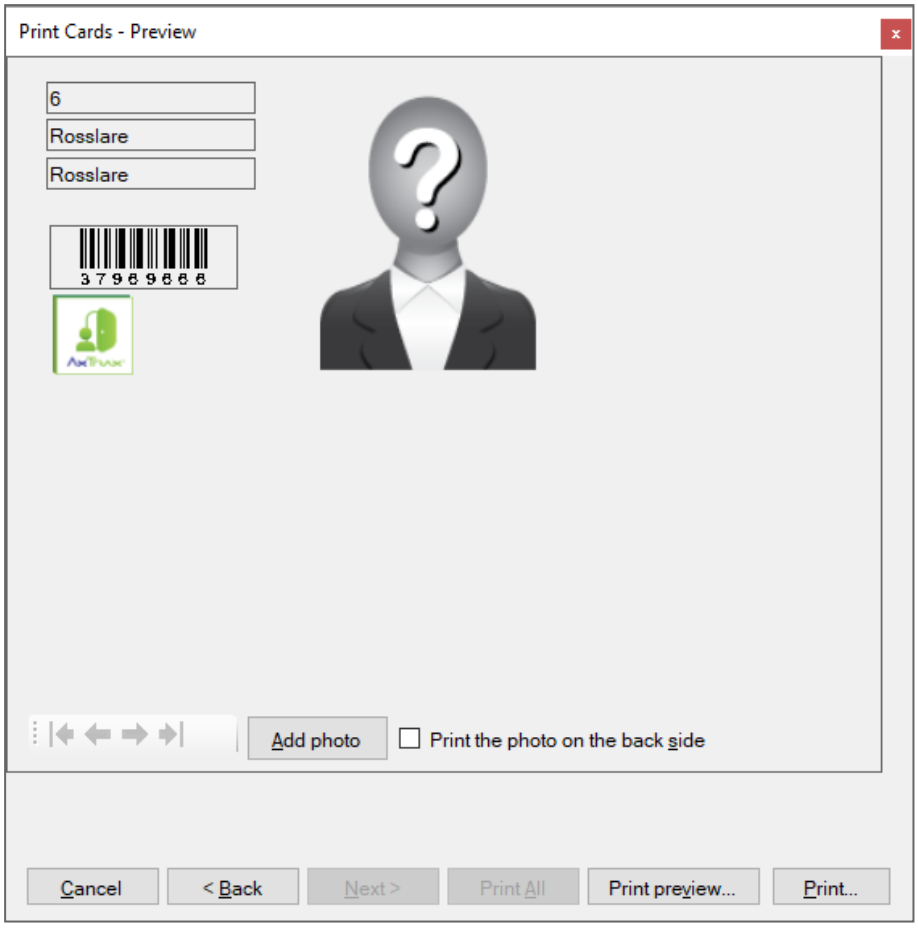
2. Select the layout you wish to use (if different than what you selected in Step From the card template list in the Display Area, select the template you wish to use and click the icon. from the corresponding drop downs.
3. Click **Next**.

> For users to appear in the Available list, they must have cards associated with them as described in Associating a User to a Card.

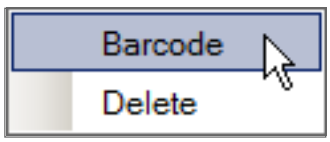


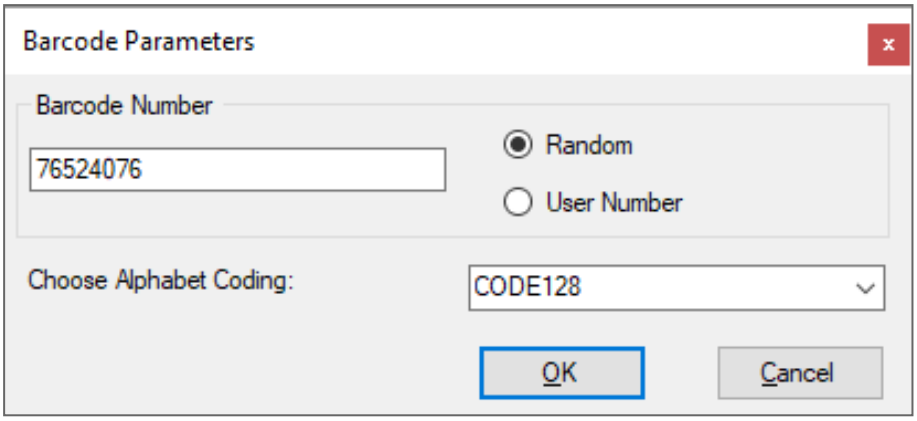
4. Select the users from the available list for whom you wish to print a card and move them to the right panel using the arrows.

5. Click **Next**.



6. Change the barcode type:
   a. Right-click on the Barcode field and select **Barcode**.

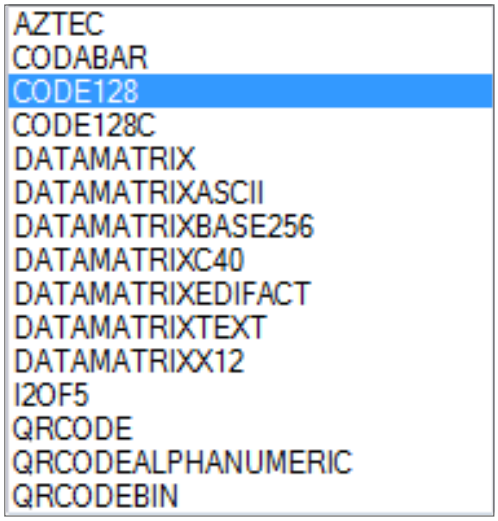




You can use the barcode that is generated automatically or enter a numeric barcode manually.

By choosing **User Number** the Barcode will be same as the user number

b. From the **Choose Alphabet coding** drop down, select the kind of coding.

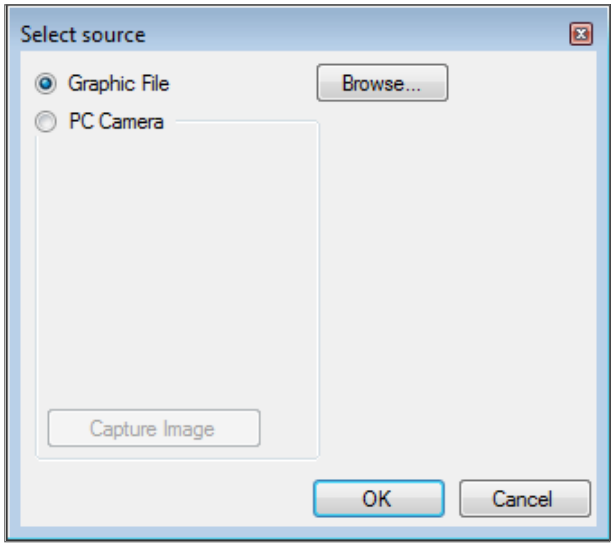


c. Click **OK**.

The barcode appears on the card template.



7. Click **Add photo** if you wish to select a different image either from a file or from a PC camera:

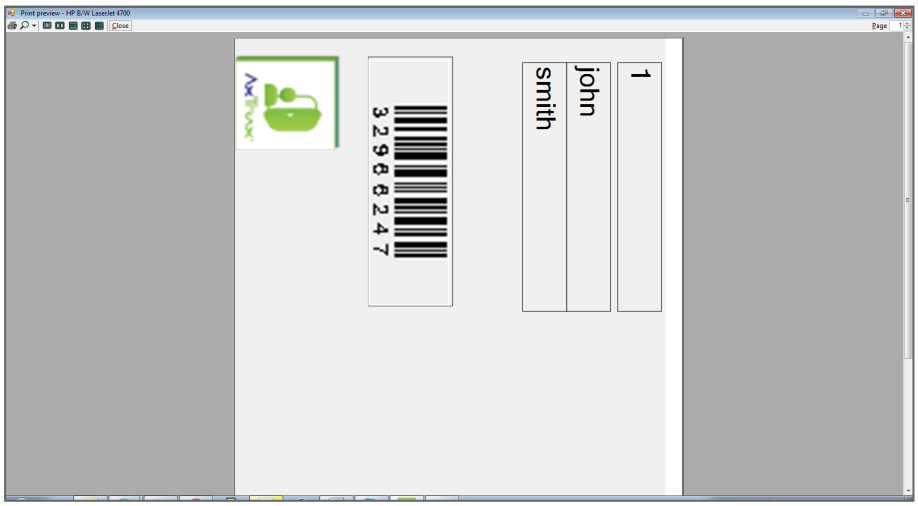


   a. Do one of the following:

   - **Select Browse** to locate an image to insert.
   - Select **PC Camera** and select **Capture Image**.

     a. Click **OK**.

8. Use the green arrows to preview additional users.
9. [Optional] Click **Print preview** to show the enlarged card screen.



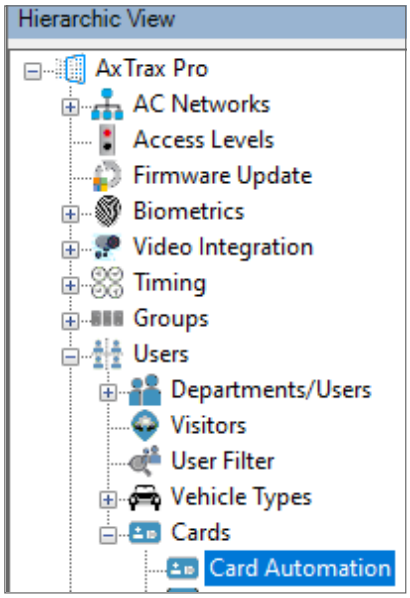
10. Click **Print** to print that particular card or click Print All to print all the available cards.

10.5.3. Setting Card Automation

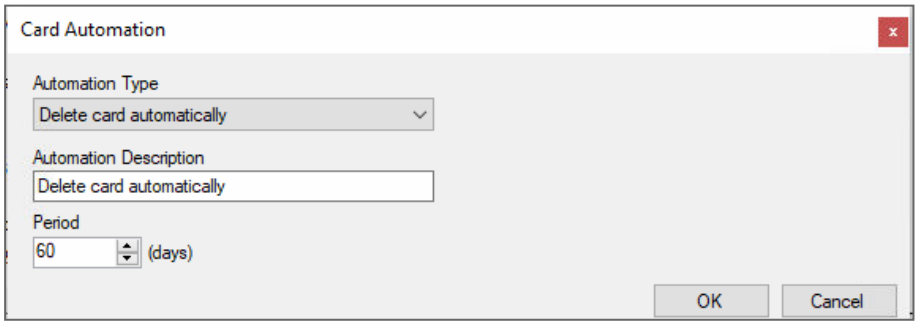
You can program the system to automatically keep track of any user card that has expired because of non-use over specified period of time. Once detected, this card can either be deleted automatically or you can be notified of it.

To set card automation:

1. In the **Users** tree view, expand the **Cards** element and select **Card Automation**.



2. Click the  icon.



3. From the **Automation Type** drop down, select the action to be taken when a card has not been used in a certain period of time.
   - Delete card automatically
   - Ask before card deletion
   - Notify by email

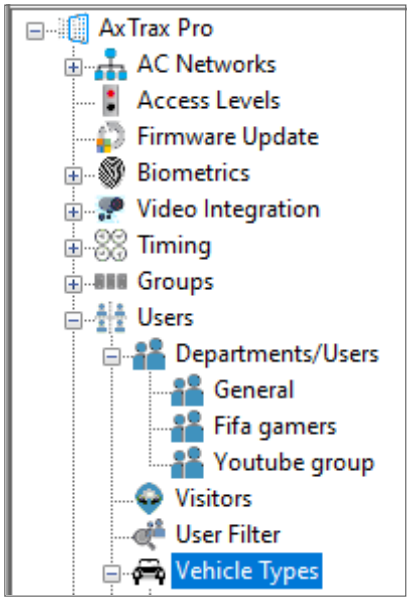
     For this option, you must supply an email address and you can add an optional signature.

   - Report in System Event Log only
4. From the **Period** box, select the time period.
5. Click **OK**.

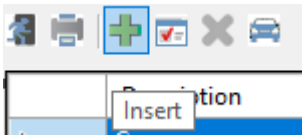
10.6. Adding Vehicle Types

To add a car and select a vehicle type:

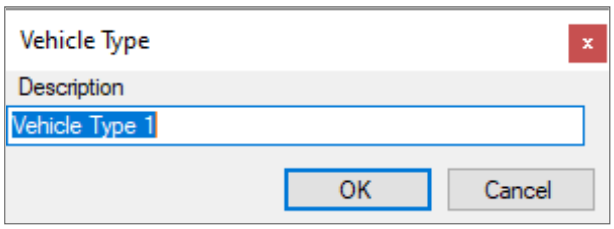
1. In the tree view, select **Vehicle Types**.



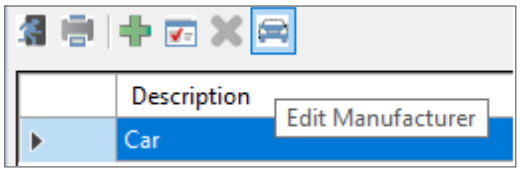
2. Click the **Insert** icon.



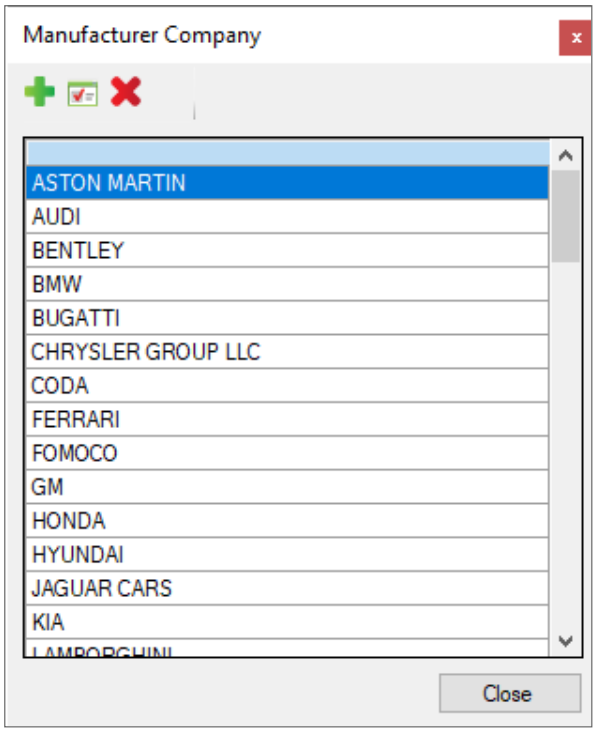
3. Type a **Description** for the vehicle type.



4. Click the **Edit Manufacturer** icon.



5. Select the vehicle manufacturer from the list.



5. Click **Close**.

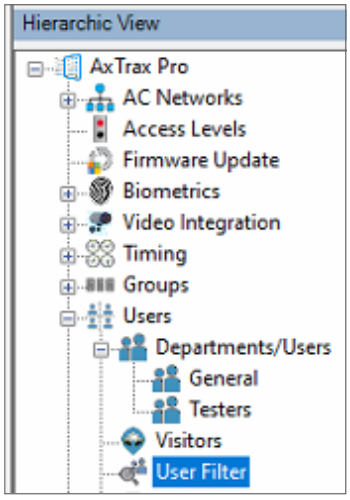
10.7. Using the User Filter to Search for Users

Search for enrolled persons in the access control system with the **User Filter**.

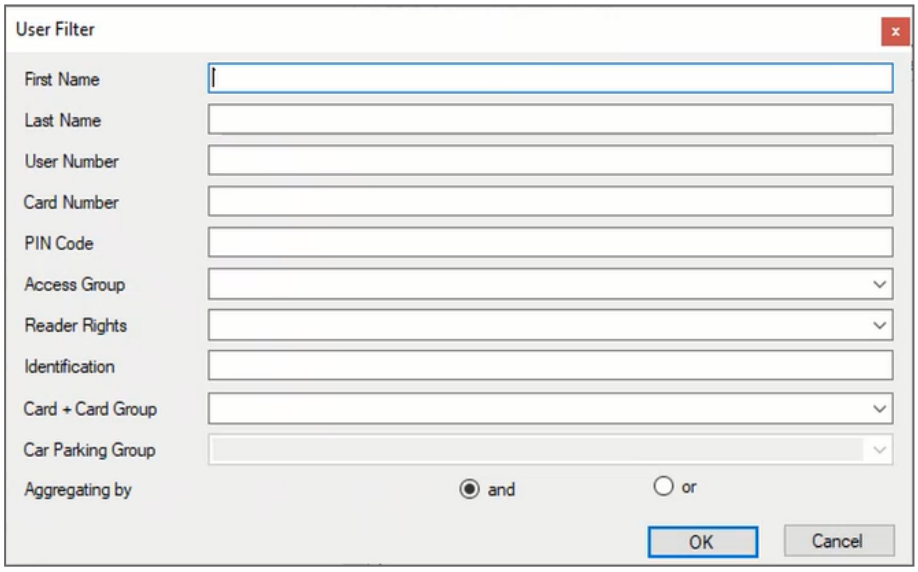
To search for users:

1. In the Tree View, expand the **Users** element.

2. Select **User Filter**.



3. Click .
4. Enter the necessary user information



5. Click **OK**.



The search filter is not case sensitive.

11. Adding Operators

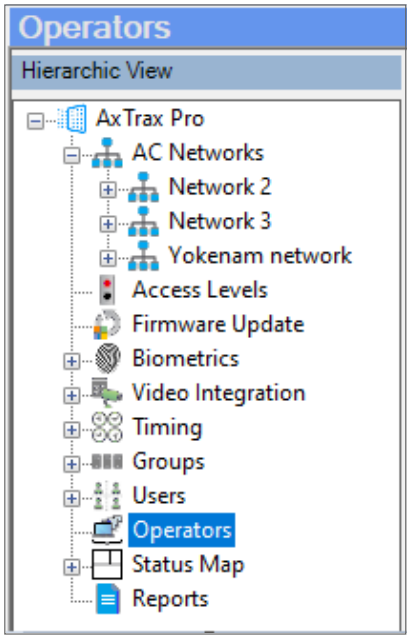
Operators are people with access to the AxTraxPro application. The default operator name is Administrator.

Different operators have wider or more restricted security rights, from complete control over the system to the ability only to view one section. All operator passwords are case-sensitive.

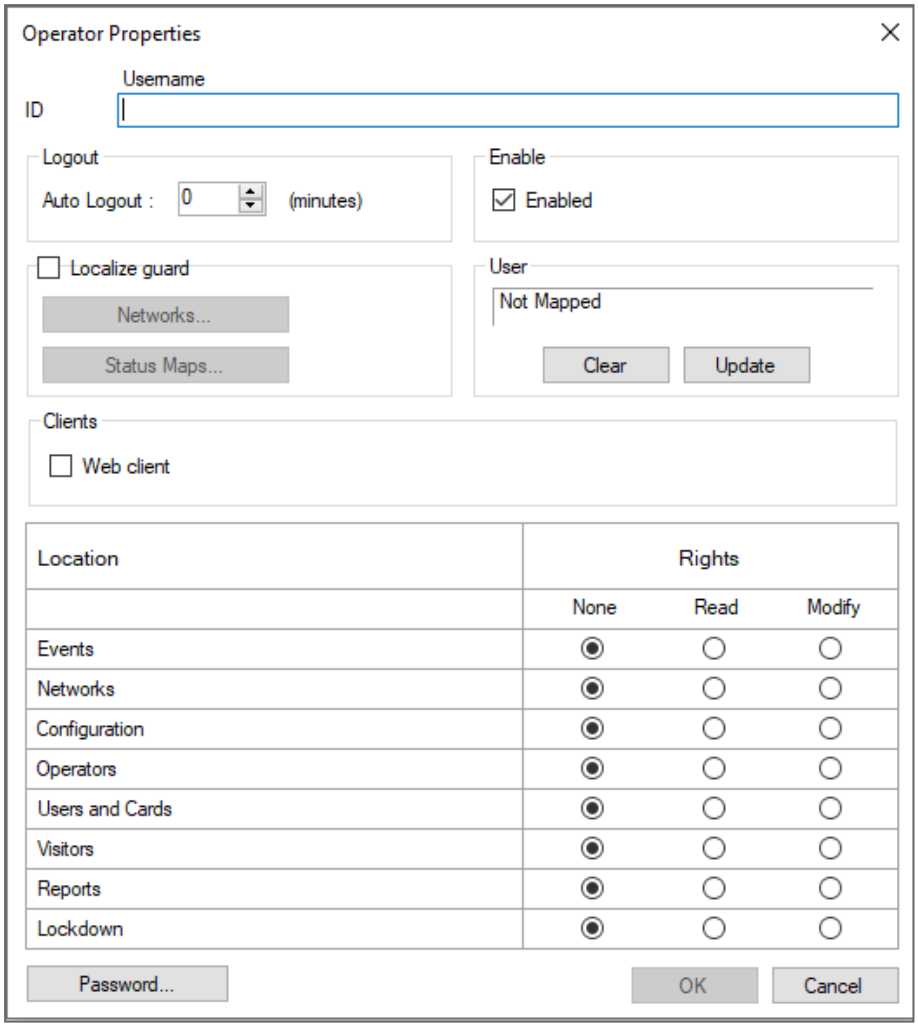
A person can only be put into the operator category if the are a regular user in the system.

To define operators:

1. In the Tree View, select the **Operators** element.

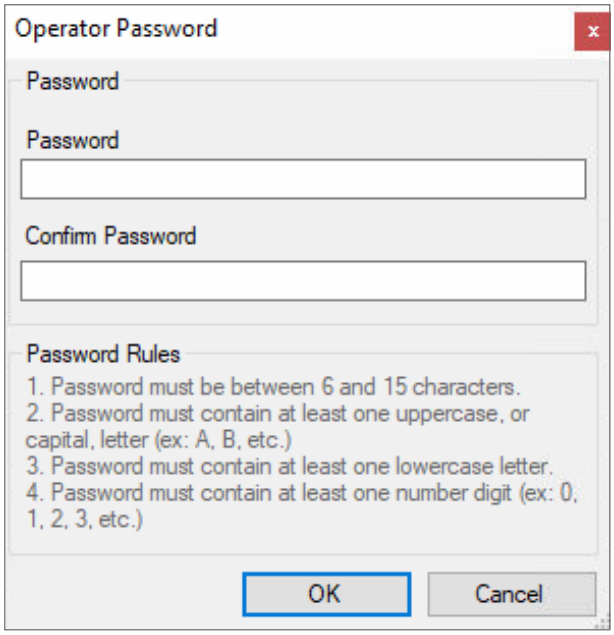


2. On the toolbar, click the icon.



3. In the **ID** field, enter the Operator's name.
4. **Auto Logout** - to define the time in minutes the AxTraxPro Client will logout.
5. Click **Enable** to enable this operator.
6. Select **Localize guard** to define the operator with limited rights.
7. Click **Networks…** and **Status maps…** to define the associated operator's local rights.
8. Click **Web client** to enable this option.
9. Set the operators global permission rights for each of the screens in the **Location** list.

10. Click **Password...** to open the **Operator Password** dialog.



11. Enter the operators' password in the Password field and re-enter the password in the Confirm Password field.

> On first time use, leave the password field empty and enter (and confirm) your new password.

12. Click **OK** to save your settings.

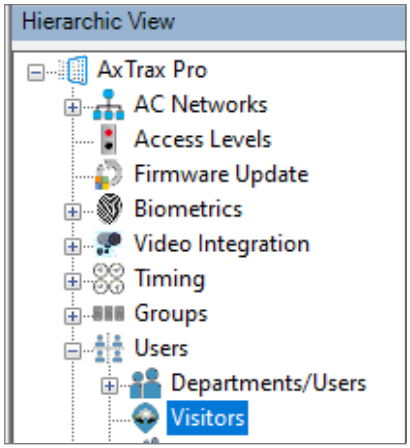
The dialog closes and the operator is shown in the Display Area.

12. Managing Visitors

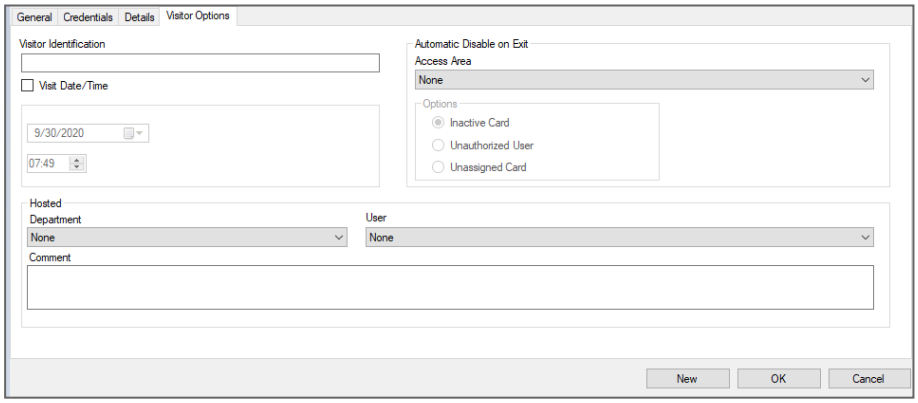
In addition to regular users, you can add visitors to the system, which includes their contact details, associated card details, and access rights.

To create visitors:

1. In the **Users** tree View, click **Visitors**.



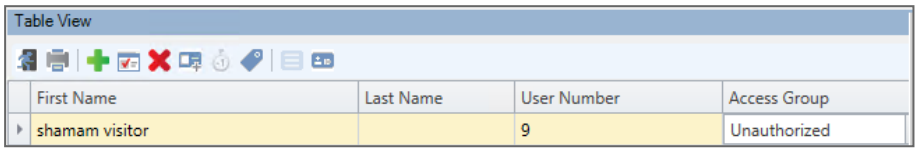
2. Click the  icon.
3. To set the **General** properties, **Credentials**, and **Details**, use the same procedure used to add a user, see Adding an Individual User.
4. To select visitor options, click the **Visitor Options** tab.



Visitors can be seen in a list or as a group of cards.

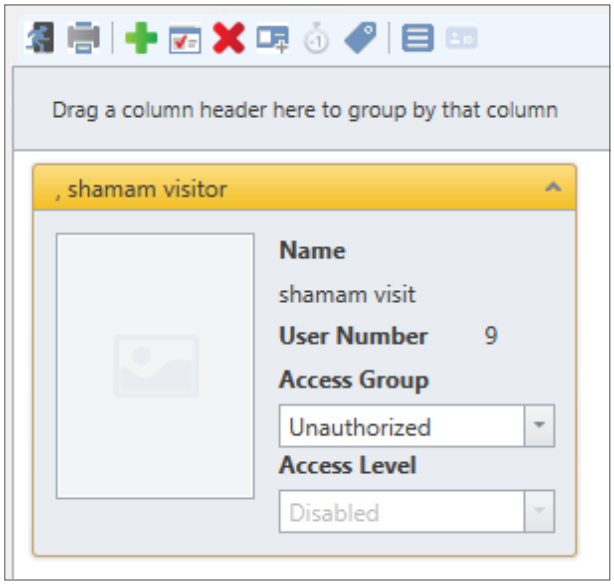
To see the visitors in a list:

1. Click the **List** icon.



To see the visitors as group of cards

1. Click the **Card** icon.



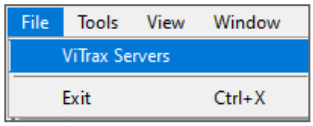
13. Integrating Video Systems

Cameras can be added to the network to allow real-time viewing of any area desired.

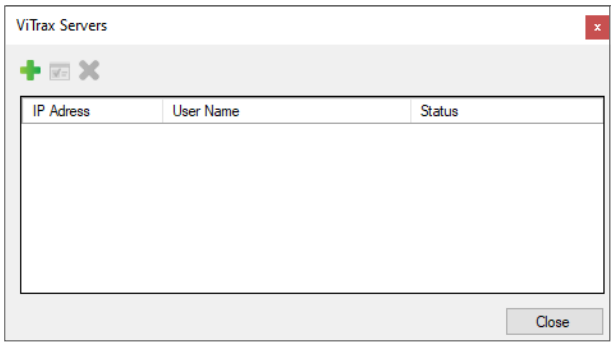
ViTrax is a video management server client solution that supports a wide range of IP, USB, and open protocol cameras, such as OnVif and PSIA. Be sure that the ViTrax Server is installed on a PC and you know that PC's IP address.

To view ViTrax Servers:

1. From the menu bar, select **File > ViTrax Servers**.



The following **ViTrax Servers** window appears.



The video integration can also be done with Hikvision or Dahua servers.

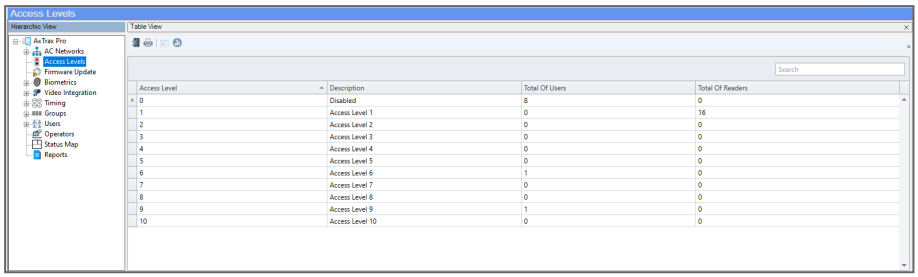
The functionality will be discussed in future versions of the manual.

14. Configuring Access Levels

Access levels can be assigned to users and readers. Thus, different security levels can be given to different access areas and only specified users have access.

A user can only access a reader which has an access level that is equivalent to or below the user's access level on the access level hierarchy.

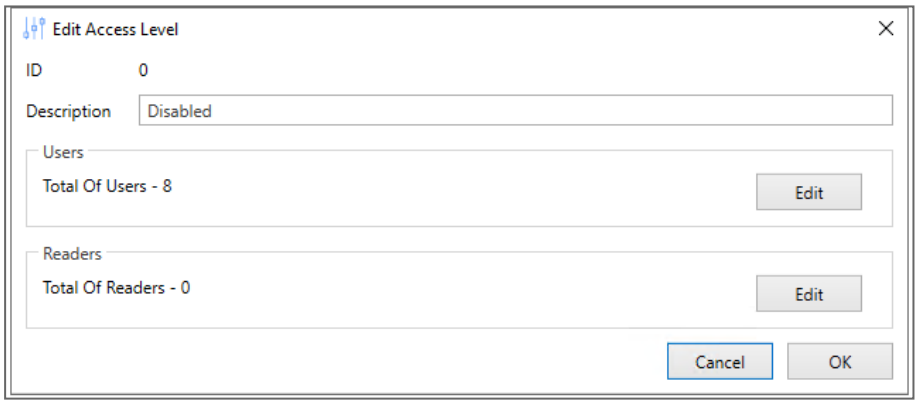
1. In the tree view, select **Access Levels**.



2. Select the access level to change and click the icon.

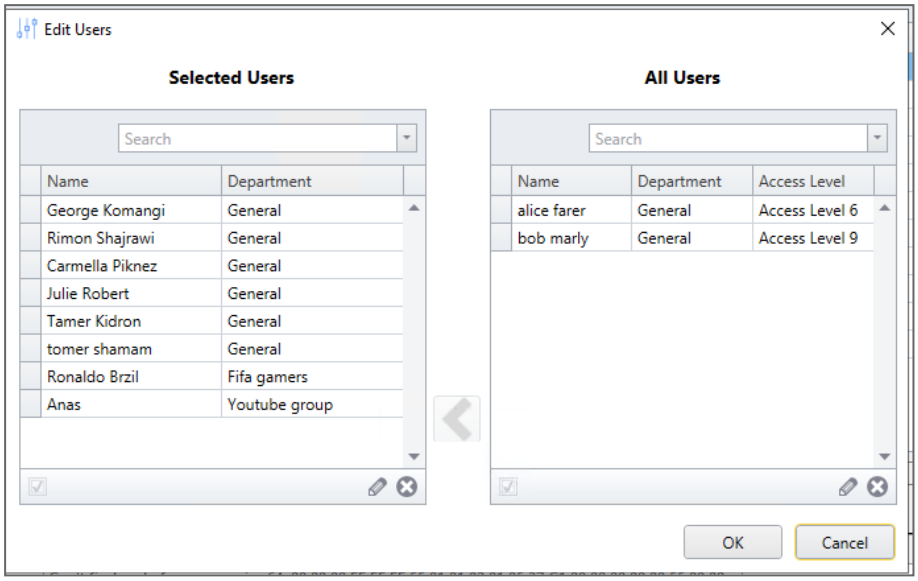


3. To add users, click **Edit** in the **Users** box.



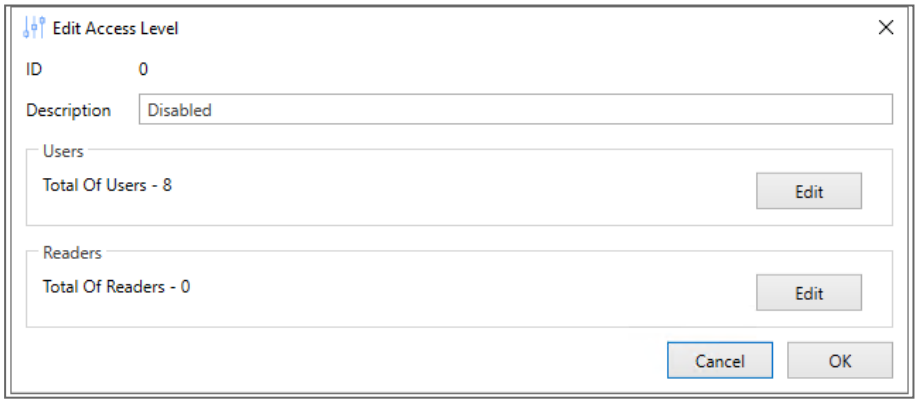
User(s) can also be added from the **General Tab** in the **User Properties** window.

4. To add users, select the users in the right table and click the arrow to move them to the list on the left.



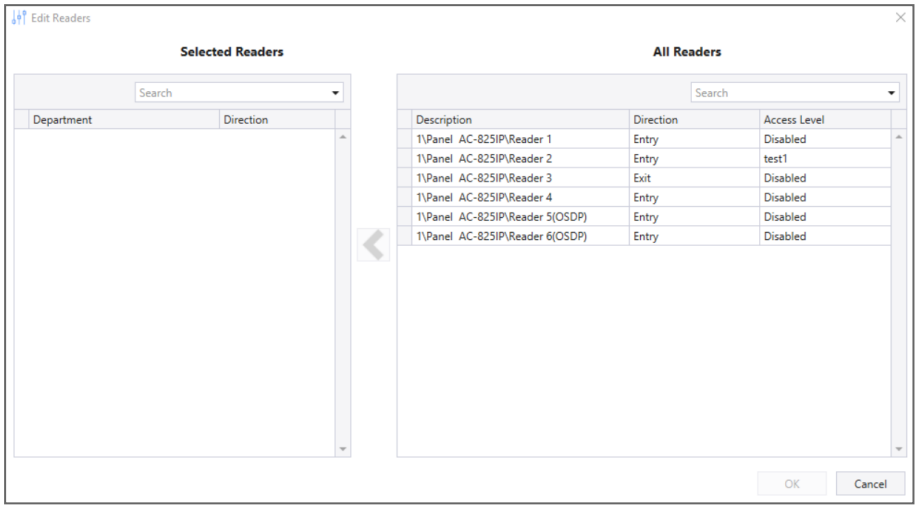
User(s) can only be removed from the **General Tab** in the **User Properties** window.

5. To add readers, click **Edit** in the **Readers** box.



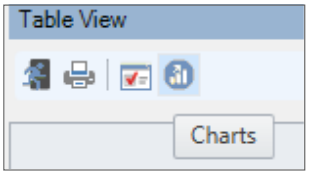
Reader(s) can also be added from the **General Tab** in the **Panel Properties** window for the reader.

6. To add readers, select the readers in the right table and click the arrow to move them to the list on the left.



Reader(s) can only be removed from the **General Tab** in the **Panel Properties** window for the reader.

7. To see a chart for users and readers, click the icon.



8. To close the chart, click the icon.



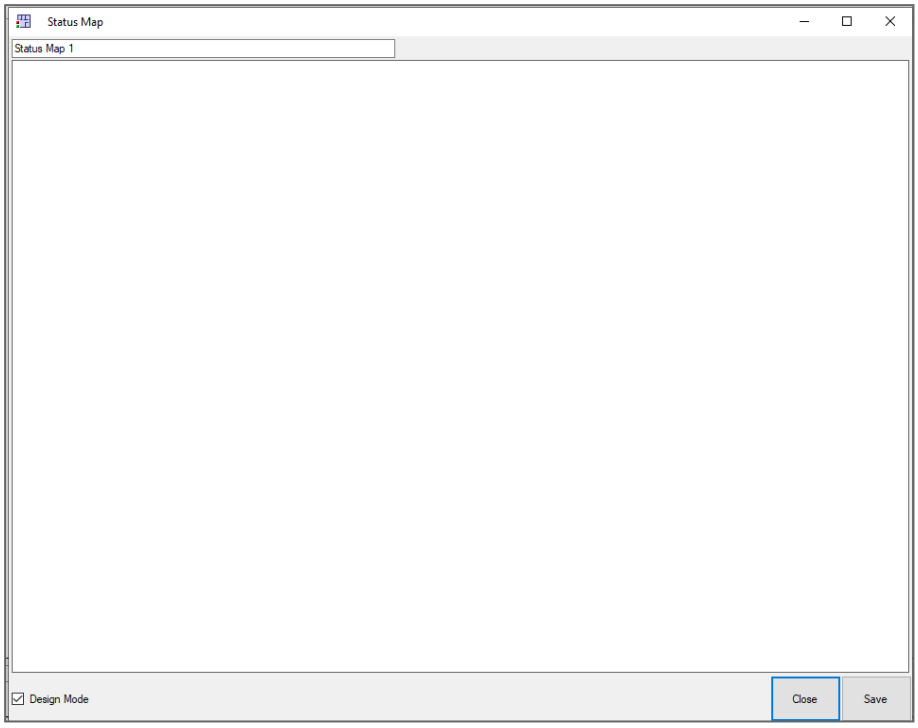
15. Creating Status Maps

The Status Map displays the status of every door, input, and output, antipassback rules, and alarms in the facility on user-selected floor plans.

To set up a Status Map:

1. In the Tree View, select **Status Map**.

2. On the toolbar, click the  icon.



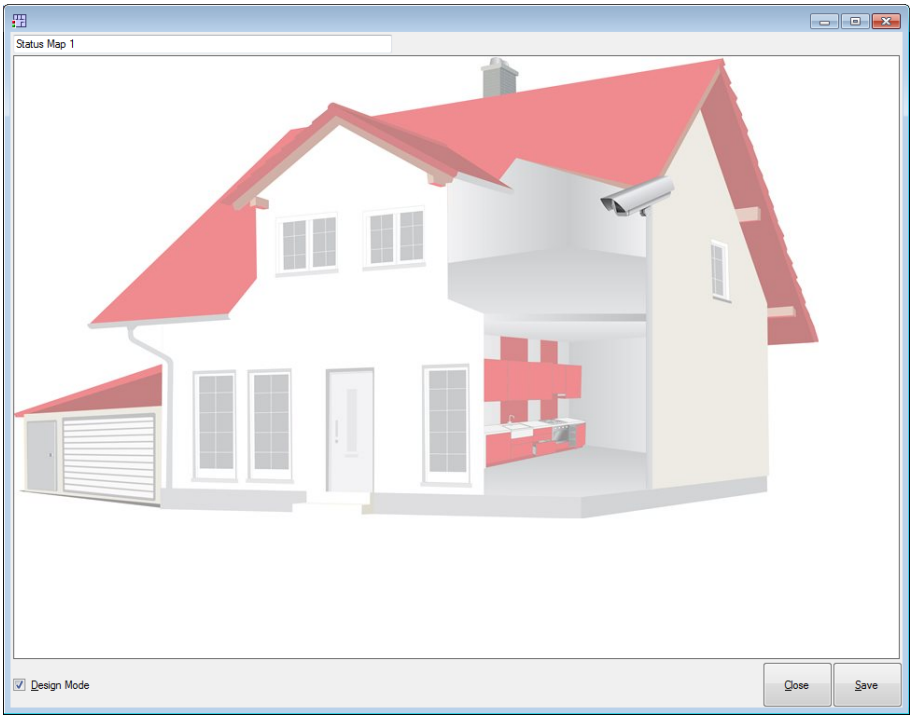
3. Right-click in the window and select **Set background** from the shortcut menu.



To change the map image and/or to add objects on the map, you must select **Design Mode**. The **Add Map** icon on the toolbar is enabled.

4. Select a graphic file (bmp, jpg, gif, or tiff) for the Status Map background.

> Status map icons can also be added to other status maps, indicating where the two map areas meet.



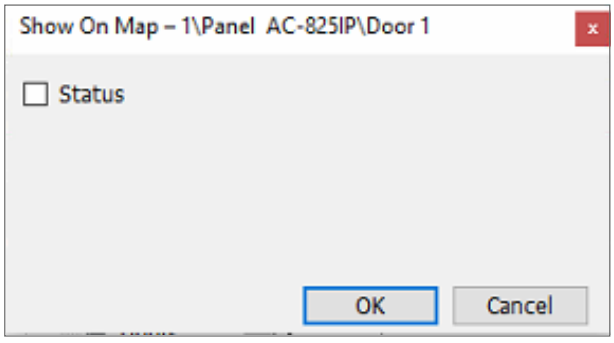
5. Ensure that **Design Mode** is checked.

6. From the **Tree View**, select readers, doors, inputs, outputs, additional status maps, cameras, or panels and click the **Add to Map** icon from the toolbar menu.

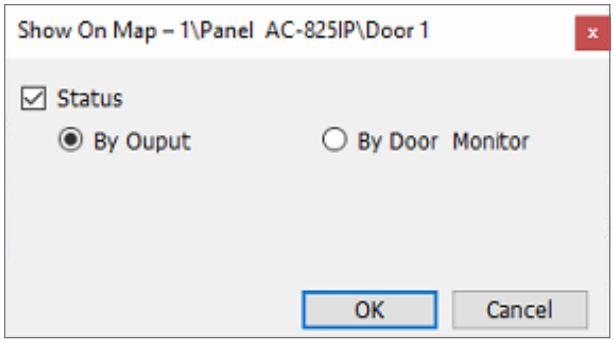
   The objects appear on the status map and can be dragged to their correct positions.



7. Right-click a map object and select **Show on Map** from the shortcut menu.



8. Select **Status** to display the object's state on the status map.



9. For a door's Show on Map properties, select:
   a. **By Door Monitor**: Shows the doors open status based on its physical position.
   b. **By Output:** Shows the doors open status based on the status of its lock.
10. Select **Alarm** to enable a visual alarm on the map for alarm events.

> The alarm option is only available for panel elements where the alarm was already defined (refer to the **Generate Alarm** field in the table in Section Adding Panel Links).

11. Repeat step 6 to 10 as required.
12. Repeats step 1 to 10 to set up additional status maps.

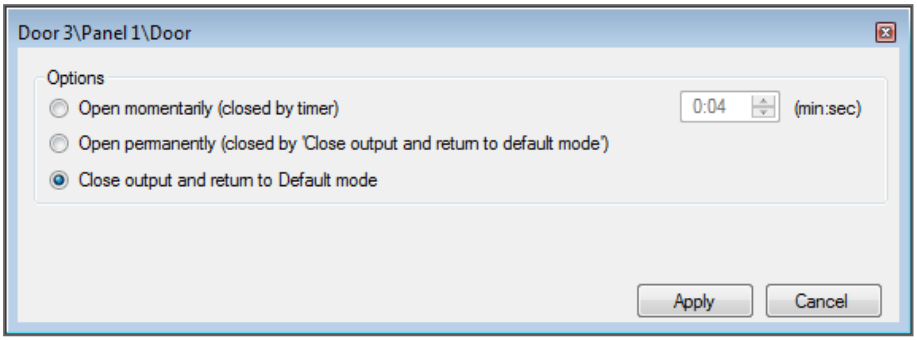
15.1. Manually Opening a Door from Status Map

You can manually open a door while in the Status Map interface.

To manually open a door from the Status Map:

1. Clear **Design Mode** in the lower left corner of the status map.

2. Right-click on a door that appears on the Status Map.



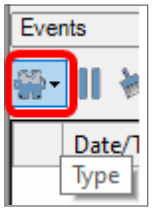
The available options are the same as those in Controlling the Door Manually.

3. From **Options**, select the option you want.
4. Click **Apply**.

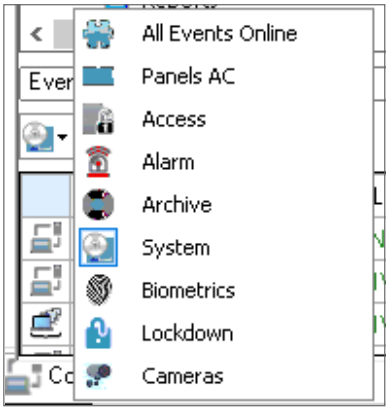
16. Viewing Events

To see events:

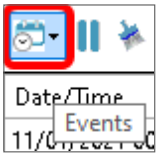
1. In the Events window, select the Type icon.



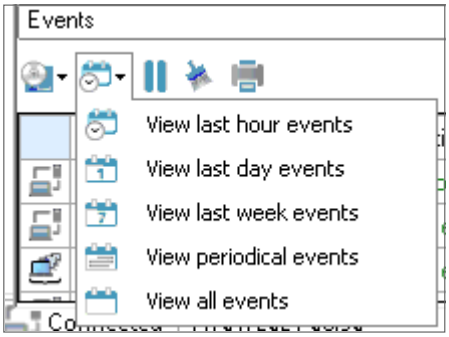
2. Click an icon to see its event list. The options are given below.



3. To select a time period for the events list, click the Events icon.



4. Select a time period.



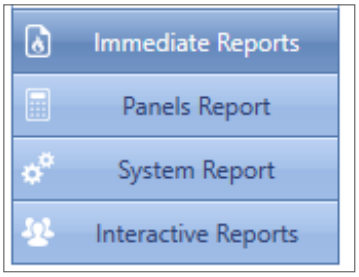
17. Viewing Reports

AxTraxPro can produce various reports, including usage reports, attendance records, visitors, and roll calls. The AxTraxPro Report Wizard allows users to design their own custom reports based on their needs. For more information.

17.1. Generating a Report

To generate a report:

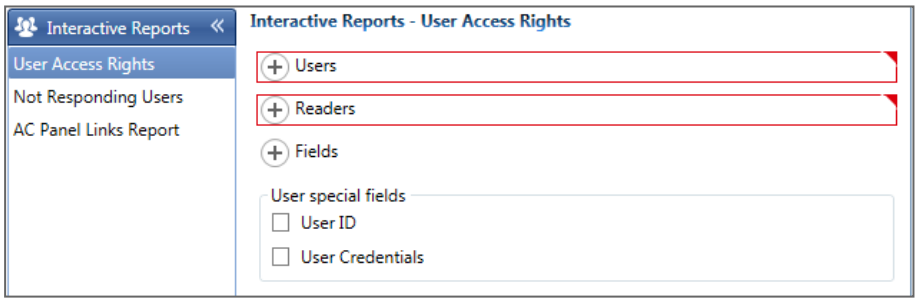
1. In the **Tree View**, select the **Reports** element.
2. Select one of the four main report categories.



3. Select a report type from that category.

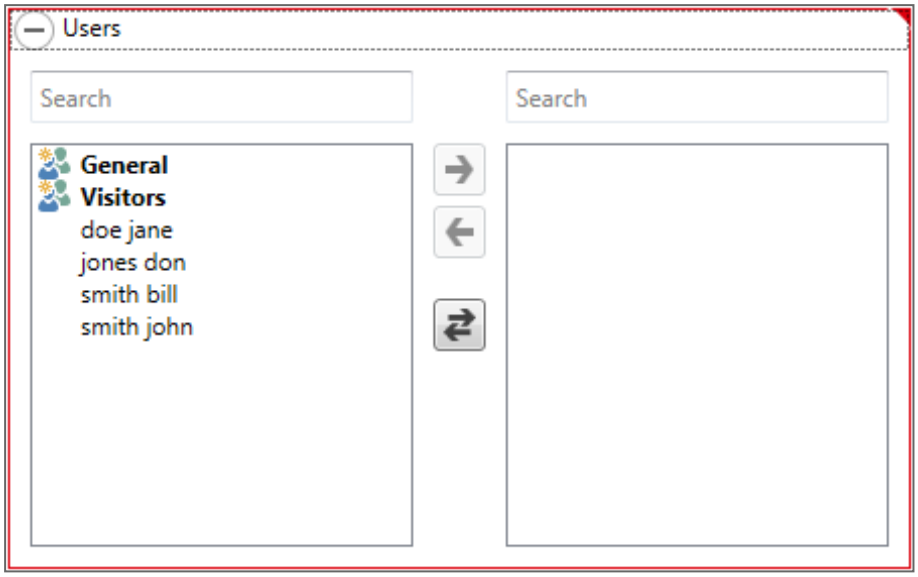
   Depending on the category and type of report selected, the relevant parameters appear in the Display Area.

   For example, the parameters needed for the User Access Rights Report are displayed.



A parameter in red must be selected while a parameter not in red is optional.

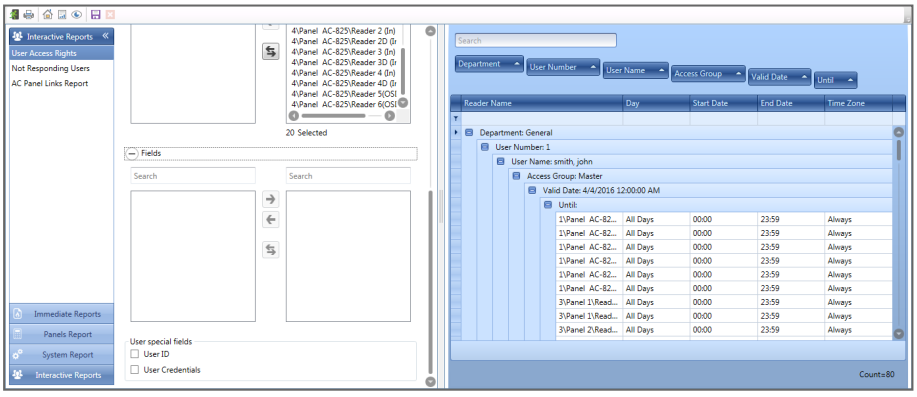
4. Click on a parameter to expand it.



5. Select and move the desired entities using the arrows.

6. Once all the entities in each parameter have been selected, click the icon on the Toolbar to generate a report.

The generated report, in this example the User Access Rights Report, appears in the Display Area.

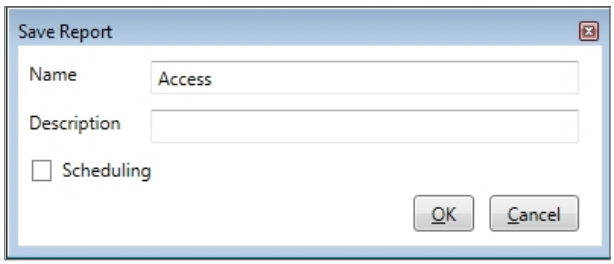


17.2. Scheduling a Report

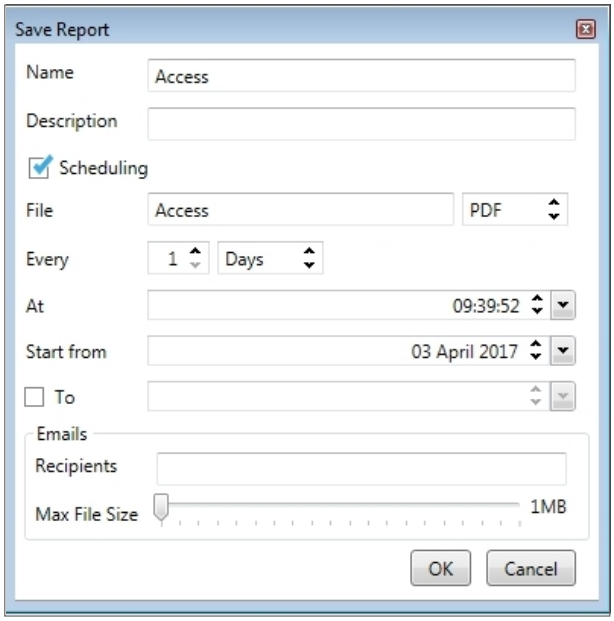
Once you have generated a report for the first time, you can schedule the same report to be generated and saved automatically at a time interval of your choosing.

To schedule a report:

1. With the generated report appearing the **Display Area**, click the  icon on the Toolbar.



2. Enter the name and description of the scheduled report.
3. Select **Scheduling** to expand the options.



4. Using the available fields, set the parameters (format, interval, period of time, email recipients) for the scheduled report to be generated.

> In order to use email notifications, you must configure the SMTP settings (see Notification Settings).

5. Click **OK**.

The saved report appears in the **Display Area**.



To access the list of saved schedule reports at any time, click the icon on the Toolbar.

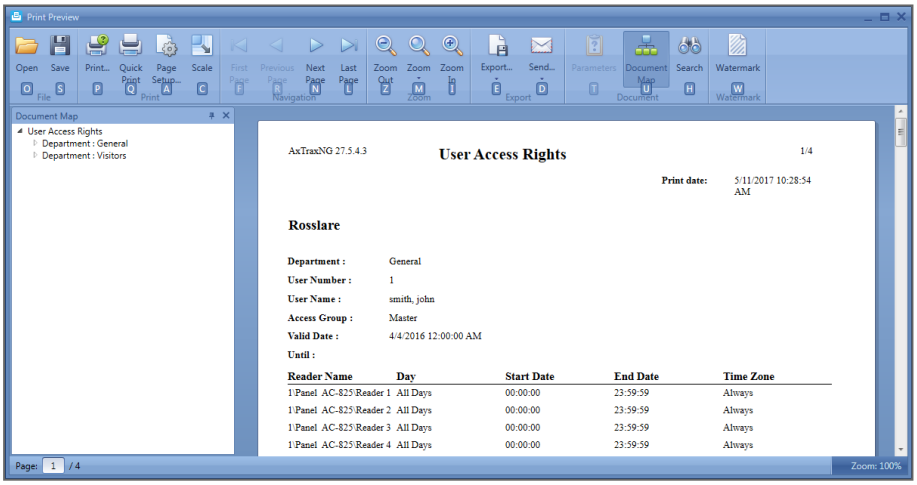
To delete a scheduled report, select that report in the **Display Area** and click the icon on the Toolbar.

17.3. Previewing a Report

You can preview a generated report in order to save or print it.

To preview a report:

1. On the Toolbar, click the icon to preview the report.



The available icons for each type of report preview are described in the following table:

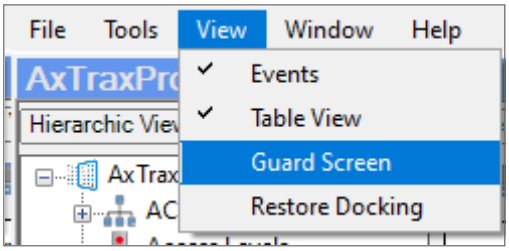
Icon	Name	Click Button To...
	Report Map	Map the report according to the different groups
	Search	Search for text in the document
	Open	Open a pre-saved report
	Save	Save the report document
	Print	Print with adjustable settings
	Quick Print	Print the document with default settings
	Page Setup	Adjust the documents settings
	Scale	Adjust the scaling of the page
	Zoom Out	To view more of the page
	Zoom In	To enlarge the script on the page
	Percentage box	Choose the percentage you wish to zoom in/out in.
	Export document	With the arrow to the right, choose in which format you wish the document to be exported.

Icon	Name	Click Button To...
	Send via email	With the arrow to the right, choose in which format you wish the document to be saved and then sent via email.

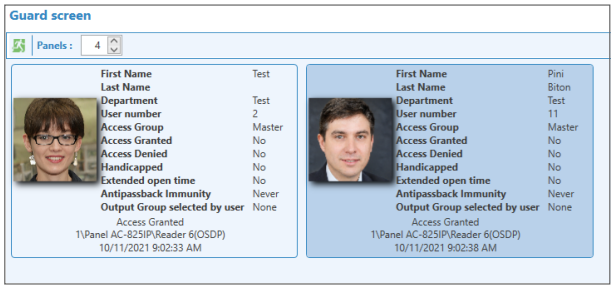
18. Viewing the Guard Screen

To see the guard screen:

1. From the menu bar, select **View > Guard Screen**.



The following Guard Screen window appears.



19. Updating Firmware

The **Update Firmware** window allows an operator to update the firmware version of the selected access control panel. For AC-825IP panels, you can also update the firmware of the connected extensions.

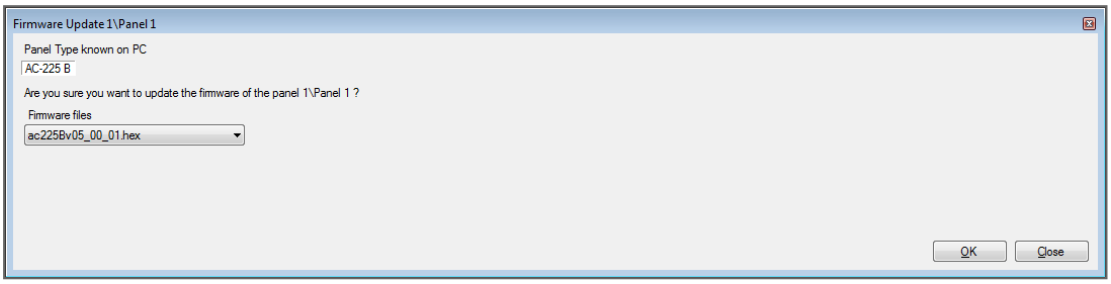
19.1. AC-215x, AC-225x, and AC-425x Panels

To update the firmware:

1. In the Tree View, expand the **AC Networks** element and expand a selected network.
2. Select a panel.

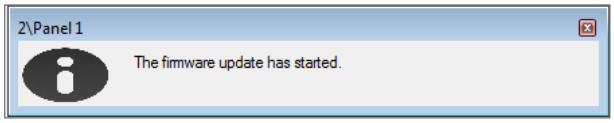
3. On the toolbar, click the  icon.

   The **Firmware Update** window opens.

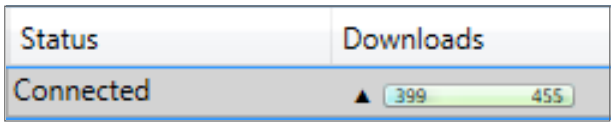


4. From the dropdown, select the HEX file relevant to the panel's hardware type.
5. Click **OK**.

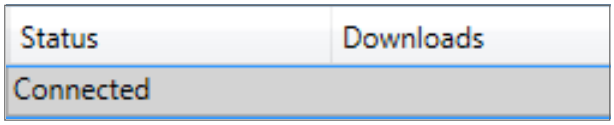
   A progress bar runs at the bottom of the screen until the firmware update is found and then a pop-up appears stating the update has begun.



6. To see the progress of the update, select the network in the **Tree View** and look at the **Downloads** column in the **Display Area.**



   The updated finishes when the number of downloads reduces to zero and then no longer appears in the column. The status of the panel is now "**Connected**".

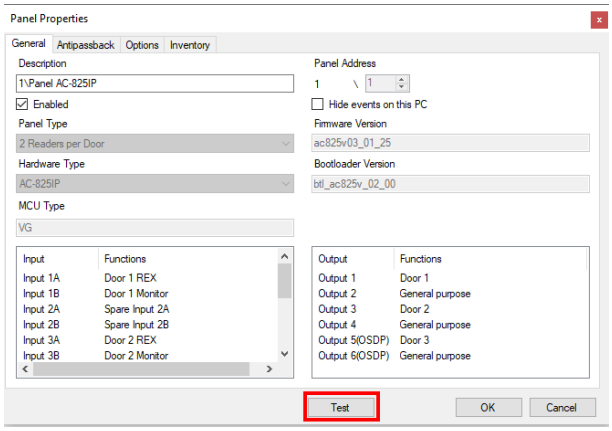


19.2. AC-825IP Panel

The following firmaware update procedure is applicable only for an AC-825IP panel with a VG MCU controller type.

To do a check for the MCU controller type:

1. In the **Tree View**, expand the **AC Networks** element and expand a selected network.
2. Select the AC-825AP panel.
3. Click **Test**.



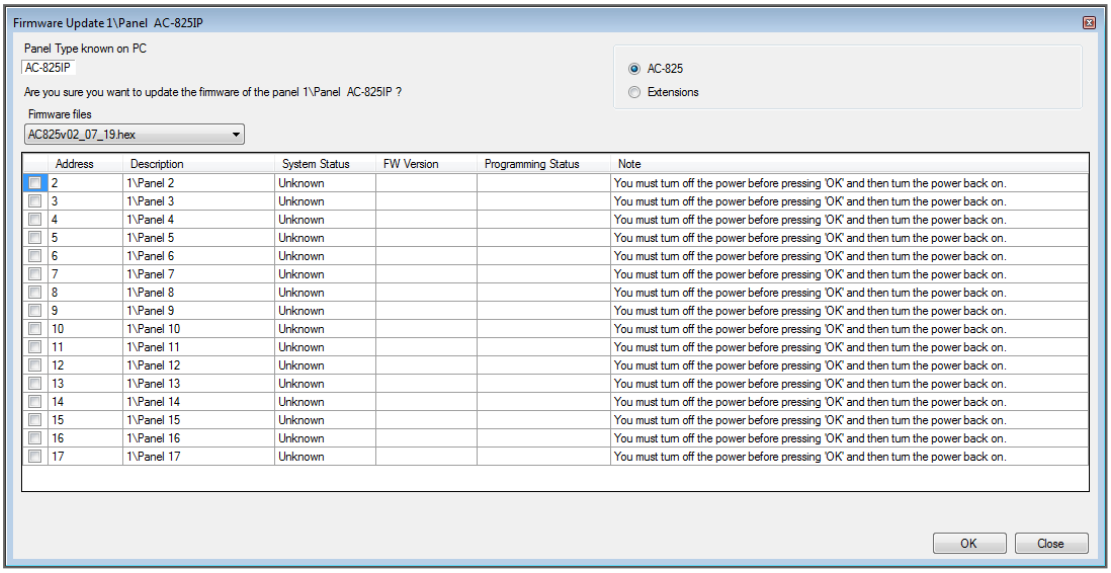
4. Verify that the MCU controller type is VG.



To update the firmware:

1. In the **Tree View**, expand the **AC Networks** element and expand a selected network.
2. Select a panel.
3. On the toolbar, click the  icon.

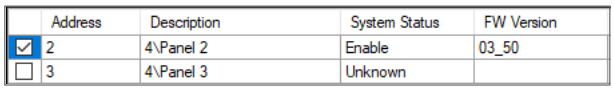
The **Firmware Update** window opens.



4. By default, the main panel is selected to update.



5. From the dropdown, select the HEX file relevant to the panel's hardware type.
6. If you select **Extensions** to update an expansion's firmware, then you must also select which expansion you wish to update.

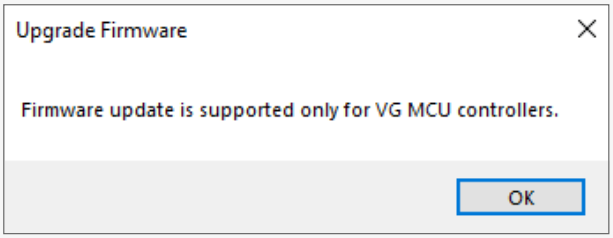


	Address	Description	System Status	FW Version
☑	2	4\Panel 2	Enable	03_50
☐	3	4\Panel 3	Unknown	

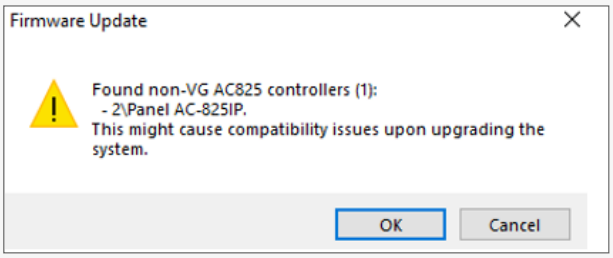
You can only select one panel at a time to update.

7. Click **OK**.

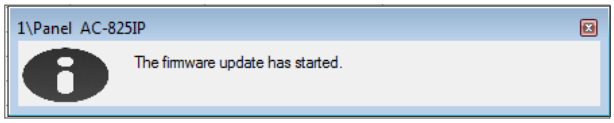
The following message is shown if the AC-825IP is a VC MCU type.



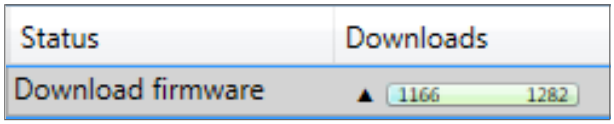
The following message is shown if the AC-825IP is not a VG MCU type or a VC MCU type.



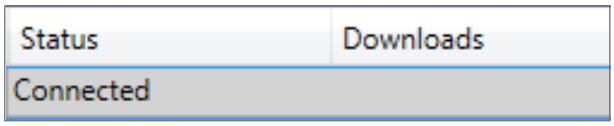
A progress bar runs at the bottom of the screen until the firmware update is found and then a pop-up appears stating the update has begun.



8. To see the progress of the update, select the network in the Tree View and observe the Downloads column in the Display Area.



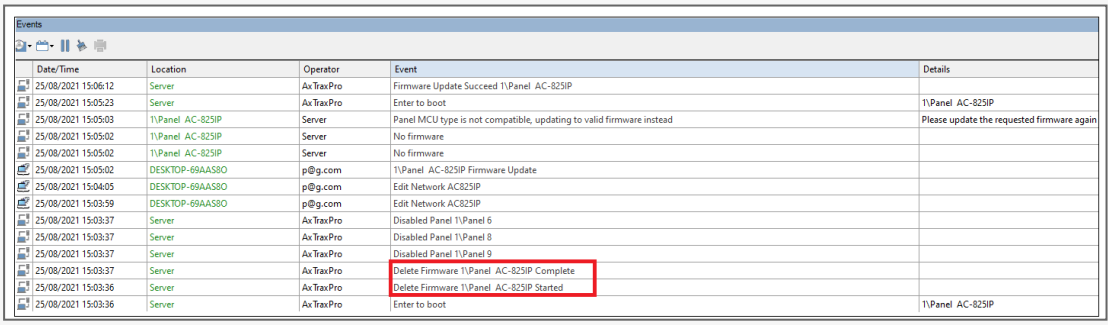
The updated finishes when the number of downloads reduces to zero and then no longer appears in the column. The status of the panel is now "**Connected**".



To delete the firmware:

1. In the **Tree View**, expand the **AC Networks** element and expand a selected network.
2. Select a panel.
3. Click the icon on the Toolbar.

After the firmware is deleted you can see the following in the event log:



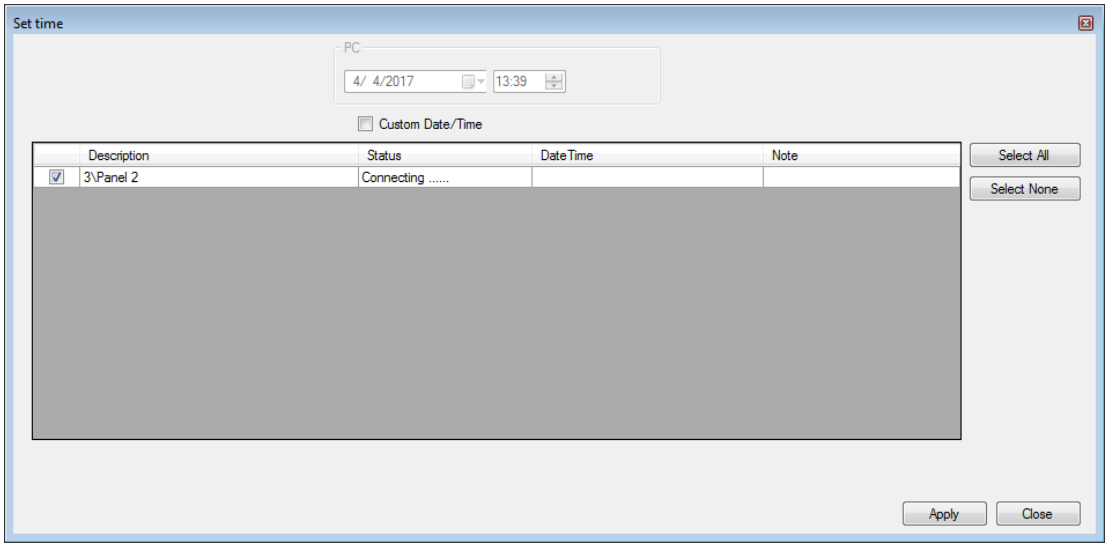
Appendix A. Administrator Operations

A.1 Setting the Time and Date

You can select panels by network and reset their date and time to the AxTraxPro server's system date and time, using the **Set Time** window.

To reset the panel time:

1. In the **Tree View**, expand the **AC Networks** element and select a network.
2. On the toolbar, click the  icon.



3. Select the panels to reset.
4. Click **Apply**.

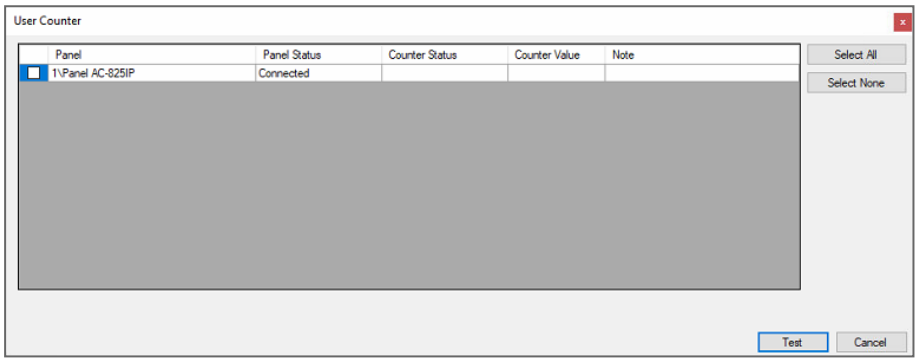
   The server connects to the panels and sets the time as requested. A dialog confirms the operation.

A.2 Testing User Counters

When using User Counters, it is possible to view the current user count value in each panel that has a reader designated with the "**Deduct User**" option.

To view user counters:

1. In the Tree View, select expand the **Users** element.
2. Select the **Visitors** element or expand the **Department/Users** element and select a department.
3. Select a user or visitor in the **Display Area**.
4. On the toolbar, click the  icon.





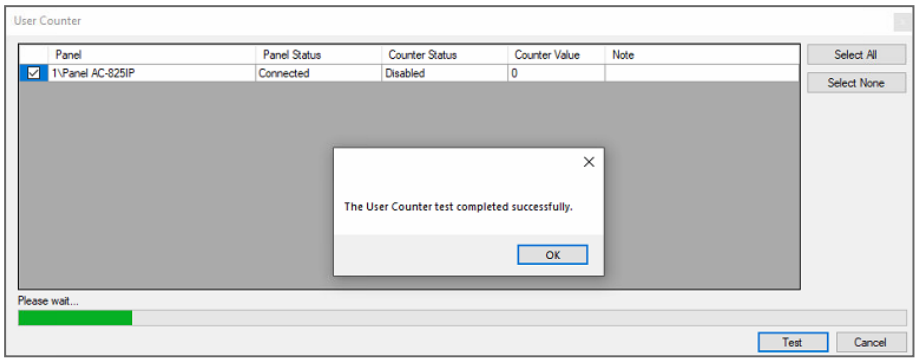
For a panel to appear in the table, that panel must have at least one reader for which the Deduct User Counter option on the General tab of the Readers Properties window is selected.

5. Select the panel(s) you wish to test.
6. Click **Test**.

   A progress bar runs at the bottom of the screen and a confirmation message appears when the test finishes.

7. Click **OK**.

   The remaining fields in the table are now populated.



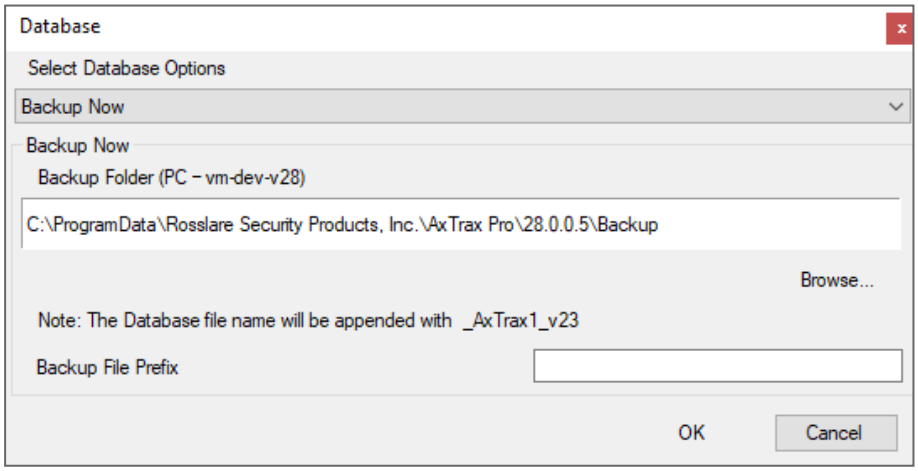
A.3 Maintaining the Database

> It is highly recommended that you back up the system database to an external storage device once a week.

Use the **Database** window to maintain the system database.

To open the Database window:

1. From the menu bar, select **Tools > Database**.



2. From the **Select Database Options** drop down, select your required option, as described in the following table:

Operation	Description
Periodic Backup	Run a scheduled backup every specified number of days at the specified time.
Backup now	Run a one-time backup immediately.
Export Configurations and Events*	Copy the contents of the database to the selected folder.
Import Configurations*	Replace the current configuration based on the imported file. A user's photo can also be imported.
Import Configurations and Events	Replace the current configuration and events based on the imported file.
Erase Configuration and Events*	Erase the current database configuration and all events.
Limit Panel Events Period	Automatically erase events when they are older than a specified number of days. Before using this option, Rosslare recommends that you set a periodic backup. It is recommended to set the value to no more than 91 days.
Erase Panel Events	Erase all events that are older than a specified number of days
Import earlier database versions from AxTraxNG/AxTraxPro	Replace the current database A user's photo can also be imported.
Export Access Events	Copy the Access events content of the database to the selected folder.

*This option is only available in the AxTraxPro PC.

3. Click **Browse** to search for the file to import or to select the folder to export to.

If you wish to import a DB file, the file should be located in the C:\ProgramData\Rosslare Enterprises Ltd folder. You may need to show all hidden files to see the Program Data folder.

The Backup and Export functions add "_AxTrax1_vX" to the end of file name of the exported or backed up database. The Import Database function executes only with a file that contains this string at the end of the file name. After a database is imported, the panel status may change to disabled. If this occurs, the operator should re-enable the panels.

4. Click **OK**.

A.4 AxTraxPro Options and Preferences

AxTraxPro can be customized to meet the preferences of the operator using the **Options** window.

To open the Options window:

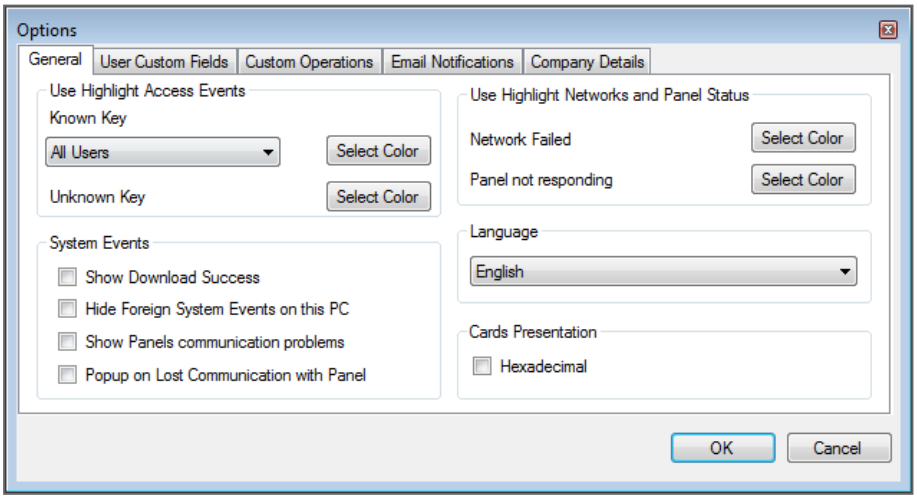
1. From the menu bar, select **Tools > Options**.

   The **Options** window has five tabs:

   - **General** – General startup and presentation settings
   - **User Custom Fields** – Additional user-defined fields for the **User Properties** window
   - **Custom Operations** – Used to upload users to the system from a text file
   - **Email Notifications** – Used to send a notification of selected events to a list of specified emails
   - **Company Details** – Site details (name and address) that are displayed on the report

A.4.1 General Tab

The **General** tab includes presentation connection settings.

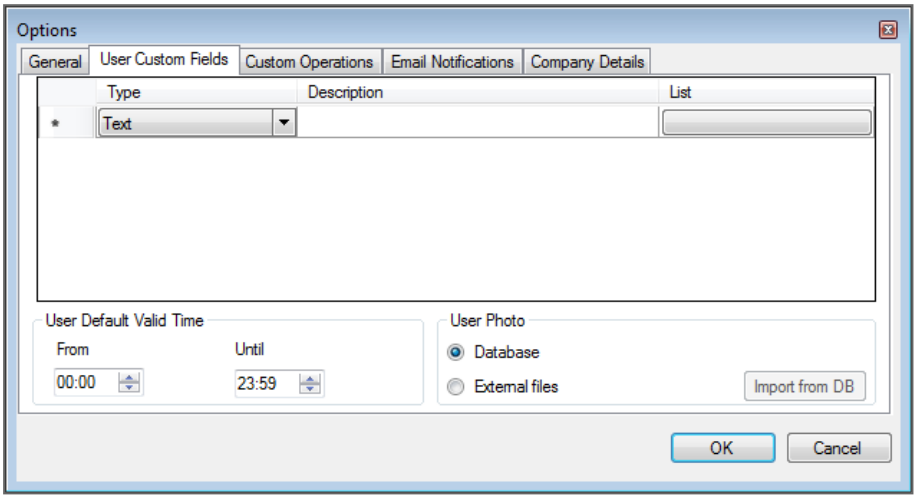


The **General** tab contains the following fields:

Field	Description
Use Highlight Access Events	From the **Known Key** drop down, select the desired option and click **Select Color** to display selected user information in a custom picked colored highlight. Click **Select Color** adjacent to **Unknown key** to define the highlight color for unknown keys.
System Events>Show Download Success	Select to add a message to the event history upon successful system parameters download from the AxTraxPro software to the panel.
System Events>Hide Foreign System Events on this PC	Select to see only local administrator and AxTraxPro Server messages.
System Events>Show Panel Communication Problems	Select to have status indicate panel communication problems
System Events>Pop-up on Lost Communication with Panel	Select to have a pop-up appear if communication with a panel is lost. After selecting the check box, disconnect the working panel and wait for a minute or two to see that the pop-up appears.
Use Highlight Networks and Panel Status	Click **Select Color** adjacent to **Network failed** to define the highlight color for network alarms. Click **Select Color** adjacent to **Panel not responding** to define the highlight color for panel communication errors.
Language	Select the system interface language.  Setting the language to Farsi also changes the date format to the Farsi date format.
Cards Presentation	Changes the display of card details to hexadecimal format.

A.4.2 User Custom Fields

The **User Custom Fields** tab controls the user-defined fields in the **General** tab of the **User Properties** window.

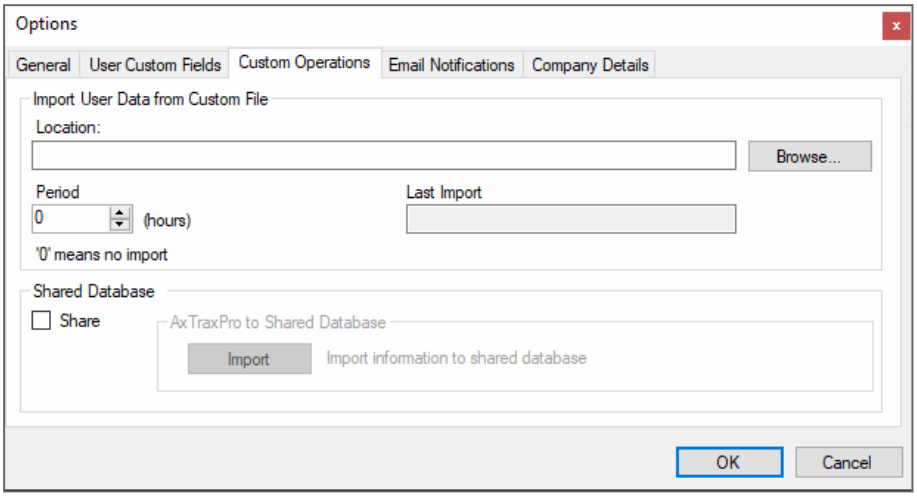


The **User Custom Fields** tab contains the following fields:

Field	Description
Type	Select the type of field. If Type is **list**, click **Edit List** and enter list items.
Description	Type a name for the new field.
User Default Valid Time	Set default start and end time for user access rights using the **From** and **Until** fields.
User Photo	Define the default photos to be used: • **Database:** Use the User photos save in the database • **External files:** Use this option to save a large user photo collection external from the database • **Export from DB:** Click to export existing photos from the database to an external folder

A.4.3 Custom Operations

The **Custom Operations** tab is used to upload user data to the system from a text file and to set the shared database option.

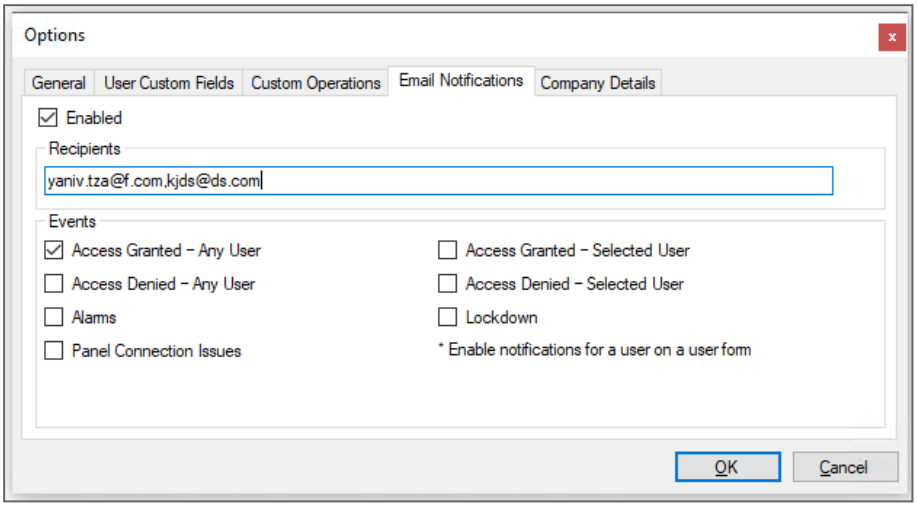


The **Custom Operations** tab contains the following fields:

Field	Description
Import User Data from Custom File	This option allows you to import visitor user data from a text (*.txt) file. The data imported is for the following fields: User Number, Last Name, First Name, Employment Date in dd/mm/yy format, Validity Date (optional). A "," separation must be between the values. Each visitor should be in a new line of the text file. Select the location of the file to import/export by using **Browse**. From the **Period** box, select the time period. The period is the time between import processes in hours where '0' means the import is only in manual operation.
Shared Database > AxTraxPro to Shared Database	Click **Import** to create a database from the above data from which the data can be shared by an external program.

A.4.4 Email Notifications

The **Email Notifications** tab is used to send a notification of selected events to a list of specified emails.

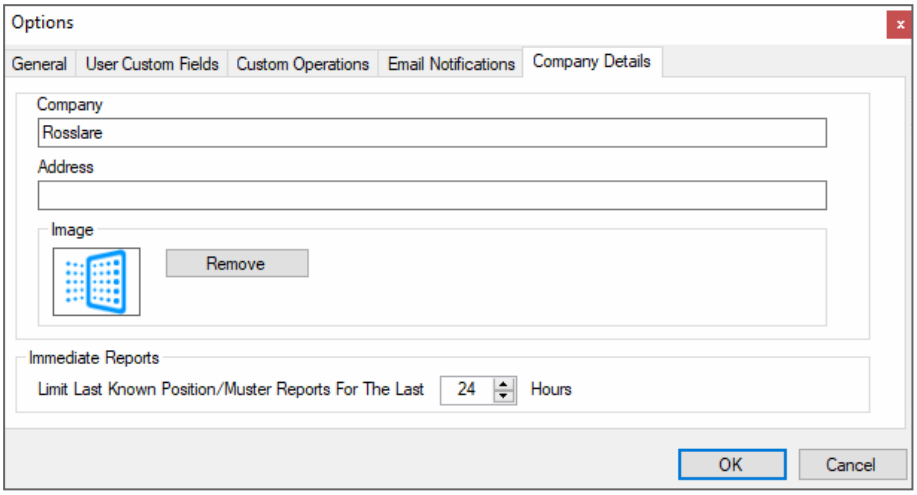


Enter the email addresses of your recipient(s) and select the events for which you wish them to receive notifications.

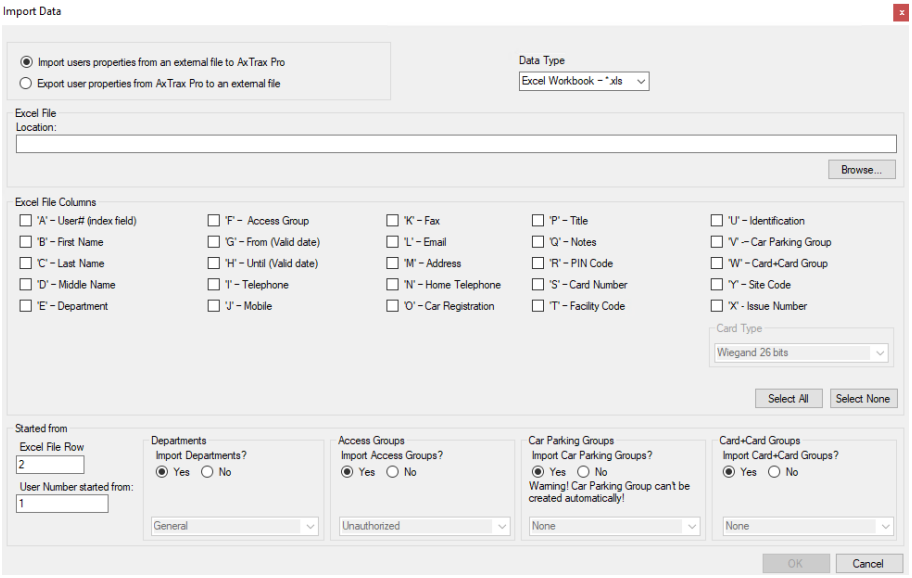
In order to use email notifications, you must configure the SMTP settings (see Notification Settings).

A.4.5 Company Details

The **Company Details** tab displays the name and address that are displayed on reports.



A.5 Importing/Exporting User Data



The **Import/Export Data** window makes it possible to import/export user information into/from the AxTraxPro database from/to a standard spreadsheet file.

To import/export user data:

1. From the menu bar, select **Tools > Import/Export Data**.

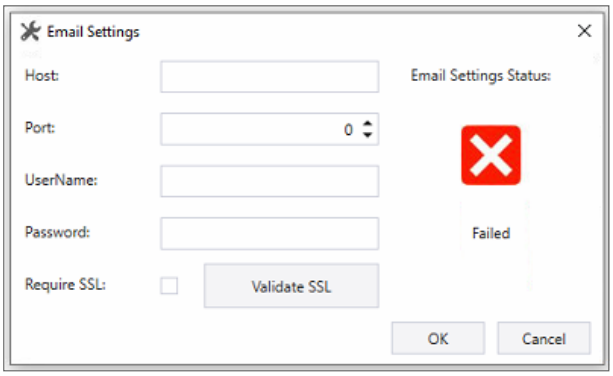
2. Set the import/export options according to the field descriptions in the following table:

Field	Description
Import Users properties from external file into AxTraxPro	Select this option to import user properties
Export Users properties from AxTraxPro into external file	Select this option to export user properties
Data Type	Select the type of data file to import/export.
Location	Select the location of the file to import/export by using **Browse**.
Excel File Columns	Select the check boxes of the columns to be imported or exported. Data in each column (A–T) are imported or exported as listed.  When exporting the Notes field (Column Q), only the first 256 characters are included.
Excel file Row	Enter the first row of user data in the spreadsheet.
User number started from	Enter the number from which to start assigning unique system user numbers.
Import Departments?	Select **Yes** to import new departments into the AxTraxPro database. Select **No** to import users without their departments.
Department	Select the department to assign to the imported users. This box is only active when the **No** option is selected in the Import Departments option.
Import Access Groups?	Select **Yes** to import new access groups into the AxTraxPro database. Select **No** to import users without their access groups.
Access Groups	Select the access group to assign to the imported users. This box is only active when the **No** option is selected in the import access group option.
Import Car Parking Groups?	Select **Yes** to import new car parking groups into the AxTraxPro database. Select **No** to import users without their car parking groups.
Car Parking Groups	Select the car parking group to assign to the imported users. This box is only active when the **No** option is selected in the import car parking group option.
Import Card+Card Groups?	Select **Yes** to import new card+card groups into the AxTraxPro database. Select **No** to import users without their card+card groups.
Card+Card Groups	Select the card+card group to assign to the imported users. This box is only active when the **No** option is selected in the import card+card group option.

3. Click **OK**.

A.6 Notification Settings

Use **Notification Settings** to set the SMTP configuration, view the reports directory, and set the static IP option.



To set the Notification Settings:

1. From the menu bar, select **Tools > Notification Settings**.
2. Set the options according to the field descriptions in the following table:

Parameter	Description
SMTP Settings > Host	The address of your SMTP server
SMTP Settings > Port	The port of your SMTP server
SMTP Settings > User Name	The account name of your SMTP server
SMTP Settings > Password	The password of the account
SMTP Settings > Require SSL	Check if you want your SMTP server to be secured
SMTP Settings > Email Validation	Click to validate the SMTP settings
Report Directory	The default location of reports that are generated and saved automatically as scheduled (see Scheduling a Report).
IP Address > Use Static IP	Check **Use Static IP** to enter a real IP address. Server communicates with clients by remote technology. Default Server's IP address is 127.0.0.1. If PC uses some network cards or virtual networks simultaneously, remote communication may be problematic.

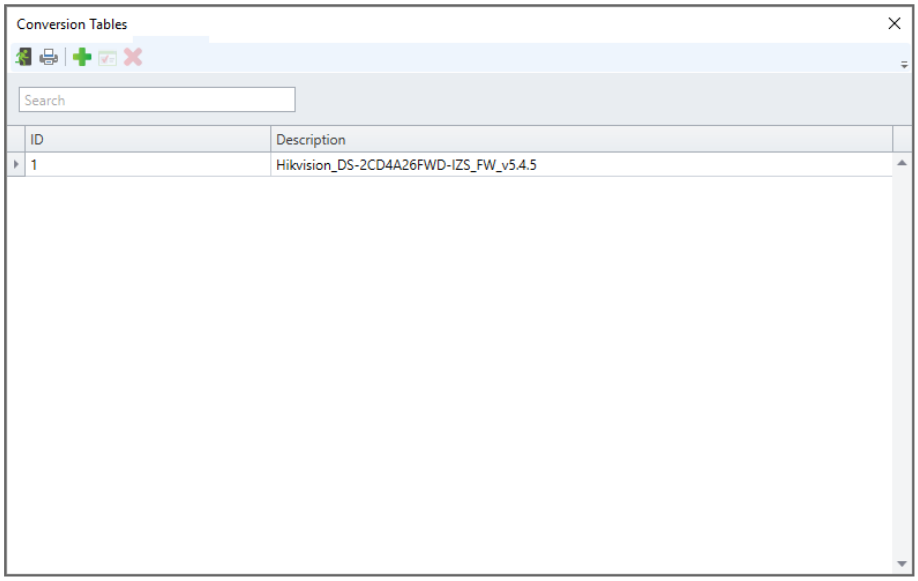
3. Click **OK**.

A.7 Conversion Tables

A conversion table converts the alphanumeric character on a license plate to a binary number that can then be understood by the relevant reader as a Wiegand input.

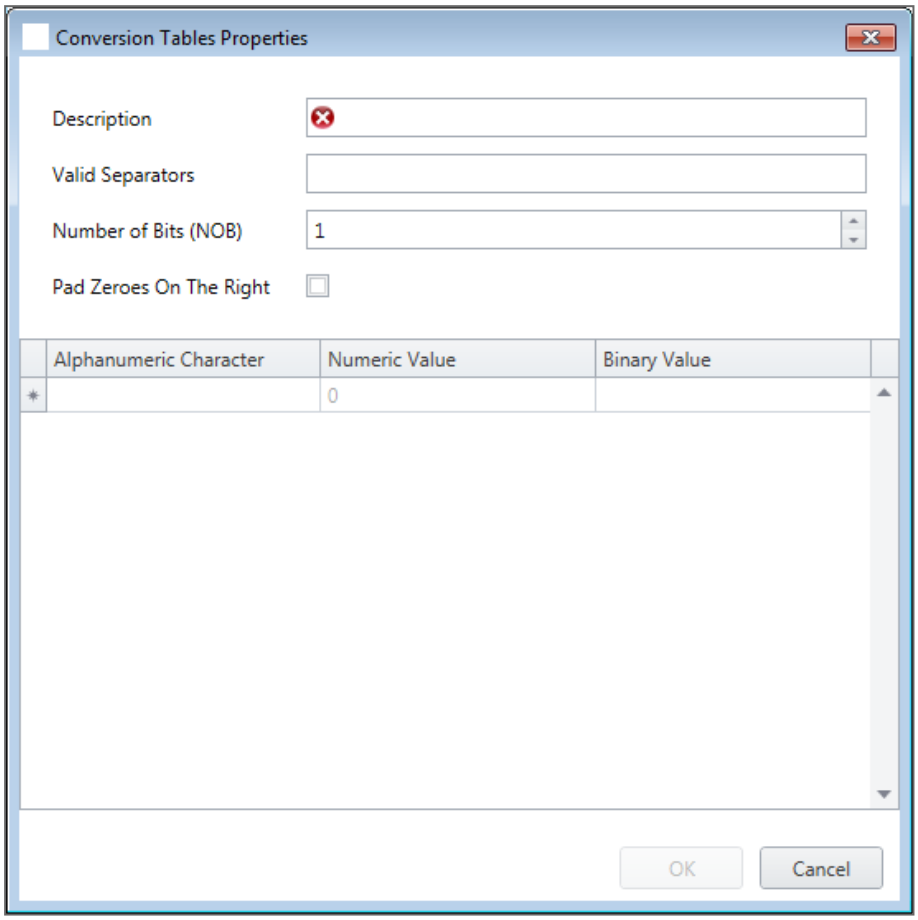
To create a conversion table:

1. From the menu bar, select **Tools > Conversion Tables**.



2. On the toolbar, click the icon.

   The window closes and the new conversion table appears in the **Display Area**.



3. Set the conversion table options according to the field descriptions in the following table:

Field	Description
Description	The name of the conversion table
Valid Separators	Enter the separator that appears in the license plate. A typical example is "-".
Number of Bits (NOB)	Enter the number of bits that each alphanumeric character uses
Pad Zeroes on the Right	Check if you wish to replace any unused bits in the chosen Wiegand format with zeroes on the right of the Wiegand code.
Alphanumeric Character	The alphanumeric character appearing on the license plate

Field	Description
Numeric Value	The numeric value given to the above alphanumeric character
Binary Value	The binary value given to the above alphanumeric character

4. Click **OK**.

Appendix B. Configuring a Network

The AxTraxPro Server connects to access control units by a serial connection, a TCP/IP connection.

B.1 TCP/IP Connection

To connect access control panels to AxTraxPro over a TCP/IP LAN or WAN, the use of a TCP/IP to Serial converter is required, unless the panel has an onboard TCP-IP connection (AC-225IP).

Each TCP/IP connection can support up to multiple access control panels that are connected to each other using RS-485 (up to 32 AC-215, AC-215IP, AC-225, or AC-425 panels, or up to 12 extensions with the AC-825IP panel).



The recommended RS-485 cable is a shielded twisted pair (22 AWG).

The hardware used to connect to the TCP/IP network may be the MD-N32, which is a serial to Ethernet converter, or the onboard converter of the AC-225IP.

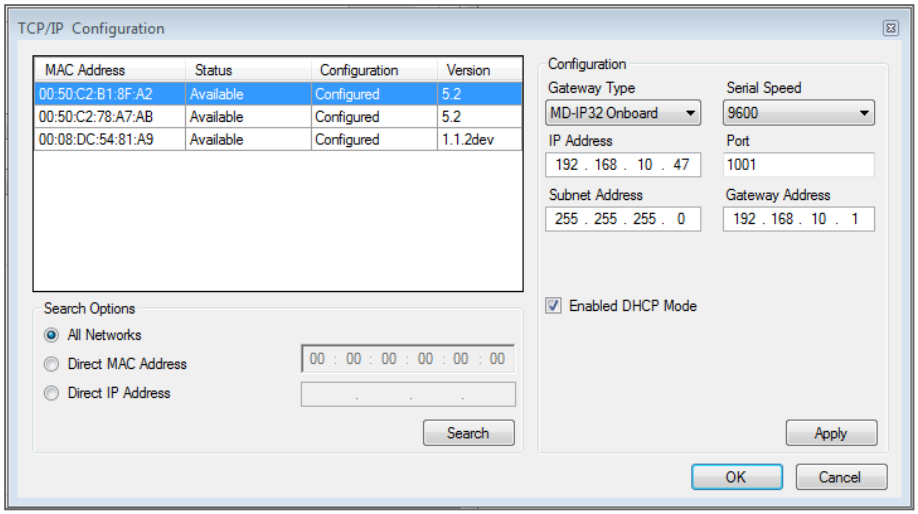
To configure a TCP/IP connection to a network:

1. In the Tree View, click **AC Networks**.
2. On the toolbar, click the  icon.
3. Set the Network type as **TCP/IP**.



If you want to work with Remote, select **Remote (WAN)** in the TCP/IP Network window, and add the WAN IP Address of the PC.

4. Click **Configuration**.



The upper left window lists all TCP/IP converters connected to the local network, identified by their MAC address, and indicates if they have been previously assigned to a network or not.

5. From the MD-N32 list (the MD-N32's MAC address should be labeled on the TCP/IP converter), select the appropriate MAC address.
6. In **Gateway Type**, select the type of TCP/IP converter (MD-N32, MD-IP32 Onboard, or any other valid option).

   For an AC-825IP panel, the IP module should be configured to the AxTraxPro server. Even if the IP module was configured before, you need to click **Apply** to configure with the server and then click **OK** to add the AC-825IP network.
7. Enter the IP address and subnet address for the computer's network.
8. Select the serial speed of your connection and enter the port number. It is recommended to select a higher value port number (4001 or higher). Note that the selected should not end with zeros (prefer setting Port value of 4243 rather than 4200). This avoids colliding with port addresses reserved for various equipment installed on the same network.
9. Enter the default gateway address of the computer's network.
10. Click **OK** to start the verification process.
11. Turn off the MD-N32 power (or panel power if using the onboard module, such as MD-IP32), and then turn the power on again. This step is necessary when using certain versions of MD-N32 or MD-IP32 models. Skip this step if not applicable.
12. If configuration applies to a WAN network, disconnect the configured unit from the local network, and reconnect to the WAN network and access control panels network working over the WAN.

Appendix C. Configuring User Counters

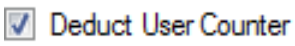
You can use the User Counter options to limit the number of entrances of a particular user. This is done using the Counter option that appears on the **User Properties** window.

To configure user counters:

1. Select the **General** tab of the **User Properties** window either as part of the procedure of adding a new user or select an existing user.
2. On the toolbar, click the  icon.
3. In the Counter section of the **User Properties** window, select **Enable**.
4. Select **Set New Counter** and specify the number of allowed entrances for the user using the **Counter Value** box.



5. Click **OK**.
6. Select the **General** tab of the **Reader Properties**.
7. In the Details section, select **Deduct User counter**.



8. Click **OK**.

C.1 Resetting Counter on Panel Re-enable

There is an additional counter option that allows you to reset the user counter to its starting value in the event that a panel is disconnected and then reconnected again.

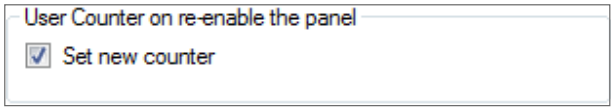


If this option is not used, then upon panel re-enable, the user counter continues with its previous value prior to having that panel disabled.

To reset the user counter on panel re-enable:

1. In the Tree View, expand the **AC Networks** element.
2. Select a network.

3. On the toolbar, click the  icon.
4. Select the **Options** tab.
5. Select **Set new counter**.



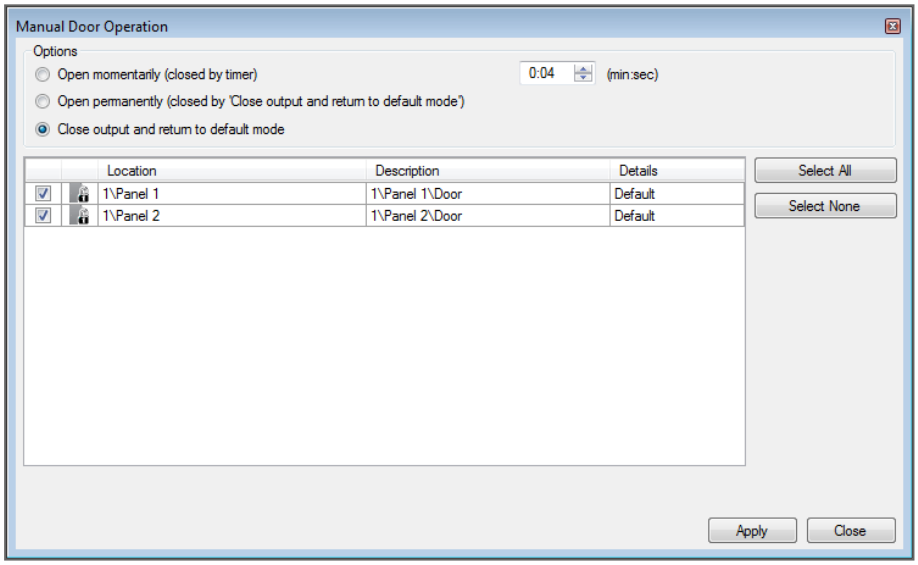
6. Click **OK**.

Appendix D. Controlling the Door Manually

The **Manual Door Operation** window allows an operator to open or close a selected group of doors directly.

To manually open or close a door:

1. In the Tree View, expand the **AC Networks** element.
2. Expand a network and expand a panel.
3. Select **Doors**.
4. On the toolbar, click the  icon.



5. Sort the listed panels/doors in regular or reverse order, by clicking the column header with the left mouse button.
6. Select an option:

   Open momentarily – Open all selected doors for the time set in the timer box

   Open permanently – Opens all selected doors

   Close output – Closes all selected doors and returns control to AxTraxPro
7. Select the checkboxes of those doors to which to apply the operation.
8. Click **Apply**.



If the **Manual Output Operation** to open a door is set to disable, the door can still be opened in a **Status Map**, see Creating Status Maps.

Appendix E. Enrolling a Face from a Terminal

This option is available for users connected to a terminal.

To enroll a face using a terminal:

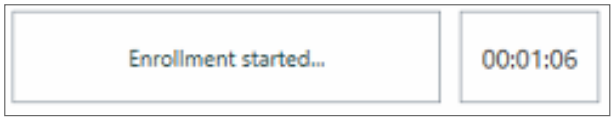
1. Be sure the biometric terminal is connected.
2. In the Tree View, expand the **Users** element.
3. Expand the **Departments/Users** element and select the relevant department.
4. Select the user and click the  icon.
5. On the **Credentials** tab in the **Users Properties** window (Section Credentials Tab), click **Enroll Face from Terminal**.



6. Select the enrollment source.

7. Click **Enroll**.

   The left box shows the status while the right box shows how much time you have left to enroll your face.



8. Stand in front of the terminal, wait until your face is identified, and follow the onscreen instructions.

   Once the face is enrolled, the left box displays a success message.

9. Click **OK**.

   The window closes and the new fingerprint appears in the **Details** area.

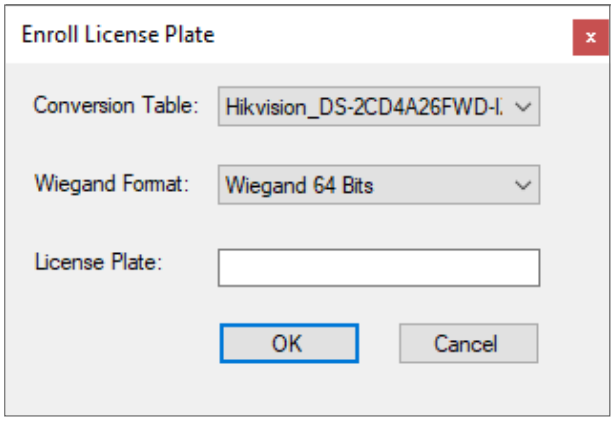
10. Click **OK** in the **Users Properties** window to accept the face credential.

Appendix F. Enrolling a License Plate

This option allows you to convert alphanumeric characters read by a third-party camera to a Wiegand format using a user-defined conversion table that is understood by the AxTraxPro system.

To enroll a license plate:

1. In the Tree View, expand the **Users** element.
2. Expand the **Departments/Users** element and select the relevant department.
3. Select the user and click the  icon.
4. On the **Credentials** tab in the **Users Properties** window (see Credentials Tab), click **Enroll License Plate**.



5. Select the conversion table (see Conversion Tables).
6. Enter the license plate number.
7. Click **OK**.

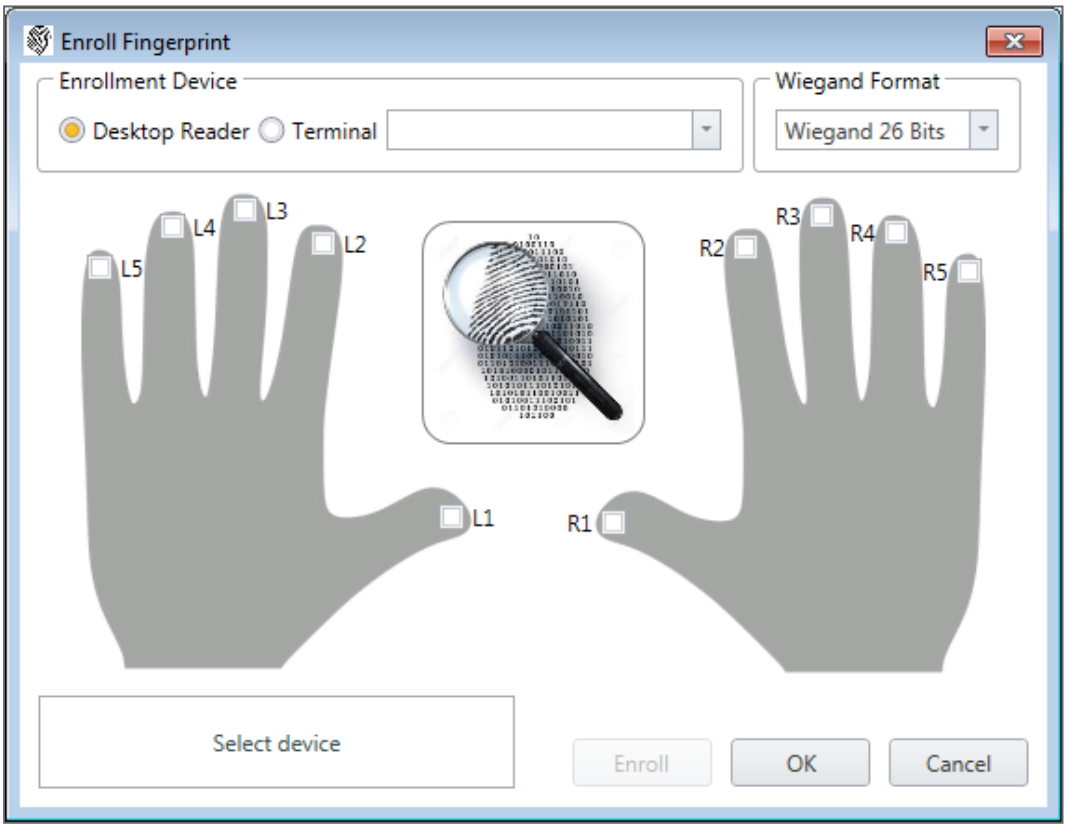
Appendix G. Enrolling a User's Fingerprint

If using DR-B9000 desktop Fingerprint scanner you have to install a dedicated driver to your Windows PC.

This option is available for users who need to use a biometric terminal.

To enroll a user's fingerprint using a biometric reader:

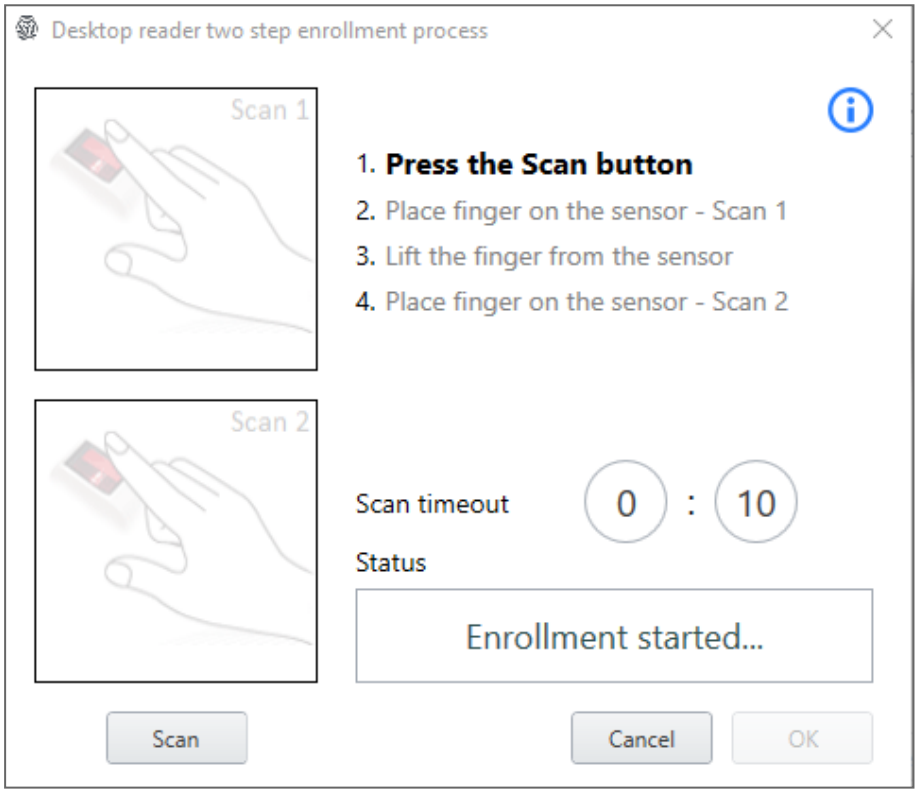
1. Be sure the biometric terminal is connected.
2. In the Tree View, expand the **Users** element.
3. Expand the **Departments/Users** element and select the relevant department.
4. Select the user and click the  icon.
5. On the **Credentials** tab in the **Users Properties** window (see Credentials Tab), click **Add from a Fingerprint Reader**.



6. Select the enrollment source (Enrollment Device).

> If using Desktop Fingerprint scanner you will have 2-step enrollment process in addition to a live Fingerprint image

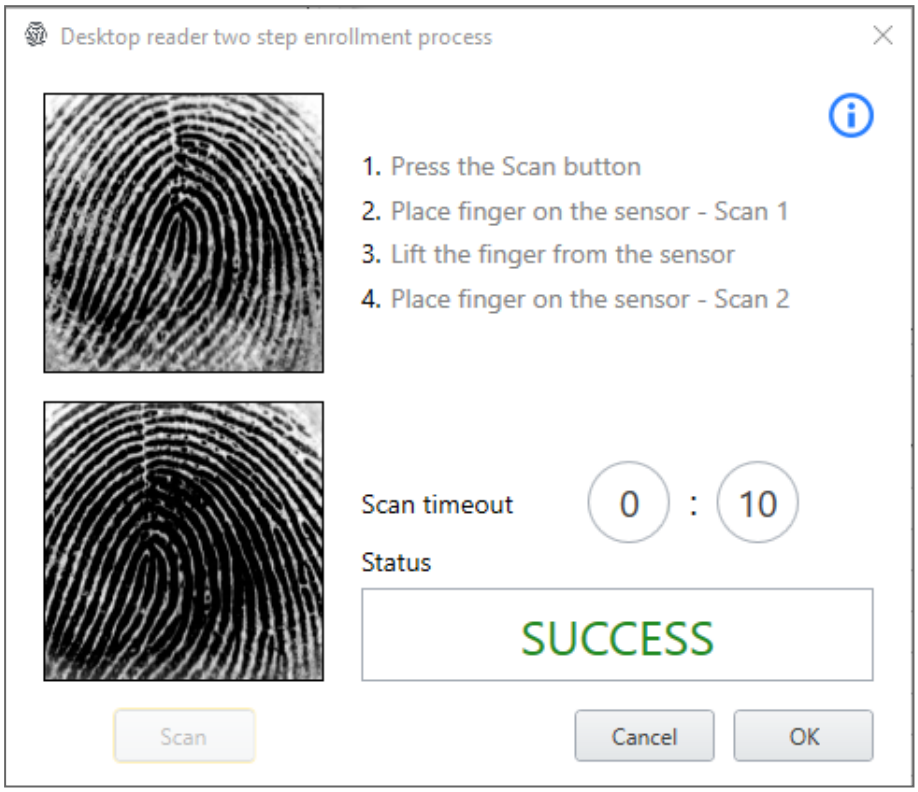
7. Select the finger that you want to enroll.
8. Click **Enroll**. You should see the screen shown below. Follow the instructions on the screen for successful enrollment.



9. Press the **Scan** button.
10. Place finger on the sensor – Scan 1.
11. Lift the finger from the sensor. Wait 3 seconds.

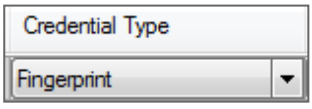
12. Place finger on the sensor – Scan 2.

    You should see that the finger was read successfully as shown below.



13. Click **OK**.

    The window closes and the new fingerprint appears in the **Details** area.



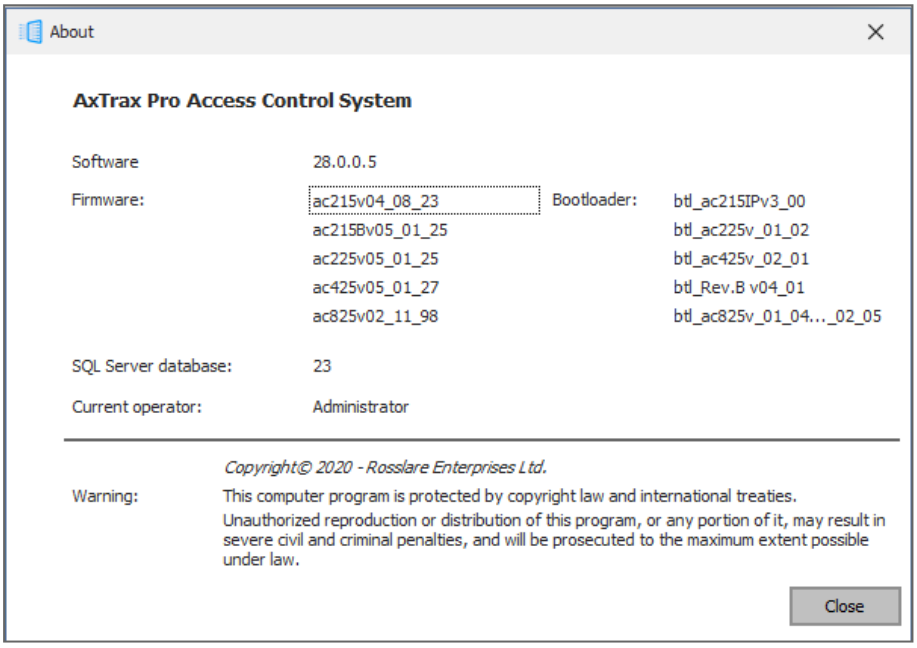
14. Click **OK** in the **Users Properties** window to accept the fingerprint.

Appendix H. Help Menu

The Help menu has four options:

H.1 About

The **About** window displays software, firmware, and database versions, the current operator, and licensing information.



H.2 User Manual

Clicking **User Manual** opens the user manual for AxTraxPro.

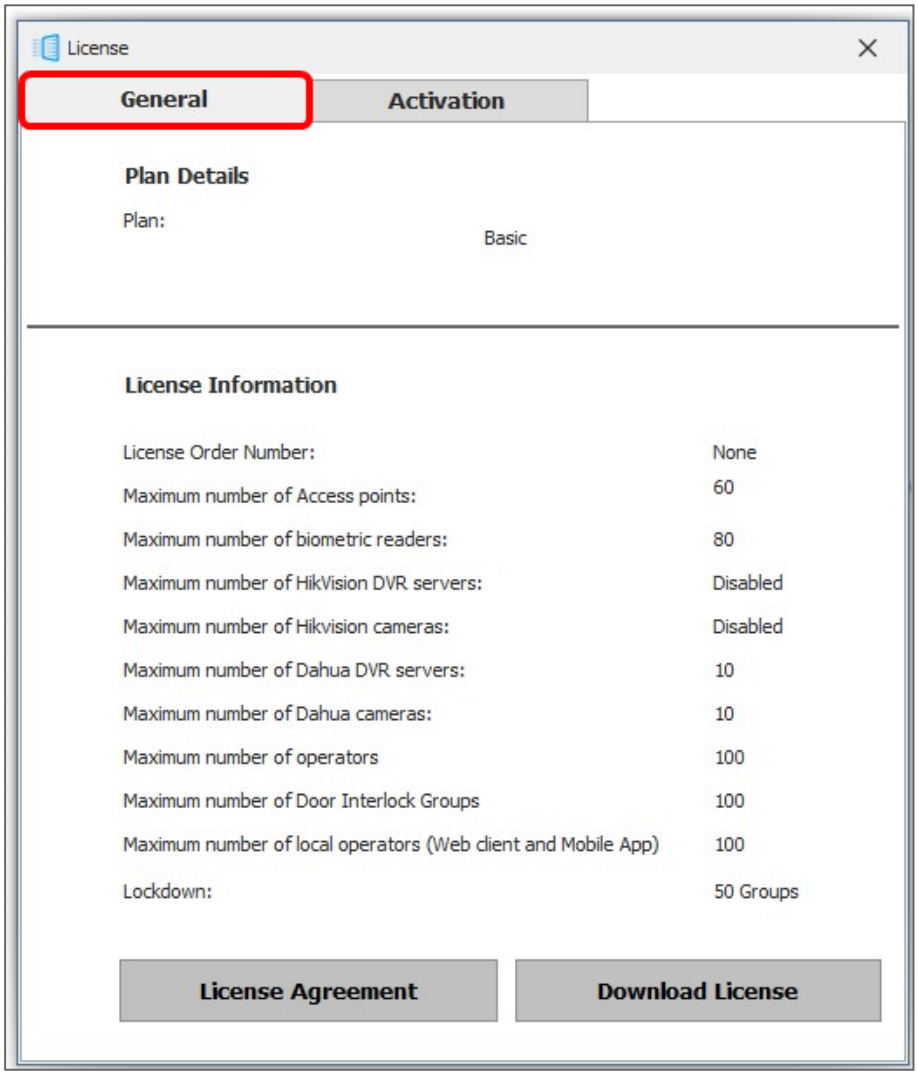
H.3 AxTraxPro Product Activation

The License window is used to see information about the current license and to activate a new license.

19.2.1. General Information about AxTraxPro and the License Agreement

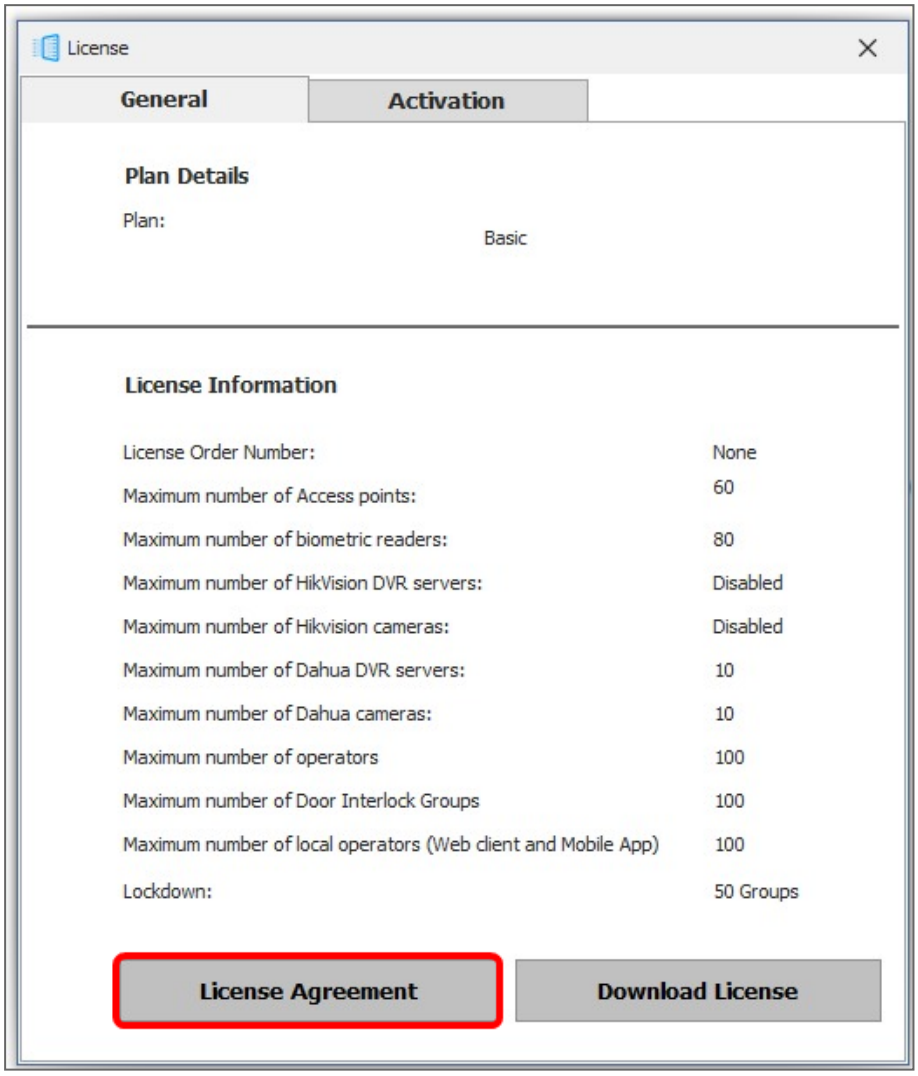
To read plan details:

1. From the menu bar, select **Help > License**.
2. Click the **General** tab.



To read the License Agreement:

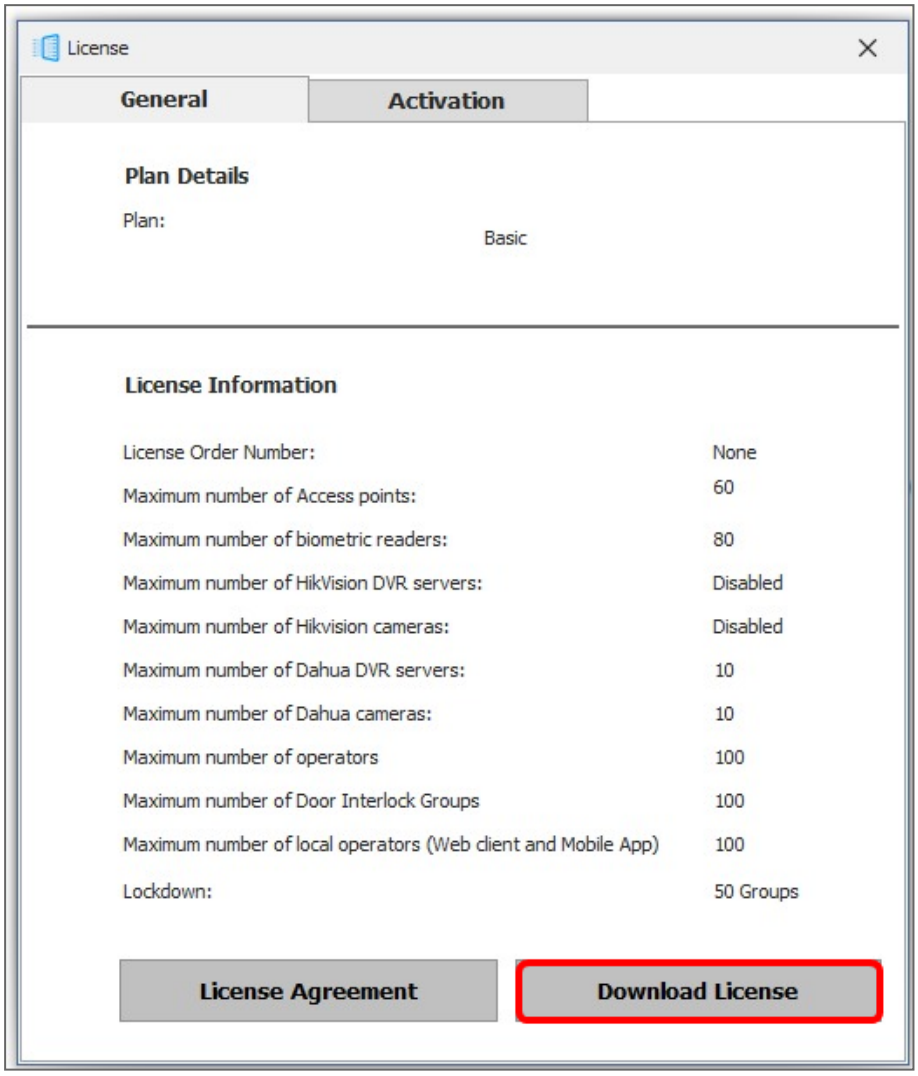
1. In the **General** tab window, click **License Agreement**



The **License Agreement** is shown in a pop-up window.

To download the current activated license:

1. In the **General** tab window, click **Download License**.



2. Browse to a location to save the file.
3. Click **Save**.

19.2.2. Activating AxTraxPro Desktop Client

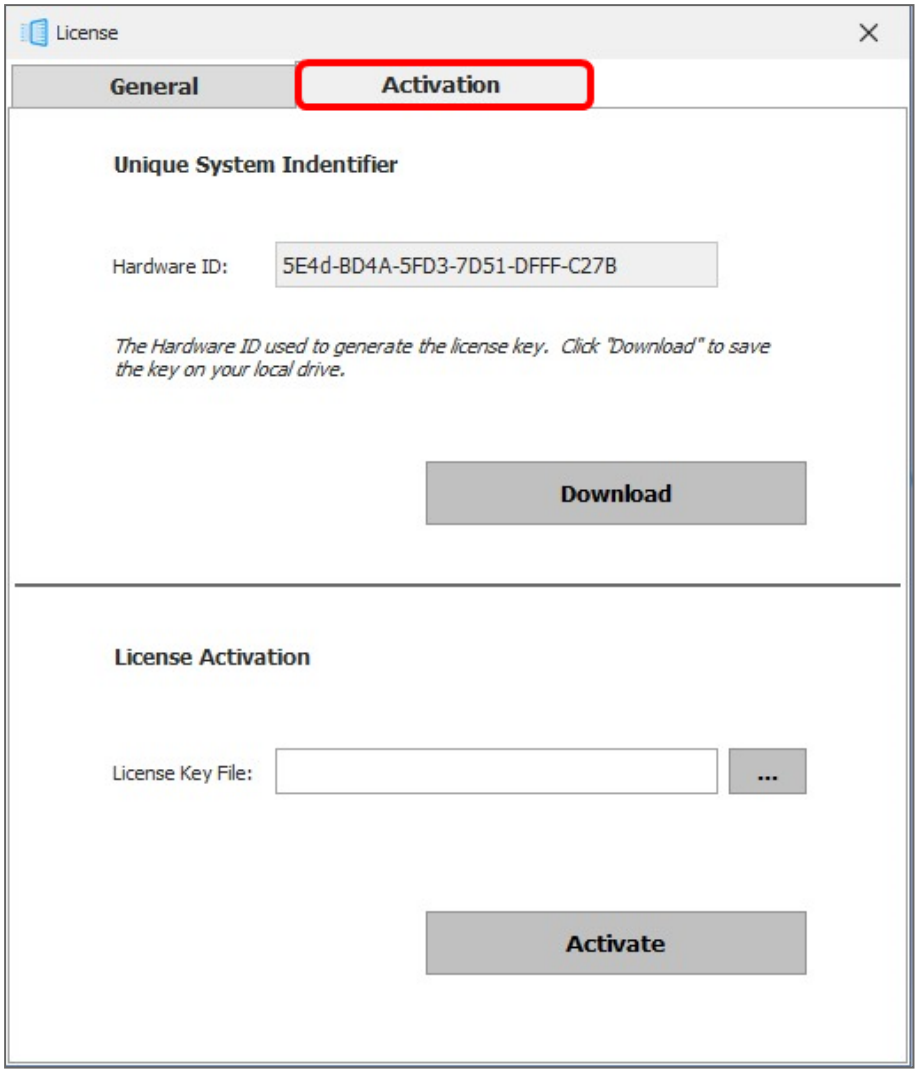
To activate AxTraxPro on a PC, it is necessary to have a license key. The activation procedure is given below.



After the installation a **Basic Plan** license is embedded in the software.

Downloading and sending the Hardware ID to Rosslare:

1. From the menu bar, select **Help > License**.
2. Click the **Activation** tab.



The Hardware ID is automatically populated.

3. Click **Download**.
4. Browse to a location to save the file.

Save the (xxx.license) file on your PC where it can be easily accessed.

5. Click **Save**.
6. Send the **Hardware ID** to Rosslare with a request to receive a **License Key File**.

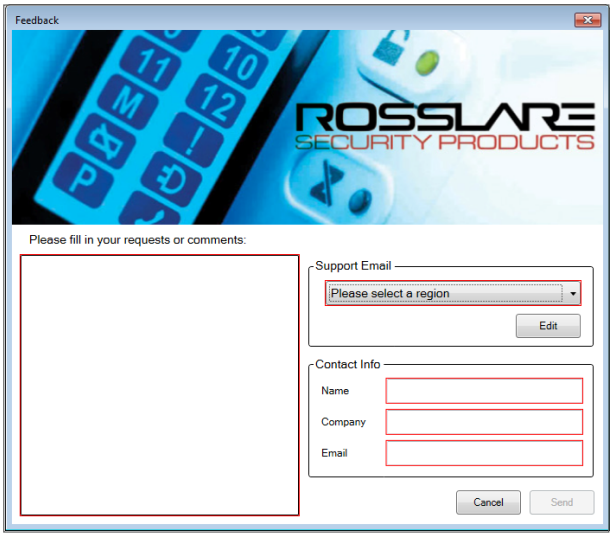
Activating Rosslare on a PC:

1. Un-zip the **License Key File** received from Rosslare.
2. Save the file (xxx.license) on your PC where it can be easily accessed.
3. Click ... to locate the **License Key File**.
4. Double-click the **License Key File**.
5. Click **Activate**.

H.4 Feedback

Use the form on the Feedback window to send feedback to Rosslare.

In order to use the Feedback form, you must configure the SMTP settings (see Notification Settings).



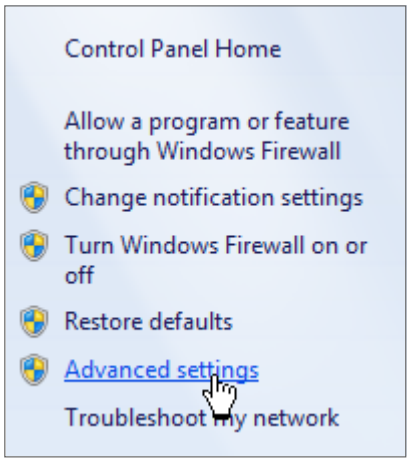
Appendix I. Opening a Program in Windows' Firewall

To open a port in Windows' firewall:

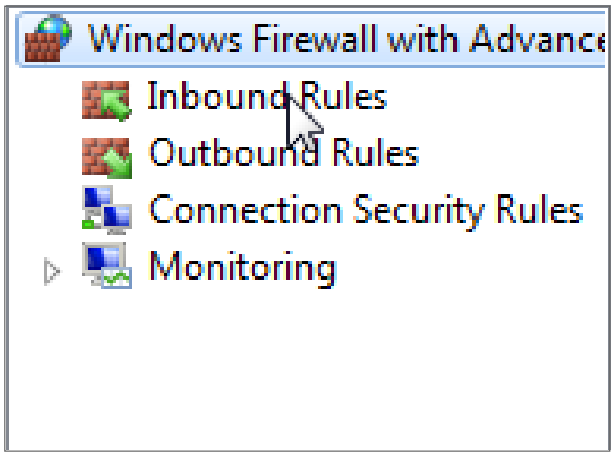
1. Open the Control Panel.
2. Click the **Windows Firewall** category.



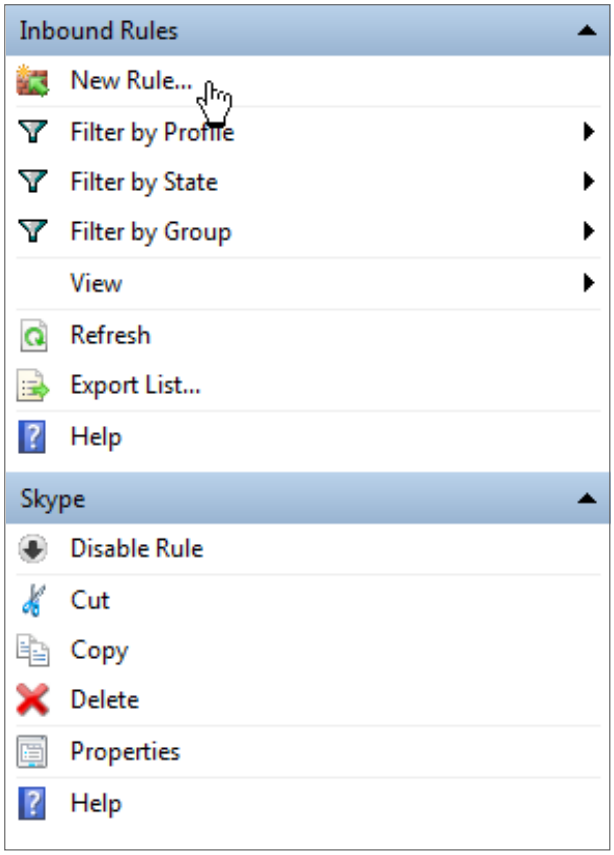
3. Click **Advanced settings** in the left column of the Windows Firewall window.



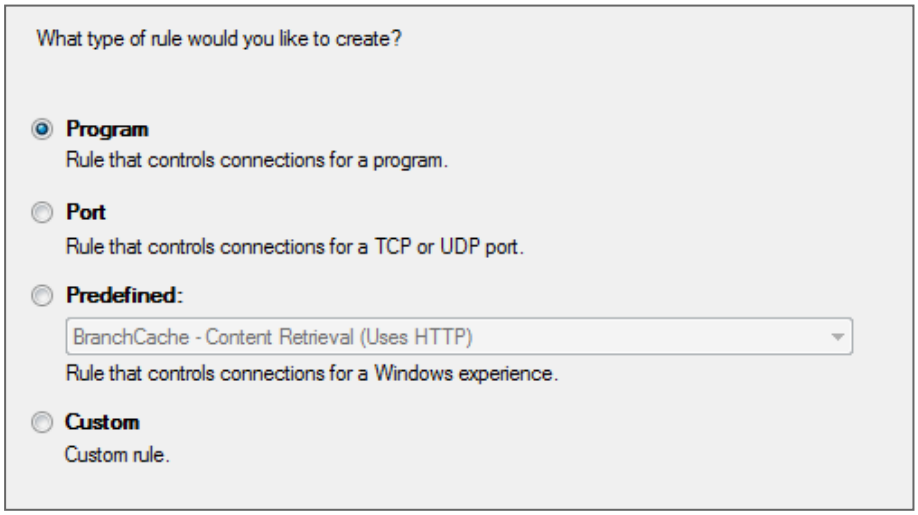
4. In the console tree on the left, click **Inbound Rules**.



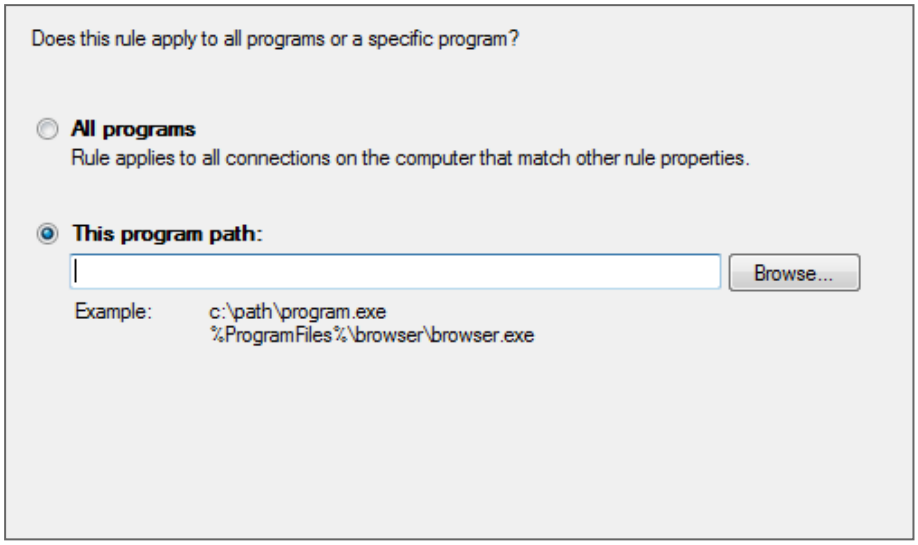
5. In the right column, click **New Rule**.



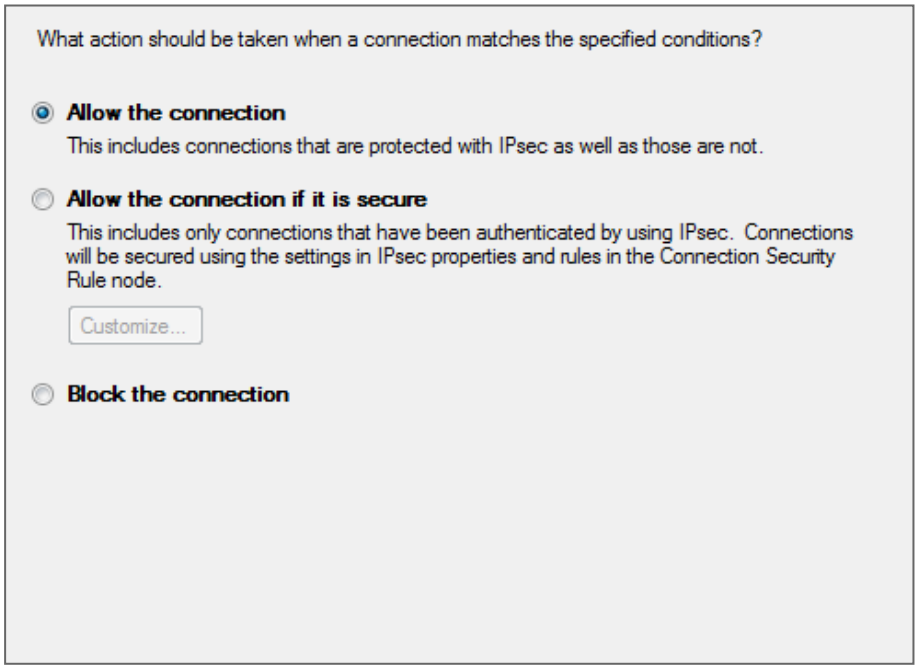
6. Make sure that **Program** is selected.



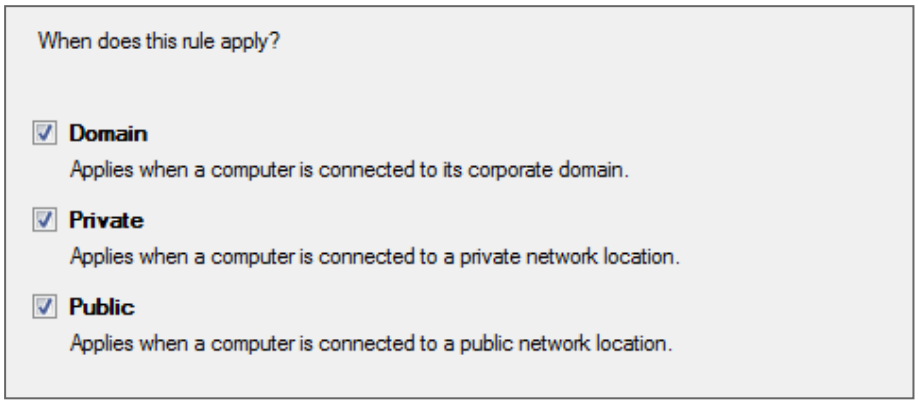
7. Click **Next**



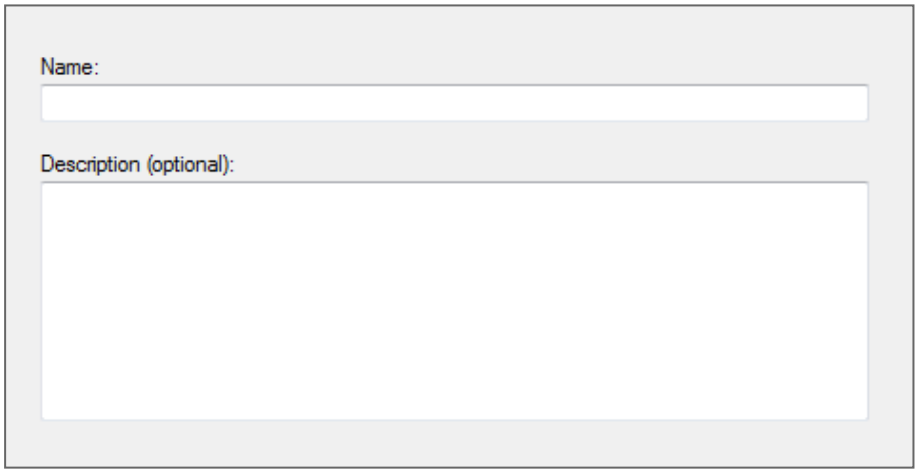
8. Make sure that **This program path** is selected.
9. Click **Browse** and locate the **AxtraxServerService.exe** file, which is located in *C:\Program Files (x86)\Rosslare\AxTraxPro Server*.
10. Click **Next**.



11. Make sure that **Allow the connection** is selected.
12. Click **Next**.



13. Make sure all three check boxes are selected.
14. Click **Next**.



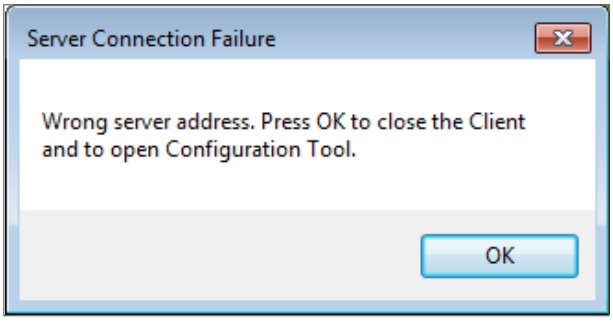
15. Enter a name of the rule, such as “Pro Server” and click **Finish**.

Appendix J. WAN Connection Troubleshooting

This appendix presents three scenarios of a server connection problem.

J.1 Server is Down or Wrong IP and Port Configuration

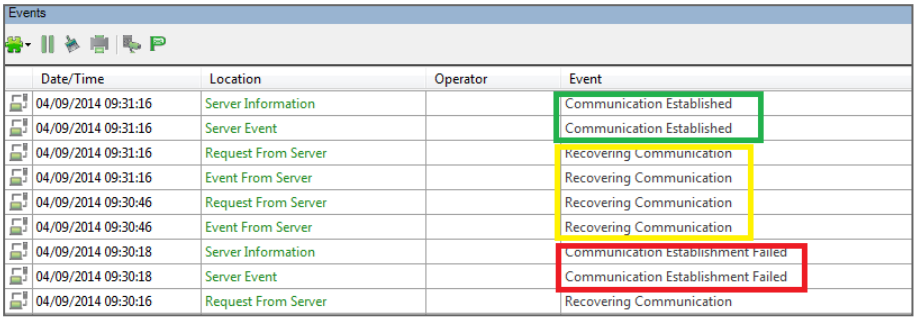
When starting the AxTraxPro Client, the following error notification appears:



Click **OK** to close the AxTraxPro client and start the AxTraxPro Configuration tool.

J.2 Server is Down or Network Failure between AxTraxPro Client and AxTraxPro Server

The Events log shows a communication error:



Check if the server is down. Check if its address was changed or if the network connection has errors.

J.3 IP + Port Setting are Fine but Client Does Not Start

Check the following possible firewall problems:

- Check firewall for server PC
- Check firewall for client PC
- Check firewall to Server network
- Check firewall to Client network

MIFARE and MIFARE Classic are trademarks of NXP B.V. | MIFARE and MIFARE Plus are registered trademarks of NXP B.V. | MIFARE and MIFARE Ultralight are registered trademarks of NXP B. V. | All product names, logos, and brands are property of their respective owners.

DISCLAIMER: The data contained within Rosslare's materials or documentation is intended to provide only general information about products available for purchase from Rosslare Enterprises Ltd. and its associated companies ("Rosslare"). Reasonable efforts have been made to ensure the accuracy of this information. However, it might contain typographic errors, inaccuracies, or omissions that may relate to product descriptions, visual pictures, specifications, and other details. All technical specifications weights, measures and colors shown, are best approximations. Rosslare can not be held responsible and assumes no legal liability for the accuracy or completeness of the information provided. Rosslare reserves the right to change, delete, or otherwise modify the information, which is represented, at any time, without any prior notice.

© 2022 Rosslare Enterprises Ltd. All rights reserved.

For more information regarding support, visit https://support.rosslaresecurity.com.

0706-0960709+04