

AxTraxNG™

Access Control Management Software

Software Manual (Version 27.7.1.x)



ROSSLARE
SECURITY PRODUCTS

Copyright © 2019 by Rosslare. 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.

Table of Contents

1. Introduction	12
1.1 AxTraxNG Server and Client	12
2. Specifications and Requirements	13
2.1 System Capabilities.....	13
2.2 System Requirements	14
2.2.1 AxTraxNG Server and Client Requirements.....	14
2.2.2 Microsoft Framework.....	14
3. Installation.....	15
3.1 Downloading the AxTraxNG Installation File	15
3.2 Beginning the Installation	16
3.3 Installing AxTraxNG Client.....	17
3.4 AxTraxNG Configuration Tool.....	18
3.5 SQL Server Setup.....	18
3.5.1 Default Setup.....	19
3.5.2 Custom Setup.....	19
3.5.3 Using Current SQL Server.....	21
3.6 Installing AxTraxNG Server Software	21
3.7 Installing AxTraxNG Server Monitor	22
3.8 Completing the Installation.....	22
3.9 Firewall Settings	23
3.10 SQL Server Settings.....	23
4. Software Overview	24
4.1 Starting the Software – Local PC	24
4.2 Starting the Software – Via WAN Connection	24
4.3 AxTraxNG Main Window	26
4.4 Menu Bar.....	27
4.4.1 File Menu	27

Table of Contents

4.4.2	Tools Menu.....	28
4.4.3	View Menu.....	28
4.4.4	Window Menu.....	28
4.4.5	Help Menu.....	29
4.5	Toolbar.....	31
4.5.1	General Icons.....	31
4.5.2	Network Icons.....	32
4.5.3	Panel Icons.....	32
4.5.4	Biometrics Icons.....	32
4.5.5	Card\Users Icons.....	33
4.5.6	Reports Icons.....	33
4.5.7	Events Toolbar Icons.....	34
4.6	Tree View.....	35
4.6.1	AC Networks.....	35
4.6.2	Biometrics.....	35
4.6.3	Video Integration.....	35
4.6.4	Timing.....	35
4.6.5	Groups.....	36
4.6.6	Global Antipassback.....	36
4.6.7	Car Parking.....	36
4.6.8	Users.....	36
4.6.9	Status Map.....	37
4.6.10	Reports.....	38
5.	Setting Up a Site.....	39
5.1	Adding Time Zones.....	39
5.2	Adding Holidays.....	41
5.3	Adding a Network.....	42
5.3.1	AC-215x, AC-225x, and AC-425x Panels.....	42
5.3.2	AC-825IP Panel.....	46
5.4	Adding Access Control Panels.....	47
5.4.1	AC-215x, AC-225x, and AC-425x Panels.....	47
5.4.2	AC-825IP Panel.....	52
5.5	Adding an Expansion Board.....	53
5.5.1	AC-225x and AC-425x.....	53

Table of Contents

5.5.2	AC-825IP.....	55
5.6	Configuring the Doors.....	55
5.7	Configuring the Readers.....	57
5.7.1	General Tab.....	58
5.7.2	Options Tab.....	60
5.7.3	Access Event.....	61
5.8	Adding a Biometric Terminal.....	62
5.8.1	On a Local Network.....	62
5.8.2	From a Remote Network.....	63
5.8.3	Mapping a Biometric Terminal to a Reader.....	64
5.8.4	Terminal Firmware Update.....	65
5.9	Configuring the Inputs.....	66
5.10	Adding Panel Links.....	67
5.10.1	Creating a Fire Alarm Input.....	70
5.10.2	Global Triggering of Output Groups.....	71
5.11	Adding Video Integration.....	72
5.12	Adding Groups.....	72
5.12.1	Adding Access Groups.....	72
5.12.2	Adding Input Groups.....	73
5.12.3	Adding Output Groups.....	75
5.12.4	Defining Card + Card Groups.....	76
5.13	Adding Access Areas.....	77
5.14	Adding Departments, Users, and Visitors.....	79
5.14.1	Adding Departments.....	79
5.14.2	Adding an Individual User.....	79
5.14.3	Auto Opening for Output Groups.....	85
5.14.4	Adding a Batch of Users and Cards.....	87
5.14.5	Setting Card Automation.....	89
5.14.6	Adding Visitors.....	90
5.14.7	Associating a User to a Card.....	91
5.15	Adding Global Antipassback Rules.....	92
5.16	Adding Car Parking.....	93
5.16.1	Viewing and Editing Car Parking Counters.....	95

Table of Contents

5.17	Adding Operators	96
5.18	Creating Elevator Control	97
5.19	Creating Status Maps.....	98
5.19.1	Manually Opening a Door from Status Map	100
6.	Card Design (Photo ID).....	102
6.1	Creating a Card Template	102
6.2	Printing a Card	104
7.	Video Integration	110
8.	Manual Operation.....	111
8.1	Controlling the Door Manually	111
8.2	Changing the Reader Mode	112
8.3	Controlling Outputs Manually	113
8.4	Manually Disarming Inputs	114
8.5	Controlling Sirens Manually	115
8.6	Updating Firmware	116
8.6.1	AC-215x, AC-225x, and AC-425x Panels	116
8.6.2	AC-825IP Panel.....	117
9.	Reports.....	119
9.1	Types of Reports	119
9.1.1	Immediate Reports.....	119
9.1.2	Panel Reports	119
9.1.3	System Reports	120
9.1.4	Interactive Report	120
9.2	Generating a Report	120
9.3	Scheduling a Report	122
9.4	Previewing a Report	124
10.	Administrator Operations	126
10.1	Setting the Time and Date	126
10.2	Testing User Counters	126
10.3	Maintaining the Database.....	128

Table of Contents

10.4	AxTraxNG Options and Preferences.....	129
10.4.1	General Tab	130
10.4.2	User Custom Fields	131
10.4.3	Custom Operations	132
10.4.4	Email Notifications.....	133
10.4.5	Company Details	134
10.5	Importing/Exporting User Data.....	134
10.6	Conversion Table.....	136
A.	Firewall Configuration	138
A.1	For Windows 7.....	138
B.	Opening a Program in Windows' Firewall	141
C.	WAN Connection Troubleshooting.....	144
C.1	Server is Down or Wrong IP and Port Configuration.....	144
C.2	Server is Down or Network Failure between AxTraxNG Client and AxTraxNG Server	144
C.3	IP + Port Setting are Fine but Client Does Not Start	144
D.	SQL Service Settings.....	145
E.	Configuring a Network	147
E.1	TCP/IP Connection.....	147
F.	Configuring a Biometric Terminal	149
G.	Restoring Factory Default Settings	151
H.	Configuring User Counters	152
H.1	Resetting Counter on Panel Re-enable.....	153
I.	Enrolling a User's Fingerprint	154
J.	Enrolling Credentials using a UHF Reader	156
K.	Enrolling a License Plate	158
L.	Enrolling a Face from a Terminal	159
M.	Enrolling Credentials using a Desktop Reader.....	160
N.	SQL Server Installation Troubleshoot	162
O.	AxTraxNG Server Monitor	165

Table of Contents

0.1	Common Info.....	166
0.2	DB Connection.....	166
0.3	Restart Server.....	167
0.4	Options.....	168
P.	Adding Custom Wiegand Formats	170
P.1	Representation	170
P.2	Facility Code	171
P.3	Authentication	171
P.4	Creating New Rules.....	172
Q.	Software License and Maintenance Agreements	176

List of Figures

Figure 1: AxTraxNG Packages Selection Screen	16
Figure 2: AxTraxNG Main Window	26
Figure 3: Departments/Users > User Properties > General Tab	80

List of Tables

Table 1: AxTraxNG Client Main Window	27
Table 2: Add Network > Options Tab.....	45
Table 3: AC Networks > Network > Panel Properties > General Tab.....	48
Table 4: AC Networks > Network > Panel Properties > Antipassback Tab...	50
Table 5: AC Networks > Network > Panel Properties > Options Tab	50
Table 6: AC Networks > Network > Panel > Doors > Door Properties	56
Table 7: AC Networks > Network > Panel > Readers > Reader Properties > General Tab	58
Table 8: AC Networks > Network > Panel > Readers > Reader Properties > Options Tab	60
Table 9: AC Networks > Network > Panel > Readers > Reader Properties > Access Event Tab.....	61
Table 10: AC Networks > Network > Panel > Inputs	66
Table 11: AC Networks > Network > Panel > AC Links > AC Link Window ...	68
Table 12: Users > Departments/Users > Department > User Properties > General Tab	80
Table 13: Users > Departments/Users > User Properties > Credentials Tab	83
Table 14: Users > Departments/Users > Department > User Properties > Details Tab.....	84
Table 15: Users > Cards > Add Users and Cards Window	87
Table 16: Users > Departments/Users > Visitors > User Properties > Visitor's Options Tab	90
Table 17: Report Preview Icons	124
Table 18: Tools > Database > Available Databases.....	128
Table 19: Tools > Options > General Tab	130
Table 20: Tools > Options > User Custom Fields Tab.....	131
Table 21: Tools > Options > Custom Operation Tab.....	132
Table 22: Tools > Import/Export Data	135
Table 23: Tools > Conversion Tables	137
Table 24: Server Monitor Topics.....	165
Table 25: Server Monitor > DB Connection Screen.....	166
Table 26: Server Monitor > Options Screen.....	168

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 or graphic of the PCB(s) are intended for clearer illustration and understanding of the product and may differ from the actual PCB(s).

1. Introduction



Note

In this manual, unless otherwise stated:

- “AC-225” refers to both the regular AC-225 and the AC-225IP models
- “AC-425” refers to both the regular AC-425 and the AC-425IP models.
- All panel and expansion references apply to both the ‘A’ and ‘B’ versions of that panel.
- ‘A’ panels work with the ‘A’ versions of the expansions; ‘B’ panels work with the ‘B’ versions of the expansions.

The AxTraxNG™ access control system is a complete server-client software management system for use with the AC-215/215IP, AC-225/225IP, AC-425/425IP, and AC-825IP access control panels.

The AxTraxNG access control system is user-friendly, intuitive, and rich in functionality. Using AxTraxNG, you can configure door functionalities based on areas and time frame for different types of personnel and for varying alarm situations.

The AxTraxNG access control system can integrate with ViTrax™ Video Management Software (VMS) application. The main purpose of the integration is to enable video recording based on access control events and convenient playback.

This manual is compatible with AxTraxNG software Version 27.x.

1.1 AxTraxNG Server and Client

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

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



Important

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

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

AxTraxNG 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

2. Specifications and Requirements

2.1 System Capabilities

General	
Software Architecture	Client-Server
Database Type	SQL Server Express 2008, 2012
Max. Number of Credentials	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

Specifications and Requirements

Networks	
	<ul style="list-style-type: none">• Legacy: AC-225, AC-225IP with MD-I084• Legacy: AC-225, AC-225IP with MD-D02• Legacy: AC-425, AC-425IP• Legacy: AC-425, AC-425IP with MD-I084• Legacy: AC-425, AC-425IP with MD-D04
Panel Networks Communication Interface	<ul style="list-style-type: none">• Serial (RS-232/485)• TCP-IP Note: AC-825IP has TCP/IP only
Communication Speed	9600, 19200, 57600, and 115200 bps

2.2 System Requirements

2.2.1 AxTraxNG Server and Client Requirements

Operating System	Windows 7 (32-bit/64-bit) SP1, 8, 10, and server editions
Processor	Minimum: Intel dual core 2.4 GHz or equivalent Recommended: Intel core i5 or i7 CPU
Memory	Minimum: 2 GB Recommended: 8 GB
Network	LAN card required for TCP/IP networking
Hard Disk Space	5 GB minimum

2.2.2 Microsoft Framework

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

3. Installation

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

- AxTraxNG Client
- SQL Server
- AxTraxNG Server

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

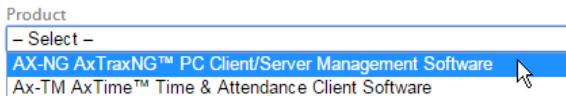
- AxTraxNG Server Monitor
- (Optional) ViTrax software – Enables video integration

3.1 Downloading the AxTraxNG Installation File

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

To download the AxTraxNG 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 AX-NG AxTraxNG PC Client/Server Management Software.



5. In *Document Types*, select Software and click **Search**.
In the search results, you'll see *AxTraxNG software*.



6. Click the Download icon on the right.
The installation file is downloaded to your computer.

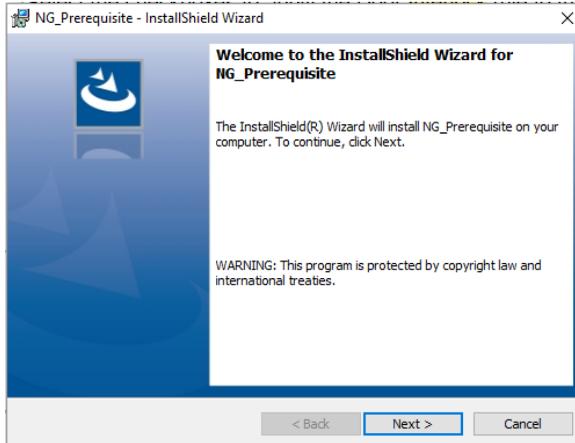
3.2 Beginning the Installation

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.

After the necessary files are extracted, the following screen opens:



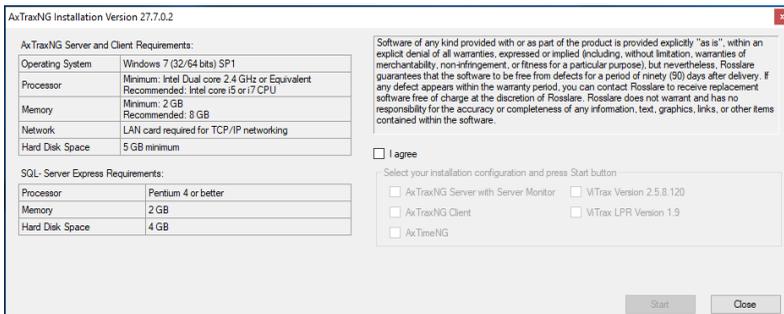
Click **Next**, and the following screen will appear



Note

In some cases the installation will require a PC restart, and after the restart double click on the installation file once more.

Figure 1: AxTraxNG Packages Selection Screen



2. Select **I agree** and select which packages you wish to install.

Installation



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

3. Click **Start**.

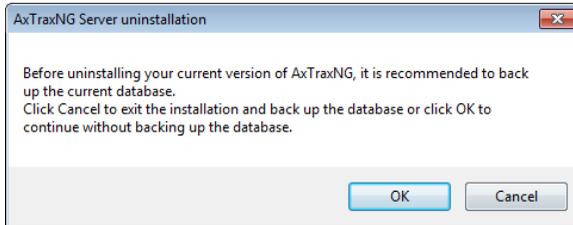


Upgrading to a newer version only uses current database information. After upgrading the AxTraxNG version, check the panel's firmware version for both old and new installations and upgrade your firmware if required. If there is no SQL server installed, the Installation Requirements screen opens.

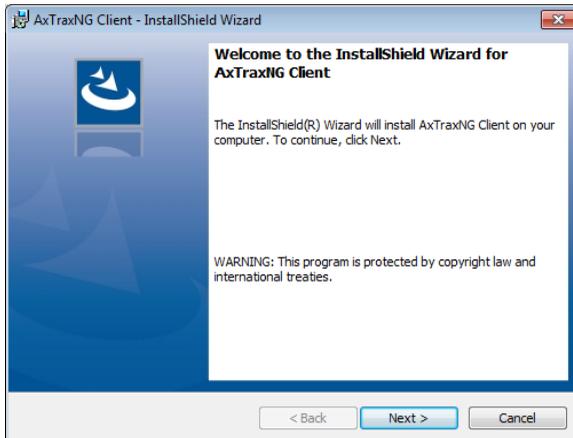
4. Accept the full licensing agreement and click **OK**.

3.3 Installing AxTraxNG Client

If you are upgrading, the following screen opens:



If you are installing for the first time, the following screen opens:

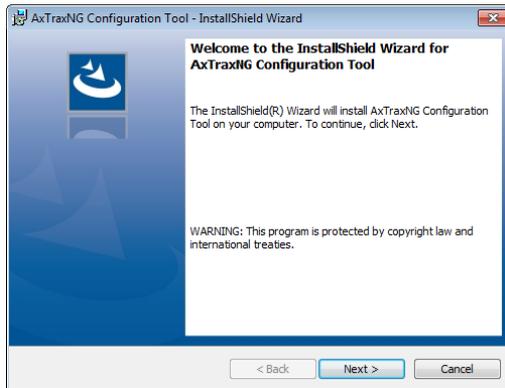


To install the AxTraxNG Client application:

1. Click **Next** to begin the AxTraxNG Client installation process.
2. Follow the onscreen instructions to install the application.
3. Click **Finish** to complete installing the AxTraxNG Client.

3.4 AxTraxNG Configuration Tool

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

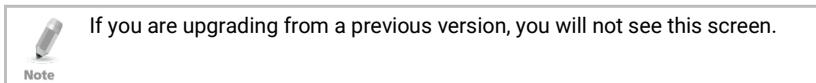


To install the AxTraxNG Configuration Tool:

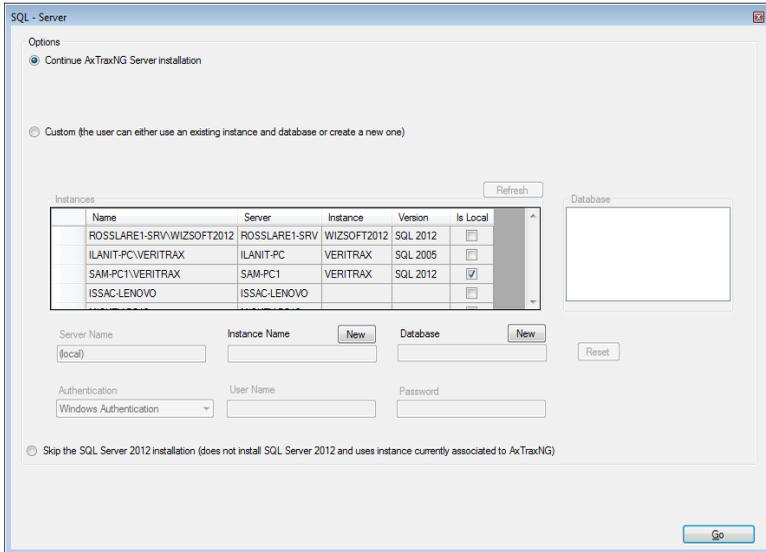
1. Click **Next** to begin the AxTraxNG Configuration Tool installation process.
2. Follow the onscreen instructions to install the application.
3. Click **Finish** to complete installing the AxTraxNG Configuration Tool.

3.5 SQL Server Setup

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



Installation



The AxTraxNG Server operates using an SQL server 2008/2012 database. There are three options in installing the SQL server:

- Select Continue (default) to install Microsoft SQL Server Express 2012
- Select Custom to use an existing instance of the SQL 2008 server available on your computer network with your SQL login credentials.
- Select Skip to use the current AxTraxNG SQL Server instance.



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

3.5.1 Default Setup

To install the default SQL Server application:

1. With the default option chosen by default, click **Go**.

Follow the onscreen instructions to install a new instance of SQL Server 2012. A confirmation sentence appears on the lower part of the screen when the process finishes.

Microsoft SQL-Server 2012 Express successfully installed.

2. Click **Done**.

3.5.2 Custom Setup

Select Custom to use an existing instance of the SQL 2008 server available on your computer network with your SQL login credentials

Installation

To install an existing instance of the SQL Server application:

1. Select **Custom**.

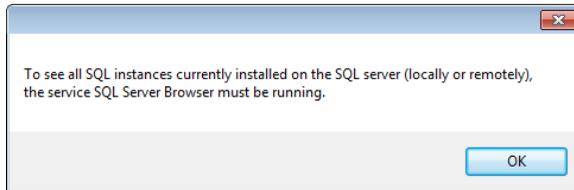
A list of existing SQL instances are listed in the table.

Name	Server	Instance	Version	Is Local
SAM-PC1-VERITRAX	SAM-PC1	VERITRAX	11.0.2100.60	<input checked="" type="checkbox"/>
ILANIT-PC-VERITRAX	ILANIT-PC	VERITRAX	9.00.4035.00	<input type="checkbox"/>
ROSSLARE1-SRV-BKUPPEXEC	ROSSLARE1-SRV	BKUPPEXEC	9.00.5000.00	<input type="checkbox"/>
ROSSLARE1-SRV-WIZSOFT	ROSSLARE1-SRV	WIZSOFT	9.00.5000.00	<input type="checkbox"/>

Server Name: (local) Instance Name: [New] Database: [New] [Reset]

Authentication: Windows Authentication User Name: Password: [Reset]

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.

 **Important** 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: !, \$, #, %)

 **Note**

- 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**.

Installation

A setup wizard for the SQL Server 2012 Express opens.

3.5.3 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 2012 installation**.

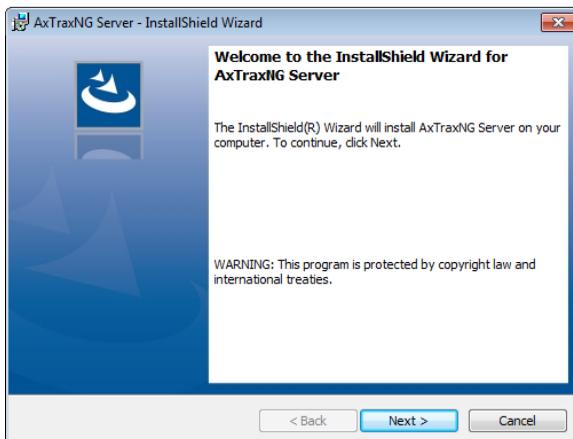
Skip the SQL Server 2012 installation (does not install SQL Server 2012 and uses instance currently associated to AxTraxNG)

2. Click **Go**.

The installation continues.

3.6 Installing AxTraxNG Server Software

Following the SQL Server Setup installation, the AxTraxNG Install Shield Wizard for the AxTraxNG Server software installation appears.

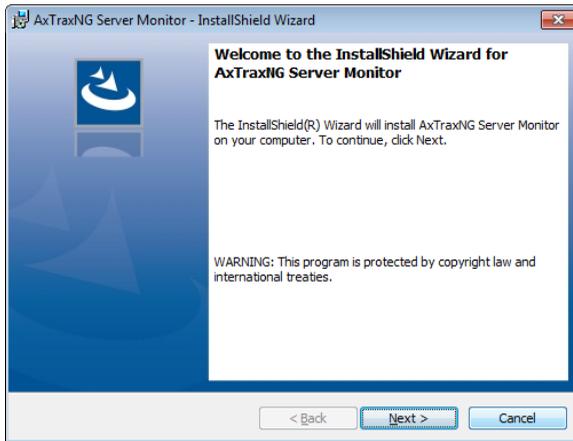


To install the AxTraxNG Server:

1. Click **Next** to begin the AxTraxNG Server installation process.
2. Follow the onscreen instructions to install the application.
3. Click **Finish** to complete installing the AxTraxNG Server.

3.7 Installing AxTraxNG Server Monitor

Once the AxTraxNG server installation finishes, the AxTraxNG Server Monitor installation opens automatically.



To install the Server Monitor:

1. Click **Next** to initiate the AxTraxNG Server Monitor installation process.
2. Follow the onscreen instructions to install the application.
3. Click **Finish** to complete the Server Monitor installation and to launch the application.

3.8 Completing the Installation

Once all the elements of the installation have completed, a confirmation screen appears.



1. Click **OK**.
2. Click **Close** on the AxTraxNG Packages Selection Screen (Figure 1).
3. Check that you see a message in the Windows system tray that the server is connected.



3.9 Firewall Settings

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

For more information on how to configure a firewall, see Appendix A. Contact your system administrator or Rosslare Technical Support for further guidance.

3.10 SQL Server Settings

After installing AxTraxNG, 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 B.



Note

If SQL Express 2012 is being installed (part of the installation package), the installation must be on the same Windows user account that is being used for AxTraxNG.

4. Software Overview

AxTraxNG is controlled through a user-friendly interface, and comes with a Tree View list of all aspects of the site setup and a toolbar for standard operations.



Starting from v25.xx, AxTraxNG is based on WCF technology and allows running the client via a WAN (Internet) connection.

4.1 Starting the Software – Local PC

This section explains how to start the software and log in to the main window.

To start AxTraxNG:

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

The *Logon AxTraxNG Client* dialog box appears.



2. Select an **Operator name** and enter a **Password**.



By default, the Administrator operator password is "admin".

3. Click **OK**.

The main AxTraxNG window opens.

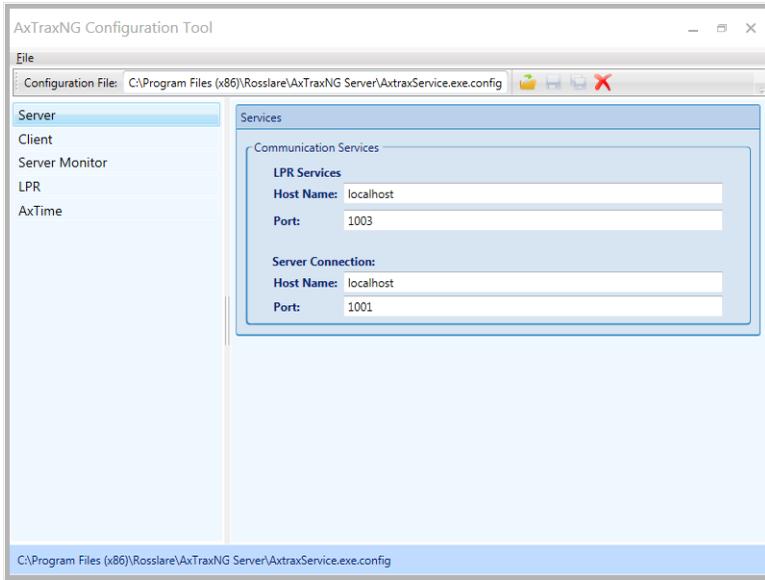
4.2 Starting the Software – Via WAN Connection

Starting from v25.xx, AxTraxNG is based on WCF technology and allows running the client via a WAN (Internet) connection. However you must first define the server and client connections using the AxTrax Configuration Tool.

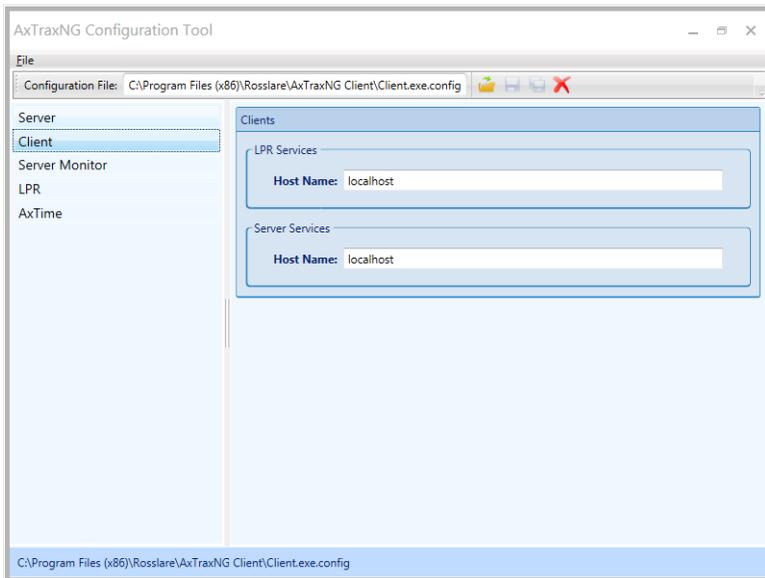
To start AxTraxNG using the AxTraxNG Configuration Tool:

1. Click **AxTraxConfigTool** () from the AxTraxNG Client folder under the Rosslare folder in the Start menu.

The AxTraxNG Configuration Tool opens.



2. Under the *Server* tab, enter the LPR and the Server Connection ports. If you are not using LPR, leave the default value.
3. Select the *Client* tab.



Software Overview

- In the Hostname field, enter the IP address of the Client server.
As soon as you enter the IP address, the Port field appears.



- Enter the same port number as you did in the Server Connection field above.
- For the Server Monitor, LPR, and AxTime tabs, enter the same IP address and port number in the respective fields.
- When you finish populating all the fields, click the **Save All** button () on the toolbar.
- Close the Configuration Tool.
- Now double-click the AxTraxNG Client icon () on the desktop or select the program from the Rosslare folder in the Start menu to see the login window as seen above in Section 4.1.

For more troubleshooting with a server connection, refer to Appendix C.

4.3 AxTraxNG Main Window

The entire central functionality of the AxTraxNG system is available from the AxTraxNG Client main window (Figure 2).

Figure 2: AxTraxNG Main Window



The AxTraxNG Client Main window is divided into six sections, as described in Table 1.

Table 1: AxTraxNG Client Main Window

Section	Description
1 Menu Bar	The Menu Bar controls the software's general operation and setup. For more information, see Section 4.4.
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. For more information, see Section 4.5.
3 Tree View	The Tree View allows users to configure, monitor, and control every aspect of access control. For more information, see Section 4.6.
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.

4.4 Menu Bar

The menu bar controls the general operation and setup of the software.

4.4.1 File Menu

The File menu has three options:

Menu	Select Menu item to...
Server Connection	Log on to the AxTraxNG server (See Section 4.1)
ViTrax Server	Log on to the ViTrax server
Exit	Exit the AxTraxNG software

4.4.2 Tools Menu

Use the Tools menu to manage the database and set software preferences. The menu has four options:

Menu	Select Menu item to...
Database	Open the Database window to back up the database or set a scheduled backup, as well as to import or export the AxTraxNG and/or AxTrax AS-525 configuration states and events logs (see Section 10.3)
Options	Set software options and preferences, including national holidays, event highlighting, custom user information fields, and GUI language (see Section 10.4)
Import/Export Data	Import/export user information from/to an Excel spreadsheet file (see Section 10.5)
Conversion Tables	Create a conversion table that converts the alphanumeric character to a binary number (see Section 10.6)

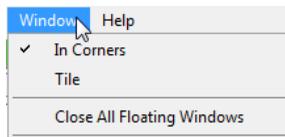
4.4.3 View Menu

Use the View menu to define and manage the view of the GUI. The menu has four options:

Menu	Select Menu item to...
Events	Select the option to show event logs
Table View	Select the option to show the Display Area
Guard Screen	Select to show the Guards Screen (if installed)
Restore Docking	Restore the default GUI view

4.4.4 Window Menu

The Window menu has three options:



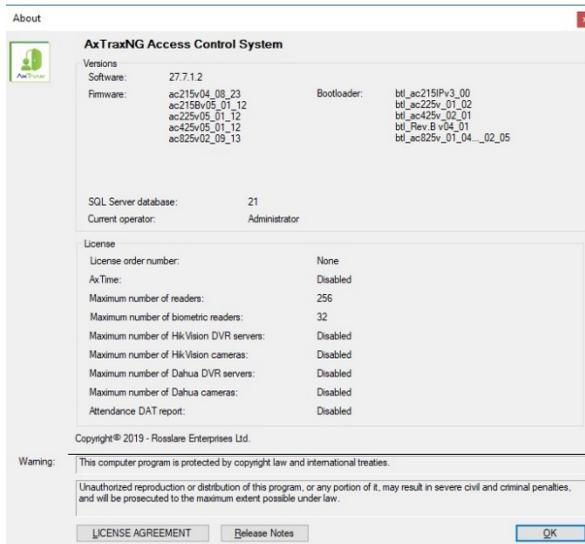
Menu	Select Menu item to...
In Corners	Place any open pop-up windows in the corners of the screen. This option is chosen by default.
Tile	To move any opened pop-up windows to available space on the screen
Close All Floating Windows	Close all of the pop-up windows You can use the list of open pop-ups to focus on any open pop-up window.

4.4.5 Help Menu

The Help menu has four options:

4.4.5.1 **About**

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



4.4.5.2 **User Manual**

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

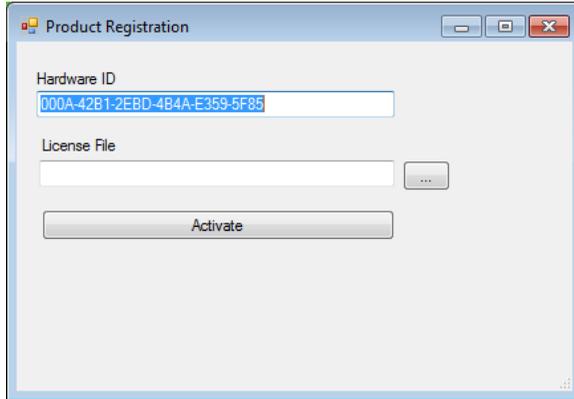
4.4.5.3 **Registration**

The Registration window is used to register your AxTraxNG license.

To register the product:

1. From the menu bar, select **Help > Registration**.

The *Product Registration* window opens.



The Hardware ID is automatically populated.

2. Un-zip the license file you received from Rosslare by email and place the file (xxx.license) on your PC where it can be easily accessed.
3. Click  to locate your license file and double-click it.
4. Click **Activate**.
5. Restart the PC.

Once your license is activated, the licensing information in the About screen (Section 4.4.5.1) is updated accordingly.

Software Overview

4.4.5.4 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 Section 0.4).

Feedback

Please fill in your requests or comments:

Support Email

Please select a region

Edit

Contact Info

Name

Company

Email

Cancel Send

4.5 Toolbar

The toolbar controls key tasks required to manage access control across an entire facility. When a new element is selected from the Tree View, the toolbar icons change to suit the selected element.

The following toolbar icons are available:

4.5.1 General Icons

Icon	Name	Click icon to...
	Manual Door Operation	Open the <i>Door Manual Operation</i> window (see Section 8.1)
	Print	Send the current Display Area view to the printer
	Add	Add a new element of the selected type
	Edit	Edit the selected element
	Delete	Delete the selected item

4.5.2 Network Icons

Icon	Name	Click icon to...
	Set Time	Set the time on the selected access control panel (see Section 10.1)
	Find Panels	Find and update panels within the network (see Section 5.4.1.2)
	Add to Status Map	Add available panels and panel components to the Status Map (see Section 4.6.9)
	Reader Type	Configure custom reader type
	Camera	View a list of connected cameras and link cameras to AxTraxNG

4.5.3 Panel Icons

Icon	Name	Click icon to...
	Manual Reader	Change the operation mode of the readers on the selected panel (see Section 8.2)
	Update Firmware	Send a firmware update to the selected access control panel (see Section 8.6)
	Control Output Manually	Change the settings for the outputs on the selected panel (see Section 8.3)
	Control Input Manually	Change the settings for the inputs on the selected panel (see Section 8.4)
	Control Siren Manually	Test the siren for the selected panel (see Section 8.5)
	Reset Panel Manually	Reset a panel command sent to the panel in case of misbehavior

4.5.4 Biometrics Icons

Icon	Name	Click icon to...
	Import	Import Biometrics terminal from a remote network (see section 5.8.2)
	Update Firmware	Send a firmware update to the selected access control panel (see Section 8.6)

4.5.5 Card\Users Icons

Icon	Name	Click icon to...
	User Counter	View the current user count value (see Section 10.2)
	Add Users and Cards	Create up to 1000 new users and cards in one batch (see Section 5.14.3)
	Card List	Batch add specific cards to a specific user
	Add Cards	Create up to 1000 new cards in one batch
	Add Cards from Desktop reader	Add and assign cards to selected users or add cards from a desktop reader (see Appendix I)
	Add Cards from UHF	Add and assign cards to selected users or add cards from a UHF reader (see Appendix J)
	Print Cards	Print a card template that has been created (see Chapter 6).
	User Filter	Filter the list of users by various parameters, such as name and card number (see Section 4.6.8.3)
	Manufacturer Brand	Find the make of your car to add to Vehicle Types when configuring a License Plate Recognition (LPR) camera (see Section 4.6.8.4)

4.5.6 Reports Icons

Icon	Name	Click icon to...
	Manual Door Operation	Open the <i>Door Manual Operation</i> window (see Section 8.1)
	Print	Print the current report
	Save Reports	View report criteria previously saved in the Display Area
	Run	Produce a report from the selected report type and criteria (Chapter 9)
	Preview	Preview a report that was just run
	Save	Save the report criteria used to generate reports
	Delete	Delete a saved set of report criteria used to generate reports

4.5.7 Events Toolbar Icons

When clicking an event icon, click the dropdown arrow to change the current view of the display.

Icon	Name	Click icon to...
	All Events Online	Display all real time events
	Panels AC	Display all event types uploaded from the access control units
	Access	Display only access events uploaded from access control units
	Alarm	Display only alarm events uploaded from access control units
	Archive	Display video stream archive events stored in either the ViTrax database, the USB key, or snapshots saved on PC
	System	Display events related to the AxTraxNG Server operation and operators activity
	Biometrics	Displays events from the Biometric terminals
	Cameras	Displays events of recorded streams from a camera
	Pause	Halt the display of events in the Display Area. New events are shown again when the Pause button is clicked a second time.
	Refresh	Manually refresh the event list
	View Events within the last Hour	Display all events that occurred within the last hour. Click the dropdown arrow to change the view.
	View Events within the last Day	Display all events that occurred within the last day
	View Events within the last Week	Display all events that occurred within the last week
	View Periodical Events	Display all events that occurred within a selected period
	View All Events	Display all events
	Clear List	Clear the entire log and empty the current event list view
	Show User	Open the <i>User</i> window for the selected user.
	Clear Alarm	Open the <i>Alarm Details</i> window to allow the operator to reset the alarm.

Software Overview

Icon	Name	Click icon to...
	Antipassback Forgive	Open the <i>Antipassback Forgive</i> window to allow the operator to cancel an Antipassback restriction for the selected user.
	Camera List	Open a list of all ViTrax cameras attached to the network
	Archive	Open the <i>Archive Camera</i> window for the selected video stream or snapshot and play the stream
	Car Parking	Opens the <i>Car Parking Counters</i> window to view and edit the car parking area and group counters.

4.6 Tree View

The Tree View allows users to configure, monitor, and control every aspect of a facility's access control network.

When the user selects an element from the Tree View, its contents are shown in the main Display Area, and the toolbar icons change to suit the selected element.

4.6.1 AC Networks

A network is a group of up to 32 access control panels. The AxTraxNG Server connects to the panels across the panel network.

For more information, see Section 5.3.



Over a certain amount of readers, you must activate you license file (see Section 4.4.5.2).

4.6.2 Biometrics

The **Biometrics** element allows you to manage biometric terminals.

For more information, see Section 5.8.

4.6.3 Video Integration

Cameras can be added to the network to allow real-time viewing of any area desired. The **Video Integration** element allows you to add cameras from ViTrax, Hikvision, and Dahua servers to the network and to configure each camera's settings (Chapter 7).

4.6.4 Timing

The Timing tree branch consists of two elements: Time Zone and Holidays.

4.6.4.1 Time Zones

A time zone defines a weekly time period or set of time periods; for example, "Office Hours" or "Out of Office Hours". Door access rights, alarms, and input and output behavior can all be set to behave differently within each Time Zone (see Section 5.1).

4.6.4.2 Holidays

This element defines annual holiday dates; it is possible to set special access behaviors for holiday time (see Section 5.2).

4.6.5 Groups

The **Groups** tree branch consists of six elements: **Access Groups**, **Access Areas**, **Output Groups**, **Input Groups**, **Card + Card Groups**, and **Vehicle Access Groups**.

4.6.5.1 Access Groups

An Access group defines when each reader on the site is available for access. All site personnel are assigned to appropriate Access Groups.

For more information, see Section 5.12.1.

4.6.5.2 Access Areas

A facility can be subdivided into several access areas to configure and manage it more effectively (see Section 5.13).

4.6.5.3 Input and Output Groups

Input and Output groups define sets of outputs or inputs that should be managed together within a panel (see Sections 5.12.2 and 5.12.3).

4.6.5.4 Card + Card Groups

Card + Card mode is a secure mode that requires two card holders (users) to grant access to a particular reader (see Sections 5.12.4).

4.6.5.5 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.

4.6.6 Global Antipassback

Antipassback rules can be applied to each access area to prevent one user's card or entry code from being used for two subsequent entries, and to prevent a second entry without a previous exit (see Section 5.14.7).

4.6.7 Car Parking

The Car Parking management option allows you set up groups with a limited number of users who can access a particular area. This feature is counter based that keeps track of the number of users in a specified area.

For more information, see Section 5.16.

4.6.8 Users

The **Users** tree branch consists of five elements: **Departments/Users**, **Visitors**, **User Filter**, **Cards**, **Vehicle Types**, and **Operators**.

4.6.8.1 Departments/Users

This element shows a list of all departments and users, as well as any visitors registered in the system. Each user is a member of a department.

For each user, it is possible to assign cards and/or a PIN code, set access rights, personal details, and include an identification photograph.

For more information, see Section 5.14.

4.6.8.2 Visitors

This element shows a list of all visitors registered in the system.

Visitor type users can also be created with specific access rights.

For more information, see Section 5.14.3.

4.6.8.3 User Filter

This element allows you to find users in the database based on various search parameters, such as name, user number, and access group. The filtered list then appears in the main window.

4.6.8.4 Vehicle Types

This element shows a list of car types that can be used when adding LPR configuration.

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

4.6.8.5 Cards

This element lists all cards in the system with their statuses, and allows the manual addition of cards to the system (see Section 5.14.3).

Cards can also be added to the system using an MD-08 reader (Appendix O) and Desktop reader (Appendix J).

In addition, the element allows you to create a card template for printing (see Chapter 6).

4.6.8.6 Operators

Operators are people with access to the AxTraxNG software. The default operator names are Administrator, Engineer, and Security.

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.

For more information, see Section 5.17.

4.6.9 Status Map

The Status Map creates a graphic display of the statuses for every door, reader, and alarm in the facility on user-selected images.

The system can display multiple nested status maps, allowing users to show either the complete access control network or a specific area in detail.

For more information, see Section 5.19.

4.6.10 Reports

AxTraxNG can produce various reports, including usage reports, attendance records, visitors, and roll calls. The AxTraxNG Report Wizard allows users to design their own custom reports based on their needs. For more information, see Chapter 9.

5. Setting Up a Site

This section outlines a recommended step-by-step process for configuring AxTraxNG for a site.

Step	Action	Section
1.	Add Time Zones	5.1
2.	Add Holidays	5.2
3.	Add a Network	5.3
4.	Add and Configure an Access Control Panel	5.4
5.	Add an Expansion Board	5.5
6.	Configure the Doors	5.6
7.	Configure the Readers	5.7
8.	Adding Biometric Readers	5.8
9.	Configure the Inputs	5.9
10.	Add Panel Links	5.10
11.	Add Video Integration	5.11
12.	Adding Groups	5.12
13.	Add Access Areas	5.13
14.	Add Departments, Users and Visitors	5.14
15.	Add Global Antipassback Rules	5.15
16.	Add Car Parking	5.16
17.	Add Operator	5.17
18.	Add Elevator Control	5.18
19.	Add a Status Map	5.19

The AxTraxNG system performs an automatic data download for any parameter related to the hardware. If panels are connected and active, a download count appears on the status bar after any downloaded parameter change.

5.1 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.

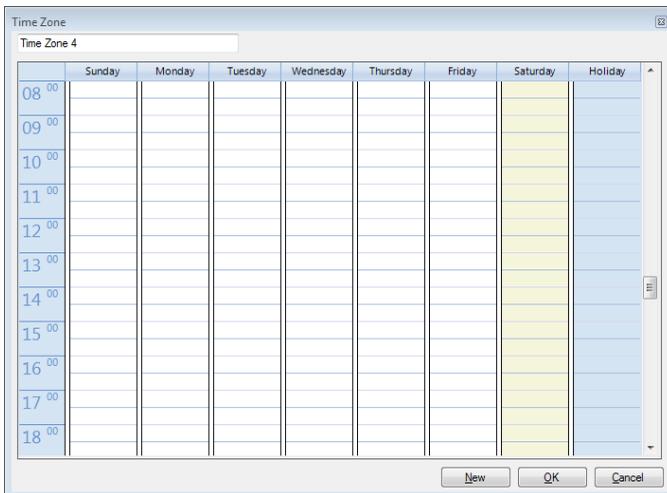
The *Time Zone Properties* window displays the selected periods for each day of the week.

To add a new time zone:

1. In the Tree View, select **Timing > Time Zone**.

Setting Up a Site

- On the toolbar, click the  icon.
The *Time Zone* properties window opens.



- Enter a name for the time zone.
- Click and drag the mouse down a day column to select a time interval.
- Right-click the selected area and select **Create**.
- Right-click the selected area again and select **Properties** to fine tune the time frame and then click **OK**.
- 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.

Note

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



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

Note

5.2 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:

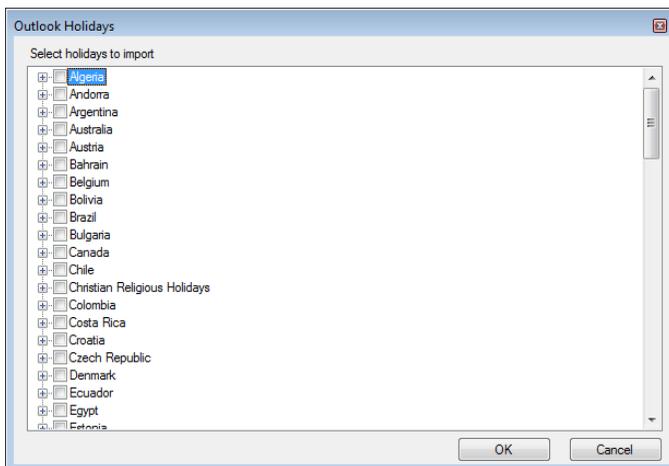
- Add a known national holiday(s)
- Add a new holiday

To add a national holiday:

1. In the Tree View, select **Timing > Holidays**.

2. On the toolbar, click the  icon.

The *Outlook Holidays* window opens.



3. From the list, find the relevant country and either:

- a. Select the main checkbox to select all holidays for that country.
- b. Expand the checkbox and select which holidays to add.

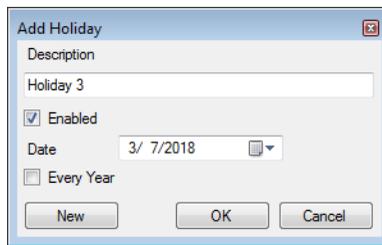
4. Click **OK**.

To add a new holiday:

1. In the Tree View, select **Timing > Holiday**.

2. On the toolbar, click the  icon.

The *Add Holiday* window opens.



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

5.3 Adding a Network

A network consists of one or more access control panels. AxTraxNG communicates with each access control panel in the network.

The *Network* window includes the following information:

- The network's name, address, and activation status
- The DIP switch settings for the communication speed (non-AC-825IP panels)
- The type of network connection and the connection settings
- Type of panel and its hardware (AC-825IP only)
- Time zone used by the network

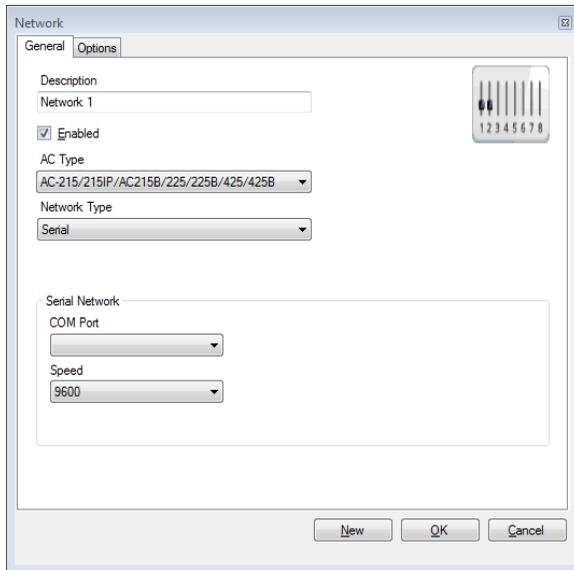
When adding a network, you must choose the type of access panels that are added to the network.

5.3.1 AC-215x, AC-225x, and AC-425x Panels

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

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

The *Network* window opens.



The display varies according to the type of network selected.

Note

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



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

Note

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.

Refer to Appendix E for how to configure an access control network. Check with your system administrator for more information, or contact Rosslare technical support.

Setting Up a Site



Note

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.

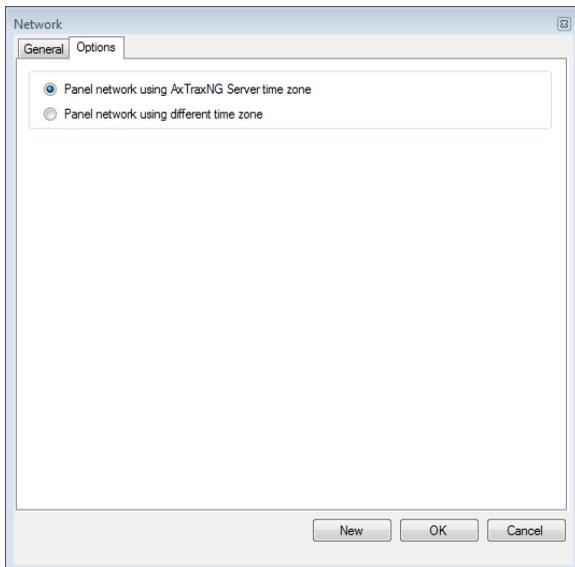
- For all types of networks, set the DIP switch on the access control panel hardware to match the diagram at the top of the screen.



Note

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

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



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

The *Network Time Zone* section appears.

- Set the Daylight Saving Time definitions according to the field descriptions in Table 2.

Table 2: Add Network > Options Tab

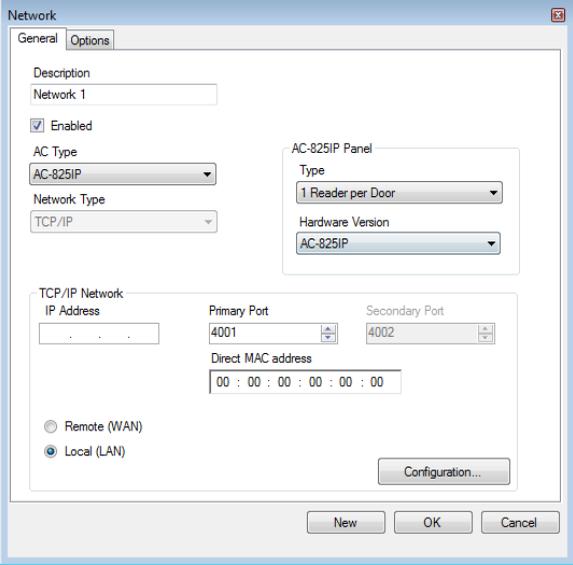
Field	Description
Select Time Zone (Windows Date and Time)	From the dropdown list, select the desired time zone.
Custom Daylight saving	Select to define custom settings.
Daylight Time	Select the new hour at the time that daylight saving time begins.
Start DST (time)	Select the hour that daylight saving 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.

- Click **OK**.

5.3.2 AC-825IP Panel

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

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



The screenshot shows the 'Network' configuration window with the following settings:

- Description:** Network 1
- Enabled:**
- AC Type:** AC-825IP
- Network Type:** TCP/IP
- AC-825IP Panel:**
 - Type:** 1 Reader per Door
 - Hardware Version:** AC-825IP
- TCP/IP Network:**
 - IP Address:** [Empty]
 - Primary Port:** 4001
 - Secondary Port:** 4002
 - Direct MAC address:** 00 : 00 : 00 : 00 : 00 : 00
- Connection Type:** Local (LAN), Remote (WAN)

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, and select whether the network is WAN or LAN.
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 Appendix E.1. Check with your system administrator for more

Setting Up a Site

information, or contact Rosslare technical support. Clear **Enabled** if you want to halt communication to panels on the network.



Note

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-825IP. Refer to the *AC-825IP Hardware Installation and User Manual* for more details.

9. In the *Network* window, select the *Options* tab and continue with the instructions as described from Step 10 in Section 5.3.1.
10. Click **OK**.

5.4 Adding Access Control Panels

5.4.1 AC-215x, AC-225x, and AC-425x Panels

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).



Note

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

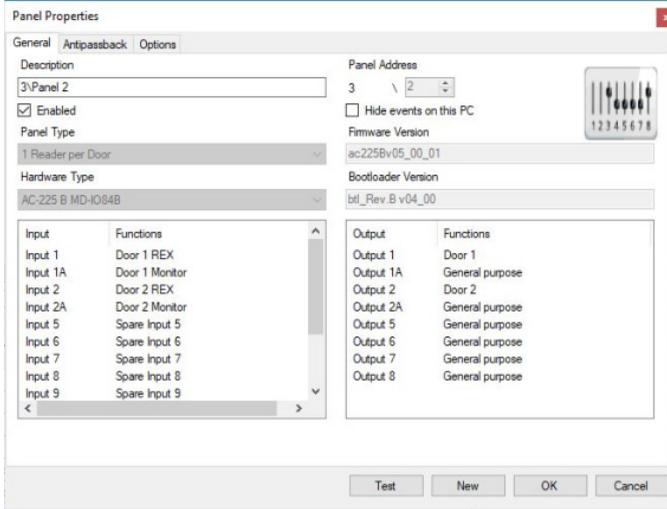
5.4.1.1 **Adding an Access Control Panel Manually**

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.

The *Panel Properties* window opens.



4. Configure the panel according to the fields described in Table 3.

Table 3: AC Networks > Network > Panel Properties > General Tab

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.

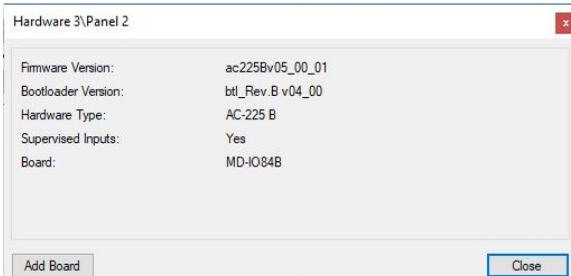
Setting Up a Site



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

5. Click **Test**.

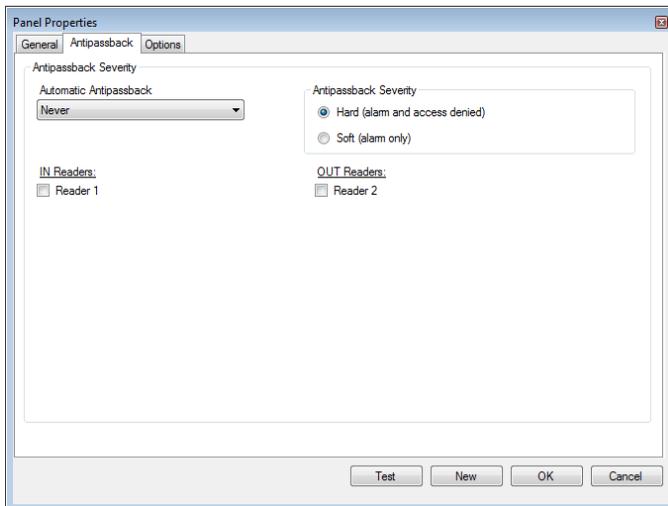
The *Hardware Test* window opens and shows the panel details.



If an expansion board is connected to the access control panel, it appears under "Board", and an **Add Board** button is visible (see Section 5.5).

6. Click **Close**.

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



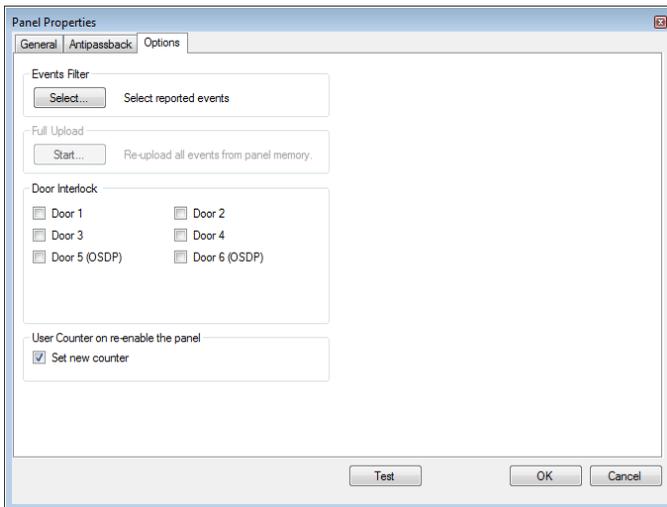
8. Set the Antipassback behavior according to the field descriptions in Table 4

Setting Up a Site

Table 4: AC Networks > Network > Panel Properties > Antipassback Tab

Field	Description
Automatic Antipassback	From the <i>Automatic Antipassback</i> dropdown, select the time zone for door antipassback rules to apply.
Antipassback Severity	<ul style="list-style-type: none"> • 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.

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



10. Set the recording events behavior according to the field descriptions in Table 5.

Table 5: AC Networks > Network > Panel Properties > Options Tab

Field	Description
Events Filter	<p>Click Select to open the Events Filter and select the events that this panel should record. Set the filter's operation method:</p> <ul style="list-style-type: none"> • Always Active – Only the selected events are recorded by the panel • Active when panel disconnected – If the panel is disconnected from the AxTraxNG server, only the selected events are recorded. When the panel is connected to the server, all events are recorded. <p>Note: In the default configuration, some events are filtered and may not be seen in the Events view</p>

Setting Up a Site

Field	Description
Full Upload	Click Start to re-upload all events from panel memory. Use the option only after consulting Rosslare's Technical Support. Note: A full upload can take up to 3 hours.
Door Interlock	This option is only visible when the panel is configured with at least two doors. Select the checkboxes 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. Note: When using a rule, be sure that it does not conflict with an existing interlock group (Section 5.4.2.1). Note: If you are configuring both antipassback (see Table 4) and door interlock features, you must configure the antipassback feature first. Note: This function doesn't work in AC-225, AC425 if reader was set in Card+Card mode
User Counter on re-enable the panel	This option allows you to reset the user counter to its starting value in the event that a panel is disconnected and then reconnected again. This option is only visible when Deduct User Counter is selected on the <i>General</i> tab of the <i>Readers Properties</i> window for one of the readers in the panel (Section 5.7.1).

11. Click **OK**.

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

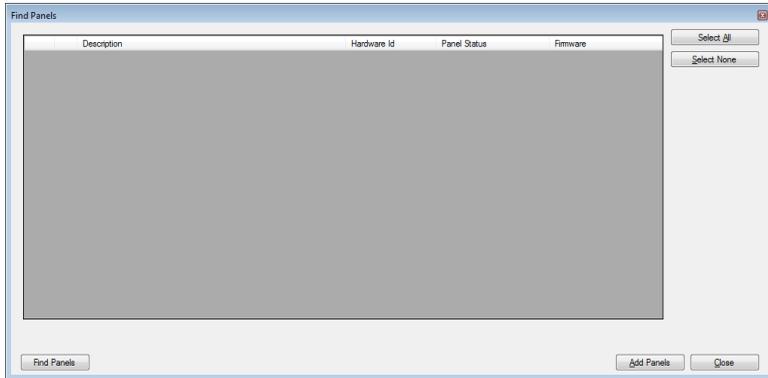
5.4.1.2 **Searching for Existing Access Control Panels**

Alternatively, it is possible to search for panels over the access control network using the *Find Panels* option. This is particularly useful during installations. AxTraxNG 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.

The *Find Panels* window opens.



3. Click **Find Panels** to search for all connected panels in the network. Once the detection process is complete (this may take a few minutes), the display shows all of the detected panels and their corresponding information.
4. Select the panels that you wish to add and click **Add Panels**. The selected panels then appear in the Tree View under current network. Configure the panel settings as described in Section 5.4.1.1.

5.4.2 AC-825IP Panel

When you create a network for an AC-825IP panel (Section 5.3.2), the AC-825IP panel is automatically added to the network.

There can be only one AC-825IP panel in a network. However, you can add one expansion board to the AC-825IP panel (Section 5.5.2) or up to 12 extensions using RS-485 (Appendix E).

5.4.2.1 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.

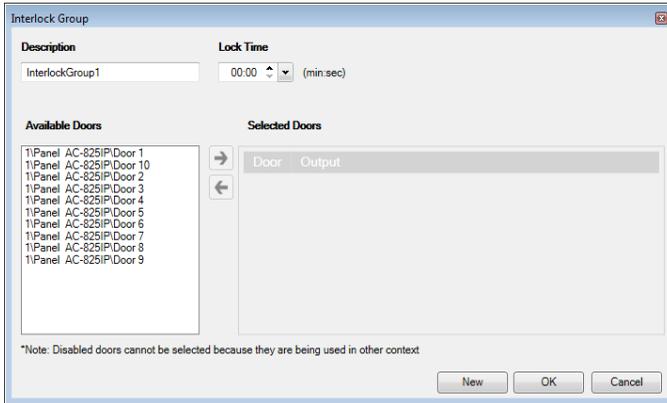


When defining an interlock group, be sure that it does not conflict with an existing interlock rule (see Door Interlock in Table 5).

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.

The *Interlock Group* window opens.



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.

5.5 Adding an Expansion Board

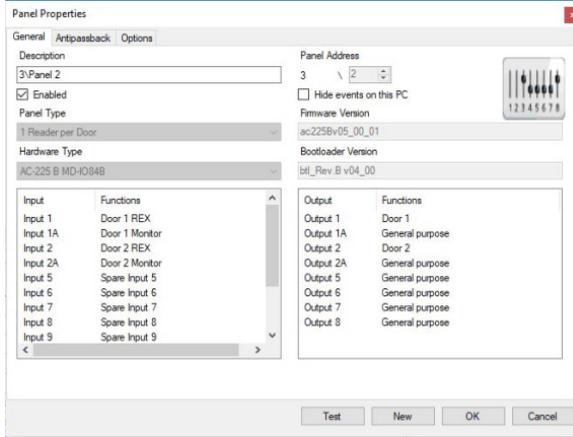
5.5.1 AC-225x and AC-425x

For the AC-225x panels, you can add one MD-D02 or MD-I084 expansion board per access control panel. For the AC-425x panels, you can add one MD-D04 or MD-I084 expansion board per access control panel.

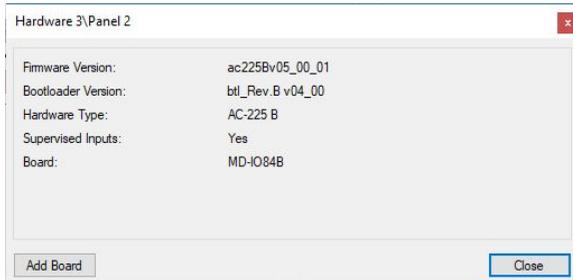
To add an expansion board:

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.

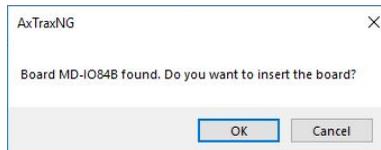
The *Panel Properties* window opens.



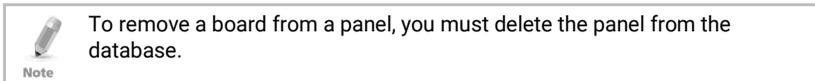
5. Click **Test**.



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.



5.5.2 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.

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.

Hardware Version
AC-825IP D-805
R-805
D-805



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

5.6 Configuring the Doors

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

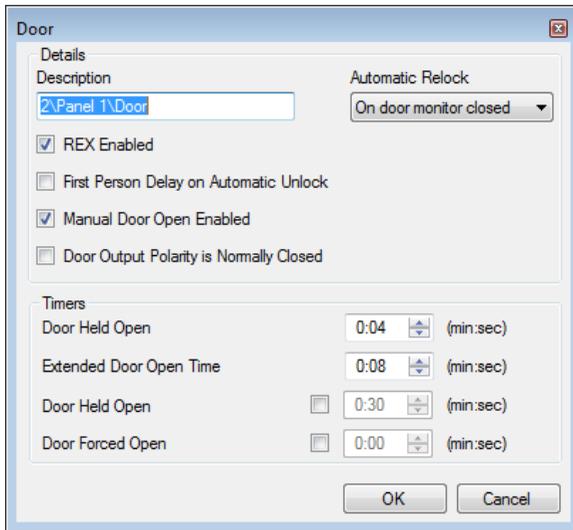
The *Door* window displays the following:

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

To edit the door properties:

1. In the Tree View, expand the **AC Networks** element.
2. Expand a network and expand a panel.
3. Select **Doors**.
The available doors are listed in the Display Area.
4. Select a door in the Display Area.
5. On the toolbar, click the  icon.

The *Door* window opens.



- Configure the door according to the fields described in Table 6.

Table 6: AC Networks > Network > Panel > Doors > Door Properties

Field	Description
Description	Type a name for the door.
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 Section 5.10).
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 Section 5.10).
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.

Field	Description
Door Held Open	<p>Set the duration for which the door can be held open without raising an alarm event.</p> <p>Select to use this timer. For the Server application, the Pop-up and Snapshot section opens.</p> <p>Note: If this feature is enabled, then the Activity start delay (Section 5.8) feature for that door must be set to 0.</p>
Door Forced Open	<p>Set the duration after which when the door is forced open, an event occurs.</p> <p>Select to use this timer. For the Server application, the Pop-up and Snapshot section opens.</p> <p>Note: If this feature is enabled, then the Activity start delay (Section 5.8) feature for that door must be set to 0.</p>

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

5.7 Configuring the Readers

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

The *Reader Properties* window has three tabs:

- *General* tab – Sets the reader general operation settings (5.7.1)
- *Options* tab – Sets access options for the reader (5.7.2)
- *Access event* tab – Sets options for window pop-ups per event (5.7.3)

To configure a reader:

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. Configure the reader as needed using the tabs described in the subsections below.
7. Click **OK**.

5.7.1 General Tab

The *General* tab in the *Reader* window displays:

- The settings for how the reader operates
- The type of reader being used

The screenshot shows the 'Reader' configuration window with the 'General' tab selected. The window is divided into several sections:

- Details:**
 - Description: 1\Panel AC-825IP\Reader 1
 - Direction: Radio buttons for 'In' (selected) and 'Out'.
 - Activation: Checkboxes for 'Open 1\Panel AC-825IP\Door 1' (checked) and 'Deduct User Counter'.
- Options:**
 - Primary Reader Format: Wiegand 26 bits
 - Secondary Reader Format: None
 - Check Facility Code Only: unchecked
 - License Plate: unchecked
 - Conversion Table: None
- Single Operation Mode:** Card Only
- User Dual Authentication:** unchecked
- Time Zone:** Never
- Number of Sessions:** 2
- Session Timeout (sec):** 10
- Keypad Type:** Inactive
- Door Opening Requirement in Card-Card Mode:** 2 Users
- Set as Muster:** unchecked
- Biometrics:** unchecked
- Biometric Terminals:** None

Buttons for 'OK' and 'Cancel' are located at the bottom right of the window.

Table 7 describes the fields that appear on the *General* tab.

Table 7: AC Networks > Network > Panel > Readers > Reader Properties > General Tab

Field	Description
Details > Description	Enter the name of the reader
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 (see Section 5.14.2.1)

Setting Up a Site

Field	Description
Details > Single Operation Mode	Select how the reader operates: <ul style="list-style-type: none"> • 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 Note: 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 <ul style="list-style-type: none"> • Always (default) • Never • Any previously defined time zone(s) in the system
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. <ul style="list-style-type: none"> • 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. Note: 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. Note: In AC-215A this function is disable
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 <i>Options</i> tab. Note: This option is only available for certain formats.

Setting Up a Site

Field	Description
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 checkbox to select from the dropdown to map a reader to a terminal (see Section 5.8.2).

5.7.2 Options Tab

The *Options* tab in the *Reader* window displays:

- Timed antipassback settings for the reader
- Restricted site access settings

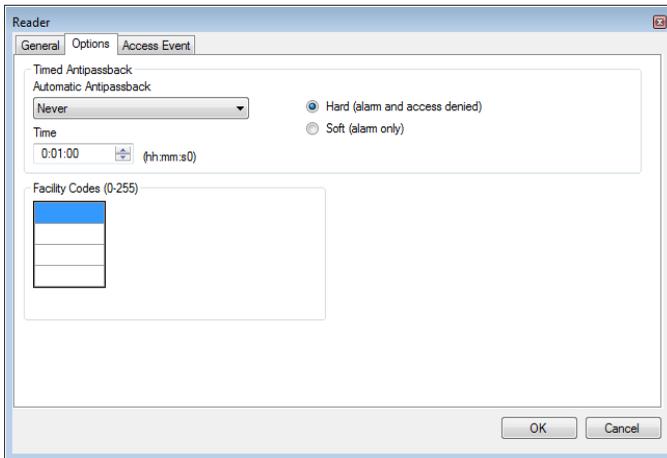


Table 8 describes the fields that appear on the *Options* tab.

Table 8: AC Networks > Network > Panel > Readers > Reader Properties > Options Tab

Field	Description
Automatic Antipassback	Select whether to apply antipassback rules. To set Time Zones, see Section 5.1.
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.

5.7.3 Access Event

The *Access Event* tab in the *Reader* window defines the alerts pop-up windows behavior on the local PC.

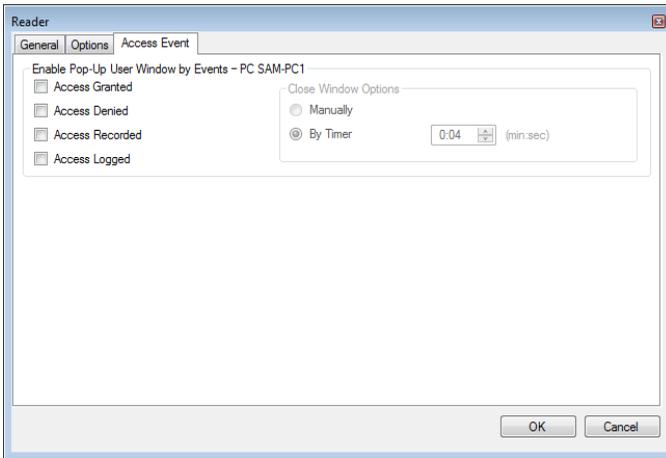


Table 9 describes the fields that appear on the *Access Event* tab.

Table 9: AC Networks > Network > Panel > Readers > Reader Properties > Access Event Tab

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	<p>Once a pop-up is enabled, the close window options are available.</p> <p>Select one of two options:</p> <ul style="list-style-type: none"> • 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.

5.8 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.

5.8.1 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.

The *Terminal Configuration* window opens.



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.

 Note	For models AY-B9250BT and AY-B9350, an additional Enable camera snapshot checkbox appears. If selected, the terminal takes a snapshot of the terminal view.
 Note	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 Appendix F for how to search for a biometric terminal and configure it.

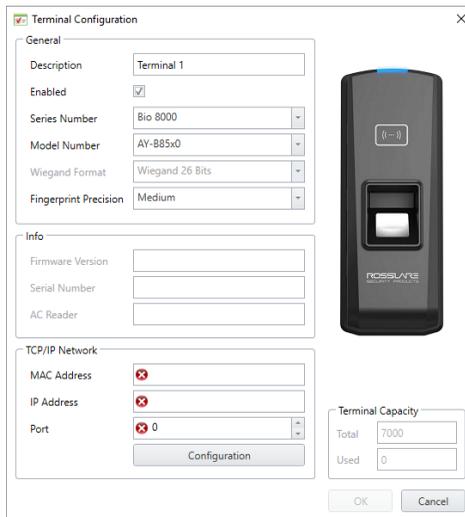
5.8.2 From a Remote Network

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.

5.8.2.1 Exporting a Terminal File

To export a terminal file:

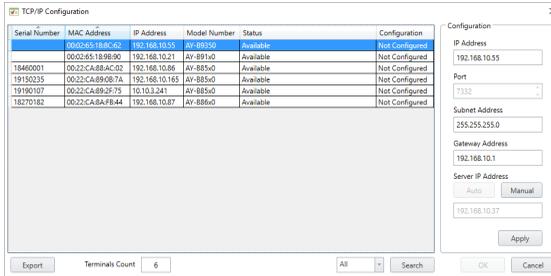
1. In the Tree View, expand the **Biometrics** element and select **Terminals**.
2. On the toolbar, click the  icon.
3. The *Terminal Configuration* window opens.



4. Click **Configuration**.

Setting Up a Site

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



- Click **Export**.
The Save as window appears.
- 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.

5.8.2.2 Importing a Terminal File

To import a terminal file:

- In the Tree View, expand the **Biometrics** element and select **Terminals**.
- On the toolbar, click the  icon.
The *Import Terminal* window opens.
- Browse to the previously exported xxx.axbio file and double-click it.
The window closes and the terminal appears in the Display Area.

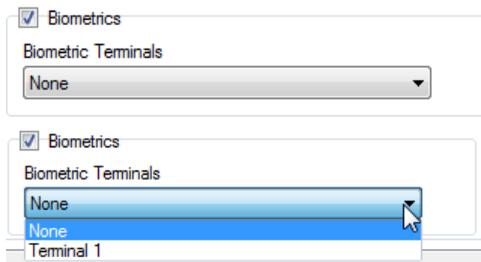
5.8.3 Mapping a Biometric Terminal to a Reader

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:

- In the Tree View, expand the **AC Networks** element.
- Expand a network and expand a panel.
- Select **Readers**.
The available readers are listed in the Display Area.
- Select a reader in the Display Area.
- On the toolbar, click the  icon.
The *Reader Properties* window opens to the *General* tab.
- Select the **Biometric** checkbox and select the relevant terminal from the dropdown.

Setting Up a Site



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.

AC Reader
1\Panel AC-825IP\Reader 1

5.8.4 Terminal Firmware Update

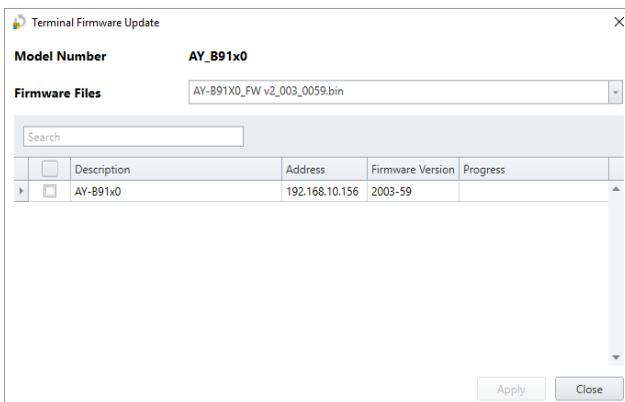
To update the firmware:



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

The following *Terminal Firmware Update* screen will appear



4. Check the terminal/s from the list

5. Click **Apply**
6. Wait till the process will finish and click **Close**

5.9 Configuring the Inputs

Each panel has four inputs. Using the MD-I084 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**.

The available inputs are listed in the Display Area.

	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

Table 10 describes the fields that appear in the Display Area.

Table 10: AC Networks > Network > Panel > Inputs

Field	Description
Location	A display field showing the input name
Description	Type a name for the input.
Type	<p>Select the type of input to be monitored.</p> <ul style="list-style-type: none"> • 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. <p>For more information, refer to the access control panel's hardware manual.</p>
Activity Start Delay	Set the delay time before this input becomes active. Note that on normally open input, the delay starts once the input contact is closed. On normally closed input, the delay starts once the input contact opens.

Setting Up a Site

Field	Description
Function	Select the door function: Door Monitor or Door REX This column is visible only if the REX enable checkbox is selected in Door properties.

4. Select an input and configure it as required.

5.10 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.

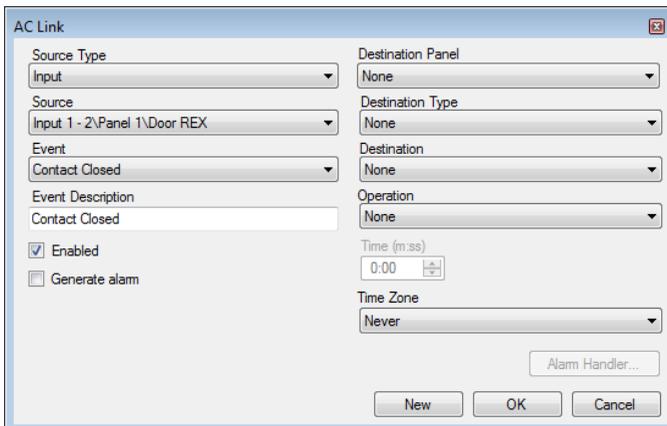
The *Link* window displays the following:

- 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 AxTraxNG 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.

The *AC Link* window opens.



AC Link

Source Type: Input

Source: Input 1 - 2\Panel 1\Door REX

Event: Contact Closed

Event Description: Contact Closed

Enabled

Generate alarm

Destination Panel: None

Destination Type: None

Destination: None

Operation: None

Time (m:ss): 0:00

Time Zone: Never

Alarm Handler...

New OK Cancel

Setting Up a Site

5. Configure the link rule as required, according to the field descriptions in Table 11.

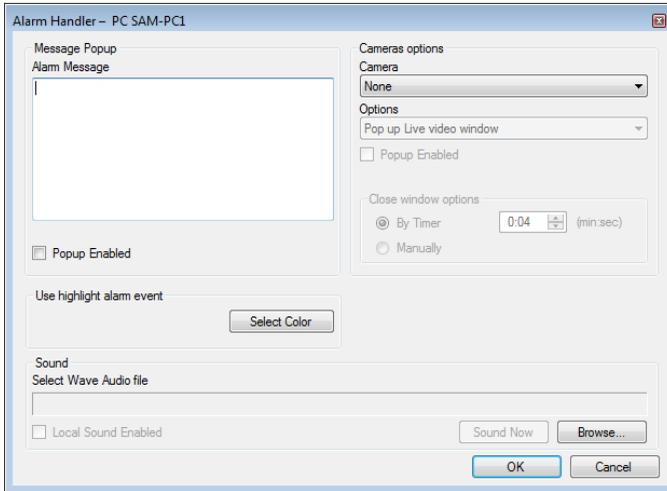
Table 11: AC Networks > Network > Panel > AC Links > AC Link Window

Field	Description
Source Type	Select the panel component type, input, output, reader, and so on which is the event source
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.
Event	Select the event type for the panel component
Event Description	Type the link or event description
Enabled	Select to enable the link rule
Generate alarm	Select to generate an alarm event in addition to the link rule activity
Open all Outputs of selected Output group	Select to enable global triggering of an output group This checkbox appears when Destination Type is Output Group .
Destination Panel	From the network, select the board to be activated by the link rule trigger event
Destination Type	Select the panel component type, which is to be activated by the link rule trigger event
Destination	Select the specific panel component, which is to be activated by the link rule trigger event
Operation	Select the operation performed by the destination panel component
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 <i>Destination Type</i> is specified.
Time Zone	Select the time zone for which the link rule applies

Field	Description
Alarm Handler	<p>The Alarm Handler function is only enabled when Generate Alarm is selected.</p> <p>The Alarm Handler configuration window contains the following fields:</p> <ul style="list-style-type: none">• Alarm Message: Type a personalized message to be displayed on the screen as an alarm message when the selected event occurs• Popup 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 <p>In addition, when a camera is linked to a panel, the following fields appear in the window:</p> <ul style="list-style-type: none">• Camera: List of available cameras• Options: Which alarm is activated• Popup 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.

The *Alarm Handler* window opens.



- c. Configure the alarm handler as required, according to the field descriptions in Table 11.
- d. Click **OK** to return to the *Link* window.

7. Click **OK**.

5.10.1 Creating a Fire Alarm Input

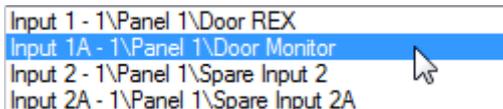
You can configure the panel properties to generate a fire alarm warning.

To create a fire alarm input:

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.

The *Link* window opens.

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**.

Setting Up a Site



Output Group only appears in Destination Type if an output group is defined for that panel (Section 5.12.3).

- e. In **Operation**, select **Timer Active**.
 - f. Select **Generate Alarm**.
6. Click **Alarm Handler**.

The *Alarm handler* window opens.

7. Configure the alarm handler as required, according to the field descriptions in Table 11.
8. Select **Open all Outputs of selected Output group**.
9. Click **OK** to return to the *Link* window.
10. Click **OK**.

5.10.2 Global Triggering of Output Groups

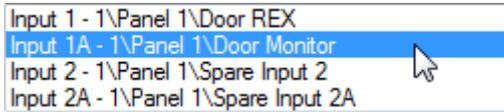
Global triggering is used for cross panel activations. For example, in case of a fire alarm, all doors in the system are opened from a single input.

To create global triggering of output groups:

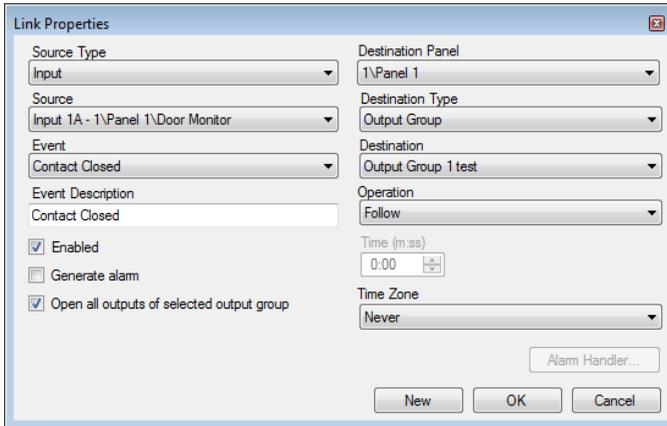
1. In the Tree View, expand the **AC Networks** element.
2. Expand a network and expand a panel.
3. Select **AC Links**.
4. On the toolbar, click the  icon.
The *Link* window opens.
5. Configure the link as follows:
 - a. In **Source Type**, select **Input**.

Setting Up a Site

- 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.



5.11 Adding Video Integration

See Chapter 7.

5.12 Adding 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.

5.12.1 Adding Access Groups

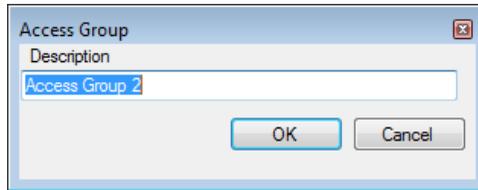
An access group includes a list of door readers and the time zones during which each of those door readers are available for access. Every user is assigned to an access group.

To add an access group:

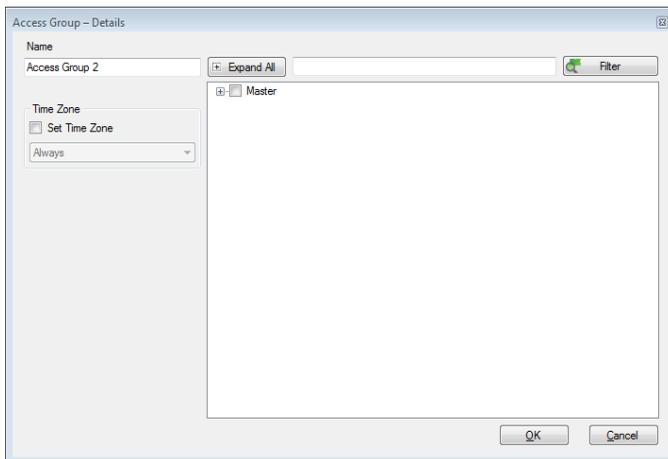
1. In the Tree View, expand the **Groups** element.
2. Select **Access Groups**.
3. On the toolbar, click the  icon.

Setting Up a Site

The *Add Access Group* window opens.



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. The *Access Group Properties* window opens.



6. From the *Time Zone* dropdown, 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.

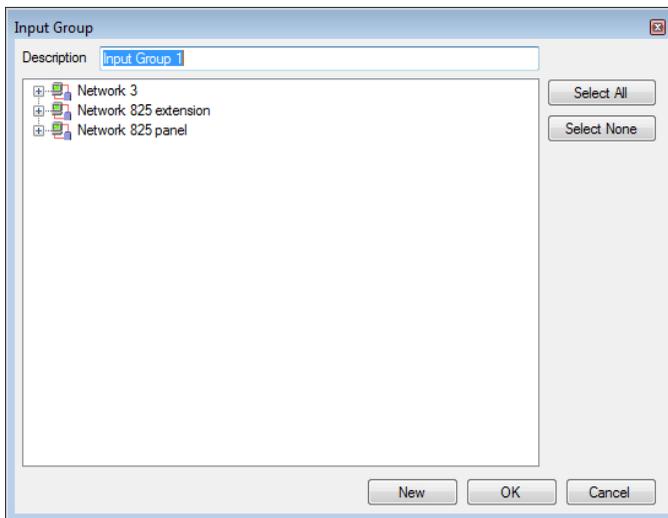
5.12.2 Adding Input Groups

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

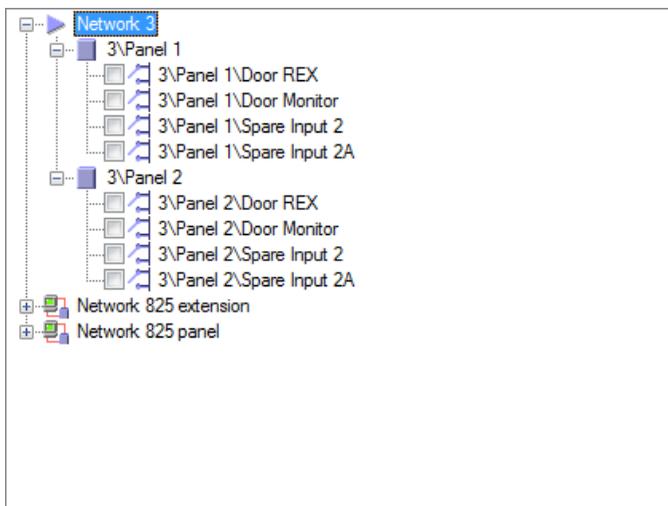
To create an input group:

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

The *Input Group* window opens.



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



6. Select the checkboxes 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.

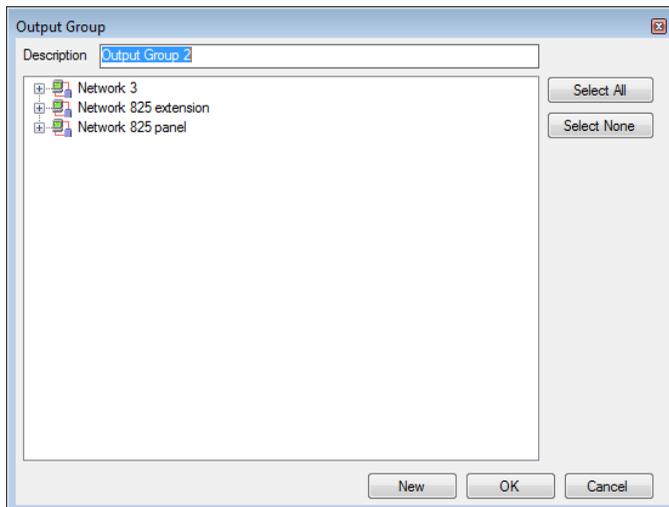
5.12.3 Adding Output Groups

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:

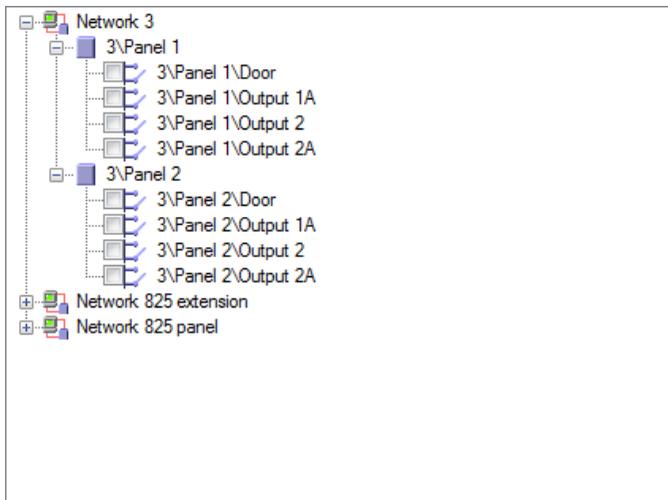
1. In the Tree View pane, expand the **Groups** element.
2. Select **Outputs Groups**.
3. On the toolbar, click the  icon.

The *Output Group* window opens.



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

- Expand a network to see its panels.



- Select the checkboxes of all relevant outputs. You can also use **Select All**.
- Click **OK**.
The window closes and the new output group appears in the Display Area.

5.12.4 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.

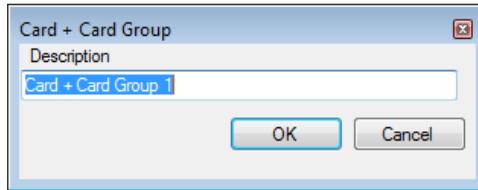
5.12.4.1 **Adding a Card + Card Group**

First, you must add a Card + Card group.

To add a Card + Card group:

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

The *Card + Card Group* window opens.



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.

5.12.4.2 **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 (see Section 5.14.2.1), select the Card + Card group from the *Card + Card Group* dropdown.
5. Click **OK**.
6. Repeat this process for each user you wish to add to a particular Card + Card group.

5.13 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.

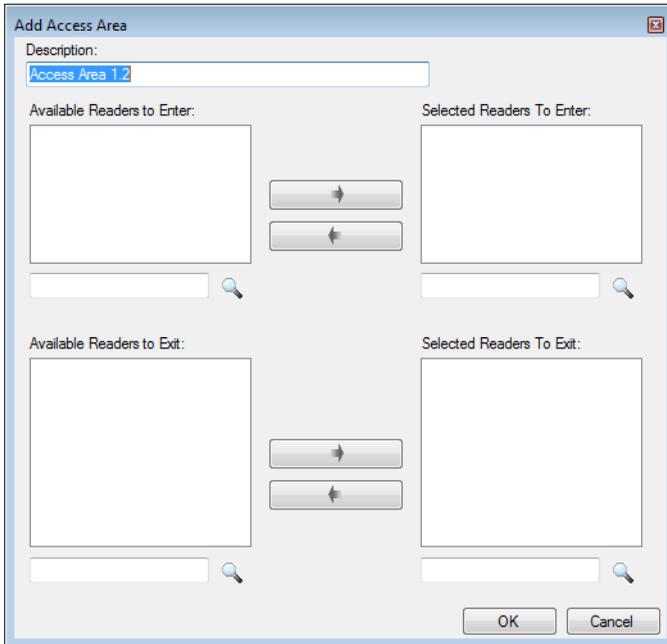
Use the *Access Area* window to add entry and exit door readers to and from an area within the facility.

Setting Up a Site

To add an access area:

1. In the Tree View, expand the **Groups** element.
2. Expand the **Access Areas** element and select **Global**.
3. On the toolbar, click the  icon.

The *Add Access Area* window opens.



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.

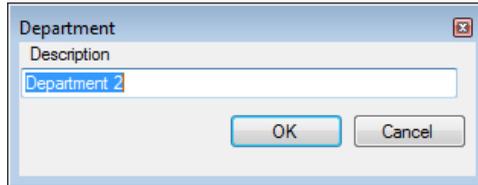
5.14 Adding Departments, Users, and Visitors

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

5.14.1 Adding Departments

To add a department:

1. In the Tree View, expand the **Users** element and select the **Departments/Users** element.
2. On the toolbar, click the  icon.
The Add *Department* window appears.



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.

5.14.2 Adding an Individual User

Adding users to a department is done by using the *User Properties* window.

The *User Properties* window contains three main tabs:

- *General* tab – Displays identification and control information (Section 5.14.2.1)
- *Codes* tab – Displays card information associated with the user (Section 5.14.2.2)
- *Details* tab – Records user contact details (Section 5.14.2.3)

In addition, there are two content-oriented windows:

- *User Fields* – Stores user-defined data (Section 5.14.2.4)
- *Visitor* Tab – Appears when the user is defined as a visitor (Section 5.14.3)

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.
The *User Properties* window opens.

Setting Up a Site

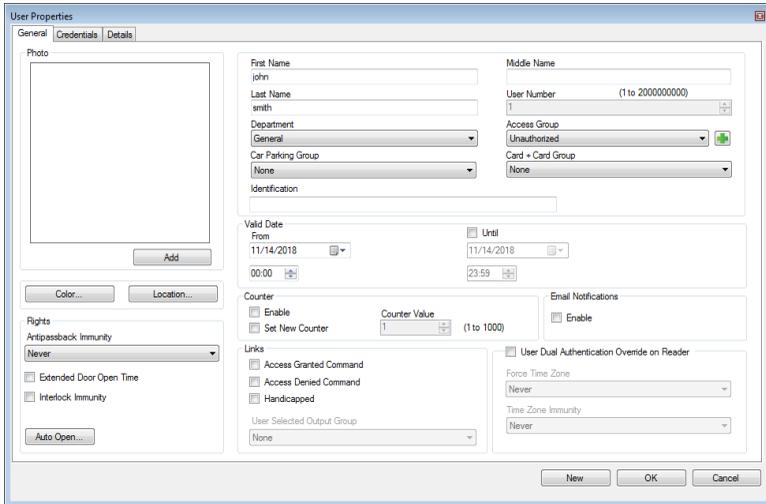
4. Enter the user details as needed using the tabs described in the subsections below.
5. In addition, you can click the  next to Access Group to open the *Access Group – Details* window, where you can select to which access panels that access group is granted permission (see Section 5.12.1).
6. Click **OK**.
The window closes and the new user appears in the Display Area.

5.14.2.1 General Tab

The *General* tab displays:

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

Figure 3: Departments/Users > User Properties > General Tab



The *General* tab fields are described in Table 12.

Table 12: Users > Departments/Users > Department > User Properties > General Tab

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.

Setting Up a Site

Field	Description
Middle Name	Type the user's middle name.
Last Name	Type the user's last name.
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
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 checkbox is selected. Note: 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 Appendix H). When the counter reaches zero, the user's access rights end.
Counter > Set new counter	Select to set a new countdown counter value for this user (see Appendix H).
Counter > Counter Value	Select a new countdown counter value for this user. This field is only enabled when the <i>Set new counter</i> checkbox is selected.
Email Notifications > Enable	Select to enable email notifications to be sent to the user's email, which is defined in the <i>Details</i> tab (see Section 5.14.2.3)

Setting Up a Site

Field	Description
Rights > Antipassback Immunity	Select to override any Antipassback restrictions for this user. <ul style="list-style-type: none">• Never• Always• User-defined time zone Note: 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 Section 5.5.2).
Rights > Interlock Immunity	Allows the user to open doors within the relevant access group regardless of the interlock status Note: This feature works only for AC-825IP
Rights > Auto Open	When defining user properties, you can define certain output groups to be active automatically (see Section 5.14.3).
Links > Access Granted Command	Select to activate a link rule initiated by access granted commands for this user (see Section 5.10).
Links > Access Denied Command	Select to activate a link rule initiated by access denied commands for this user (see Section 5.10).
Links > Handicapped	Select to activate a dedicated output a short time after the door is unlocked (see Section 5.10).
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 <i>Links</i> window (see Section 5.10).
User Dual Authentication Override on Reader	Select to override the dual authentication defined by the system (Section 5.7.1). <ul style="list-style-type: none">• Force Time Zone: The user must present two credentials, even though the reader does not require it. Note: For this feature to be active, the Dual Authentication Mode checkbox in the Reader window (Section 5.7.1) must be selected. <ul style="list-style-type: none">• 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.

Setting Up a Site

5.14.2.2 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.

User Properties x

General | Credentials | Details

Details

Protocol	Issue Number	Site Code	Facility Code	Card ID	Credential Type	Details	Status
Wiegand 26 bits			221	801	Fingerprint	R2 Bio8000	Active
Wiegand 26 bits			111	2222	BLE		Active
Wiegand 26 bits			123	2333	Card		Active
Wiegand 26 bits			111	4444	UHF		Active
Wiegand 26 bits			122	5555	NFC		Active
Wiegand 64 Bits				32247214414883717...	License Plate	AB-123-CD	Active
** Wiegand 26 bits					Card		Active

PIN Code

Number of Digits (4 to 8)

Duress PIN Code

Number of Digits (4 to 8)

The *Credentials* tab fields are described in Table 13.

Table 13: Users > Departments/Users > User Properties > Credentials Tab

Field	Description
Details	Displays the various properties of the credential added to the system for the user Note: 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 Appendix I)
Details > Enroll from UHF Reader	Click to enroll credentials using UHF desktop programmer (see Appendix J)
Details > Enroll License Plate	Click to enroll a license plate (see Appendix K)
Details > Enroll Face from Terminal	
Details > Enroll from Desktop Reader	Click to enroll credentials using a desktop reader (see Appendix K)

Setting Up a Site

Field	Description
Details > Add from List	Click to associate a user to a card or multiple cards (Section 5.14.7). Note: Before you can associate a user to a card, you must be sure that the card has been added to the system (see Section 5.14.3). All cards within the user's specified Facility code are listed
PIN/Duress PIN Code	Define PIN and Duress PIN code options: <ul style="list-style-type: none"> • 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

5.14.2.3 Details Tab

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

The screenshot shows a 'User Properties' dialog box with the 'Details' tab selected. The fields are arranged in two columns. The left column contains Telephone, Mobile, Fax, Email, and Address. The right column contains Home Telephone, Car Registration, Title, Employment Date (with a dropdown arrow and the date 11/14/2018), and Notes. A 'Details...' button is located below the Notes field. At the bottom of the dialog are 'New', 'OK', and 'Cancel' buttons.

The *Details* tab fields are described in Table 14.

Table 14: Users > Departments/Users > Department > User Properties > Details Tab

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.

Setting Up a Site

Field	Description
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.

5.14.2.4 **User Fields Tab**

The *User Fields* tab can be used to store any information required by the system operator.

User fields are defined on the *User Custom Fields* tab under **Tools > Options** (see Section 10.4.2).

5.14.3 **Auto Opening for Output Groups**

When defining user properties (Section 5.14.2), you can define certain output groups to be active automatically.

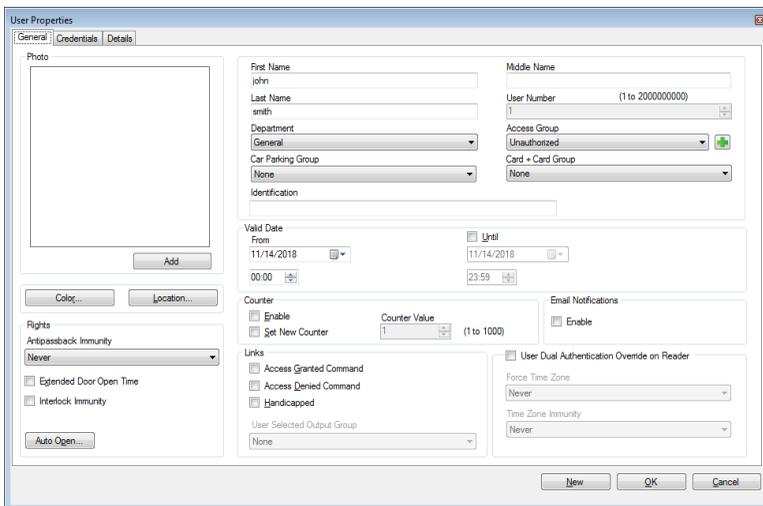


Output that needs to activate this function must be always in Active state in the "Event Filter" (**Panel properties > Options**)

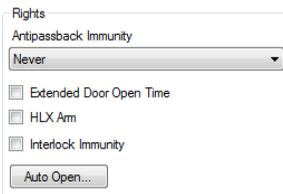
To define Auto Open for output groups:

1. In the 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 for a user.

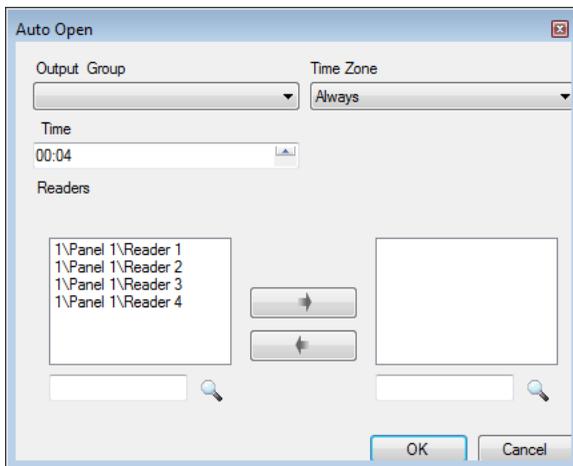
The *User Properties* window opens.



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



The *Auto Open* window opens.



Setting Up a Site

5. For each output group selected in the *Output Group* dropdown:
 - a. From the *Time Zone* dropdown, select a time zone.
 - a. From the *Time* box, select a duration time of the activation.
 - b. Select and move the desired readers using the arrows.
6. Click **OK**.

5.14.4 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.
The *Add Users and Cards* window opens.

3. Configure the card properties as required, according to the field descriptions in Table 15.

Table 15: Users > Cards > Add Users and Cards Window

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

Setting Up a Site

Field	Description
Sequential Cards	<p>Define the card properties:</p> <ul style="list-style-type: none"> • 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
Sequential Users > General	<p>Define the users general properties:</p> <ul style="list-style-type: none"> • Department: Associate to the new user(s) created to a department • Access Group: Associate to the new user(s) created to an Access group <p>Click  to add the user to a custom access group within all available readers.</p>
Sequential Users > Rights	<p>Define the users right properties:</p> <ul style="list-style-type: none"> • 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	<p>Select to define automatic pin codes, select between:</p> <ul style="list-style-type: none"> • 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	<p>Define the access right validity:</p> <ul style="list-style-type: none"> • 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	<p>Select to define associated link commands:</p> <ul style="list-style-type: none"> • Access Granted checkbox: Activate a user-defined set of inputs or outputs for access granted events • Access Denied checkbox: Activate a user-defined set of inputs or outputs for access denied events • Handicapped checkbox: 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. <p>The operations, inputs, and outputs are defined in the Links window (see Section 5.10).</p>
Sequential Users > Counter	<p>Select Enable to use the counter option then type or select the counter number to be used for the first user</p>

Setting Up a Site

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.

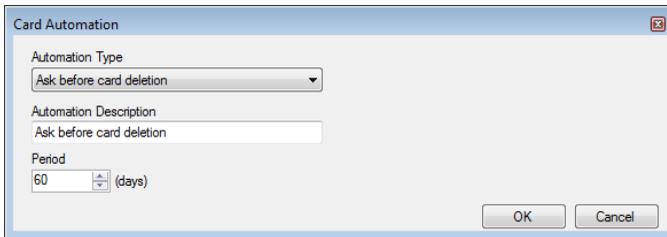
5.14.5 Setting Card Automation

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 Tree View, expand the **Users** element.
2. Expand the **Cards** element and select **Card Automation**.
3. On the toolbar, click the  icon.

The *Card automation* window opens.



4. From the *Automation Type* dropdown, 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
5. From the *Period* box, select the time period.
 6. Click **OK**.

5.14.6 Adding Visitors

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

The *Visitor's options* tab contains the following fields:

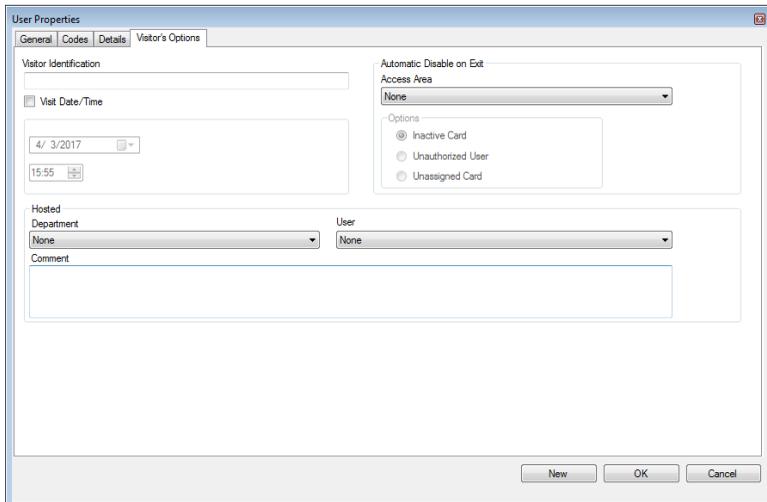
Table 16: Users > Departments/Users > Visitors > User Properties > Visitor's Options Tab

Field	Description
Visitor Identification	Type a unique visitor identification
Visit Date/Time	Select and specify the date and time for the visit
Automatic disable on exit	Define automatic disable access right options: <ul style="list-style-type: none">• Access Area: Select the Access Area to disable access to• Inactive card: The designated card automatically becomes inactive upon exit• Unauthorized user: the designated access group changes to Unauthorized upon exit
Hosted	Define the details for the hosting party: <ul style="list-style-type: none">• Department: Select the Department• User: Select the hosting User• Comment: Type any additional information

To create visitors:

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

The same *User Properties* window as before opens; however, now the *Visitor's Options* tab is available.



The screenshot shows the 'User Properties' dialog box with the 'Visitor's Options' tab selected. The dialog has three tabs: 'General', 'Codes', and 'Details'. The 'Visitor's Options' tab contains the following fields and controls:

- Visitor Identification:** A text input field.
- Visit Date/Time:** A checkbox labeled 'Visit Date/Time' is checked. Below it, a date field shows '4/ 3/2017' and a time field shows '15:55'.
- Automatic Disable on Exit:** A section with a dropdown menu for 'Access Area' set to 'None'. Below it, a section titled 'Options' contains three radio buttons: 'Inactive Card' (selected), 'Unauthorized User', and 'Unassigned Card'.
- Hosted:** A section with two dropdown menus: 'Department' set to 'None' and 'User' set to 'None'. Below them is a 'Comment' text area.
- Buttons:** 'New', 'OK', and 'Cancel' buttons are located at the bottom right.

Setting Up a Site

3. Enter the visitor specific options as needed.
4. Enter the visitor's details in the various tabs as explained in detail in the user subsections.
5. Click **OK**.

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



Note

Users may be moved to other department or redefined as a Visitor. A visitor may be moved into any department and changed to a regular user. These can be done by using the *General* tab and selecting the new department to which you wish to the user or visitor.

5.14.7 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, select the *Codes* tab.

User Properties

General | Credentials | **Details**

Protocol	Issue Number	Site Code	Facility Code	Card ID	Credential Type	Details	Status
Wiegand 26 bits			221	801	Fingerprint	R2 Bio8000	Active
Wiegand 26 bits			111	2222	BLE		Active
Wiegand 26 bits			123	2333	Card		Active
Wiegand 26 bits			111	4444	UHF		Active
Wiegand 26 bits			122	5555	NFC		Active
Wiegand 64 Bits				32247214414883717...	License Plate	AB-123-CD	Active
** Wiegand 26 bits					Card		Active

Enroll from Fingerprint Terminal | Enroll from Face Terminal | Enroll from Desktop Reader | Enroll from License Plate | Add from List...

PIN Code

Number of Digits (4 to 8) | Code | Random PIN Code

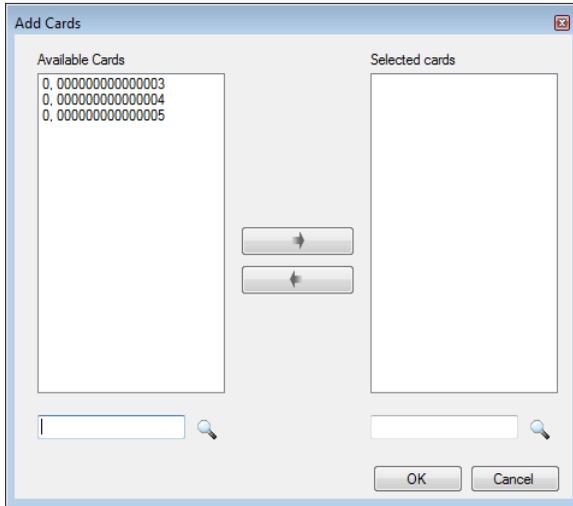
Duress PIN Code

Number of Digits (4 to 8) | Code | Random PIN Code

New | OK | Cancel

2. Click **Add from List**.

The *Add Cards* window opens.



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.

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

5.15 Adding Global Antipassback Rules

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

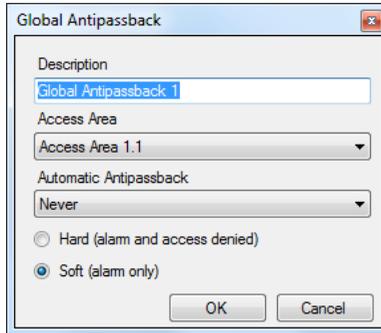


A global antipassback rule can only be added if an access area has previously been defined (see Section 5.13).

To create antipassback rules:

1. In the Tree View, select **Global Antipassback**.
2. On the toolbar, click the  icon.

The *Global Antipassback* window opens.



3. In the *Description* field, enter a name for the antipassback rule.
4. From the *Access Area* dropdown, select the access area.
5. From the *Automatic Antipassback* dropdown, 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.



Note

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.

5.16 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.



Note

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



Note

Only one car park area can be added per panel.

Setting Up a Site

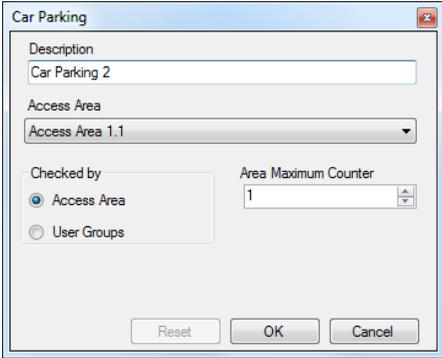


A car parking area can only be added if an access area has previously been defined (see Section 5.13).

To define a car parking area:

1. Create an access area with Enter and Exit readers (see Section 5.13).
2. In the Tree View, select **Car Parking**.
3. On the toolbar, click the  icon.

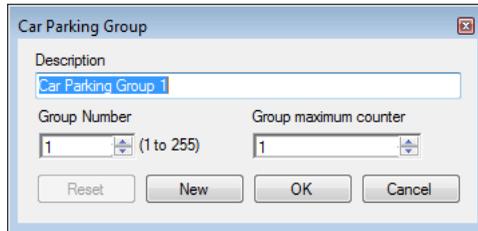
The *Car Parking* window opens.



The screenshot shows a dialog box titled "Car Parking". It has the following fields and controls:

- Description:** A text box containing "Car Parking 2".
- Access Area:** A dropdown menu showing "Access Area 1.1".
- Checked by:** Two radio buttons: "Access Area" (selected) and "User Groups".
- Area Maximum Counter:** A spin box containing the number "1".
- Buttons:** "Reset", "OK", and "Cancel" at the bottom.

4. In *Description*, enter a name of the car parking area.
5. In *Access Area*, select the relevant access area that you defined in Step 1.
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.
The *Car Parking Group* window opens.



The screenshot shows a dialog box titled "Car Parking Group". It has a "Description" text box containing "Car Parking Group 1". Below that are two spinners: "Group Number" (set to 1, with "(1 to 255)" next to it) and "Group maximum counter" (set to 1). At the bottom are four buttons: "Reset", "New", "OK", and "Cancel".

- 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 (see Section 5.14.2.1), select the Car Parking sub-group from the *Car Parking Group* dropdown.
- xi. Click **OK**.

The window closes and the new car parking group appears in the Display Area.
- xii. Repeat Steps viii to x for each user you wish to add to a particular Card + Card group.
- xiii. Repeat Steps iii to xii for each group that you wish to add to the car parking area.

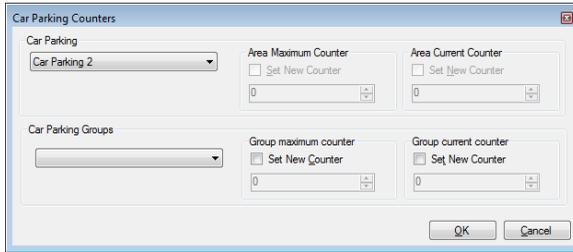
5.16.1 Viewing and Editing Car Parking Counters

Once you set up your various car parking groups and areas, the counters for these groups and areas can be easily viewed and edited.

To view and edit the Car Parking counters:

1. In the Events toolbar (above the Event Log area), click the  icon.

The *Car Parking Counters* window opens.



2. Update the maximum or current counters of either the car parking areas or the car parking groups, depending on how the car parking element is defined.

The values of the maximum counters entered in this screen override the values of the maximum counters that you entered in Section 5.16.

3. Click **OK**.

5.17 Adding Operators

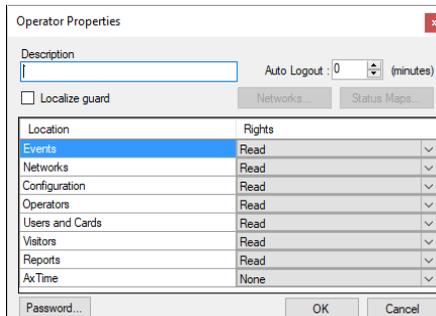
Operators are people with access to the AxTraxNG application. The default operator name is Administrator.

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.

To define operators:

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

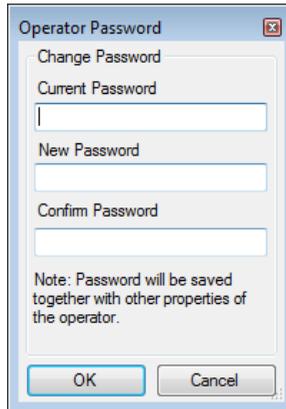
The *Operator Properties* window opens.



3. In the *Description* field, enter the Operator's name.
4. *Auto Logout* - to define the time in minutes the AxTraxNG Client will logout.
5. Select **Localize guard** to define the operator with limited rights.

Setting Up a Site

6. Click **Networks...** and **Status maps...** to define the associated operator's local rights.
7. Set the operators global permission rights for each of the screens in the *Location* list.
8. Click **Password...** to open the *Operator Password* dialog.



The image shows a dialog box titled "Operator Password". It has a close button in the top right corner. The dialog contains the following elements:

- A label "Change Password" above a group box.
- Inside the group box, there are three text input fields labeled "Current Password", "New Password", and "Confirm Password".
- Below the input fields is a note: "Note: Password will be saved together with other properties of the operator."
- At the bottom are two buttons: "OK" and "Cancel".

9. 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.

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

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

5.18 Creating Elevator Control

Normally, a reader is associated with a door. For elevator control, a selected reader should be associated with outputs groups, with each output group representing a floor.

To create elevator control:

1. Select a reader (see Section 7) in the Display Area.
2. On the toolbar, click the  icon.
3. On the *General* tab in the *Reader Properties* window, clear **Activation**.

Activation:  Open 1\Panel 1\Door 2

4. Click **OK**.
5. Create output groups (see Section 5.12.3).
Each output group represents a floor or several floors.

Setting Up a Site



When creating an output group for the elevator control, the selection only applies to outputs from the same panel.

6. On the *General* tab of the User window, associate a user with the relevant output groups (see Section 5.14.2.1).
Each user can be associated with the relevant output groups to allow user access to specific floors, as needed.
7. Create a panel link (see Section 5.10). Only one panel link is required.

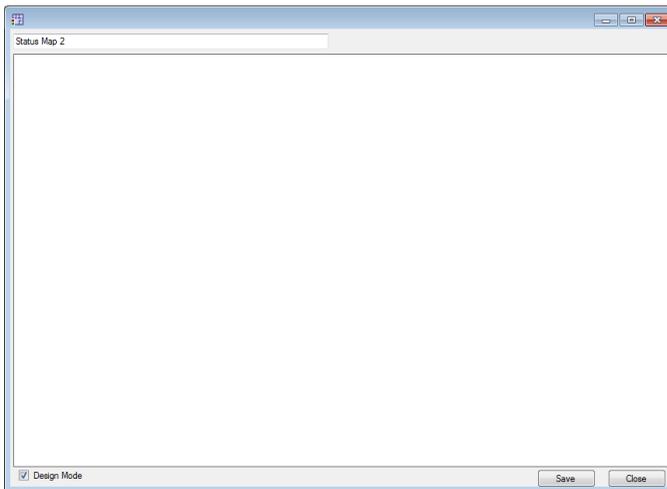
5.19 Creating Status Maps

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.

The *Add Status Map* window opens.



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

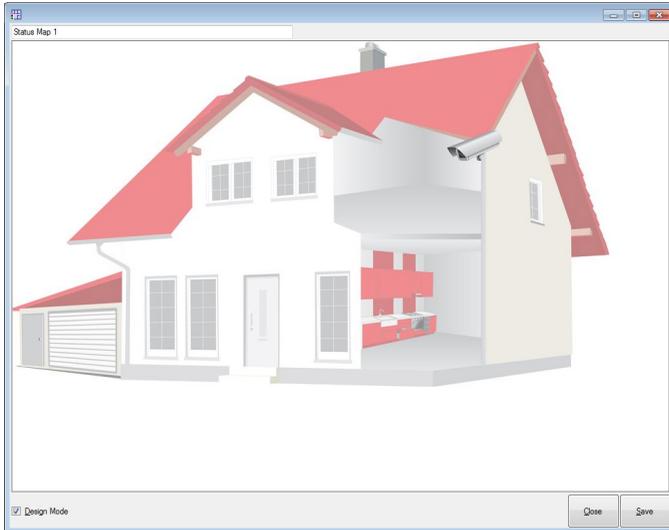
The *Select Picture File* window opens.



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.

Setting Up a Site

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



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.



Setting Up a Site

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

The *Show on Map* window opens.



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 Table 11).

11. Repeat Steps 6 to 10 until all objects are shown on the status map, as required.
12. Repeats Steps 1 to 10 to set up additional status maps.



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

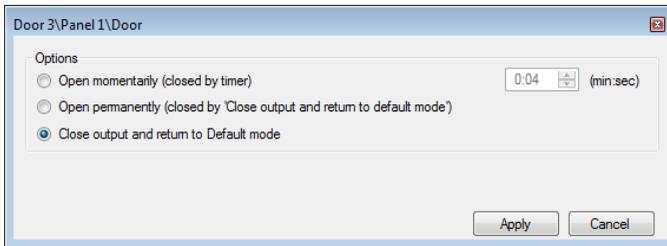
5.19.1 Manually Opening a Door from Status Map

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 following window opens.



The available options are the same as those in Section 8.1.

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

6. Card Design (Photo ID)

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

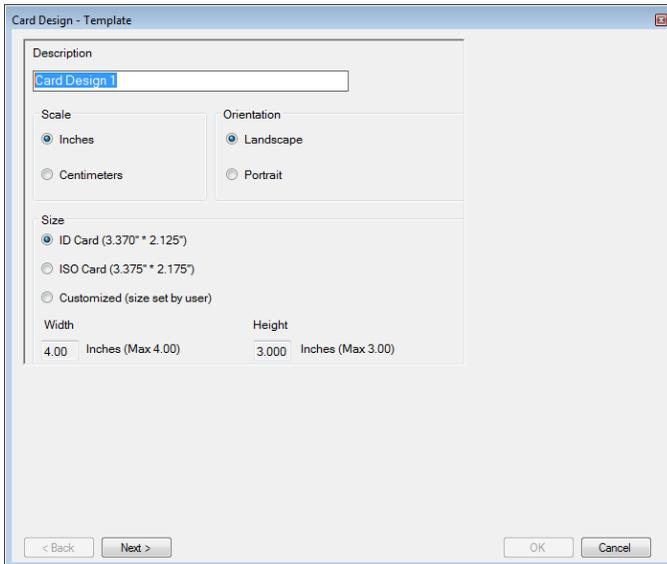
This chapter instructs installers and users how to use the **Card Design** element.

6.1 Creating a Card Template

To create a card template:

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

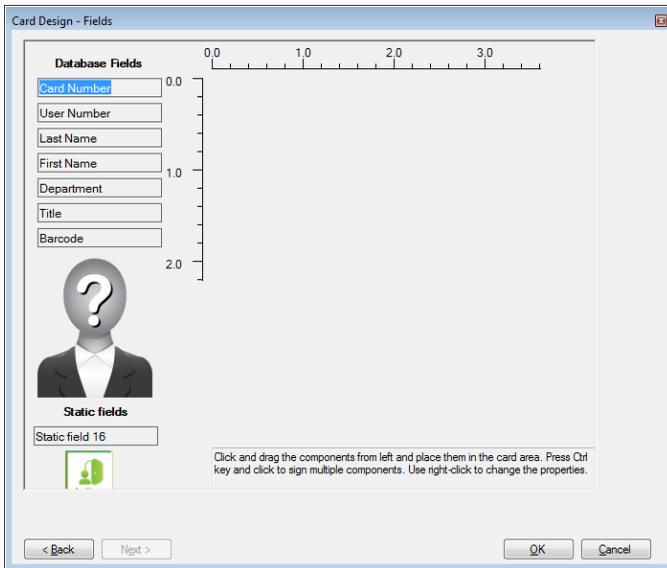
The *Card Design - Template* screen opens.



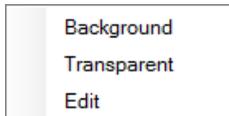
4. Enter a description for the template and define the scale, orientation, and size.
5. Click **Next**.

Card Design (Photo ID)

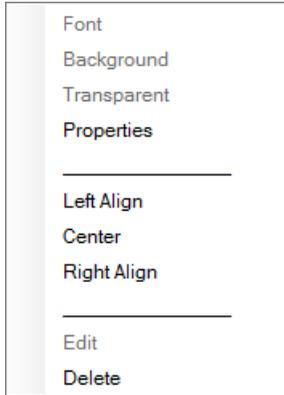
The *Card Design - Fields* screen opens.



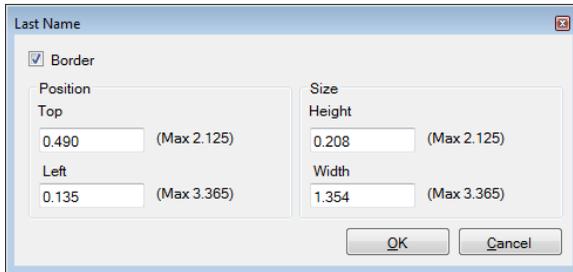
6. Right-click the card area background to set the background color or to select a file to use as the background.



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. Select **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.

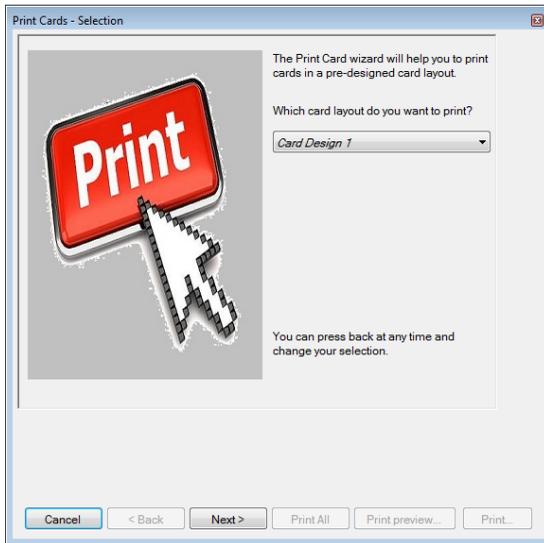
6.2 Printing a Card

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.
The *Print Card – Selection* window opens.



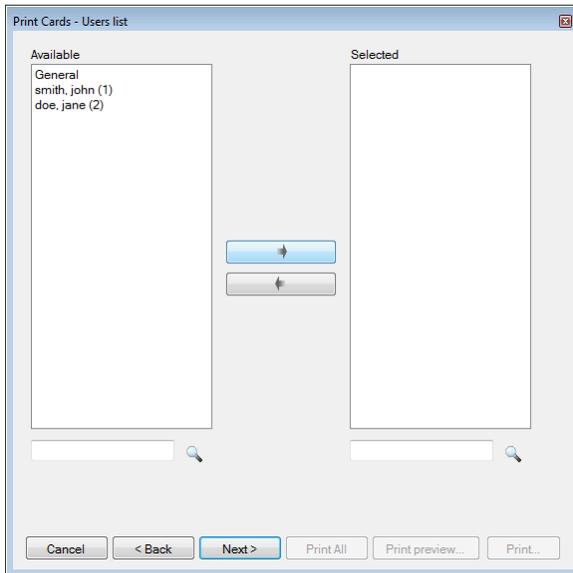
2. Select the layout you wish to use (if different than what you selected in Step 1 from the corresponding dropdowns).
3. Click **Next**.

The *Print Card – Users List* screen opens.

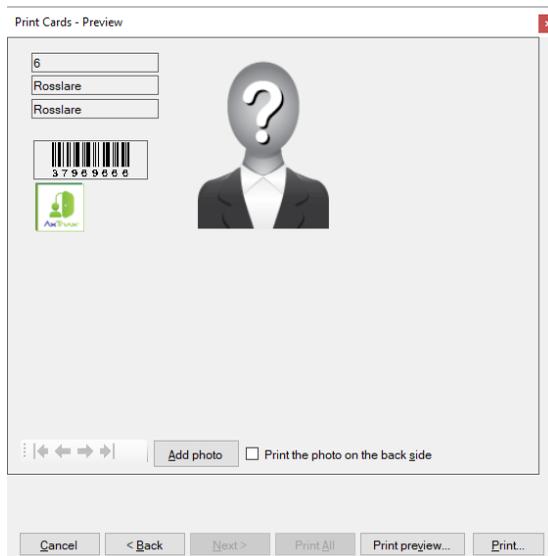


For users to appear in the Available list, they must have cards associated with them as described in Section 5.14.7.

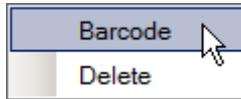
Card Design (Photo ID)



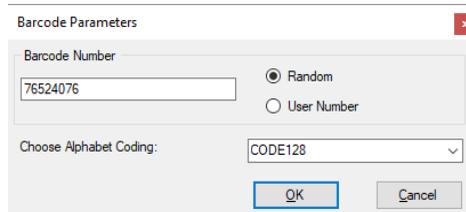
4. Select the users from the available list for whom you wish to print a card and move them to the right panel using the arrows.
5. Click **Next**.
The *Print Card – Preview* screen opens.



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



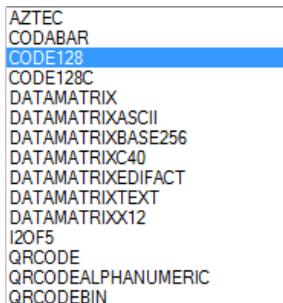
The *Barcode Parameters* window opens.



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* dropdown, select the kind of coding.



- c. Click **OK**.

The barcode appears on the card template.



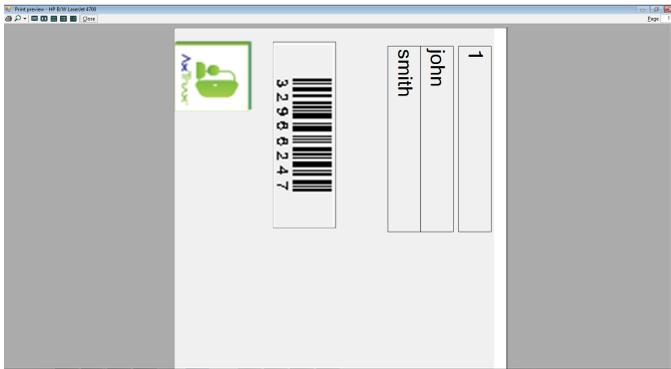
7. Click **Add photo** if you wish to select a different image either from a file or from a PC camera:

The *Select Source* window opens.



- a. Do one of the following:
 - Select **Browse** to locate an image to insert.
 - Select PC Camera and select **Capture Image**.
 - b. Click **OK**.
8. Use the green arrows to preview additional users.
 9. [Optional] Click **Print preview** to show the enlarged card screen.

Card Design (Photo ID)



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

7. Video Integration

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.

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

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

8. Manual Operation

In addition to AxTraxNG's automated access control network monitoring and control, there is the option to manually control the network directly.

 Door Manual Operation can only control doors that have been set as "Manual Door Open Enabled" in the *Door Properties* window (see Section 5.5.2).

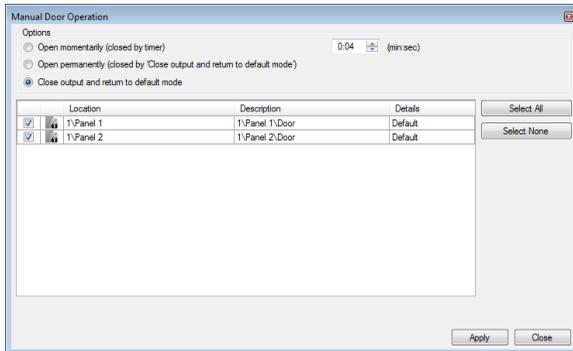
8.1 Controlling the Door Manually

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.

The *Manual Door Operation* window opens.



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 AxTraxNG
7. Select the checkboxes of those doors to which to apply the operation.
8. Click **Apply**.

8.2 Changing the Reader Mode

The *Manual Reader Operation* window allows an operator to change the operation mode of a reader.

Readers have eight possible operation modes:

- **Inactive:** The reader is not in use.
- **Card Only:** The reader accepts cards only.
- **PIN Only:** The reader accepts PIN inputs only.
- **Card or PIN:** The reader accepts both cards and PINs.
- **Desktop:** The reader is inactive, but can record new cards for the AxTraxNG database.
- **User Dual Authentication:** The reader grants access only for 2 credentials per user per access



Note

The AC-215A panel does not support User Dual Authentication mode, and instead supports Secure (Card + PIN) mode.

- **No Access:** The reader does not grant access to users.
- **Card + Card:** The reader grants access only when two separate users present their cards.



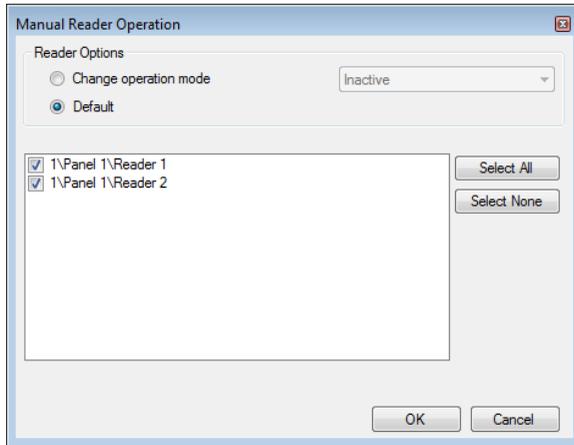
Note

The AC-215A panel does not support Card + Card mode

To change the reader mode manually:

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 *Manual Reader Operation* window opens.



4. Select an option:
 - **Change operation mode** – Resets all selected readers to the selected operation mode.
 - **Default** – Returns control of the readers to the system.
5. Select the checkboxes of those readers to which to apply the operation.
6. Click **OK**.

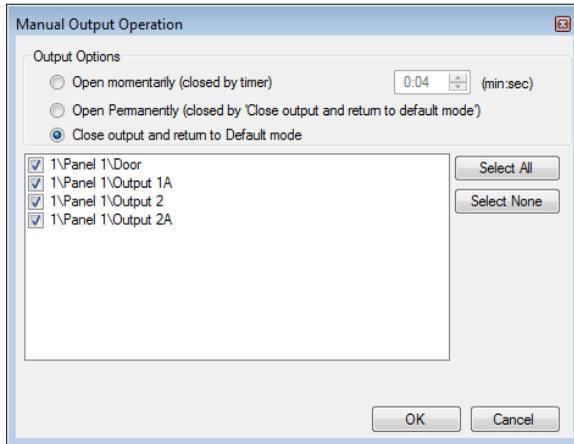
8.3 Controlling Outputs Manually

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.

The *Manual Output Operations* window appears.



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 checkboxes of the outputs to which to apply the operation.
6. Click **OK**.

8.4 Manually Disarming Inputs

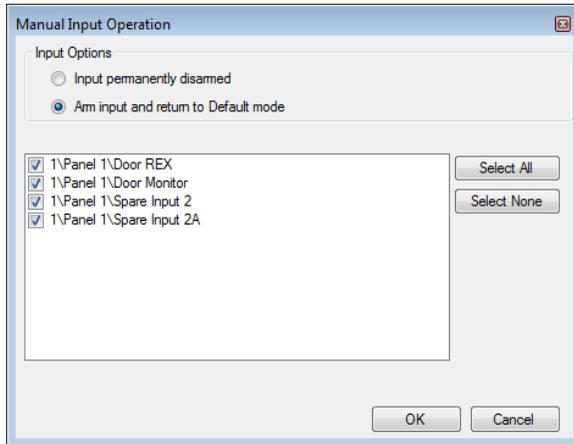
The *Manual Input Operation* window allows an operator to disarm a selected group of inputs directly on a panel.

An armed input means the input is active; a disarmed input is inactive and does not trigger any operation or alarms.

To manually disarm or rearm an input:

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 *Manual Input Operations* window opens.



4. Select an option:
 - **Input permanently disarmed** – Deactivates all selected inputs.
 - **Arm input and return to default mode** – Reactivates the selected inputs and returns control to default.
5. Select the checkboxes of the inputs to which to apply the operation.
6. Click **OK**.

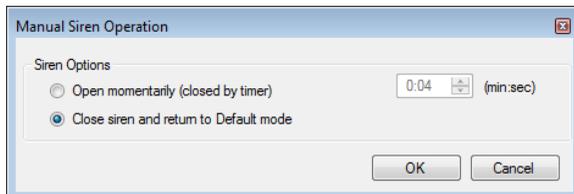
8.5 Controlling Sirens Manually

The *Manual Siren Operation* window allows an operator to test the siren for a selected panel.

To manually open or close a siren:

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 *Manual Siren Operations* window opens.



4. Select an option:
 - **Open momentarily** – Sounds the siren for the time set in the timer box.

- **Close siren and return to default mode** – Silences the siren and returns control to default.

5. Click **OK**.

8.6 Updating Firmware

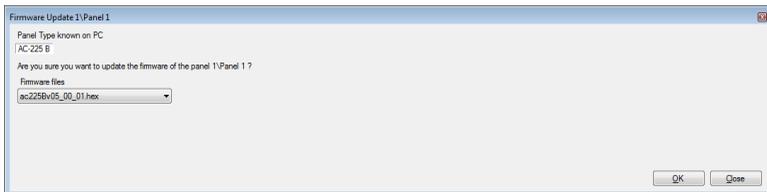
The *Update Firmware* window allows an operator to update the firmware version of the selected access control panel. For AC-825IP panels, you can also update the firmware of the connected extensions.

8.6.1 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.

Status	Downloads
Connected	

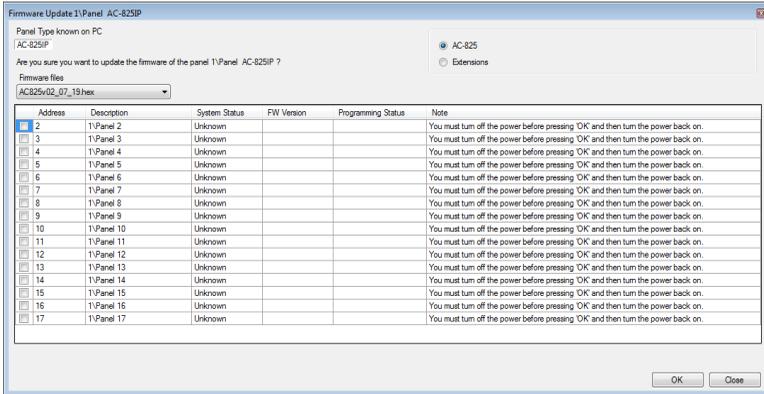
The updated finishes when the number of downloads reduces to zero and then no longer appears in the column. The status of the panel is now "Connected".

Status	Downloads
Connected	

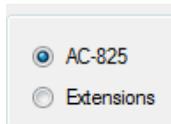
8.6.2 AC-825IP Panel

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.

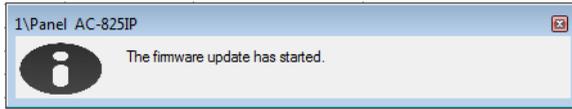
	Address	Description	System Status	FW Version
<input checked="" type="checkbox"/>	2	4\Panel 2	Enable	03_50
<input type="checkbox"/>	3	4\Panel 3	Unknown	

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

7. Click **OK**.

Manual Operation

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.

Status	Downloads
Download firmware	▲ 1166  1282

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".

Status	Downloads
Connected	

9. Reports



Note

When printing a report, be sure that the default printer is a standard printer and not a special printer for printing cards; otherwise, the reports may not print correctly.

9.1 Types of Reports

AxTraxNG includes four main categories of reports and each category contains multiple kinds of reports.

- **Immediate Reports** – Lists details of recent movements (within the last few hours). They are shown in the Display Area and can be exported.
- **Panel Reports** – Displays details of all recorded panel events
- **System Reports** – Lists details of system and operator activity
- **Interactive Report** – Lists details of users and their access activity

9.1.1 Immediate Reports

There are four types of immediate reports:

- **Who's been in today** – Lists where and at what time each user was granted access for the first time today.
- **Last known Position** – Lists where and at what time today each user was most recently granted access.
- **Roll-Call Readers** – Lists the last time each reader was given access, and by whom, within the last 1–99 hours.
- **Roll-Call Areas** – Lists all users currently within the selected area, sorted by department and entry time. The report lists all personnel who entered the facility within the last 1–99 hours.
- **Access Area Occupancy** – Lists all of the personnel in the designated access area

9.1.2 Panel Reports

Panel reports display details of all recorded panel events.

There are seven available panel event reports:

- **Attendance Report** – Lists the attendance hours for selected users, sorted by date. Results include hours present, time in, and time out.
- **AC Panels Report** – Lists all the events recorded by the selected AC panels, sorted by date.
- **Access Report** – Lists all access events recorded by the selected readers, sorted by reader and date.
- **Readers Report** – Lists all users who have accessed the selected readers, sorted by department and date.

Reports

- **Bio Terminals**– Lists specific Biometric terminals events, sorted by terminal and date.
- **Visitors**– Lists visitors who have made a visit to a certain user or department, or lists all related visitors.

9.1.3 System Reports

System reports list details of system and operator activity.

There are three available system event reports.

- **System Report** – Lists all operations performed by the AxTraxNG server, sorted by date.
- **Operators Report** – Lists all the operations performed by registered system operators, sorted by operation event type and date.
- **Alarm and Antipassback Handler Report** – Lists all raised system alarms, sorted by operator and date.

9.1.4 Interactive Report

Interactive reports list details of users and their access activity.

There are three available interactive reports:

- **User Access Rights Report** – Lists site access details for selected users, with full details of readers accessed and in which time zones.
- **Not Responding Users Report** – Lists users for whom there have been no access events for a selected period of time.
- **AC Panel Links Report** – Displays the links in the system per selected access control panel.

9.2 Generating a Report

To generate a report:

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

Reports

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.

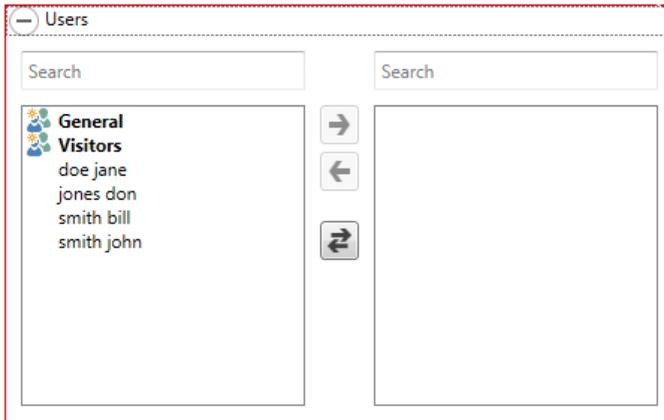
For example, the parameters needed for the User Access Rights Report are displayed.



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

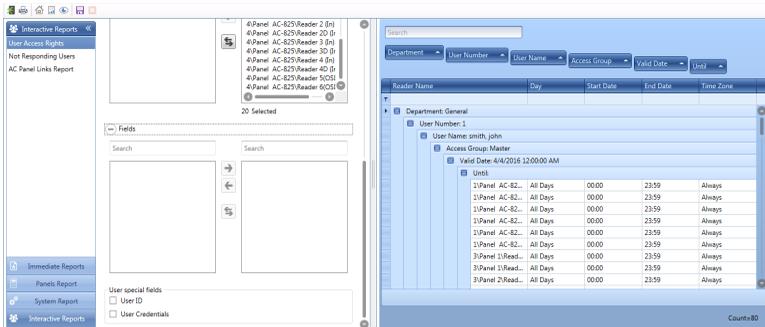
Reports

- Click on a parameter to expand it.



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



9.3 Scheduling a Report

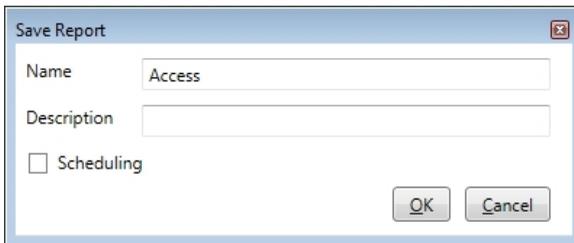
Once you have generated a report for the first time, you can schedule the same report to be generated and saved automatically at a time interval of your choosing.

To schedule a report:

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

The *Save Report* window opens.

Reports



Save Report

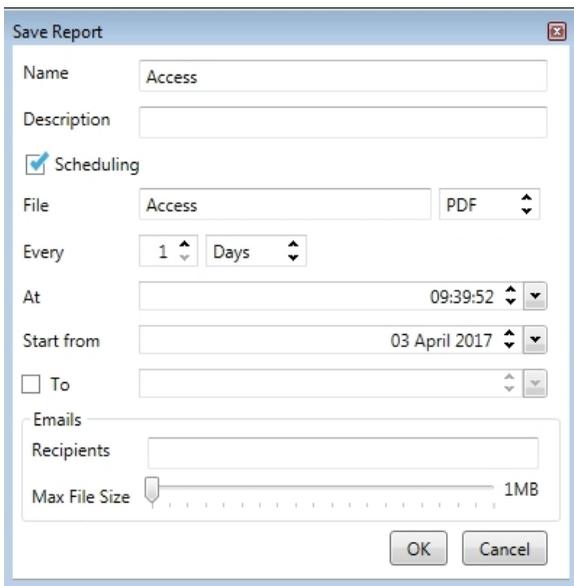
Name: Access

Description:

Scheduling

OK Cancel

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



Save Report

Name: Access

Description:

Scheduling

File: Access PDF

Every: 1 Days

At: 09:39:52

Start from: 03 April 2017

To:

Emails

Recipients:

Max File Size: 1MB

OK Cancel

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 Section 0.4).

5. Click **OK**.

The saved report appears in the Display Area.

Report Id	Report Categ...	Report Type	Name	Description	Updated At	Is Scheduled
1	Interactive	User Access Ri...	User Access R...	test	03/04/2017 0...	<input type="checkbox"/>

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

Reports

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

Reports that are automatically generated as scheduled are saved to a default location, which is set in the AxTraxNG Server Monitor (Appendix O.4).

9.4 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.

A separate window opens showing the report.

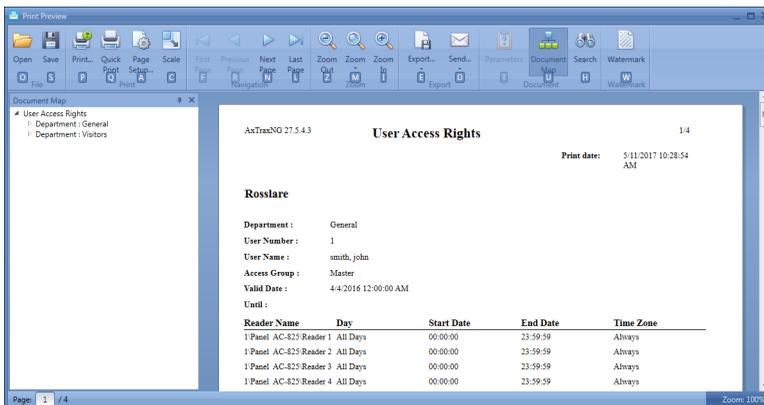


Table 17 presents the icons that are available for each type of report preview:

Table 17: Report Preview Icons

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 reports
	Save	Save the report document
	Print	Print with adjustable settings

Reports

Icon	Name	Click button to...
	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.
	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.

10. Administrator Operations

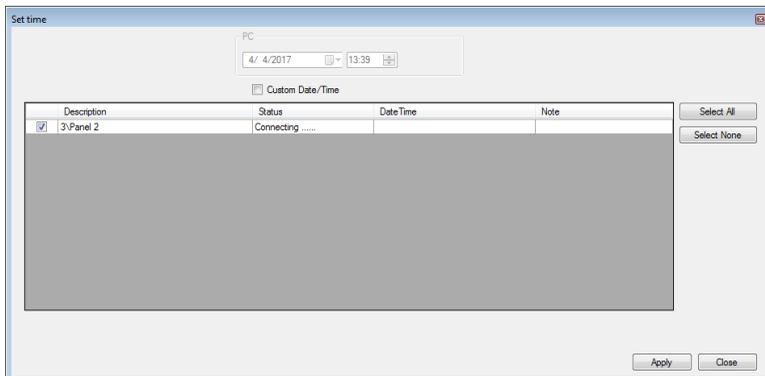
10.1 Setting the Time and Date

You can select panels by network and reset their date and time to the AxTraxNG 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.

The *Set Time* window opens.



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.

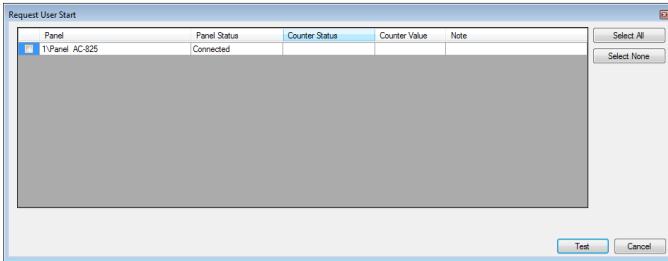
10.2 Testing User Counters

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.

The *Request User Start* window opens.



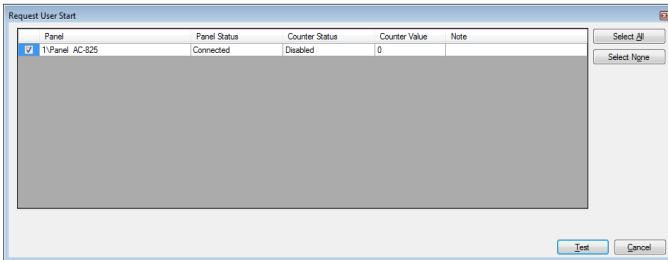
For a panel to appear in the table, that panel must have at least one reader for which the Deduct User Counter option on the General tab of the Readers Properties window (Section 5.7.1) is selected.

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.



10.3 Maintaining the Database



It is highly recommended that you back up the system database to an external storage device once a week (see Section 10.3).

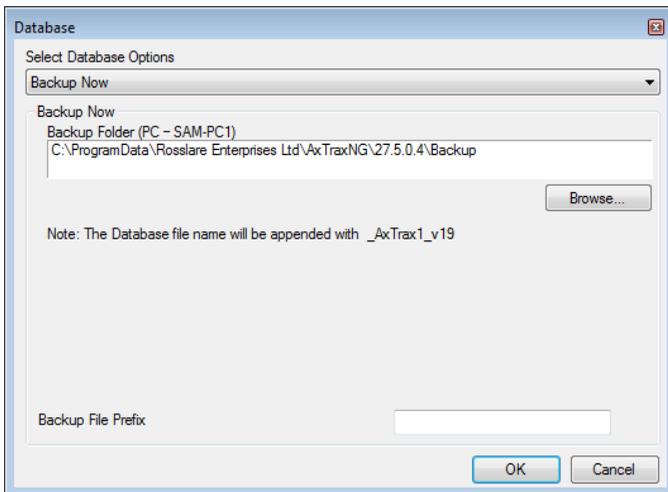
Important

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

To open the Database window:

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

The *Database* window opens.



- From the *Select Database Options* dropdown, select your desired option. The following database operations are available:

Table 18: Tools > Database > Available Databases

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.

Administrator Operations

Operation	Description
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. Note: 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 from AxTrax* (AS-525)	Replace the current database with an AxTrax database A user's photo can also be imported.
Import earlier database versions from AxTraxNG	Replace the current database A user's photo can also be imported. Note: This option does not allow importing a database from a current AxTraxNG version.
Export Access Events	Copy the Access events content of the database to the selected folder.

*This option is only available in the AxTraxNG Server PC.

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



Note

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 ProgramData folder.



Note

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.

- Click **OK**.

10.4 AxTraxNG Options and Preferences

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

To open the Options window:

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

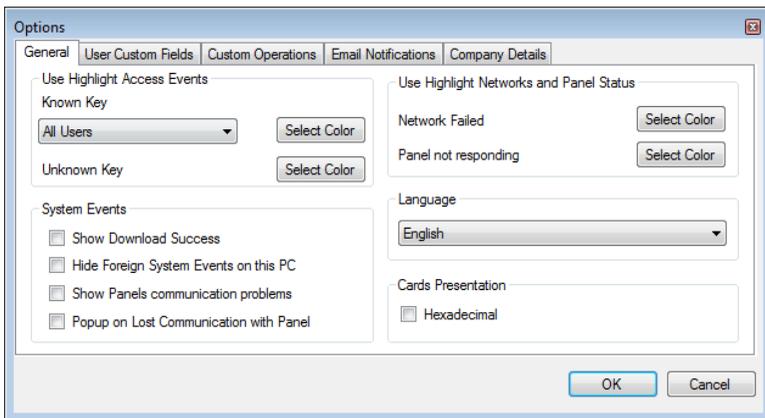
The Options window has five tabs:

Administrator Operations

- **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

10.4.1 General Tab

The *General* tab includes presentation connection settings.



The *General* tab contains the following fields:

Table 19: Tools > Options > General Tab

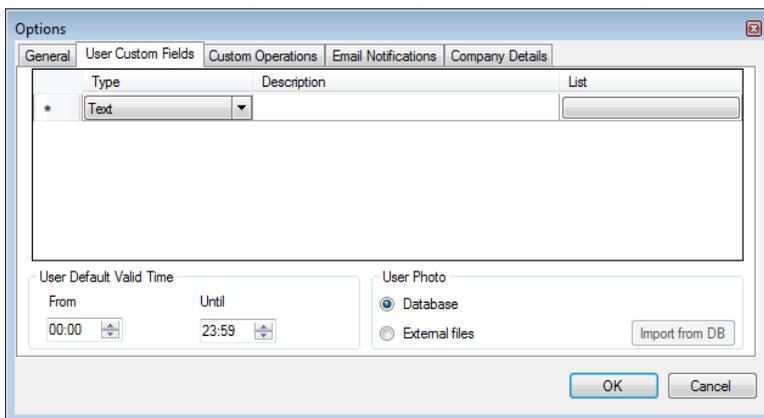
Field	Description
Use Highlight Access Events	From the <i>Known Key</i> dropdown, select the desired option and click Select Color to display selected user information in a custom picked colored highlight. Click Select Color adjacent to <i>Unknown key</i> to define the highlight color for unknown keys.
System Events>Show Download Success	Select to add a message to the event history upon successful system parameters download from the AxTraxNG software to the panel.
System Events>Hide Foreign System Events on this PC	Select to see only local administrator and AxTraxNG Server messages.
System Events>Show Panel Communication Problems	Select to have status indicate panel communication problems

Administrator Operations

Field	Description
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 checkbox, 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 <i>Network failed</i> to define the highlight color for network alarms. Click Select Color adjacent to <i>Panel not responding</i> to define the highlight color for panel communication errors.
Language	Select the system interface language. Note: 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.

10.4.2 User Custom Fields

The *User Custom Fields* tab controls the user-defined fields on the *User Fields* tab of the *User Properties* window (see Section 5.14.2.4).



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

Table 20: Tools > Options > User Custom Fields Tab

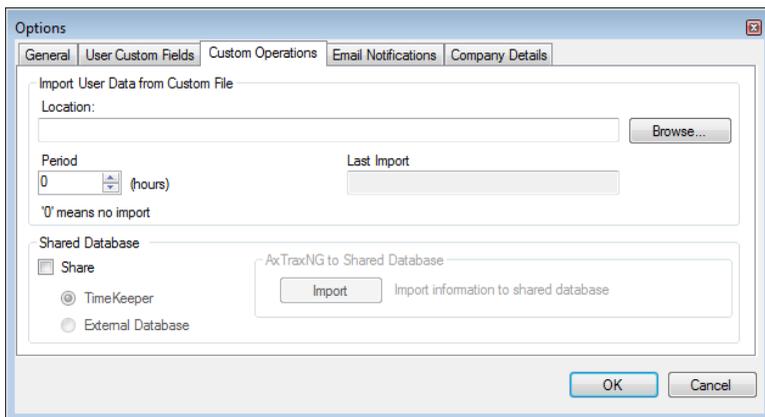
Field	Description
Type	Select the type of field. If Type is list , click Edit List and enter list items.
Description	Type a name for the new field.
User Default Valid Time	Set default start and end time for user access rights using the From and Until fields.

Administrator Operations

Field	Description
User Photo	Define the default photos to be used: <ul style="list-style-type: none"> • 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

10.4.3 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:

Table 21: Tools > Options > Custom Operation Tab

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.

Administrator Operations

Field	Description
Shared Database > Share	Select to allow sharing the AxTraxNG DB with an external program for the following data: System Configuration, Departments and Users, Cards, Access Groups and Database Version. Select the option: <ul style="list-style-type: none">• TimeKeep – Sets the DB sharing for the TimeKeeper program• External Database – Sets the DB sharing for other generic formats
Shared Database > AxTraxNG to Shared Database	Click Import to create a database from the above data from which the data can be shared by an external program.

10.4.4 Email Notifications

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

The screenshot shows the 'Options' dialog box with the 'Email Notifications' tab selected. The 'Enabled' checkbox is checked. The 'Recipients' field contains the email addresses 'yaniv.tza@f.com,kjds@ds.com'. Under the 'Events' section, the following options are checked: 'Access Granted - Any User' and 'Panel Connection Issues'. Other options include 'Access Denied - Any User', 'Alarms', 'Access Granted - Selected User', and 'Access Denied - Selected User'. A note states: '* Enable notifications for a user on a user form'. The 'OK' and 'Cancel' buttons are located at the bottom right of the dialog.

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

 **Note** In order to use email notifications, you must configure the SMTP settings (see Section 0.4).

10.4.5 Company Details

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

The screenshot shows the 'Options' dialog box with the 'Company Details' tab selected. The 'Company' field contains 'Rosslare'. The 'Address' field is empty. The 'Immediate Reports' section has a dropdown for 'Limit Last Known Position/Muster Reports For The Last' set to '24' hours. The 'OK' and 'Cancel' buttons are at the bottom right.

10.5 Importing/Exporting User Data

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

The screenshot shows the 'Import Data' dialog box. The 'Import users properties from an external file to AxTraxNG' radio button is selected. The 'Data Type' is 'Excel Workbook - *.xls'. The 'Excel File Location' field is empty with a 'Browse...' button. The 'Excel File Columns' section has checkboxes for various fields: 'A' - User# (index field), 'B' - First Name, 'C' - Last Name, 'D' - Middle Name, 'E' - Department, 'F' - Access Group, 'G' - From (Valid date), 'H' - Until (Valid date), 'I' - Mobile, 'K' - Fax, 'L' - Email, 'M' - Address, 'N' - Home Telephone, 'O' - Car Registration, 'P' - Title, 'Q' - Notes, 'R' - PIN Code, 'S' - Card Number, 'T' - Facility Code, 'U' - Identification, 'V' - Car Parking Group, 'W' - Card+Card Group, 'Y' - Site Code, and 'X' - Issue Number. The 'Card Type' is 'Wiegand 26 bits'. The 'Select All' and 'Select None' buttons are present. The 'Started from' section has 'Excel File Row' set to '2' and 'User Number started from' set to '1'. The 'Departments' section has 'Import Departments?' checked and 'General' selected. The 'Access Groups' section has 'Import Access Groups?' checked and 'Master' selected. The 'Car Parking Groups' section has 'Import Car Parking Groups?' checked and 'None' selected. The 'Card+Card Groups' section has 'Import Card+Card Groups?' checked and 'None' selected. The 'OK' and 'Cancel' buttons are at the bottom right.

Administrator Operations

The *Import/Export Data* window contains the following fields:

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 Table 22.

Table 22: Tools > Import/Export Data

Field	Description
Import Users properties from external file into AxTraxNG	Select this option to import user properties
Export Users properties from AxTraxNG 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 checkboxes of the columns to be imported or exported. Data in each column (A–T) are imported or exported as listed. Note: 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 AxTraxNG 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 <i>No</i> option is selected in the Import Departments option.
Import Access Groups?	Select Yes to import new access groups into the AxTraxNG 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 <i>No</i> option is selected in the import access group option.

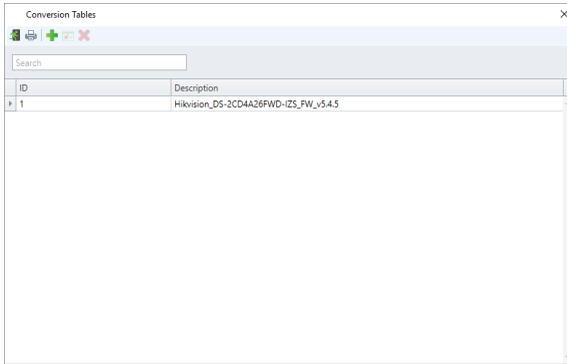
3. Click **OK**.

10.6 Conversion Table

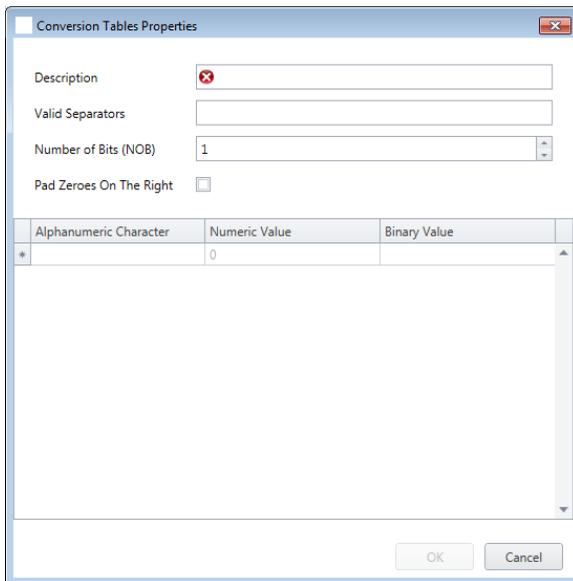
A conversion table converts the alphanumeric character on a license plate to a binary number that can then be understood by the relevant reader as a Wiegand input.

To create a conversion table:

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



2. On the toolbar, click the  icon.
The *Conversion Tables Properties* window opens.



Administrator Operations

3. Set the conversion table options according to the field descriptions in Table 22.

Table 23: Tools > Conversion Tables

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

A. Firewall Configuration

A.1 For Windows 7

The following instructions explain how to configure the standard Windows Firewall for Windows 7.

To configure the firewall:

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



3. Click **Allow a program through Windows Firewall**.

Allow a program or feature through Windows Firewall

The *Allowed Programs* window opens.

Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Change settings

For your security, some settings are managed by your system administrator.

Allowed programs and features:

Name	Domain	Home/Work (Pri...	Public	Group Policy
<input type="checkbox"/> BranchCache - Hosted Cache Server (U...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No
<input type="checkbox"/> BranchCache - Peer Discovery (Uses W...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No
<input type="checkbox"/> Connect to a Network Projector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No
<input checked="" type="checkbox"/> Core Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No
<input type="checkbox"/> Distributed Transaction Coordinator	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No
<input checked="" type="checkbox"/> Dropbox	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No
<input checked="" type="checkbox"/> File and Printer Sharing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No
<input checked="" type="checkbox"/> Google Chrome	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No
<input type="checkbox"/> HomeGroup	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No
<input type="checkbox"/> iSCSI Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No
<input type="checkbox"/> Media Center Extenders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No
<input checked="" type="checkbox"/> Microsoft Office Outlook	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No

Details...

Remove

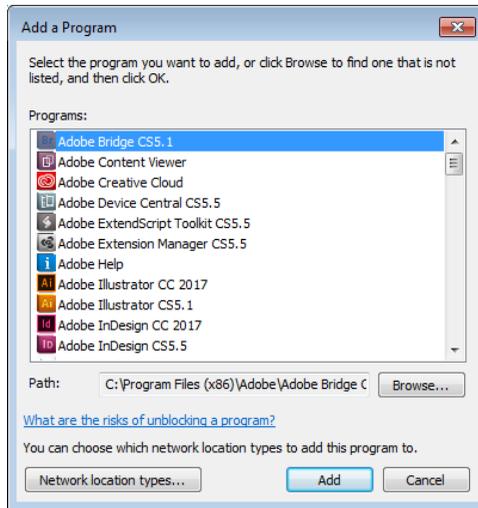
Allow another program...

OK

Cancel

4. Click **Allow another program**.

The *Add a Program* dialog appears.



5. Click **Browse**.
The *Browse* window appears.
6. In the **File Name** box, type:
"C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\BINN\sqlservr.exe" and click **Open**.
7. Click **OK**.
The SQL Server program appears in the *Add a Program* dialog.
8. Repeat Steps 6 and 7.
9. In the **File Name** box, type:
"C:\Program Files\Microsoft SQL Server\90\Shared\sqlbrowser.exe" and click **Open**.
10. Click **OK**.
The SQL Browser program appears in the *Add a Program* dialog.
11. In the Control Panel, click **Administrative Tools**.

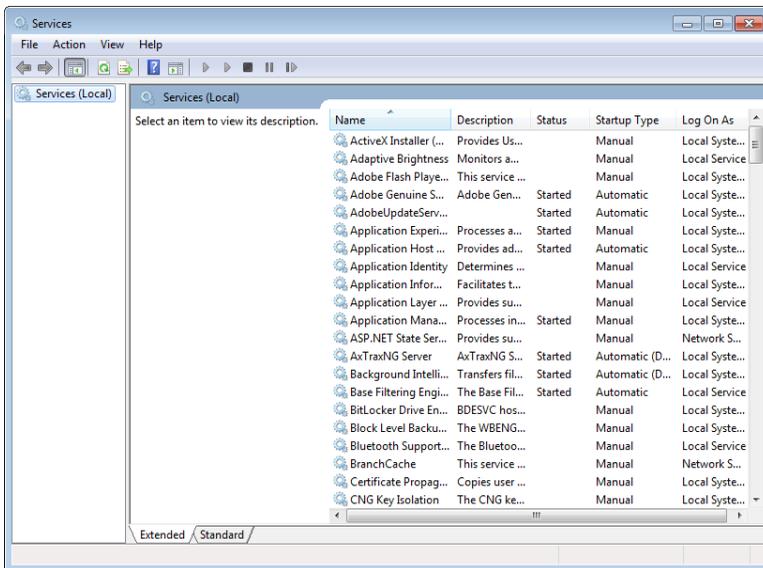


The *Administrative Tools* window opens.

Firewall Configuration

Name	Date modified	Type	Size
Component Services	7/14/2009 6:57 AM	Shortcut	2 KB
Computer Management	7/14/2009 6:54 AM	Shortcut	2 KB
Data Sources (ODBC)	7/14/2009 6:53 AM	Shortcut	2 KB
Event Viewer	7/14/2009 6:54 AM	Shortcut	2 KB
Internet Information Services (IIS) Manager	12/26/2013 1:09 PM	Shortcut	2 KB
iSCSI Initiator	7/14/2009 6:54 AM	Shortcut	2 KB
Local Security Policy	9/15/2013 4:07 PM	Shortcut	2 KB
Performance Monitor	7/14/2009 6:53 AM	Shortcut	2 KB
Print Management	9/15/2013 4:07 PM	Shortcut	2 KB
Services	7/14/2009 6:54 AM	Shortcut	2 KB
System Configuration	7/14/2009 6:53 AM	Shortcut	2 KB
Task Scheduler	7/14/2009 6:54 AM	Shortcut	2 KB
Windows Firewall with Advanced Security	7/14/2009 6:54 AM	Shortcut	2 KB
Windows Memory Diagnostic	7/14/2009 6:53 AM	Shortcut	2 KB
Windows PowerShell Modules	7/14/2009 7:32 AM	Shortcut	3 KB

12. Double-click **Services**.
The **Services** console opens.



13. Scroll down and right-click **Windows Firewall** and click **Restart** from the pop-up menu.
14. Right-click **SQL Server (AXTRAXNG)** and click **Restart** from the pop-up menu.
15. Right-click **SQL Server Browser** and click **Restart** from the pop-up menu.
The Firewall is now configured for AxTraxNG.

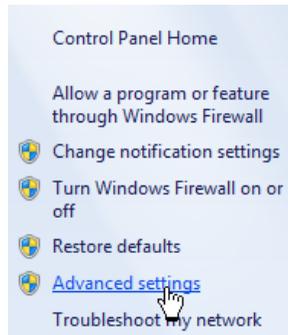
B. Opening a Program in Windows' Firewall

To open a port in Windows' firewall:

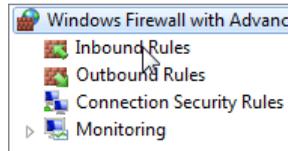
1. Open the Control Panel.
2. Click the **Windows Firewall** category.



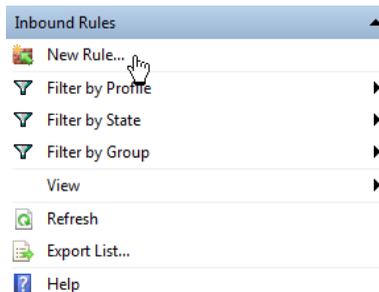
3. Click **Advanced settings** in the left column of the Windows Firewall window.



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

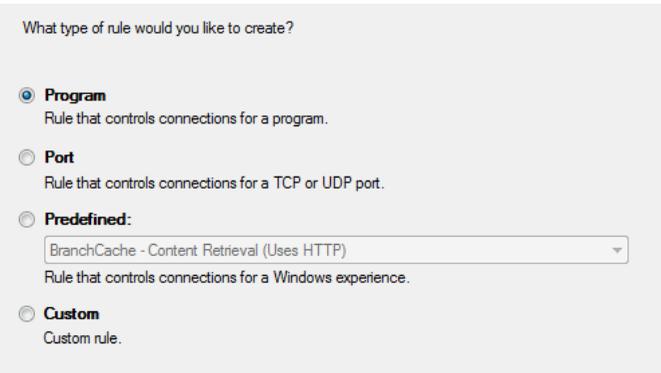


5. In the right column, click **New Rule**.



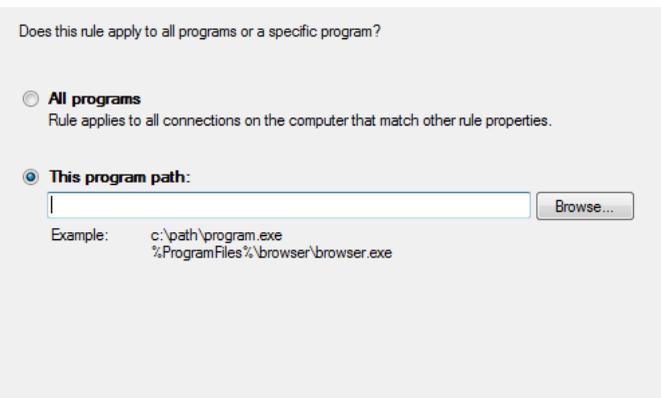
The following screen opens:

Opening a Program in Windows' Firewall



6. With **Program** selected by default, click **Next**.

The following screen opens:



7. With **This program path** selected by default, click **Browse** and locate the *AxtraxServerService.exe* file, which is located in **C:\Program Files (x86)\Rosslare\AxTraxNG Server**.

8. Click **Next**.

The following screen opens:

Opening a Program in Windows' Firewall

What action should be taken when a connection matches the specified conditions?

- Allow the connection**
This includes connections that are protected with IPsec as well as those are not.
- Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
- Block the connection**

9. With **Allow the connection** selected by default, click **Next**.
The following screen opens:

When does this rule apply?

- Domain**
Applies when a computer is connected to its corporate domain.
- Private**
Applies when a computer is connected to a private network location.
- Public**
Applies when a computer is connected to a public network location.

10. With all three checkboxes selected by default, click **Next**.
The following screen opens:

Name:

Description (optional):

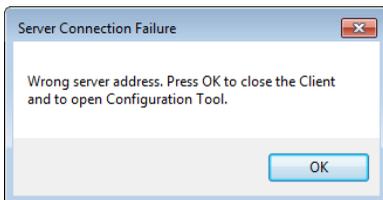
11. Enter a name of the rule, such as "NG Server" and click **Finish**.

C. WAN Connection Troubleshooting

This appendix presents three scenarios of a server connection problem.

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

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



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

C.2 Server is Down or Network Failure between AxTraxNG Client and AxTraxNG Server

The Events log shows a communication error:

Date/Time	Location	Operator	Event
04/09/2014 09:31:16	Server Information		Communication Established
04/09/2014 09:31:16	Server Event		Communication Established
04/09/2014 09:31:16	Request From Server		Recovering Communication
04/09/2014 09:31:16	Event From Server		Recovering Communication
04/09/2014 09:30:46	Request From Server		Recovering Communication
04/09/2014 09:30:46	Event From Server		Recovering Communication
04/09/2014 09:30:18	Server Information		Communication Establishment Failed
04/09/2014 09:30:18	Server Event		Communication Establishment Failed
04/09/2014 09:30:16	Request From Server		Recovering Communication

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

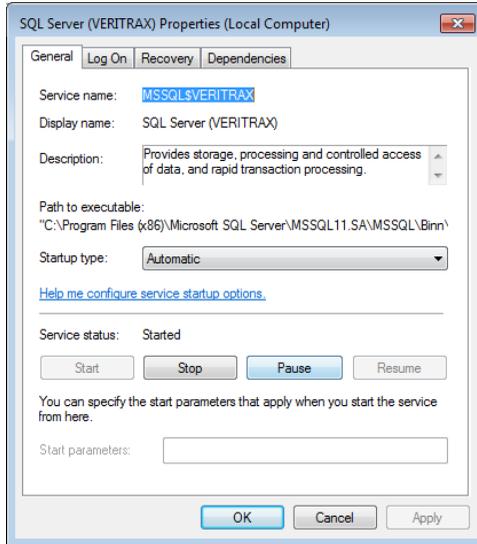
C.3 IP + Port Setting are Fine but Client Does Not Start

Check the following possible firewall problems:

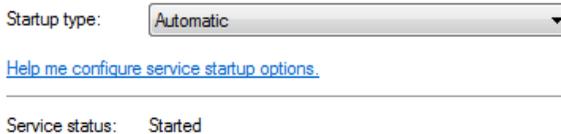
- Check firewall for server PC
- Check firewall for client PC
- Check firewall to Server network
- Check firewall to Client network

D. SQL Service Settings

1. To reach the SQL Service Settings, click the following path from the Control Panel in Windows XP:
Control Panel > Administrative Tools > Services and Applications > Services > SQL Server (VERITRAX)
2. Double click "**SQL Service (VERITRAX)**" the following dialog opens:

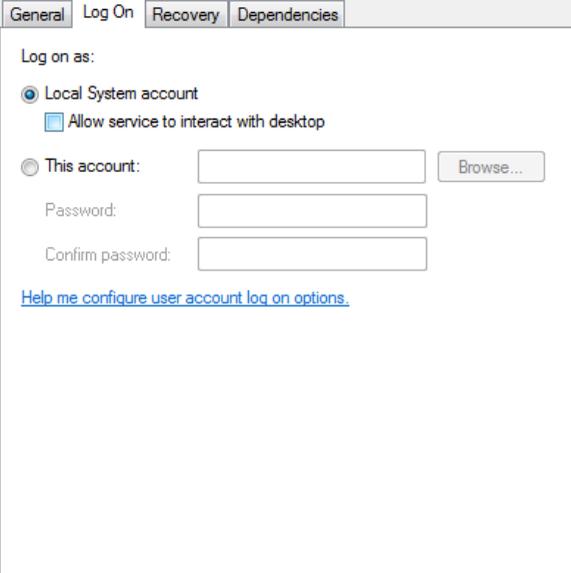


3. On the *General* tab, verify that the Startup type is "Automatic" and that the Service status is "Started".



SQL Service Settings

4. On the *Log On* tab, verify that the *Local System Account* option is selected. Restart the computer for the changes to take effect.



The screenshot shows the 'Log On' tab of the SQL Service Settings dialog box. The 'Log on as:' section has two radio buttons: 'Local System account' (selected) and 'This account:'. The 'Local System account' option has a checked checkbox for 'Allow service to interact with desktop'. The 'This account:' option has an empty text box and a 'Browse...' button. Below these are fields for 'Password:' and 'Confirm password:'. A blue hyperlink at the bottom reads '[Help me configure user account log on options.](#)'

5. If you've made any changes, restart the computer for the changes to take effect.

E. Configuring a Network

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

E.1 TCP/IP Connection

To connect access control panels to AxTraxNG 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).



Note

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.
The *Networks* window opens.
3. Set the Network type as **TCP/IP**.



Note

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.

Configuring a Network

4. Click **Configuration**.

The *TCP/IP Configuration* window opens.

MAC Address	Status	Configuration	Version
00:50:C2:B1:8F:A2	Available	Configured	5.2
00:50:C2:78:A7:AB	Available	Configured	5.2
00:08:DC:54:81:A5	Available	Configured	1.1.2dev

Search Options

All Networks

Direct MAC Address

Direct IP Address

Search

Configuration

Gateway Type: MD-IP32 Onboard

Serial Speed: 9600

IP Address: 192 . 168 . 10 . 47

Port: 1001

Subnet Address: 255 . 255 . 255 . 0

Gateway Address: 192 . 168 . 10 . 1

Enabled DHCP Mode

Apply

OK Cancel

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.

- From the MD-N32 list (the MD-N32's MAC address should be labeled on the TCP/IP converter), select the appropriate MAC address.
- 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 AxTraxNG 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.

- Enter the IP address and subnet address for the computer's network.
- 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.
- Enter the default gateway address of the computer's network.
- Click **OK** to start the verification process.
- 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.
- 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.

F. Configuring a Biometric Terminal

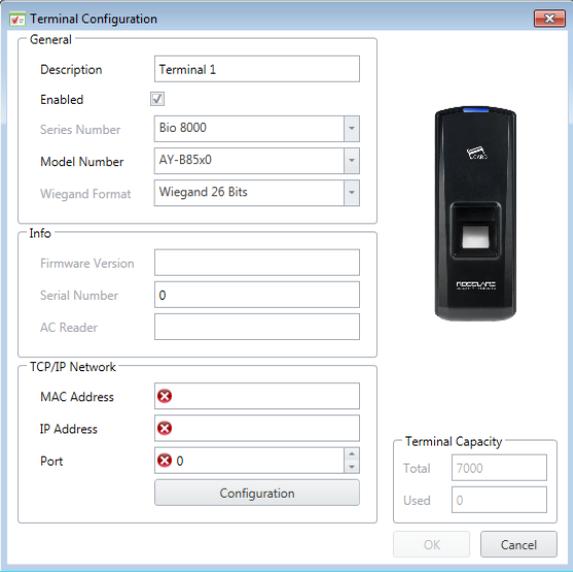
The AxTraxNG server communicates with a biometric terminal in two ways: TCP/IP (either LAN or WAN) and Wiegand protocols.

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

The AxTraxNG server supports multiple terminals per access control network.

To configure a TCP/IP connection to a biometric terminal:

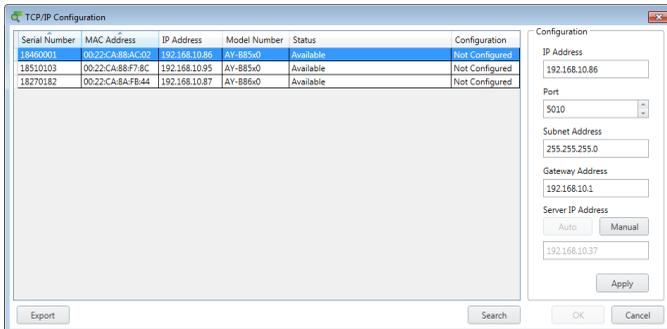
1. In the Tree View, expand the **Biometrics** element and select **Terminals**.
2. On the toolbar, click the  icon.
3. The *Terminal Configuration* window opens.



4. Click **Configuration**.

Configuring a Biometric Terminal

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.

5. Select the appropriate terminal.

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

6. For a terminal that has not yet been configured:
 - a. Click **Apply**.
 - b. Wait for the list to refresh and see that the terminal's status is now "Configured".
 - c. Select the terminal from the list again.
7. Click **OK**.

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

G. Restoring Factory Default Settings



Restoring factory default settings resets all doors and reader configurations to their factory defaults and clears all user properties.

Caution

To restore the factory default settings:

1. Turn off the supply power.
2. Disconnect all doors and readers wiring.
3. Connect Data 0, Data 1, and Tamper inputs to GND (-) in both reader 1 and 2 (total of six wires)
4. Power up the supply power for a few seconds. Wait for the "LED3" and "LED4" LEDs to flash alternately.
5. Turn off the supply power.
6. Connect the doors and readers wiring again.
7. In AxTraxNG, delete the panel by clearing **Enable panel** in the panel screen and click **OK**.
8. Select **Enable panel** in the panel screen and click **OK**. This action causes a full reset of the access control panel with the factory settings.

H. 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 (Figure 3 in Section 5.14.2).

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 as described in Section 5.14.2, or select an existing user in the **Departments/Users** element.
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* (Section 5.7.1).
7. In the Details section, select **Deduct User counter**.

Deduct User Counter

8. Click **OK**.

H.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.



Note

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.
The *Panel Properties* window opens.
4. Select the *Options* tab.
5. Select **Set new counter**.

User Counter on re-enable the panel

Set new counter

6. Click **OK**.

I. Enrolling a User's Fingerprint



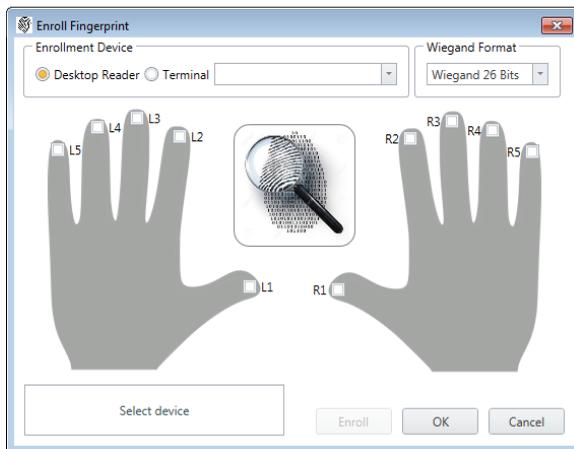
If using DR-B9000 desktop Fingerprint scanner you have to install a dedicated driver to your Windows PC.

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 (Section 5.14.2.2), click **Add from a Fingerprint Reader**.

The *Enroll Fingerprint* window opens.



6. Select the enrollment source (Enrollment Device).



If using Desktop Fingerprint scanner you will have 2 step enrolment process
In addition to a live Fingerprint image

7. Select the finger that you want to enroll.
8. Click **Enroll**.

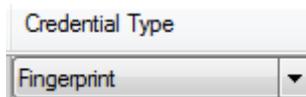
Enrolling a User's Fingerprint

- Place the relevant finger on the scanner area of the reader or terminal and wait until the finger is identified.

You should see that the finger was read successfully.



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



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

J. Enrolling Credentials using a UHF Reader

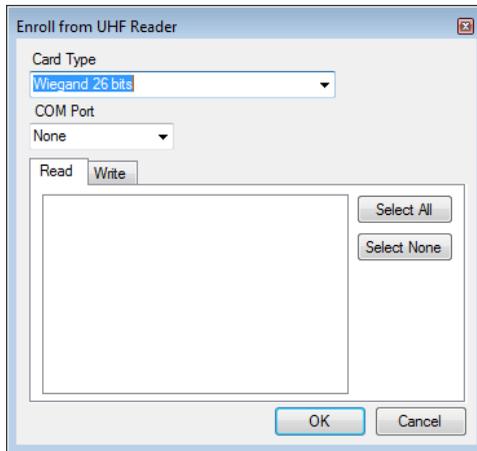
This option is available for users connected to a UHF reader.

To enroll credentials using a UHF reader:

1. Be sure the UHF reader 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 5.14.2.2), click **Enroll from UHF Reader**.

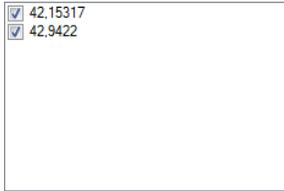
Alternatively, you can expand the **Users** element in the Tree View, select the **Cards** element, and click the **Enroll from UHF Reader** icon () on the toolbar.

The *Enroll from UHF Reader* window opens.

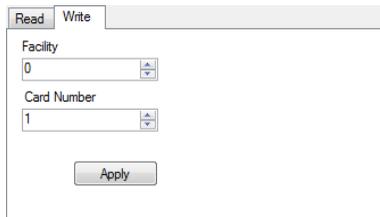


6. Select the card type and COM port from the respective dropdown lists.
7. Enroll a card by presenting it to the reader. Each card enrolled appears in the screen.

Enrolling Credentials using a UHF Reader



8. Select the cards to add (added cards are selected by default).
9. Click the *Write* tab if you wish to assign a Facility code and card number to the enrolled card.



10. Select the Facility code (0 to 255) and card number (1 to 65535) from the respective boxes and click **Apply**.
11. Click **OK**.

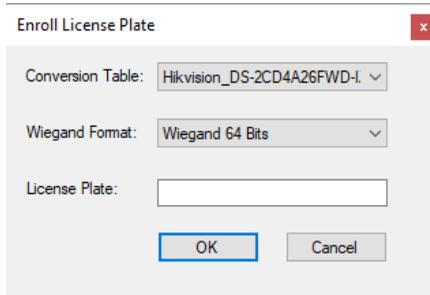
K. Enrolling a License Plate

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 AxTraxNG 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 (Section 5.14.2.2), click **Enroll License Plate**.

The *Enroll License Plate* window opens.



5. Select the conversion table (see Section 10.6).
6. Enter the license plate number.
7. Click **OK**.

L. Enrolling a Face from a Terminal

This option is available for users connected to a desktop reader.

To enroll credentials using a desktop reader:

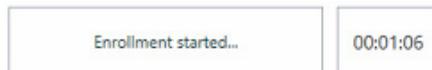
1. Be sure the biometric terminal is connected.
2. In the Tree View, expand the **Users** element.
3. Expand the **Departments/Users** element and select the relevant department.
4. Select the user and click the  icon.
5. On the *Credentials* tab in the *Users Properties* window (Section 5.14.2.2), click **Enroll Face from Terminal**.

The *Face Enrollment* window opens.



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.

M. Enrolling Credentials using a Desktop Reader

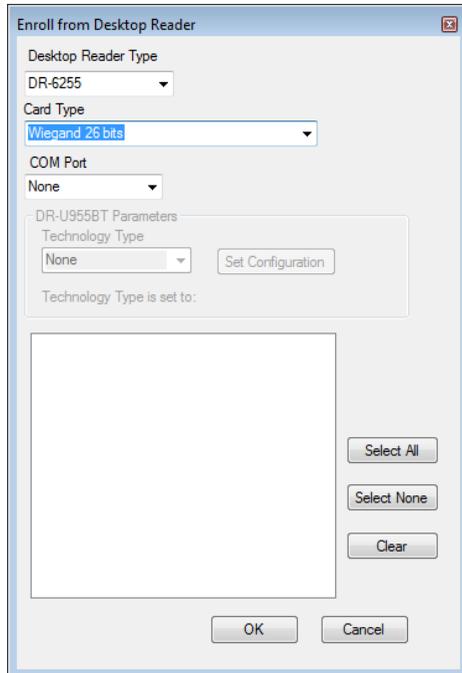
This option is available for users connected to a desktop reader.

To enroll credentials using a desktop reader:

1. Be sure the desktop reader is connected.
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 (Section 5.14.2.2), click **Enroll from Desktop Reader**.

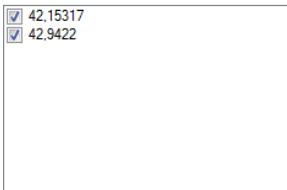
Alternatively, you can expand the **Users** element in the Tree View, select the **Cards** element, and click the **Enroll from Desktop Reader** icon () on the toolbar.

The *Enroll from Desktop Reader* window opens.



Enrolling Credentials using a Desktop Reader

5. Select the desktop reader type, card type, and COM port from the respective dropdown lists.
6. If the DR-U955BT is selected in *Desktop Reader Type*, then you must also select the technology type from the dropdown and click **Set Configuration**.
7. Enroll a card by presenting it to the reader. Each card enrolled appears in the screen.



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

N. SQL Server Installation Troubleshoot

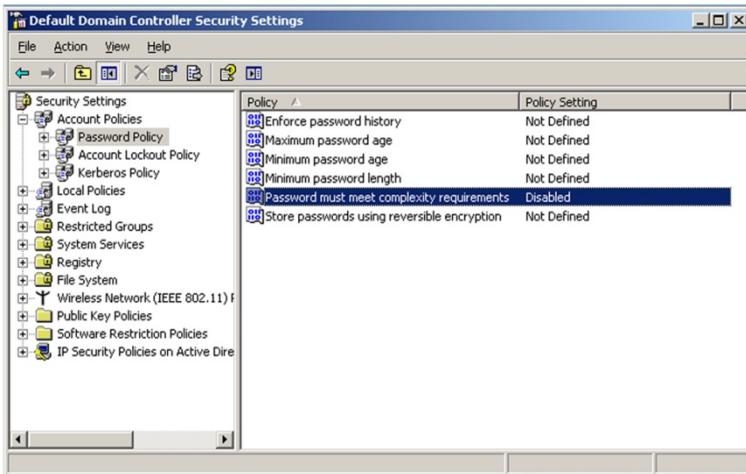
When installing the MS SQL Server Express component in a Windows Server (2003 or 2008) environment, you might get the following error message: *"The sa password must meet SQL Server password policy requirements."*

This is because either:

- The domain-enforced policy is preventing the installer from setting the SA user's password, or
- The local security policy is preventing the installer from setting the password

You can temporarily disable this policy while the installation is running and click **Retry** to let the installation complete successfully. After installation is finished, you can restore the policy to the desired setting.

If you are on a Domain Controller, check the Domain Controller security settings first:



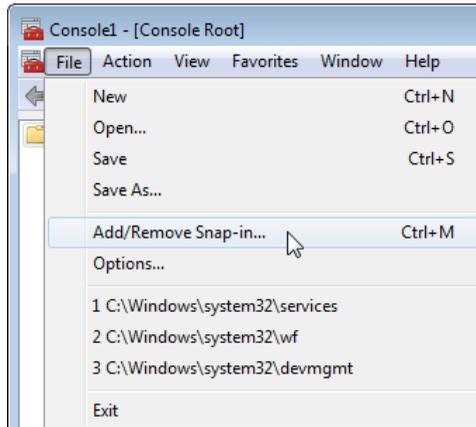
 If the setting is set on a domain controller, you may need to run `gpupdate` to force the changes to propagate.

SQL Server Installation Troubleshoot

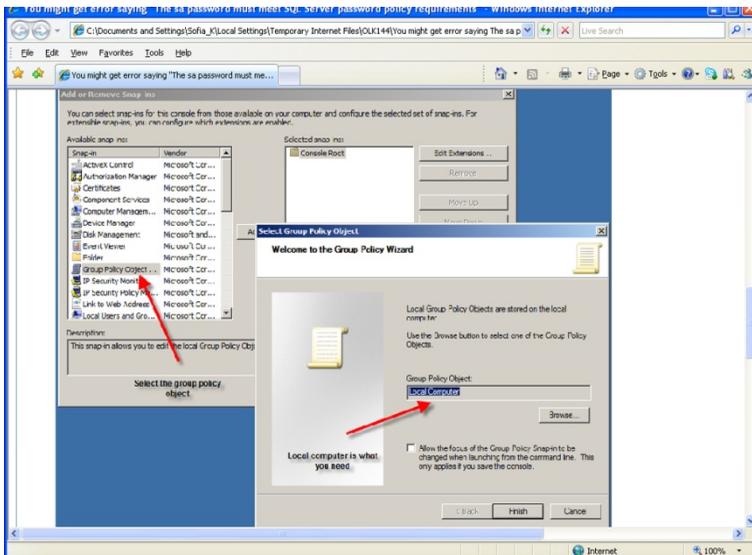
If the server is not part of a domain, check the local security policy.

To check the local security policy

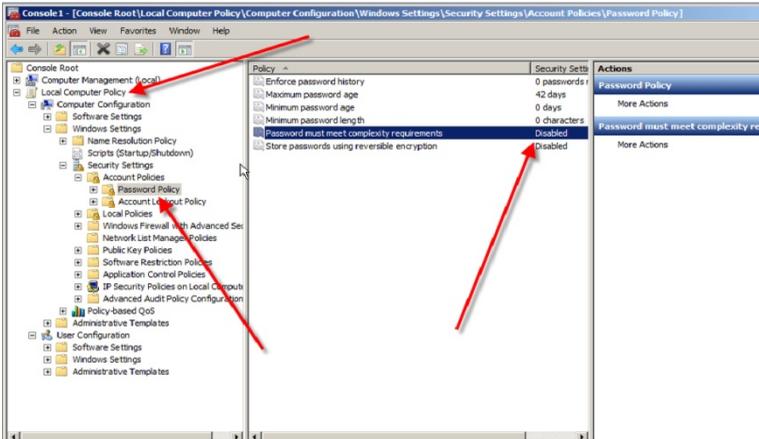
1. Open the MMC console: **Start -> Run -> mmc.exe**
2. Click **File -> Add/Remove Snap-in:**



3. Add the Group policy object for the Local Computer:

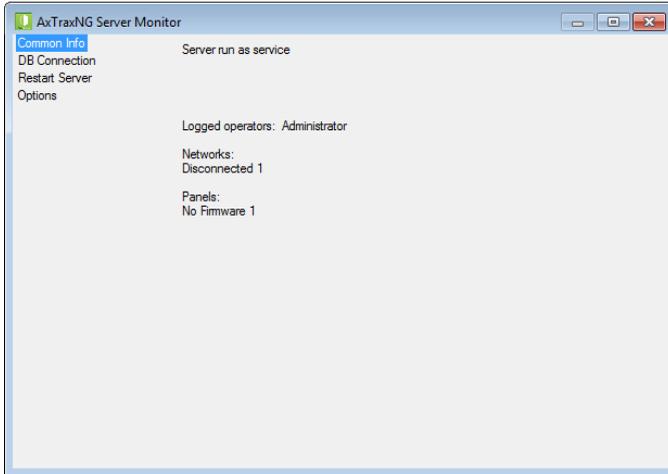


4. Disable (temporarily) the security policy:



0. AxTraxNG Server Monitor

The AxTraxNG Server Monitor is a program that monitors the AxTrax server. Double-click the  icon in the Window system tray to open the program.



The main window contains the following four topics:

Table 24: Server Monitor Topics

Parameter	Description
Common Info	Shows general system information
DB Connection	Changes the DB connection string Note: Administrator password is required
Restart Server	Restarts the AxTraxNG server Note: Administrator password is required
Options	<ul style="list-style-type: none">• SMTP configuration• Reports directory• Use static IP option

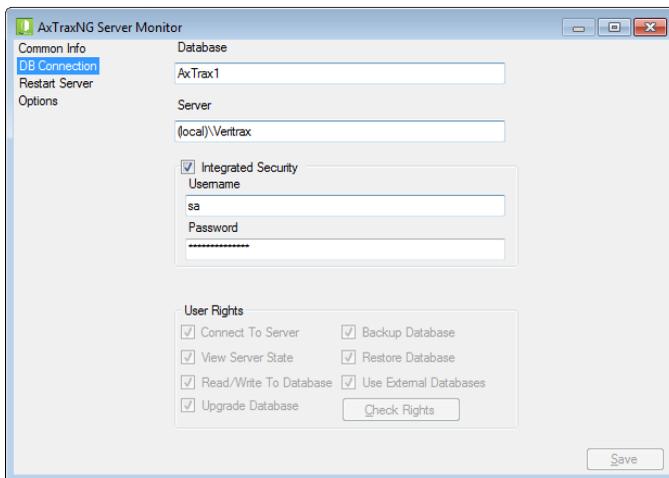
Once the main window opens, you can click on any of the main topics to open that topic's screen.

0.1 Common Info

This screen shows general system information: server status, downloads counter, number of networks, number of panels, and networks and panels status.

0.2 DB Connection

This feature allows you to change the database connection strings.



The *DB connection* screen contains following fields:

Table 25: Server Monitor > DB Connection Screen

Parameter	Description
Database	Database name
Server	DB Server path
Integrated Security checkbox	Select to send username and password of database
Username	Database username
Password	Database Password
User Rights	These fields monitor the user rights in the current database.



You must enter the administrator password to view this screen.

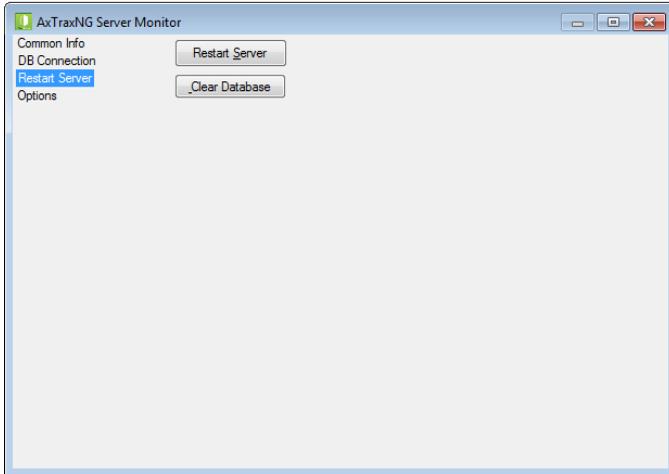
0.3 Restart Server

If you try to open the AxTraxNG Client but you get an error that the server is not connected, you may need to restart the server.

To restart the server:

1. Click the *Restart Server* topic.

The *Restart Server* screen is displayed.



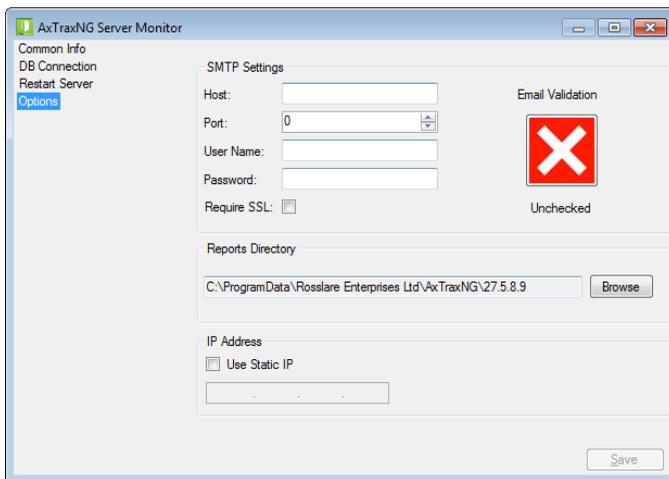
2. Click **Restart server**.
3. Enter the administrator password and click **OK**.

The server restarts within a few seconds.

In addition, click **Clear Database** to return the database to its factory default values.

0.4 Options

This screen allows you to set the SMTP configuration, view the reports directory, and set the static IP option.



The *Options* screen contains following fields:

Table 26: Server Monitor > Options Screen

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 Section 9.3).

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.

Note: **If Server Monitor does not have permission to write in the server's directory, the option will fail. Use the Readme.txt file to learn about Windows permissions.**

P. Adding Custom Wiegand Formats

The Wiegand protocol is the most common protocol between readers and controllers. This protocol is actually a collection of bits that represents the number of the user card ID.

There are many types of Wiegand protocols. Protocols differ from one another depending on the following three factors:

- The number of bits sent per card
The most common format is 26-bit, but there are many more types such as 30-, 32-, 35-, and 36-bit.
- The representation of the user number
In each card, there is a number that defines the user, but the representation of this number inside the Wiegand protocol can be changed. In addition, there is a Facility code in most protocols, which is not part of the number but is common to all users in this particular area. There are cards with additional codes such as Site code, but AxTraxNG recognizes them as a Facility code only. This means that if a card has both a Site code and a Facility code, AxTraxNG recognizes the first Facility code and the second Facility code is ignored.
- The authentication mechanism and its type inside the bit stream
In most protocols, there is a certain type of authentication of the data transferred from the reader to the controller.

Once the user knows the format of the card, meaning how many bits there are per card, the user can use the other two factors to create new rules, which can then be enrolled into the software to teach the controller to understand the new format.

P.1 Representation

The following options are available when discussing the number representation:

- Card number is represented in a binary or hexadecimal code
All the bits in the protocol are represented with 'D', which stands for data.
- Card number is represented in the protocol as a "reverse bytes". For example, if the number (hexadecimal) is 34 65 89 32, then it is represented as: 32 89 65 34.
All the bits in the protocol are represented with 'R'.

- Card number is represented in the protocol as a “reverse bits”. For example, if the number (hexadecimal) is 34 65 89 32, which is represented in binary code as:
00110100 01100101 10001001 00110010
then in reversed bits format, it is 4C 91 A6 2C, which is represented as:
01001100 10010001 10100110 00101100 in binary.
All the bits in the protocol are represented with ‘Z’.
- Card number is represented in the protocol as a BCD code (each nibble represents one decimal character). For example, if the number (decimal) is 658723, then it is represented in binary as: 01100101 10000111 00100011.
All the bits in the protocol are represented with ‘B’.

P.2 Facility Code

If supported in the card, the software must know where it is placed inside the bit array and how many bits it takes.

Of the 5 representation options presented in P.1, only the data format can be used with the Facility code; however, all the bits in the protocol are represented with ‘F’ to differentiate it from regular data.

P.3 Authentication

Usually the array of bits that represents the card number also contains an authentication mechanism that checks that the data was transferred correctly.

AxTraxNG supports several types of authentication mechanisms as follows:

- Even Parity – One bit provides authentication to either several bits proceeding or following it (according to the defined protocol). This bit makes the total number of related bits an even number.
The Even Parity bits in the protocol are represented with ‘E’ and all the bits that they verify are represented with ‘1’.
- Odd Parity – One bit provides authentication to either several bits proceeding or following it (according to the defined protocol). This bit makes the total number of related bits an odd number.
The Even Parity bits in the protocol are represented with ‘O’ and all the bits that they verify are represented with ‘1’.
- CheckSum – The number of bits (usually 8) provides the sum of the previous bytes.
Checksum bits in the protocol are represented with ‘S’ and all the bits that they verify are represented with ‘1’.

Adding Custom Wiegand Formats

- CheckXor – The number of bits (usually 8) provides a logical XOR value of the sum of the previous bytes.
CheckXor bits in the protocol are represented with 'X' and all the bits that they verify are represented with '1'.

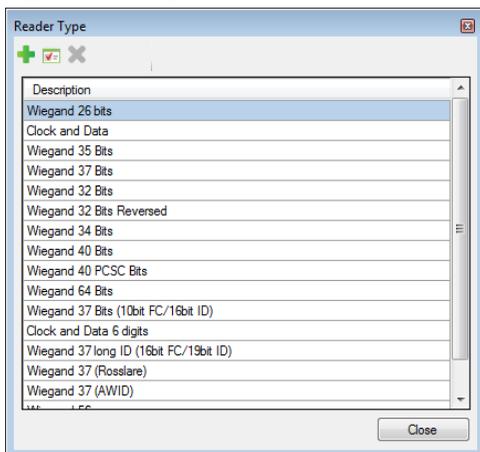
P.4 Creating New Rules

Using the above principles, we can create new rules for AxTraxNG.

To create a new rule:

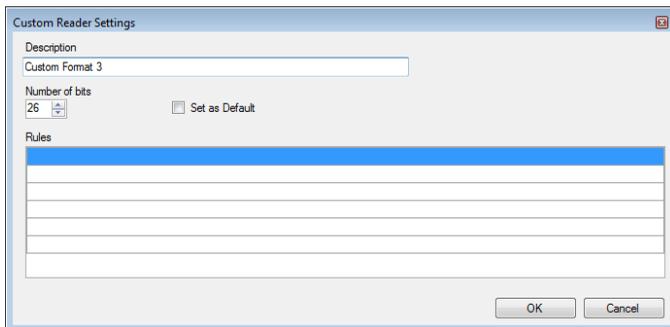
1. In the Tree View, click **AC Networks**.
2. Click  icon.

The *Reader Type* window opens.



3. Click the  icon.

The *Custom Reader Settings* window opens.



4. Enter a description of the new rule.
5. Select the number of bits the new rule will use.

Adding Custom Wiegand Formats

- [Optional] Select **Set as Default**.
- In the Rules section, enter the protocol rules according to the guidelines described in Sections P.1 through P.3 and as shown in the example below.



The protocol definition is for the entire system and not per controller.

Example

Enter a new Wiegand 29-bit protocol with the following rules:

- Rule 1: Bit 1 – Odd parity on the bits 3–15
- Rule 2: Bit 2 – Even parity on the bits 16–28
- Rule 3: Bit 29 – Odd parity on the bits 1–28
- Rule 4: Bits 11–28 – ID data
- Rule 5: Bit 3–10 – Facility code

The new protocol appears in the *Custom Reader Settings* window.

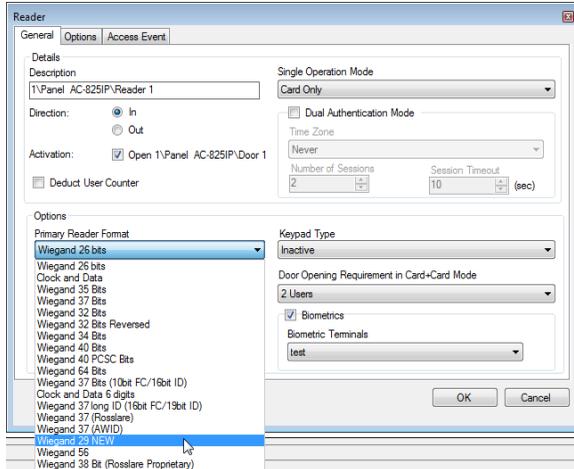
Rule	Bit Pattern
Bit 1 – Odd Parity on Bits 3 to 15 (the other bits are 0)	001111111111111100000000000000
Bit 2 – Even Parity on Bits 16 to 28 (the other bits are 0)	0E00000000000001111111111110
Bit 29 – Odd Parity on Bits 1 to 28 (the other bits are 0)	111111111111111111111111111110
Facility – Bits 3 to 10 (the other bits are 0)	0000000000DDDDDDDDDDDDDDDDDD
ID – Bits 11 to 28 (the other bits are 0)	00FFFFFFF0000000000000000000



Please note that the first character in the first row and the last character in the third row, which represents the odd parity, is a capital "O" and not a zero (0).

Adding Custom Wiegand Formats

The new protocol now appears in the list of available protocols.

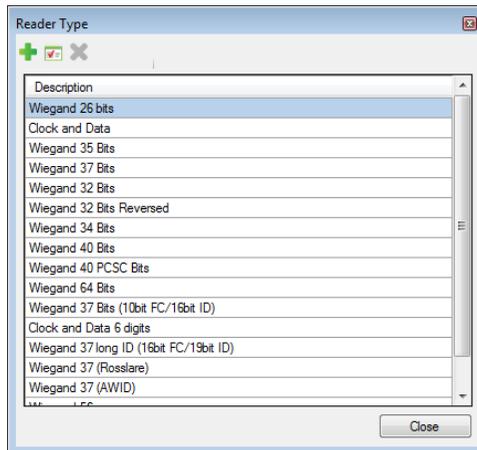


The representation of each existing protocol can be viewed.

To view the format of existing protocols:

1. In the Tree View, click **AC Networks**.
2. Click the  icon.

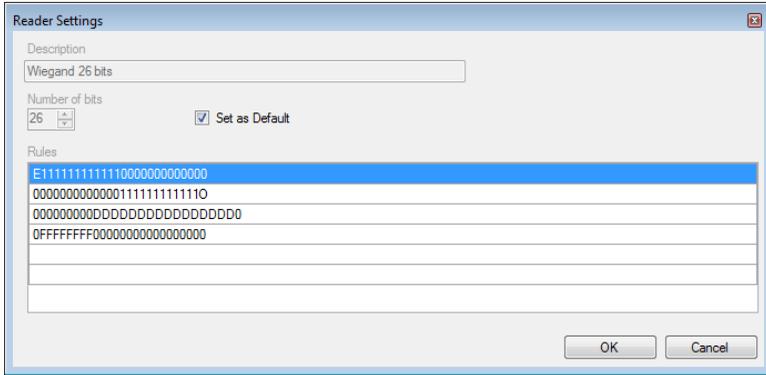
The *Reader Type* window opens.



3. Double-click the protocol you wish you view (in this case, Wiegand 26-Bit). Alternatively, you can select the protocol you wish to view and click the  icon.

Adding Custom Wiegand Formats

The *Reader Settings* window opens.



The protocol representation is for viewing only and cannot be edited.

Note

For help in creating a new protocol, please refer to Customer Support.

Q. Software License and Maintenance Agreements

The full ROSSLARE Software License Agreement (SLA) and Maintenance Agreement are available in the Quick Links section on the ROSSLARE website at www.rosslaresecurity.com.

Rosslare considers any use of this product as agreement to the REL Software License Agreement (SLA) and Maintenance Agreement terms even if you do not review them.



AxTraxNG

**Asia Pacific, Middle East,
Africa**

Rosslare Enterprises Ltd.
Kowloon Bay, Hong Kong
Tel: +852 2795-5630
Fax: +852 2795-1508
support.apac@rosslaresecurity.com

United States and Canada

Rosslare Security Products, Inc.
Southlake, TX, USA
Toll Free: +1-866-632-1101
Local: +1-817-305-0006
Fax: +1-817-305-0069
support.na@rosslaresecurity.com

Europe

Rosslare Israel Ltd.
22 Ha'Melacha St., P.O.B. 11407
Rosh HaAyin, Israel
Tel: +972 3 938-6838
Fax: +972 3 938-6830
support.eu@rosslaresecurity.com

Latin America

Rosslare Latin America
Buenos Aires, Argentina
support.la@rosslaresecurity.com

China

Rosslare Electronics (Shenzhen) Ltd.
Shenzhen, China
Tel: +86 755 8610 6842
Fax: +86 755 8610 6101
support.cn@rosslaresecurity.com

India

Rosslare Electronics India Pvt Ltd.
Tel/Fax: +91 20 40147830
Mobile: +91 9975768824
sales.in@rosslaresecurity.com

ROSSLARE
SECURITY PRODUCTS



• EN ISO 13485

