AxTraxNG™

Access Control Management Software

Software Manual (Version 27.x)

ROSSLARE
SECURITY PRODUCTS

Table of Contents

List of Figures

List of Tables

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.
- ROSSLARE exclusive warranty and liability is limited to the warranty and liability statement provided in an appendix at the end of this document.
- 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

The AxTraxNG™ Access Control System is a complete Server-Client software management system for use with the AC-215, AC-225, AC-425, AC-525, 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 Surveillance software 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 00.23.02 and above.

1.1 System Features

AxTraxNG makes it possible to control and monitor every aspect of access control on a site. The system includes a built-in software security system that controls access to the system database, and logs all performed operations. In addition, the system boasts the following Professional Grade features:

- User-friendly PC software with intuitive layout reduces the complexity of access control
- Manages user data, photo and information fields, access rights, alarms, strike time, and door mode, all from one central location
- Produces reports from acquired data, such as entry and exit times, as well as alarm types initiated by user, location, and time events
- Available in multiple languages and date formats
- Compatible with additional video management software modules from Rosslare (ViTrax)
- Backward compatibility with VeriTrax AS-225 and AxTrax AS-525

1.1.1 Access Control

Access groups define access rights for every part of the site. Access rights are time dependent; for example, users in the "Mornings Only" access group can have access to certain areas of the site between 9 AM and 12 PM only. Assign each individual user to an access group.

The system also stores an identification photograph and personal details for each user, as well as user specific access settings, such as antipassback immunity, requirements for an extended open door period, configurable special privileges, and triggered outputs.

1.1.2 Access Monitoring

The AxTraxNG software records every attempt to open a door within the site. Status maps show the state of every part of a facility, while an Events log records complete details of every time access is granted or denied for every door on a site, and records possible door tampering and forced entries.

AxTraxNG can also produce a variety of access reports, including usage reports, attendance records, and roll calls. Using the AxTraxNG Report Wizard, users can design their custom reports to meet their specific needs.

1.1.3 Software Security

Access to the AxTraxNG software is password controlled. It is possible to grant individually based restricted security rights for different operators, with access to only specified elements of the system or with read-only access.

1.2 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.

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 draw 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

Important

It is highly recommended that you back up the system database to an external storage device once a week (see Section 11.4).

1.3 Using this User Guide

This user guide provides all the information required to start working with AxTraxNG software. Refer to the AC-215, AC-225, AC-425, AC-525, or AC-825 hardware manuals for wiring and installation instructions.

The manual explains the following in detail:

- How to install the AxTraxNG server
- How to install the AxTraxNG client
- The basic functionality of AxTraxNG
- How to set up a new site from the AxTraxNG
- How to monitor and manage a site using the AxTraxNG client

2. Specifications and Requirements

2.1 System Capabilities

General	
Software Architecture	Client-Server
Database Type	SQL Server Express 2005, 2008, 2012
Max. Number of Users	• 30,000 per panel (AC-215IP, AC-225, AC-425, AC-525) • 5000 (AC-215) • 60000 (AC-825)
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-825)
Max. Cards per User	15
Max. Access Control Panels	1023
Antipassback	• Timed • Door • Global – across the entire facility
International Holiday Support	Up to 64 holidays

Networks	
Max. Number of Networks	Up to 1023 (depending on network topology)
Supported Access Control Panel Models	• AC-215 • AC-215 (SPV) • AC-215IP • AC-225 • AC-225 with MD-IO84 • AC-225 with MD-D02 • AC-425 • AC-425 with MD-IO84 • AC-425 with MD-D04 • AC-525 • AC-525 with MD-IO84 • AC-525 with MD-D02 • AC-825 • AC-825 with x805

Networks	
Panel Networks Communication Interface	• Serial (RS-232/485) • TCP-IP • Modem **Note: AC-825 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, 8.1
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

> Note When upgrading to AxTraxNG v24.0, it is possible to use Windows XP SP3, provided that you continue to use SQL Server 2005 and do not upgrade to SQL Server 2012.

2.2.2 SQL Express Server Requirements

Processor	Pentium 4 or better
Memory	2 GB
Hard Disk Space	4 GB

2.2.3 Microsoft Framework

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

3. Installation

The AxTraxNG installation CD-ROM includes the setup file required to install the AxTraxNG Access Control software on the system's main computer. The software system consists of the following five main components:

- Prerequisite applications
- AxTraxNG Server
- AxTraxNG Client

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

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

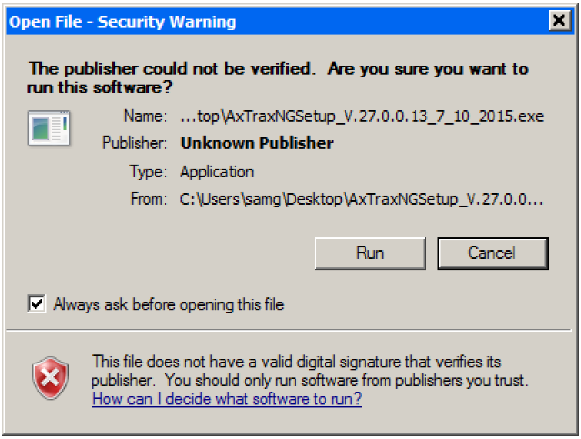
3.1 Beginning the AxTraxNG Installation

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

To begin the AxTraxNG installation:

1. Insert the CD into your computer's CD drive or download the installation file from the Download Center link on the Rosslare website.
2. Double-click the AxTraxNG setup file.

   The following verification screen may open:



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

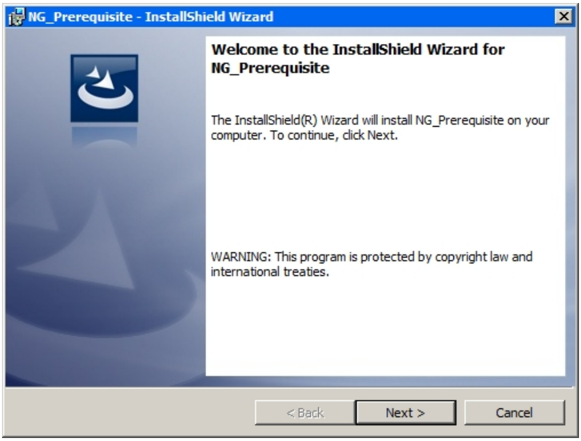
Name: ...top\AxTraxNGSetup_V.27.0.0.13_7_10_2015.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Users\samg\Desktop\AxTraxNGSetup_V.27.0.0...

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

3. Click **Run**.

   Once the necessary files are extracted, the Welcome to the *InstallShield Wizard for NG_Prerequisite* screen opens:



NG_Prerequisite - InstallShield Wizard

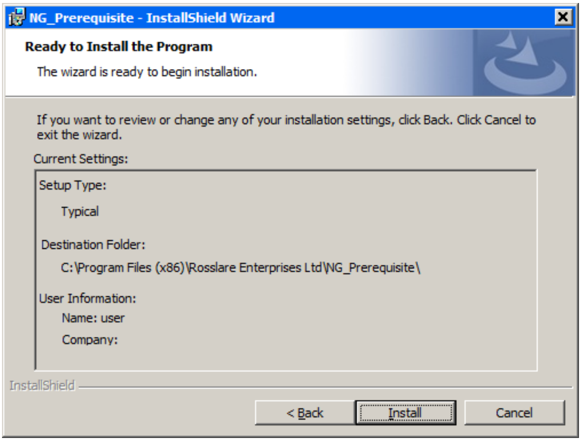
Welcome to the InstallShield Wizard for NG_Prerequisite

The InstallShield(R) Wizard will install NG_Prerequisite on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

4. Click **Next**.

   The *Ready to Install Program* screen opens.



NG_Prerequisite - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

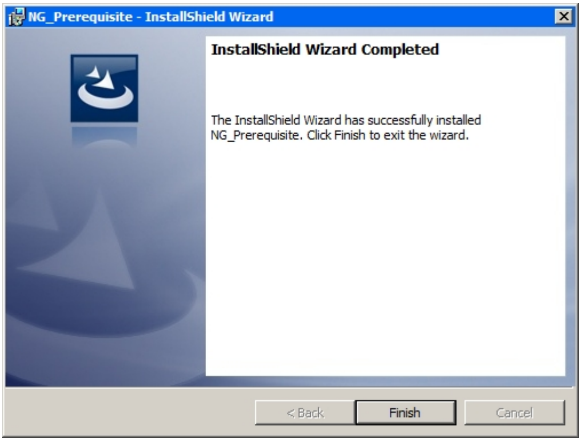
Current Settings:

Setup Type:
Typical

Destination Folder:
C:\Program Files (x86)\Rosslare Enterprises Ltd\NG_Prerequisite\

User Information:
Name: user
Company:

5. Click **Install**. After a few moments, the *InstallShield Wizard Completed* screen opens.



NG_Prerequisite - InstallShield Wizard

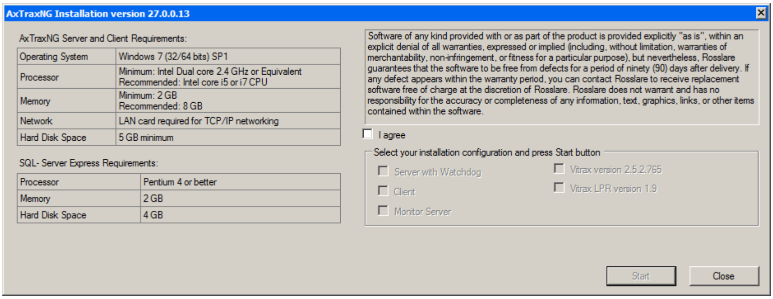
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed NG_Prerequisite. Click Finish to exit the wizard.

6. Click **Finish**.

   After a few moments, the following screen opens.

Figure 1: AxTraxNG Packages Selection Screen



AxTraxNG Installation version 27.0.0.13

AxTraxNG Server and Client Requirements:

Operating System	Windows 7 (32/64 bits) SP1
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

SQL- Server Express Requirements:

Processor	Pentium 4 or better
Memory	2 GB
Hard Disk Space	4 GB

Software of any kind provided with or as part of the product is provided explicitly "as is", within an explicit denial of all warranties, expressed or implied (including, without limitation, warranties of merchantability, non-infringement, or fitness for a particular purpose), but nevertheless, Rosslare guarantees that the software to be free from defects for a period of ninety (90) days after delivery. If any defect appears within the warranty period, you can contact Rosslare to receive replacement software free of charge at the discretion of Rosslare. Rosslare does not warrant and has no responsibility for the accuracy or completeness of any information, text, graphics, links, or other items contained within the software.

□ I agree

Select your installation configuration and press Start button

□ Server with Watchdog
□ Client
□ Monitor Server
□ Vitrax version 2.5.2.765
□ Vitrax LPR version 1.9

7. Accept the licensing agreement and select which packages you wish to install.

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

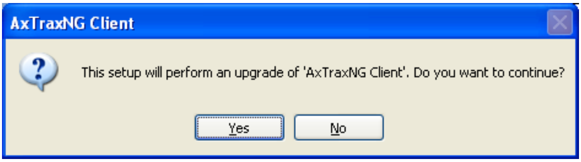
8. Click **Start**.

> Note
>
> 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.

Once these installations finish, the AxTraxNG Client installation begins.

3.2 Installing AxTraxNG Client Software

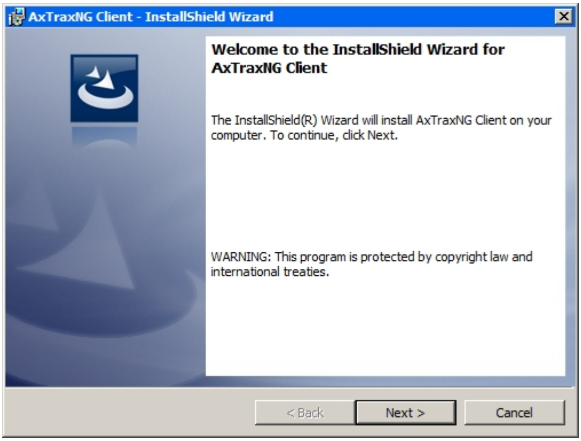
If you are upgrading, the following screen opens:



AxTraxNG Client

This setup will perform an upgrade of 'AxTraxNG Client'. Do you want to continue?

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



AxTraxNG Client - InstallShield Wizard

Welcome to the InstallShield Wizard for AxTraxNG Client

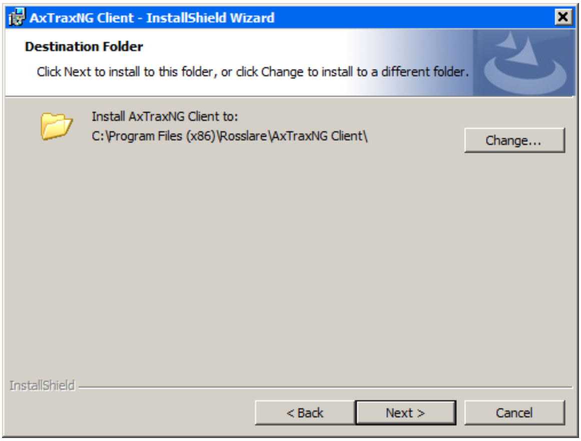
The InstallShield(R) Wizard will install AxTraxNG Client on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

To install the AxTraxNG Client application:

1. Click **Next** to begin the AxTraxNG Client installation process.
2. If you are installing an upgrade, skip to Step 4.

   The *Destination Folder* screen opens.



AxTraxNG Client - InstallShield Wizard

Destination Folder

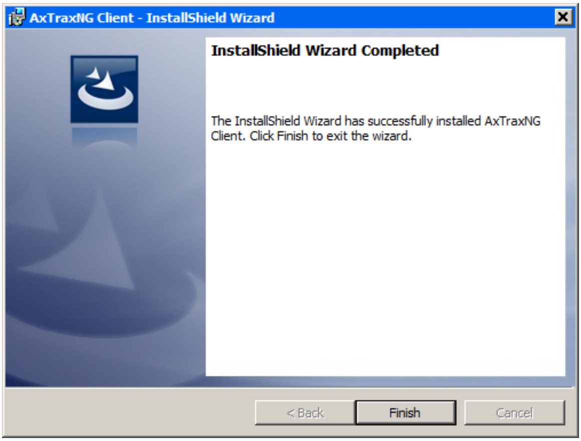
Click Next to install to this folder, or click Change to install to a different folder.

Install AxTraxNG Client to:
C:\Program Files (x86)\Rosslare\AxTraxNG Client\

3. Select the required installation location by clicking **Change** or click **Next** to use the default destination.

   The *Installing AxTraxNG Client* screen opens.

   When the installation is complete, the *InstallShield Wizard Completed* screen opens.



AxTraxNG Client - InstallShield Wizard

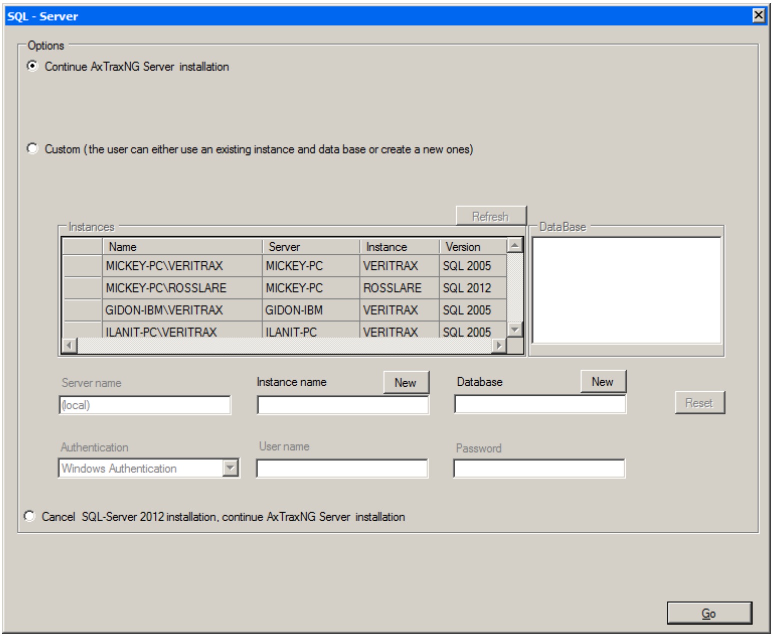
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed AxTraxNG Client. Click Finish to exit the wizard.

4. Click **Finish** to complete installing the AxTraxNG Client software.

3.3 SQL Server Setup

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



SQL - Server

Options

● Continue AxTraxNG Server installation

○ Custom (the user can either use an existing instance and data base or create a new ones)

Instances

Name	Server	Instance	Version
MICKEY-PC\VERITRAX	MICKEY-PC	VERITRAX	SQL 2005
MICKEY-PC\ROSSLARE	MICKEY-PC	ROSSLARE	SQL 2012
GIDON-IBM\VERITRAX	GIDON-IBM	VERITRAX	SQL 2005
ILANIT-PC\VERITRAX	ILANIT-PC	VERITRAX	SQL 2005

Server name: (local)

Authentication: Windows Authentication

○ Cancel SQL-Server 2012 installation, continue AxTraxNG Server installation

The AxTraxNG Server operates using an SQL server 2005/2008/2012 database. There are three options in installing the SQL server:

- Select Continue to install Microsoft SQL Server Express 2012
- Select Custom to use an existing instance of the SQL 2005/2008 server available on your computer network with your SQL login credentials.
- Select Cancel when upgrading to use the current SQL Server instance

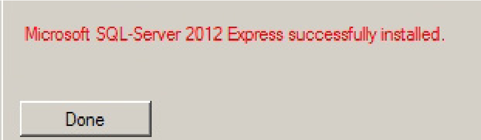
> Note
>
> Do not install the SQL server when installing additional AxTraxNG clients that connect to the AxTraxNG Server database.

3.3.1 Default Setup

To install the default SQL Server application:

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

   A new instance of SQL Server 2012 is installed and a confirmation sentence appears on the lower part of the screen.



Microsoft SQL-Server 2012 Express successfully installed.

2. Click **Done**.

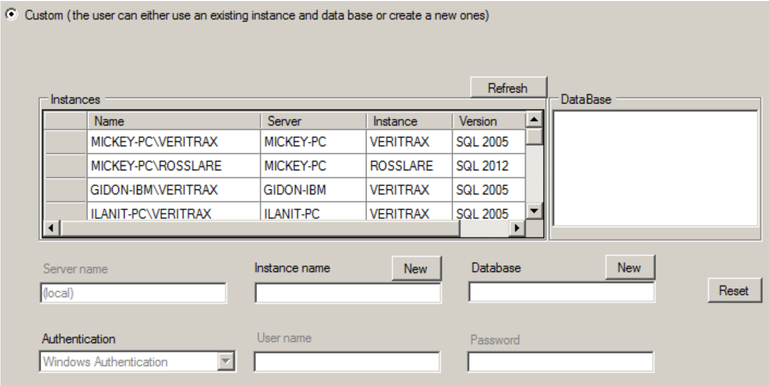
3.3.2 Custom Setup

Select Custom to use an existing instance of the SQL 2005/2008 server available on your computer network with your SQL login credentials

To install an existing instance of the SQL Server application:

1. Select **Custom**.

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



● Custom (the user can either use an existing instance and data base or create a new ones)

Instances

	Name	Server	Instance	Version
	MICKEY-PC\VERITRAX	MICKEY-PC	VERITRAX	SQL 2005
	MICKEY-PC\ROSSLARE	MICKEY-PC	ROSSLARE	SQL 2012
	GIDON-IBM\VERITRAX	GIDON-IBM	VERITRAX	SQL 2005
	ILANIT-PC\VERITRAX	ILANIT-PC	VERITRAX	SQL 2005

DataBase

Server name: (local)

Instance name:

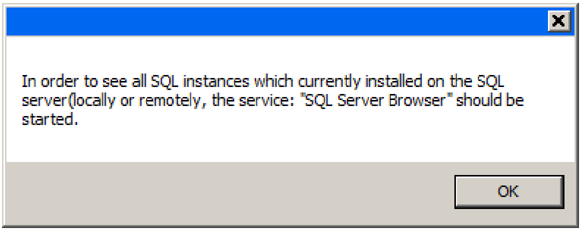
Database:

Authentication: Windows Authentication

User name:

Password:

   You may receive the following message:



In order to see all SQL instances which currently installed on the SQL server(locally or remotely, the service: "SQL Server Browser" should be started.

2. Select the instance in 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.
- A strong password is a MUST!! Without defining strong password, SQL Server setup does not build a database for the AxTraxNG server.
- When creating a new instance, be sure that the instance name is different than the existing instance name.
- The new instance is created with System Administrator rights (User 'SA'). To create an instance with limited rights, please ask your DB Administrator.

4. Click **Go**.

   A setup wizard for the SQL Server 2012 Express opens.

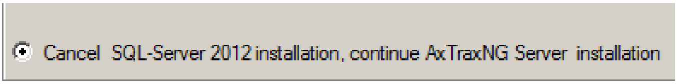
5. Click **Done**.

3.3.3 Using Current SQL Server for Upgrade

Select Cancel to use the current SQL Server instance when upgrading.

To use the current instance of the SQL Server application:

1. Select **Cancel**.



● Cancel SQL-Server 2012 installation, continue AxTraxNG Server installation

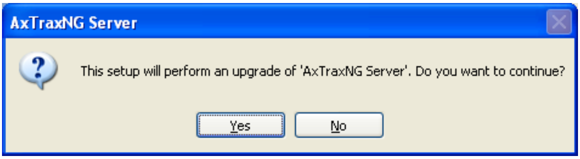
2. Click **Go**.

   The installation continues.

3.4 Installing AxTraxNG Network Server Software

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

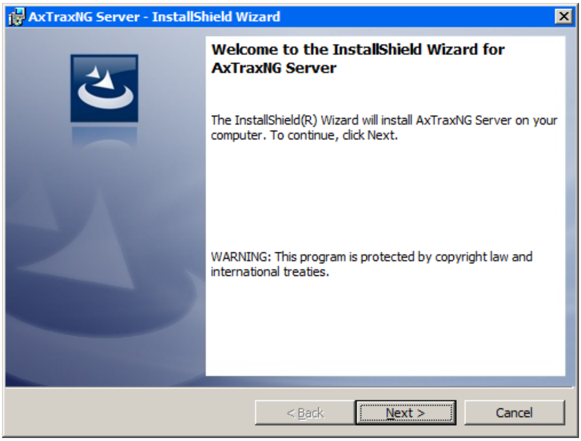
If you are upgrading, the following screen opens:



AxTraxNG Server

This setup will perform an upgrade of 'AxTraxNG Server'. Do you want to continue?

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



AxTraxNG Server - InstallShield Wizard

Welcome to the InstallShield Wizard for AxTraxNG Server

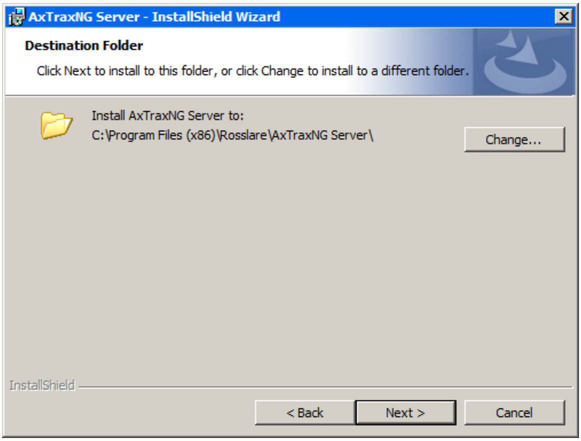
The InstallShield(R) Wizard will install AxTraxNG Server on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

To install the AxTraxNG Server:

1. Click **Next** to begin the AxTraxNG Server installation process.

   The *Destination Folder* screen opens.



AxTraxNG Server - InstallShield Wizard

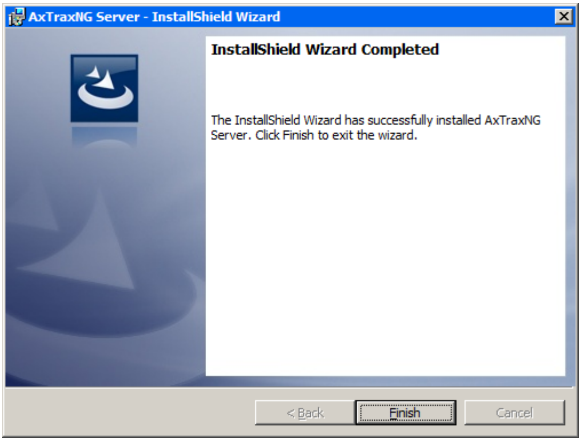
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install AxTraxNG Server to:
C:\Program Files (x86)\Rosslare\AxTraxNG Server\

2. Click **Next**.

When the installation is complete, the *Install Shield Wizard Completed* screen opens.



InstallShield Wizard Completed

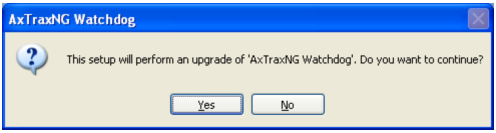
The InstallShield Wizard has successfully installed AxTraxNG Server. Click Finish to exit the wizard.

3. Click **Finish** to complete installing the AxTraxNG Server software.

3.5 Installing AxTraxNG Watchdog

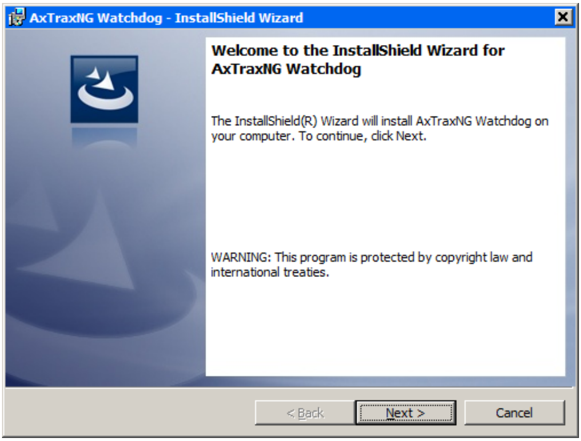
Once the AxTraxNG server installation finishes, the AxTraxNG Watchdog installation opens automatically.

If you are upgrading, the following screen opens:



This setup will perform an upgrade of 'AxTraxNG Watchdog'. Do you want to continue?

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



Welcome to the InstallShield Wizard for AxTraxNG Watchdog

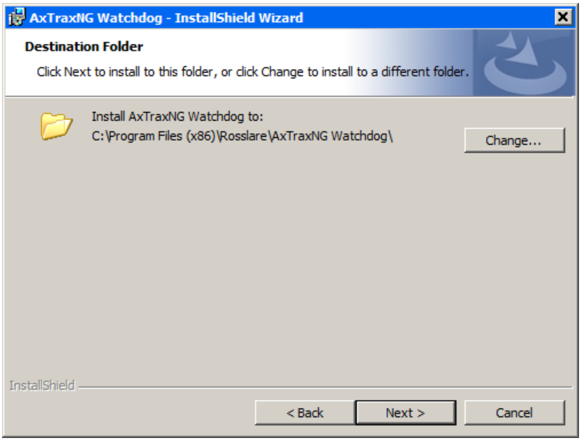
The InstallShield(R) Wizard will install AxTraxNG Watchdog on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

To install the AxTraxNG Watchdog:

1. Click **Next** to initiate the AxTraxNG Watchdog installation process.

   The *Destination Folder* screen opens.



AxTraxNG Watchdog - InstallShield Wizard

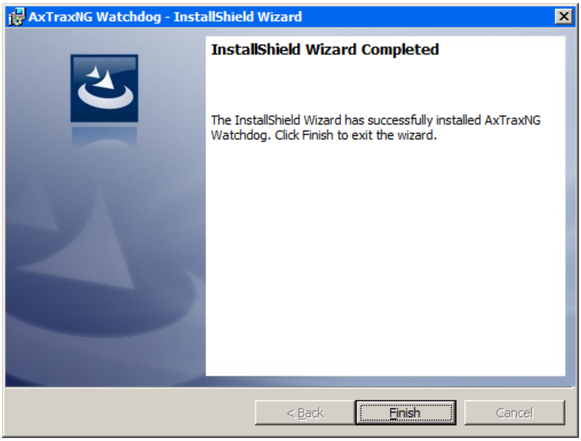
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install AxTraxNG Watchdog to:
C:\Program Files (x86)\Rosslare\AxTraxNG Watchdog\

2. Select the required installation location by clicking **Browse** or click **Next** to use the default destination.

   When the installation is complete, the *InstallShield Wizard Completed* screen opens.



AxTraxNG Watchdog - InstallShield Wizard

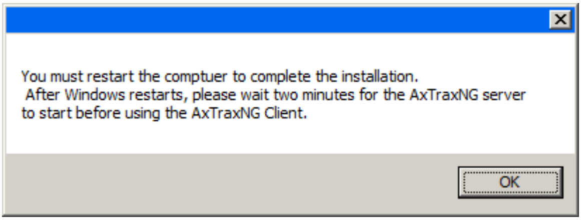
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed AxTraxNG Watchdog. Click Finish to exit the wizard.

3. Click **Finish** to complete the AxTraxNG Watchdog software installation.
4. Click **OK**.

3.6 Completing the Installation

Once all the elements of the installation have completed, a window opens telling you to restart the computer.

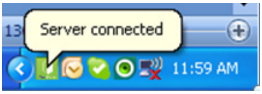


You must restart the comptuer to complete the installation.
After Windows restarts, please wait two minutes for the AxTraxNG server to start before using the AxTraxNG Client.

1. Click **OK**.
2. Click **Close** on the Return to the AxTraxNG Packages Selection Screen (Figure 1).
3. Restart the computer.

The AxTraxNG server is now fully installed on your computer.

Once the computer restarts, you must wait until you see a message in the Windows system tray that the server is connected.



Server connected

3.7 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.

3.8 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.

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

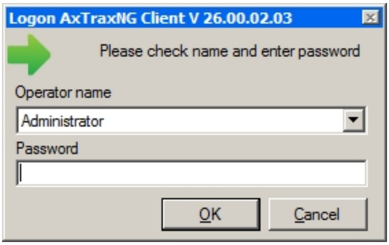
4.1 Starting the Software – Local PC

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.



Logon AxTraxNG Client V 26.00.02.03

Please check name and enter password

Operator name: Administrator

Password:

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

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

3. Click **OK**.

   The main AxTraxNG window opens.

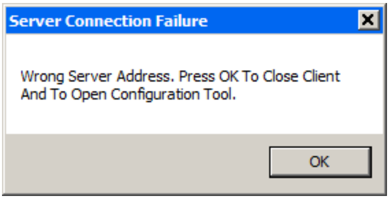
4.2 Starting the Software – Via WAN Connection

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

   Because the server and client are on different machines, the following window opens:



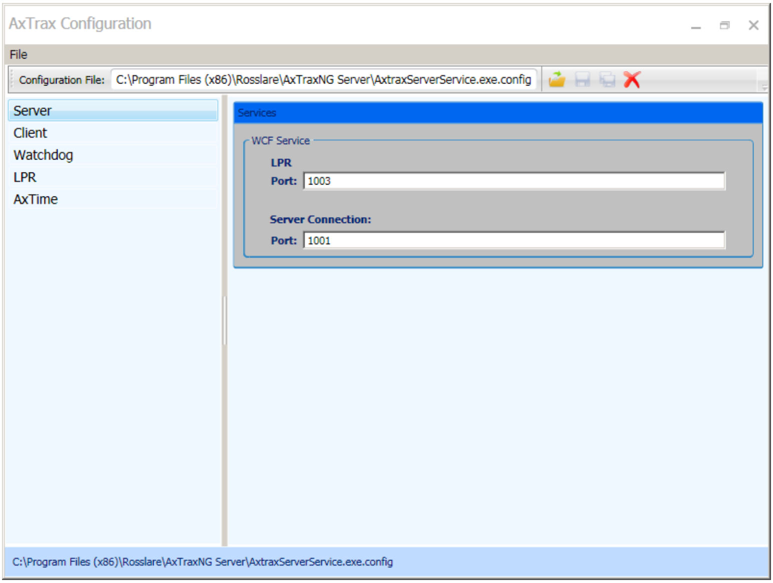
Server Connection Failure

Wrong Server Address. Press OK To Close Client And To Open Configuration Tool.

2. Click **OK**.

   Alternatively, you can open the AxTrax Configuration Tool directly by clicking **AxTraxConfigTool** (🛢) from the AxTraxNG Client folder under the Rosslare folder in the Start menu.

   The AxTrax Configuration Tool opens.



Configuration File: C:\Program Files (x86)\Rosslare\AxTraxNG Server\AxtraxServerService.exe.config

LPR

Port: 1003

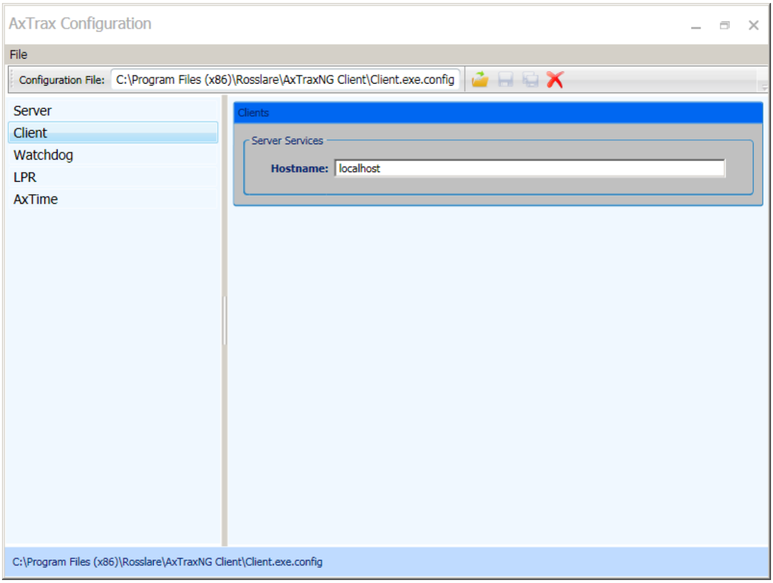
Server Connection:

Port: 1001

C:\Program Files (x86)\Rosslare\AxTraxNG Server\AxtraxServerService.exe.config

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

4. Click the *Client* tab.



AxTrax Configuration

File

Configuration File: C:\Program Files (x86)\Rosslare\AxTraxNG Client\Client.exe.config

Clients

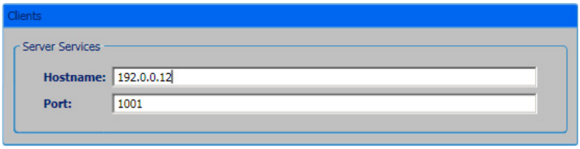
Server Services

Hostname: localhost

C:\Program Files (x86)\Rosslare\AxTraxNG Client\Client.exe.config

5. In the Hostname field, enter the IP address of the Client server.

   As soon as you enter the IP address, the Port field appears.



Clients

Server Services

Hostname: 192.0.0.12

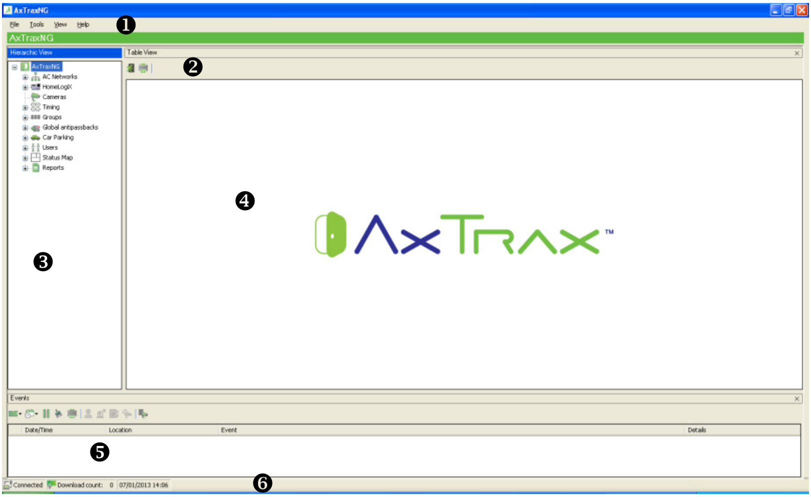
Port: 1001

6. Enter the same port number as you did in the Server Connection field above.
7. For the Watchdog, LPR, and AxTime tabs, enter the same IP address and port number in the respective fields.
8. When you finish populating all the fields, clicks the Save All button ( ) in the toolbar.
9. Close the Configuration Tool.
10. 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 D.

4.3 AxTraxNG Main Window

The entire central functionality of the AxTraxNG system is available from the AxTraxNG Client main window.



The AxTraxNG Client Main window is divided into six sections, as show 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.

Section		Description
6	**Status Bar**	The Status Bar displays server connection status, Downloads Counter, and the Firmware programming progress bar.

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 three 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 VeriTrax AS-225/AxTrax AS-525 configuration states and events logs (see Section 11.4)
Options	Set software options and preferences, including national holidays, event highlighting, custom user information fields, and GUI language (see Section 11.5)
Import/Export Data	Import/export user information from/to an Excel spreadsheet file (see Section 11.5.3)

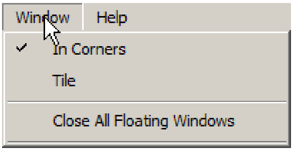
4.4.3 View Menu

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 a detailed table view
Restore Docking	Restore the default GUI view

4.4.4 Window Menu

The Window menu has three options:



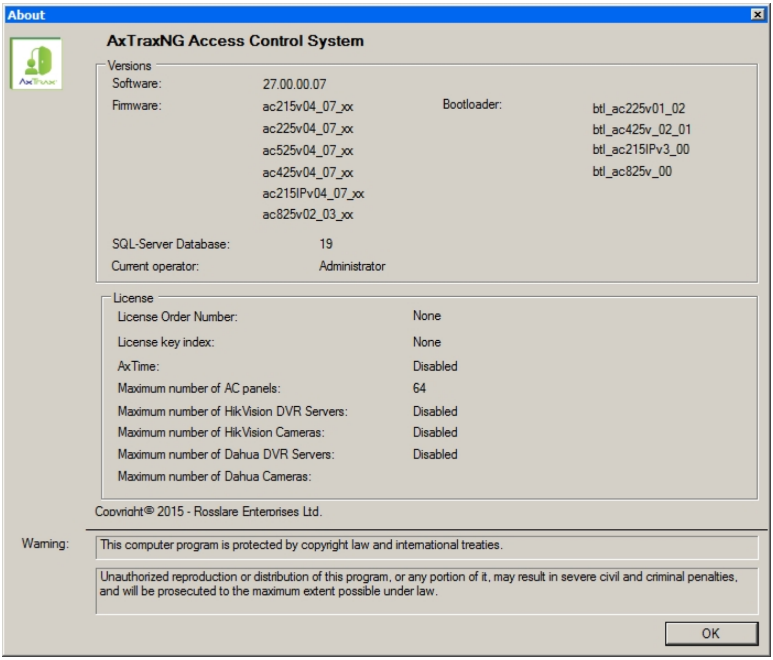
Menu	Select Menu item to…
In Corners	Place any open pop-up windows in the corners of the screen. This option is chosen by default.
Tile	To move any opened pop-up windows to available space on the screen
Close All Floating Windows	Close all of the pop-up windows You can use the list of open pop-ups to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

4.4.5 Help Menu

The Help menu has two options:

4.4.5.1 About

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



AxTraxNG Access Control System

Versions

Software: 27.00.00.07

Firmware: ac215v04_07_xx, ac225v04_07_xx, ac525v04_07_xx, ac425v04_07_xx, ac215IPv04_07_xx, ac825v02_03_xx

Bootloader: btl_ac225v01_02, btl_ac425v_02_01, btl_ac215IPv3_00, btl_ac825v_00

SQL-Server Database: 19

Current operator: Administrator

License

License Order Number:	None
License key index:	None
AxTime:	Disabled
Maximum number of AC panels:	64
Maximum number of HikVision DVR Servers:	Disabled
Maximum number of HikVision Cameras:	Disabled
Maximum number of Dahua DVR Servers:	Disabled
Maximum number of Dahua Cameras:	

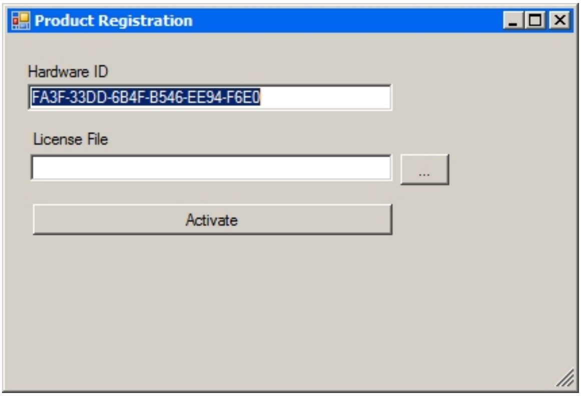
Copyright© 2015 - Rosslare Enterprises Ltd.

Warning: This computer program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

4.4.5.2 Product Registration

The Product Registration window is used to register your version of AxTraxNG.



Hardware ID
FA3F-33DD-6B4F-B546-EE94-F6E0

License File

The Hardware ID is automatically populated.

Click the Browse button to locate your license file and click **Activate**.

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

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 *Door Manual Operation* window (see Section 9.1)
🖨	**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
▯	**Reader Type**	Configure custom reader type

4.5.2 General Network Icons

Icon	Name	Click icon to...
⊞	**Add to Status Map**	Add available panels and panel components to the Status Map (see Section 4.6.9)

Icon	Name	Click icon to…
	Download Failed Data Manually	Download the entire panels' failed database (see Section 11.2)

4.5.3 Network Icons

Icon	Name	Click icon to…
	Set Time	Set the time on the selected access control panel (see Section 11.1)
	Find Panels	Find and update panels within the network (see Section 5.4.1.1)
	Manual Modem	Open the *Modem Status* window to allow the operator to connect or disconnect the modem and change the connection password (see Appendix F)
	Camera	View a list of connected cameras, and assign the cameras to panels (see the AxTraxNG™ Video Integration Manual)

4.5.4 Panel Icons

Icon	Name	Click icon to…
	Manual Reader	Change the operation mode of the readers on the selected panel (see Section 9.2)
	Update Firmware	Send a firmware update to the selected access control panel (see Section 9.6)
	Control Output Manually	Change the settings for the outputs on the selected panel (see Section 9.3)
	Control Input Manually	Change the settings for the inputs on the selected panel (see Section 9.4)
	Control Siren Manually	Test the siren for the selected panel (see Section 9.5)

4.5.5 Card\Users Icons

Icon	Name	Click icon to…
-1	**User Counter**	View the current user count value (see Section 11.3)
	Add Users and Cards	Create up to 1000 new users and cards in one batch (see Section 5.12)
	Card List	Batch add specific cards to a specific user
	Add Cards	Create up to 1000 new cards in one batch
	Add Cards by MD-08	Add and assign cards to selected users or add cards from an MD-08 reader (see Appendix I)
	Add Cards By UHF	Add and assign cards to selected users or add cards from a UHF reader (see Appendix J)

Icon	Name	Click icon to…
	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 card to add to Vehicle Types when configuring an License Plate Recognition (LPR) camera (see the *AxTraxNG™ Video Integration Manual*).

4.5.6 Reports Icons

Icon	Name	Click icon to…
	Manual Door Operation	Open the *Door Manual Operation* window (see Section 9.1)
	Print	Print the current report
	Save Reports	To view previously saved reports in the Display Area
	Run	Produce the selected report (Chapter 10)
	Preview	To preview a report that was just produced
	Save	To save a report that was just produced
	Delete	To delete a report that was produced

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
	Panels HLX	Displays events from the HomeLogiX™ panel.

Icon	Name	Click icon to...
📹	**Cameras**	Displays events 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.
1	**View Events within the last Day**	Display all events that occurred within the last day
7	**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 *User* window for the selected user.
🚨	**Clear Alarm**	Open the *Alarm Details* window to allow the operator to reset the alarm.
⇄	**Antipassback Forgive**	Open the *Antipassback Forgive* 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 *Archive Camera* window for the selected video stream or snapshot.
P	**Car Parking**	Opens the *Car Parking Counters* 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.

Note

To work with 65 panels or more, you must activate you license file (see Section 4.4.5.2).

4.6.2 HomeLogiX

The HomeLogiX element allows you to add HLX panels to the network and to configure each panel’s settings.

For more information, see the *AxTraxNG™ Intrusion Integration Manual*.

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 setting.

For more information, see the *AxTraxNG™ Video Integration Manual*.

4.6.4 Timing

The Timing tree branch consists of two elements: time zones 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 four elements: **Access Groups**, **Access Areas, Output Groups,** and **Input 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 5.11.1.

4.6.5.2 Access Areas

A facility can be subdivided into several access areas to configure and manage it more effectively (see Section 5.15).

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 5.11.1, 5.11.2, and 5.11.3).

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 5.11.4).

4.6.5.5 Vehicle Access Groups

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

For more information, see the *AxTraxNG™ Video Integration 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 5.16).

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 5.17.

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.

For more information, see the *AxTraxNG™ Video Integration Manual*.

4.6.8.5 Cards

This element lists all cards in the system with their statuses, and allows the manual or automatic addition of cards to the system (see Section 5.11.4.2).

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 5.18.

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 5.20.

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 10.

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 and Holidays**	5.1 and 5.2
2	**Add a Network**	5.3
3	**Add and Configure an Access Control Panel**	5.4
4	**Adding an Expansion Board**	5.5
5	**Configure the Doors**	5.6
6	**Configure the Readers**	5.7
7	**Configure the Inputs**	5.8
8	**Add Video Integration**	5.9
9	**Add Panel Links**	5.10
10	**Create Groups: Access Groups, Input Groups, Card + Card Groups, Output Groups**	5.11.1, 5.11.2, 5.11.3, 5.11.4
12	**Add New Users and Cards**	5.12
13	**Card Design**	5.13
14	**Add Departments, Users and Visitors**	5.14
15	**Add Access Areas and Add Global Antipassback Rules**	5.15 and 5.16
16	**Add Car Parking**	5.17
17	**Add Operator**	5.18
18	**Add Elevator Control**	5.19
19	**Add a Status Map**	5.20

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. The counter shows “**0**” when a download is complete; however, it may also appear after a failed download.

Note

It is the operator’s responsibility to verify that the download operation succeeded or failed. This can be verified in the system event list or by checking the failed download data manually (see Section 11.2).

5.1 Adding Time Zones

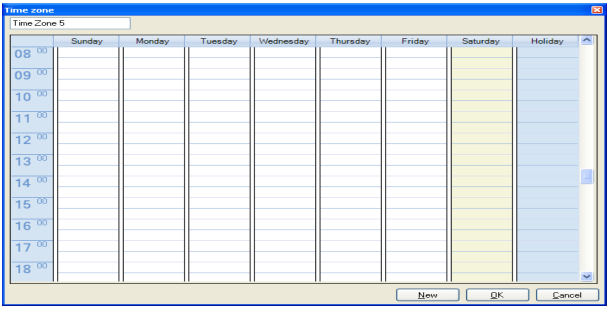
A time zone is a group of periods within a week. Door access rights, as well as alarms and input and output behavior, can all be set to behave differently for each time zone. Many operations can be automatically enabled or disabled within a selected time zone.

The *Time Zone Properties* window displays the selected periods for each day of the week. It is possible to set a maximum of eight different time zone periods.

To add a new time zone:

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

   The Add *Time Zone* properties window opens.



Time Zone 5

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

Note

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

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

Note

You can create up to 8 time intervals for each day.

5.2 Adding Holidays

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

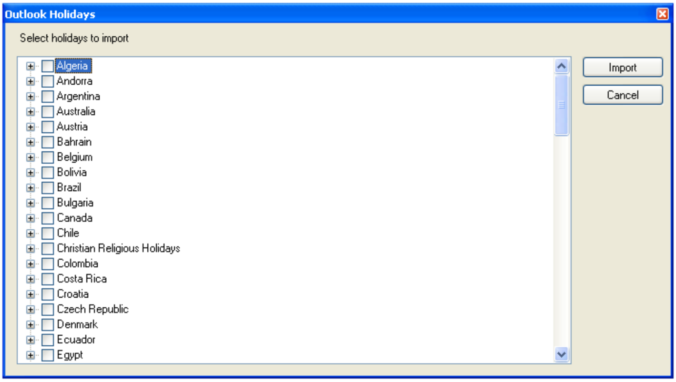
There are two ways to add holidays:

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

To add a national holiday:

1. In the Tree View, select the **Holidays** element.
2. On the toolbar, click the ✓ icon.

   The *Outlook Holidays* window opens.



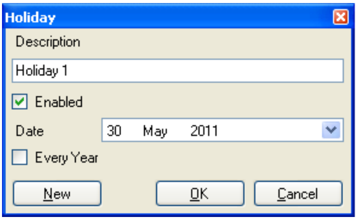
□ Algeria
□ Andorra
□ Argentina
□ Australia
□ Austria
□ Bahrain
□ Belgium
□ Bolivia
□ Brazil
□ Bulgaria
□ Canada
□ Chile
□ Christian Religious Holidays
□ Colombia
□ Costa Rica
□ Croatia
□ Czech Republic
□ Denmark
□ Ecuador
□ Egypt

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 **Import**.
5. Click **OK** to confirm.
6. Click **OK** to close the *Options* window.

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.



Description: Holiday 1

☑ Enabled

Date: 30 May 2011

□ Every Year

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

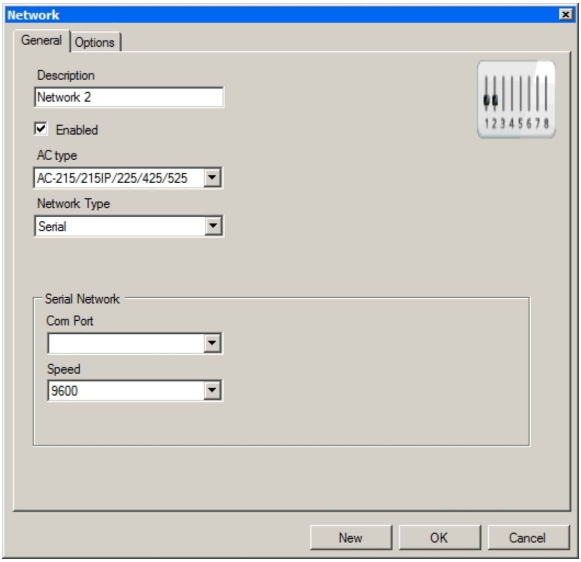
A network is a group of up to 32 access control panels. AxTraxNG communicates with each access control panel that is part of the network.

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-825 panels)
- The type of network connection and the connection settings
- Type of panel and its hardware (AC-825 only)

5.3.1 For AC-215, AC-225, AC-425, and AC-215IP

When adding an AC-215, AC-225, AC-425, or AC-215IP panel, the *Network* window looks as follows:



Description: Network 2

☑ Enabled

AC type: AC-215/215IP/225/425/525

Network Type: Serial

Serial Network

Com Port:

Speed: 9600

The *General* tab contains the following fields:

Table 2: Add Network > General Tab

Field	Description
Description	Name for the network The network address appears to the right of the network name.
Enabled	Checkbox is selected when the network is connected and operational.
AC Type	AC type: AC-215/215IP/425/525 or AC-825
Network Type	Network type: Serial, TCP/IP, or Modem **Note: Modem not supported by AC-425.**

Field	Description
Serial Network	
COM Port	The port used for the network
Speed	Speed of the connection
Modem Network	
COM Port	The port used for the network
Speed	Speed of the connection
Configuration Button	Configuration window to set communication preferences. This button appears when selecting a Modem or TCP/IP network.
TCP/IP Network	
IP Address	The IP address of the network
Port	The port used for the network
Speed	Speed of the connection
Remote (WAN)/ Local (LAN)	Select the kind of network
Configuration Button	Configuration window to set communication preferences. This button appears when selecting a Modem or TCP/IP network.

To add a network:

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

   The *Add Network* window opens.
3. In *Description*, enter a name for the new network.
4. Select **Enabled**.
5. In *AC type*, select **AC-215/215IP/225/425/525** or **AC-825**.
6. In *Network type*, select the network type and set the connection settings:
   a. For serial and modem, select the correct COM port and speed.
   b. For a TCP/IP LAN, 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.
   a. For a modem connection, click **Configuration** to set dialing preferences for the computer's and the receiving modems.

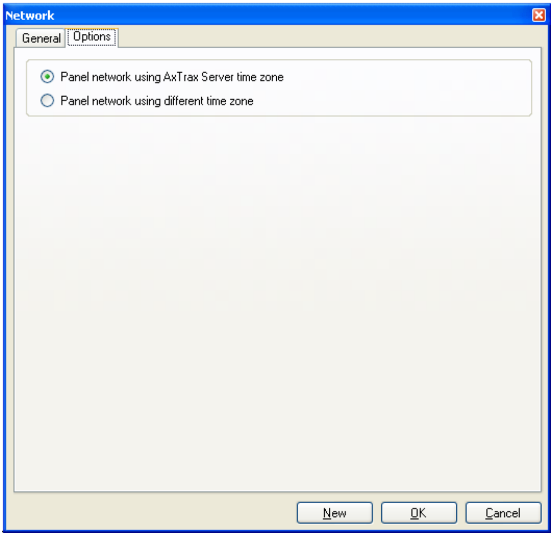
   For more information on how to configure an access control network, see Appendix F. Check with your system administrator for more information, or contact Rosslare technical support. Clear **Enabled** if you want to halt communication to panels on the network.

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/AC-425IP/AC-525. Refer to the relevant hardware installation guides for more details.

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

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

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



Network

General | Options

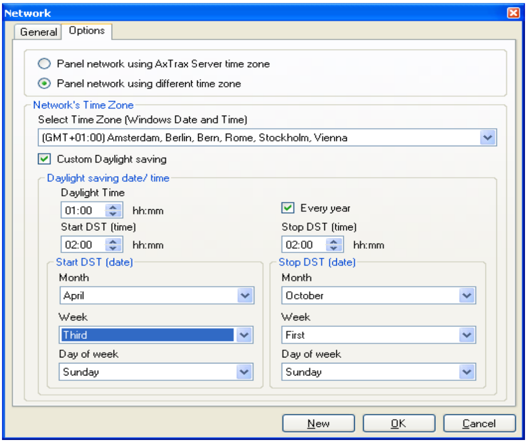
● Panel network using AxTrax Server time zone

○ Panel network using different time zone

10. 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 12.

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

The *Network Time Zone* section appears.



○ Panel network using AxTrax Server time zone

● Panel network using different time zone

Network's Time Zone

Select Time Zone (Windows Date and Time): (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

☑ Custom Daylight saving

Daylight saving date/ time

Daylight Time: 01:00 hh:mm

☑ Every year

Start DST (time): 02:00 hh:mm

Stop DST (time): 02:00 hh:mm

Start DST (date)
Month: April
Week: Third
Day of week: Sunday

Stop DST (date)
Month: October
Week: First
Day of week: Sunday

The *Network Time Zone* area contains the following fields:

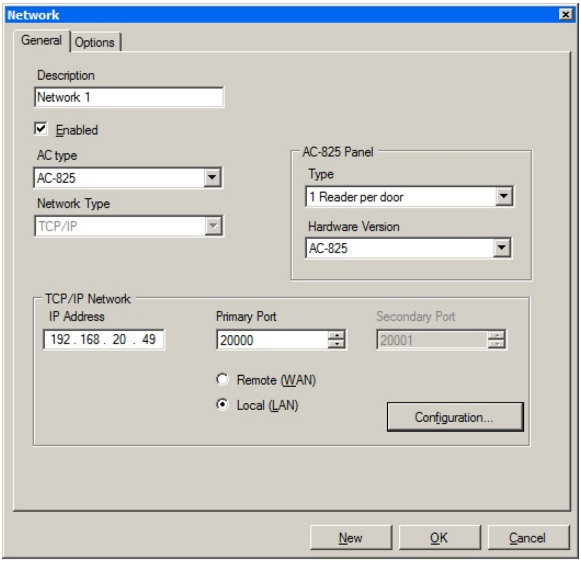
Table 3: Add Network > Options Tab

Field	Description
Select Time Zone (Windows Date and Time)	From the dropdown list, select the desired time zone.
Custom Daylight saving	Select the checkbox 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.
Month, Week, Day of Week	These fields are enabled when **Every year** is selected. Select the month, week within the month, and day of the week when daylight saving time is to begin every year.
Stop DST (date)	If **Every year** is not selected, select the end date for daylight saving time.
Month, Week, Day of Week	These fields are enabled when **Every year** is selected. Select the month, week within the month, and day of the week when daylight saving time is to end every year.

12. Set the Daylight Saving Time definitions according to the field descriptions in Table 3.
13. Click **OK**.

5.3.2 For AC-825

When adding an AC-825 panel, the *General* tab of the *Network* window looks as follows:



Description: Network 1

☑ Enabled

AC type: AC-825

Network Type: TCP/IP

AC-825 Panel

Type: 1 Reader per door

Hardware Version: AC-825

TCP/IP Network

IP Address: 192 . 168 . 20 . 49

Primary Port: 20000

Secondary Port: 20001

○ Remote (WAN)

● Local (LAN)

Configuration...

The *General* tab contains the following fields:

Table 4: Add Network > General Tab for AC-825

Field	**Description**
Description	Name for the network The network address appears to the right of the network name.
Enabled	Checkbox is selected when the network is connected and operational.
AC Type	AC type: AC-825
Network Type	For the AC-825, this field is grayed out because it cannot be changed. To configure a TCP/IP connection, see Appendix F.1.
AC-825 Panel	
Type	Select whether there will be one reader or two readers per door. **Note: Once this parameter is chosen, it cannot be changed.**
Hardware Version	Select whether this is an AC-825 panel or one of its expansions (R/S/D/P-805) **Note: Once this parameter is chosen, it cannot be changed**.

Field	Description
TCP/IP Network	
IP Address	The IP address of the network
Primary Port	The primary port used for the network
Secondary Port	The secondary port used for the network
Remote (WAN)/ Local (LAN)	Select the kind of network
Configuration Button	Configuration window to set communication preferences. To configure a TCP/IP connection, see Appendix F.1.

To add a network:

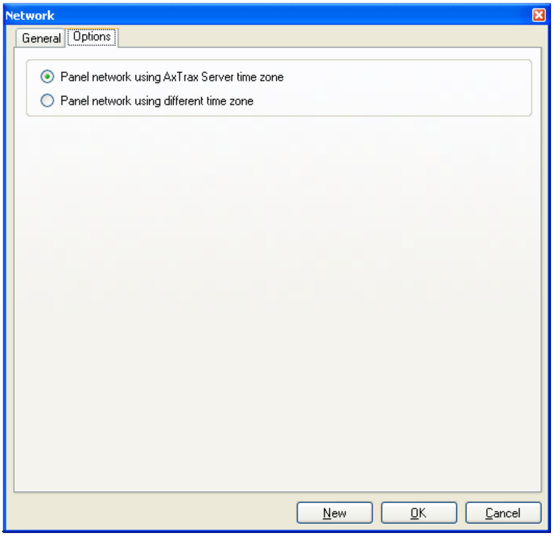
1. In the Tree view, select *Networks*.
2. On the toolbar, click the ✚ icon.

   The *Network* window opens.
3. In *Description*, enter a name for the new network.
4. Select **Enabled**.
5. In *AC type*, select **AC-825**.
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-825 panel or one of its expansions (R/S/D/P-805).
7. Enter the IP address, select the port and speed, 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 F.1. Check with your system administrator for more information, or contact Rosslare technical support. Clear **Enabled** if you want to halt communication to panels on the network.

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

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

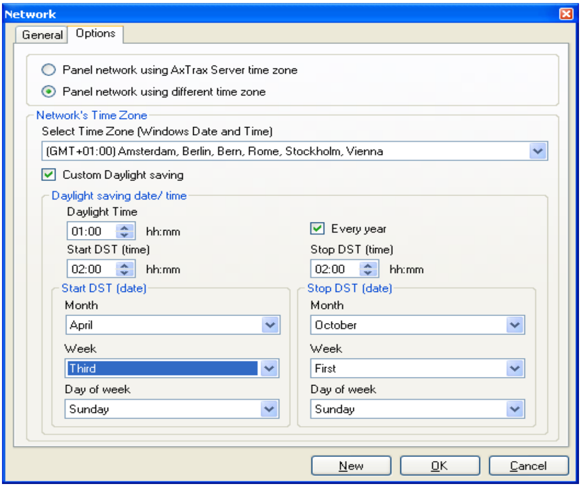


● Panel network using AxTrax Server time zone
○ Panel network using different time zone

10. 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 12.

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

    The *Network Time Zone* section appears.



○ Panel network using AxTrax Server time zone
● Panel network using different time zone

Network's Time Zone

Select Time Zone (Windows Date and Time)

(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

☑ Custom Daylight saving

Daylight saving date/ time

Daylight Time: 01:00 hh:mm

☑ Every year

Start DST (time): 02:00 hh:mm

Stop DST (time): 02:00 hh:mm

Start DST (date)
Month: April
Week: Third
Day of week: Sunday

Stop DST (date)
Month: October
Week: First
Day of week: Sunday

The *Network Time Zone* section is described in Table 3 in Section 5.3.1 above.

12. Set the Daylight Saving Time definitions according to the field descriptions in Table 3.
13. Click **OK**.

5.4 Adding Access Control Panels

5.4.1 For AC-215, AC-225, AC-425, and AC-215IP

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-215, AC-225, and AC-525 panels have two readers and can be configured as a one or two-door panel. Each AC-425 panel has four readers and can be configured as a two or four-door panel.

When using an optional MD-D02 (supported by AC-225 or AC-525) or MD-D04 (supported by the AC-425) 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.

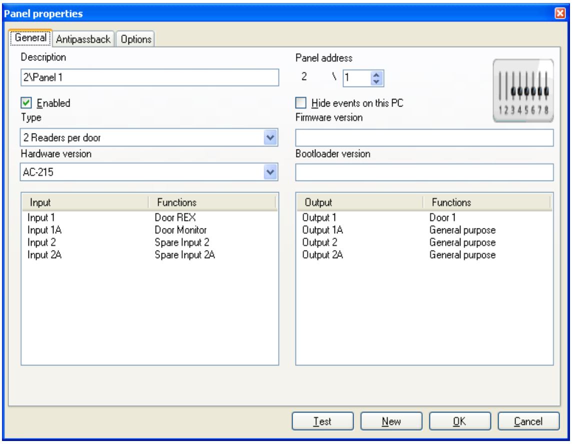
5.4.1.1 Adding an Access Control Panel Manually

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.



Description: 2\Panel 1

Panel address: 2 \ 1

☑ Enabled

☐ Hide events on this PC

Type: 2 Readers per door

Firmware version:

Hardware version: AC-215

Bootloader version:

Input	Functions
Input 1	Door REX
Input 1A	Door Monitor
Input 2	Spare Input 2
Input 2A	Spare Input 2A

Output	Functions
Output 1	Door 1
Output 1A	General purpose
Output 2	General purpose
Output 2A	General purpose

The *General* tab of the Door Controller *Panel properties* window contains the following fields:

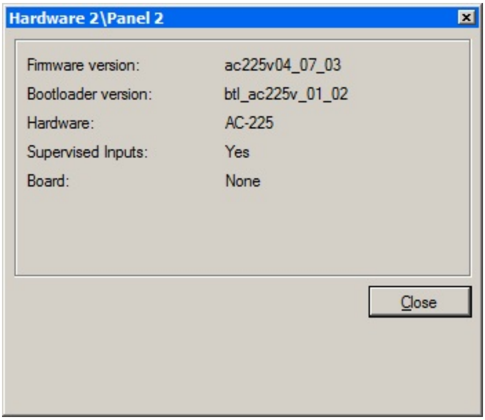
Table 5: Door Controller > Panel Properties > General Tab

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 the checkbox to activate this panel Clear the checkbox if the panel is not connected
Hide events on this PC	Select the checkbox to hide events originating from this PC
Type	Select one or two readers per door
Hardware Version	Select the appropriate panel hardware type
Firmware version	Upon selection of the hardware version, the field displays the current firmware version
Boot loader version	Upon selection of the hardware version, the field displays the current boot loader 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 computer The Test Panel window displays hardware details, including hardware type, firmware, and boot loader versions, and indicates whether a reader or I/O expansion board is installed on the panel.

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

4. Configure the panel according to the fields described in Table 5.
5. Click **Test**.

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



Firmware version: ac225v04_07_03
Bootloader version: btl_ac225v_01_02
Hardware: AC-225
Supervised Inputs: Yes
Board: None

Note: 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**.

   The window closes and the display area displays the newly configured panel.

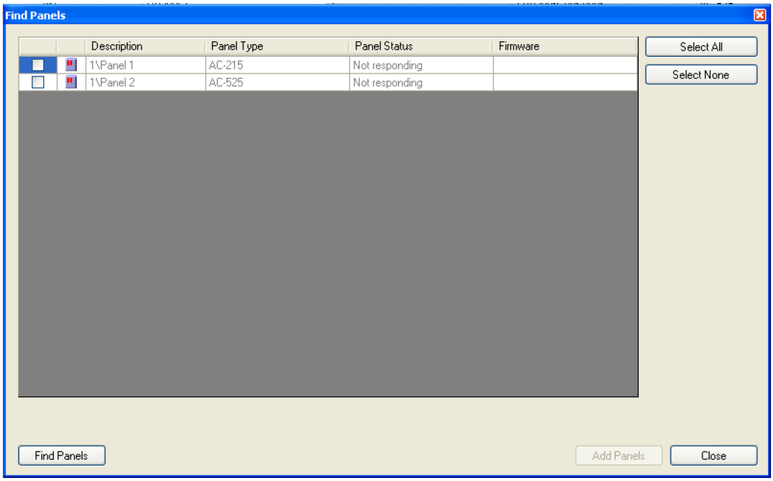
5.4.1.2 Searching for Existing Access Control Panels

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.



		Description	Panel Type	Panel Status	Firmware
□		1\Panel 1	AC-215	Not responding	
□		1\Panel 2	AC-525	Not responding	

3. Click **Find Panels** to search for all connected panels in the network.

   Once the detection process is complete (this may take 2–3 minutes), the display shows all of the detected panels and their corresponding information.

4. Select the panels that you wish to activate and click **Add Panels**.

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

5.4.1.3 Editing an Existing Access Control Panel

Each panel has individual settings for antipassback behavior and for recording events.

Once the panel is connected, edit the panel's options from the *Antipassback* and *Options* tabs in the *Panel properties* window.

The Antipassback tab contains the following fields:

Table 6: Network > Panel Properties > Antipassback Tab

Field	Description
Automatic Antipassback	From the *Automatic Antipassback* dropdown menu, select the time zone for door Antipassback rules to apply.
Antipassback severity	Select the antipassback severity: • **Hard** – When hard Antipassback is selected, an event is generated and the door does not open. • **Soft** – When soft Antipassback is selected, an event is generated and the door opens.

Field	Description
In/Out reader list	From the IN/OUT readers list, select the checkboxes to apply Antipassback restrictions to Reader 1 through Reader 8, as required. The reader antipassback is enabled when the checkbox is selected.

The *Options* tab contains the following fields:

Table 7: Network > Panel Properties > Options Tab

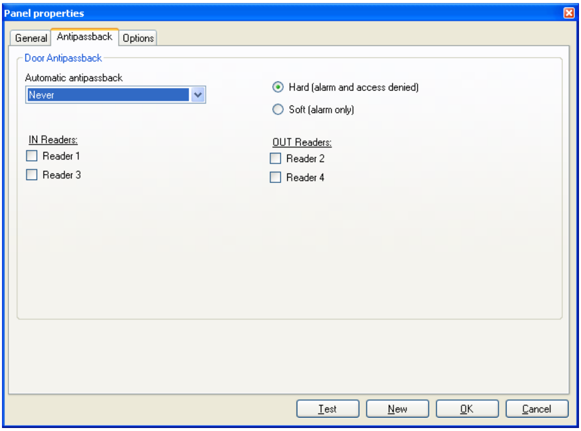
Field	Description
Events filter	Click **Select** to open the Events Filter and select the events that this panel should record. Set the filter's operation method: • **Always Active** – Only the selected events are recorded by the panel • **Active when panel disconnected** – If the panel is disconnected from the AxTraxNG server, only the selected events are recorded. When the panel is connected to the server, all events are recorded. **Note: In the default configuration, some events are filtered and may not be seen in the display area Events view**
Door Interlock	Select the checkboxes to apply the Door Interlock restrictions to the relevant doors. At least two door must be selected for the Door Interlock function to be enabled.
AC-525 USB Storage **(applicable when connected to AC-525 only)**	From the **Alarm Threshold Range (%)** dropdown menu, select the percentage of available memory consumed to determine when the system generates the "USB Disk Low Level" event. The USB disk on key status is monitored roughly once an hour. Therefore, be sure to select an acceptably low threshold level and consider that any related alarm may be set off up to one minute after the actual event occurs.
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.**
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 in the *General* tab of the *Readers Properties* window (Section 5.7.1).

To edit a panel:

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 appears.

4. Click the *Antipassback* tab.



Door Antipassback

Automatic antipassback: Never

● Hard (alarm and access denied)

○ Soft (alarm only)

IN Readers:

□ Reader 1

□ Reader 3

OUT Readers:

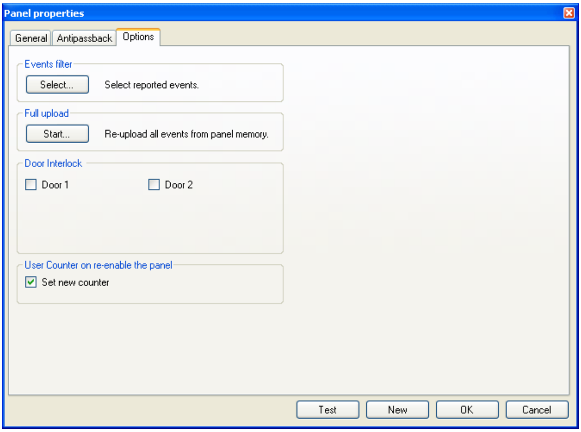
□ Reader 2

□ Reader 4

Each panel has individual antipassback settings for door antipassback behavior.

5. Set the Antipassback behavior according to the field descriptions in Table 6.

6. Click the *Options* tab.



Events filter

Select reported events.

Full upload

Re-upload all events from panel memory.

Door Interlock

□ Door 1 □ Door 2

User Counter on re-enable the panel

☑ Set new counter

7. Set the event filtering options for this panel.

8. Click **OK**.

The window closes and the configured panel is displayed.

5.4.2 For AC-825

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

There can be only one AC-825 panel in a network.

5.5 Adding an Expansion Board

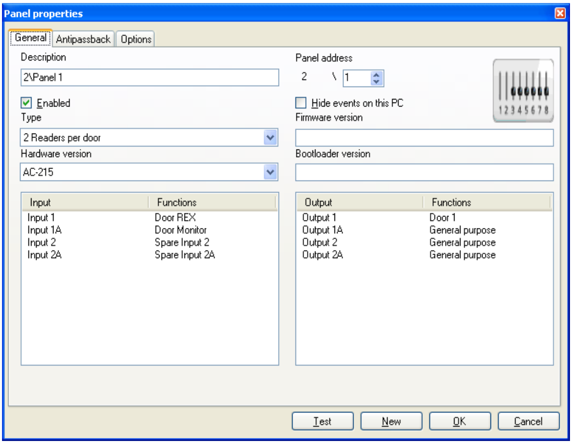
For any kind of access control panel, you can add an expansion board to the network.

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

To add an expansion board:

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

   The *Panel Properties* window opens.



Description: 2\Panel 1

☑ Enabled

Type: 2 Readers per door

Hardware version: AC-215

Panel address: 2 \ 1

□ Hide events on this PC

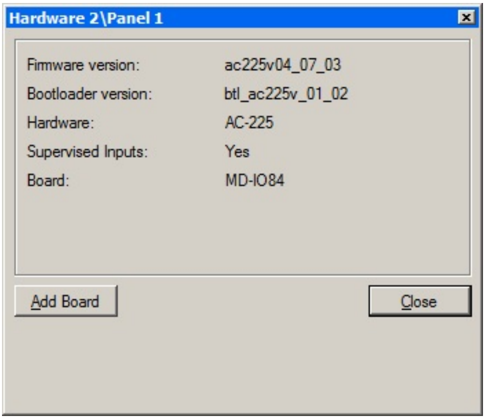
Firmware version:

Bootloader version:

Input	Functions
Input 1	Door REX
Input 1A	Door Monitor
Input 2	Spare Input 2
Input 2A	Spare Input 2A

Output	Functions
Output 1	Door 1
Output 1A	General purpose
Output 2	General purpose
Output 2A	General purpose

4. Click **Test**.



Firmware version: ac225v04_07_03

Bootloader version: btl_ac225v_01_02

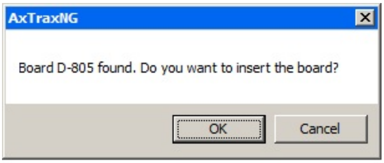
Hardware: AC-225

Supervised Inputs: Yes

Board: MD-IO84

5. Click **Add Board**.

6. After a few moments, the following confirmation appears.



AxTraxNG

Board D-805 found. Do you want to insert the board?

7. Click **OK**.

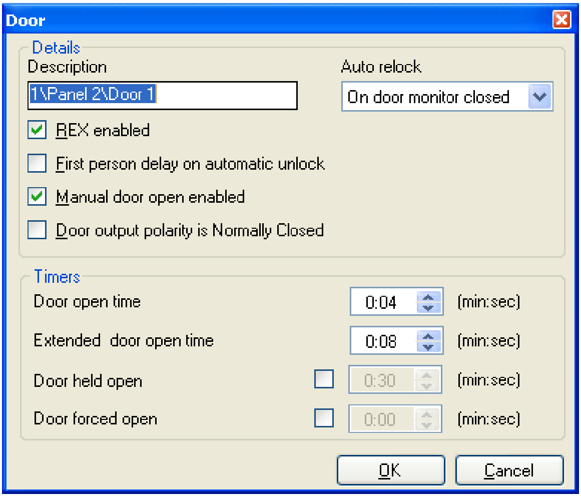
> Note
>
> To remove a board from a panel, you must delete the panel from the database.

5.6 Configuring the Doors

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

The *Door Properties* window displays the following:

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



Door

Details

Description: 1\Panel 2\Door 1

Auto relock: On door monitor closed

☑ REX enabled

□ First person delay on automatic unlock

☑ Manual door open enabled

□ Door output polarity is Normally Closed

Timers

Door open time: 0:04 (min:sec)

Extended door open time: 0:08 (min:sec)

Door held open: □ 0:30 (min:sec)

Door forced open: □ 0:00 (min:sec)

The *Door Properties* window contains the following fields:

Table 8: Network > Panel > Doors > Door Properties

Field	Description
Description	Type a name for the door.
Auto-Relock	Select the event that causes the door to relock automatically.

Field	Description
REX enabled	A Request-to-Exit unlocks the door for a user-defined duration. Select the checkbox 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 the checkbox 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 this checkbox 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 this checkbox 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.
Door held open	Set the duration for which the door can be held open without raising an alarm event. Select the checkbox to use this timer; for the Server application, the Pop-up and Snapshot section opens. **Note: If this feature is enabled, then the Activity start delay (Section 5.8) feature for that door must be set to 0.**
Door forced open	Set the duration after which when the door is forced open, an event occurs. Select the checkbox to use this timer; for the Server application, the Pop-up and Snapshot section opens. **Note: If this feature is enabled, then the Activity start delay (Section 5.8) feature for that door must be set to 0.**

To edit the door properties:

1. In the Tree View, expand the **AC Networks** element.
2. In the Tree View, 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 Properties* window opens.
6. Configure the door as required.
7. 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.

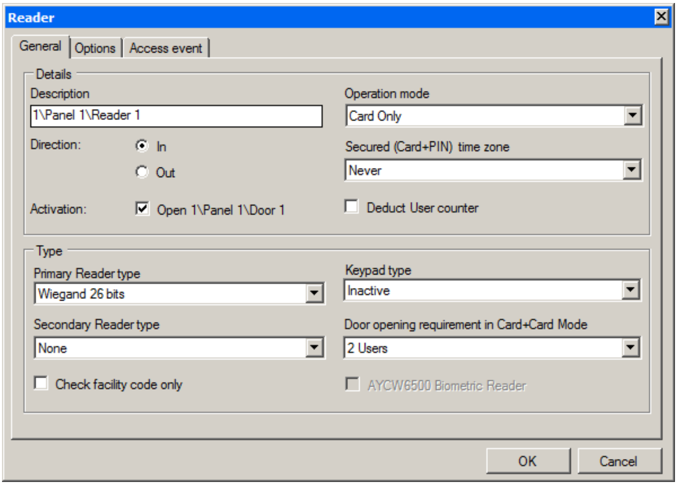
The *Reader Properties* window has three tabs:

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

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



Description: 1\Panel 1\Reader 1

Operation mode: Card Only

Direction: ● In ○ Out

Secured (Card+PIN) time zone: Never

Activation: ☑ Open 1\Panel 1\Door 1

□ Deduct User counter

Primary Reader type: Wiegand 26 bits

Keypad type: Inactive

Secondary Reader type: None

Door opening requirement in Card+Card Mode: 2 Users

□ Check facility code only

□ AYCW6500 Biometric Reader

The *General* tab in the *Reader* window contains the following:

Table 9: Network > Panel > Readers > Reader Properties > General Tab

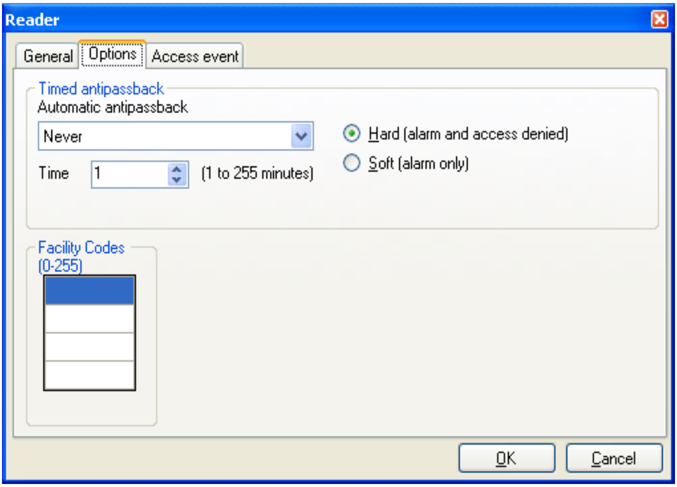
Field	Description
Description	Type the name of the reader
Operation Mode	Select how the reader operates • **Inactive:** The reader is not in use • **Card Only:** The reader uses RFID cards only • **PIN Only:** The reader uses PIN inputs only • **Card or PIN:** The reader uses both cards and PIN codes • **Desktop:** The reader is inactive, but is being used to record new cards on the computer • **No Access Mode:** The reader does not grant access to any users

Field	Description
Direction	Select whether the reader is allowing entry into the area or exit out of the area
Secured (Card+PIN) time zone	Select a time zone during which access should be granted only after both the card and PIN are entered. The PIN must be entered within 10 seconds of card entry. **Note: When using a secured time zone, *Keypad type* must be defined.**
Activation	Select the checkbox 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.
Deduct User Counter	Select the checkbox to record this entry against the user's entry allowance counter (see Section 5.14.2.1)
Primary Reader type	Select the data transmission type for the primary reader hardware
Secondary Reader type	Select the data transmission type for the secondary reader hardware. **Note: This field is used when 2 different types of cards are used.**
Keypad type	Select the data transmission type for the type of keypad hardware
Door opening requirement in Card + Card mode	Select 2 or 3 users needed to open the door in Card + Card mode
Check facility code only	Select the checkbox to allow access to any user assigned to a facility listed in the selected list of facilities. The list of facilities is defined in the *Options* tab.
AYCW6500 Biometric Reader	Select the checkbox to interface with the AYC-W6500 biometric reader and its PC application, BioTrax

5.7.2 Options Tab

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

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



Reader

Timed antipassback

Automatic antipassback: Never

Time: 1 (1 to 255 minutes)

● Hard (alarm and access denied)

○ Soft (alarm only)

Facility Codes (0-255)

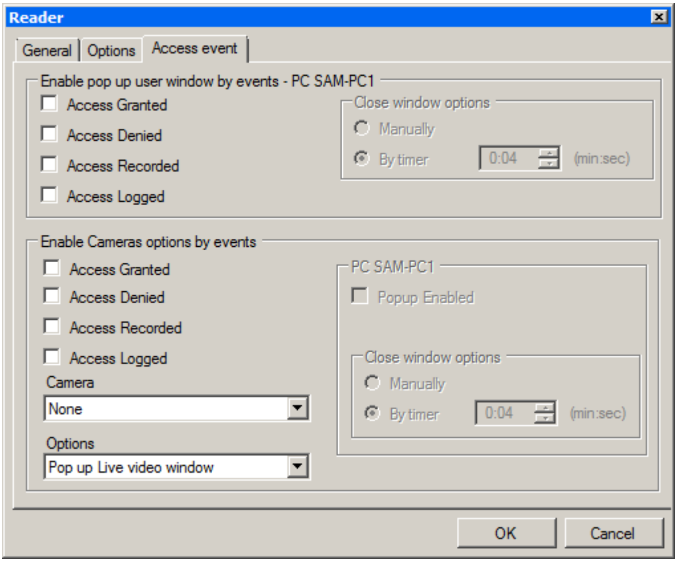
The *Options* tab in the *Reader* window contains the following fields:

Table 10: 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.



Enable pop up user window by events - PC SAM-PC1

□ Access Granted
□ Access Denied
□ Access Recorded
□ Access Logged

Close window options
○ Manually
● By timer 0:04 (min:sec)

Enable Cameras options by events

□ Access Granted
□ Access Denied
□ Access Recorded
□ Access Logged

Camera: None

Options: Pop up Live video window

PC SAM-PC1
□ Popup Enabled

Close window options
○ Manually
● By timer 0:04 (min:sec)

It contains the following fields:

Table 11: Network > Panel > Readers > Reader Properties > Access Event Tab

Field	**Description**
Access Granted	Mark to checkbox to enable a pop-up window for Access Granted event type alerts.
Access Denied	Mark to checkbox to enable a pop-up window for Access Denied event type alerts.
Access Recorded	Mark to checkbox to enable a pop-up window for Access Recorded event type alerts.
Access Logged	Mark to checkbox to enable a pop-up window for Access Logged event type alerts.
Close window Options	Once a pop-up is enabled, the close window options are available. Select one of two options: • **Manually:** The operator is required to manually close the pop-up window. • **By timer:** The pop-up window closes automatically based on the predefined timer.
Camera (available only with AC-525)	Select the name of the camera that takes snapshots or that appears when triggered by this reader. For example, the camera named 1\Panel 1\Camera A AC-525.

To configure a reader:

1. In the Tree View, expand the **AC Networks** element.
2. In the Tree View, 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 above subsections.
7. Click **OK**.

5.8 Configuring the Inputs

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

The *Input Properties* 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.

The *Input Properties* table contains the following fields:

Table 12: Network > Panel > Inputs > Input Properties

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

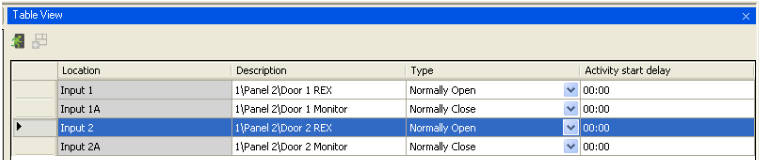
Field	Description
Function	Select the door function: **Door Monitor** or **Door REX** This column is visible only if the **REX enable** checkbox is selected in Door properties.

To configure an input:

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

   The available inputs are listed in the display area
4. Select an input from the display area.
5. On the toolbar, click the icon.

   The *Input Properties* window opens.



	Location	Description	Type	Activity start delay
	Input 1	1\Panel 2\Door 1 REX	Normally Open	00:00
	Input 1A	1\Panel 2\Door 1 Monitor	Normally Close	00:00
▸	Input 2	1\Panel 2\Door 2 REX	Normally Open	00:00
	Input 2A	1\Panel 2\Door 2 Monitor	Normally Close	00:00

6. Select an input and configure it as required.

5.9 Adding Video Integration

See Chapter 7.

5.10 Adding Panel Links

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

The *Link Properties* 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

The *Add Link* window contains the following fields:

Table 13: AC Networks > Network > Panel > Links > Add 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-525 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 the checkbox to enable the link rule
Generate Alarm	Select the checkbox to generate an alarm event in addition to the link rule activity
Open all Outputs of selected Output group	Select the checkbox to enable global triggering of an output group This checkbox appears when Destination Type is **Output Group**.
Destination Panel	From the AC-825IP 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 *Destination Type* is specified.
Time Zone	Select the time zone for which the link rule applies
PTZ Preset position (available with AC-525)	Set the default preset PTZ (Pan, Tilt, Zoom) camera position **Note: To activate this feature, you must set the preset to ViTrax.**

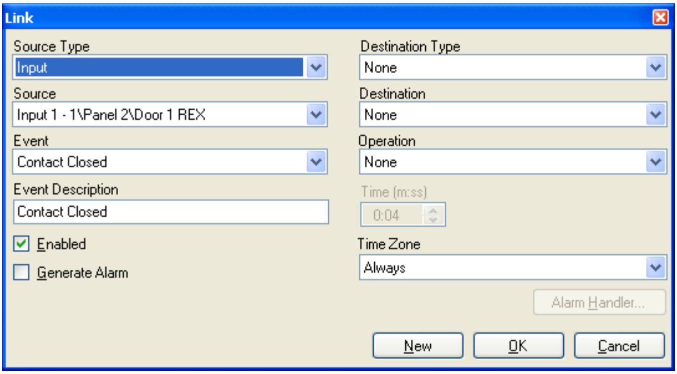
Field	Description
Alarm Handler	Opens the Alarm Handler configuration window, which contains the following fields: • **Alarm Message:** Type a personalized message to be displayed on the screen as an alarm message when the selected event occurs • **Popup Enabled:** Select the checkbox to enable an alarm 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 the checkbox to enable sound for the alarm • **Fire Input Alarm:** Select this checkbox to open all outputs, usually relevant for fire alarms The Alarm Handler function is only enabled when **Generate Alarm** is selected. In addition, when a camera is linked to a panel, the following fields appear in the window: • **Camera**: List of available cameras • **Options**: How the alarm is displayed • **Popup Enabled**: Activates a popup to appear on the user's screen when alarm is triggered • **Close window options**: Can select **By timer** and specify the time, or Manually

Numerous events and links can be defined in Panel Links. It is the operators' responsibility to avoid conflicting or non-logical definitions. Not all events sources that appear in the *Links* 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.

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 *Add Link* window opens.



Link

Source Type: Input

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

Event: Contact Closed

Event Description: Contact Closed

☑ Enabled

□ Generate Alarm

Destination Type: None

Destination: None

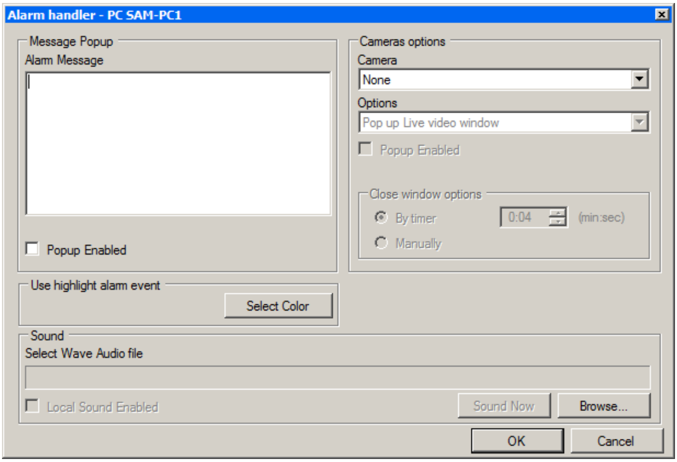
Operation: None

Time (m:ss): 0:04

Time Zone: Always

5. Configure the link rule as required, according to the field descriptions in the Table 13.
6. Select **Generate Alarm** to activate the Alarm Handler button.
7. Click **Alarm Handler**.

   The *Alarm Handler* window opens.



Alarm handler - PC SAM-PC1

Message Popup

Alarm Message:

□ Popup Enabled

Use highlight alarm event

Sound

Select Wave Audio file:

□ Local Sound Enabled

Cameras options

Camera: None

Options: Pop up Live video window

□ Popup Enabled

Close window options

● By timer 0:04 (min:sec)

○ Manually

8. Configure the alarm handler as required, according to the field descriptions in Table 13 above.
9. Click **OK** to close the *Alarm handler* window and return to the *Link* window.
10. Click **OK** to close the *Link* window and save the link rule configuration.

5.10.1 Creating a Fire Alarm Input

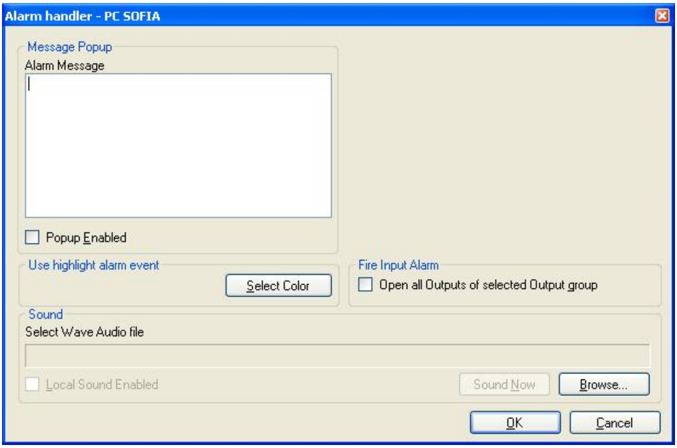
You can configure the panel properties to generate a fire alarm warning.

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 *Add Link* window opens.
5. Configure the link as follows:
   a. In **Source Type**, select **Input**.
   b. In **Destination Panel**, select the relevant panel.
   c. In **Destination Type**, select **Output Group**.
   d. In **Operation**, select **Timer**.
   e. 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 13 above.
8. Select **Open all Outputs of selected Output group**.
9. Click **OK** to close the *Alarm handler* window and return to the Add *Link* window.
10. Click **OK**.

5.10.2 Global Triggering of Output Groups

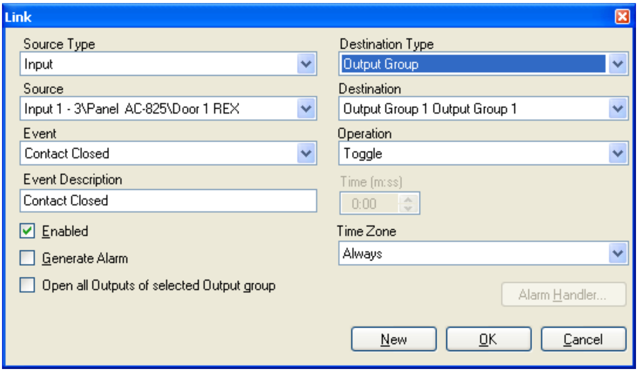
Global triggering is used for cross panel activations. For example, in case of fire alarm, all doors in the system are opened from a single input.

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 *Add Link* window opens.
5. Configure the link as follows:
   a. In **Source Type**, select **Input**.
   b. In **Destination Type**, select **Output Group**.

      Select **Open all Outputs of selected Output group**, which is now visible.



Link

Source Type: Input

Source: Input 1 - 3\Panel AC-825\Door 1 REX

Event: Contact Closed

Event Description: Contact Closed

☑ Enabled

☐ Generate Alarm

☐ Open all Outputs of selected Output group

Destination Type: Output Group

Destination: Output Group 1 Output Group 1

Operation: Toggle

Time (m:ss): 0:00

Time Zone: Always

5.11 Creating 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.

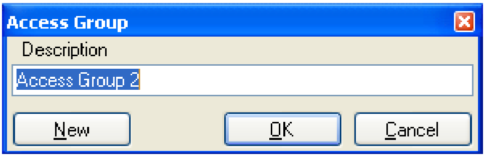
5.11.1 Adding Access Groups

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.

The *Add Access Group* window opens.



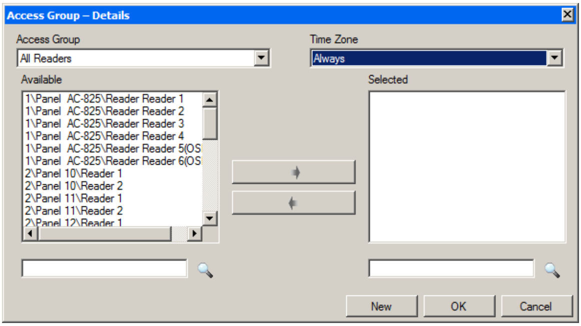
Description: Access Group 2

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.



Access Group: All Readers

Time Zone: Always

Available:

1\Panel AC-825\Reader Reader 1
1\Panel AC-825\Reader Reader 2
1\Panel AC-825\Reader Reader 3
1\Panel AC-825\Reader Reader 4
1\Panel AC-825\Reader Reader 5(OS
1\Panel AC-825\Reader Reader 6(OS
2\Panel 10\Reader 1
2\Panel 10\Reader 2
2\Panel 11\Reader 1
2\Panel 11\Reader 2
2\Panel 12\Reader 1

Selected:

6. From the *Time zone* dropdown, select a time.
7. Select and move the desired readers from **Available** to **Selected** using the arrows.
8. Click **OK**.

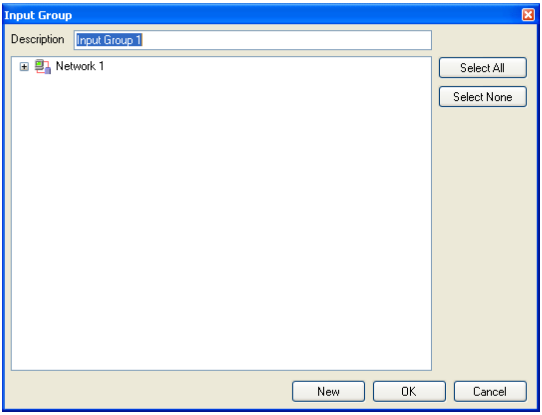
5.11.2 Adding Input Groups

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.

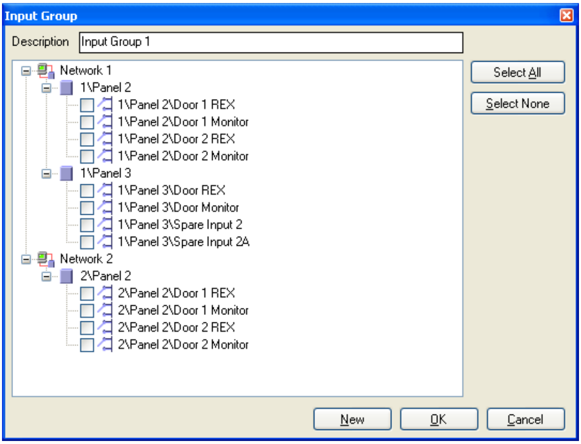
The *Input Group* window opens.



Description: Input Group 1

Network 1

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



Description: Input Group 1

- Network 1
  - 1\Panel 2
    - □ 1\Panel 2\Door 1 REX
    - □ 1\Panel 2\Door 1 Monitor
    - □ 1\Panel 2\Door 2 REX
    - □ 1\Panel 2\Door 2 Monitor
  - 1\Panel 3
    - □ 1\Panel 3\Door REX
    - □ 1\Panel 3\Door Monitor
    - □ 1\Panel 3\Spare Input 2
    - □ 1\Panel 3\Spare Input 2A
- Network 2
  - 2\Panel 2
    - □ 2\Panel 2\Door 1 REX
    - □ 2\Panel 2\Door 1 Monitor
    - □ 2\Panel 2\Door 2 REX
    - □ 2\Panel 2\Door 2 Monitor

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.

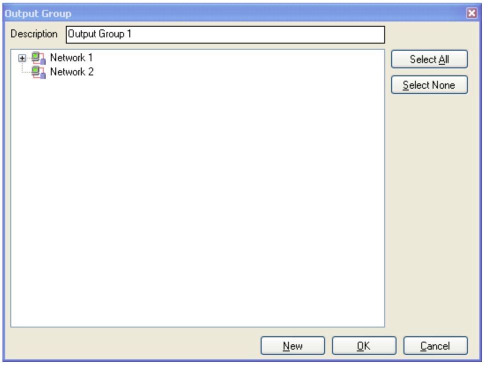
5.11.3 Adding Output Groups

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:

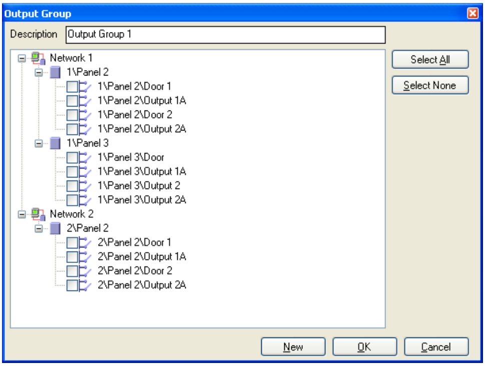
1. In the Tree View pane, expand the **Groups** element.
2. Select **Outputs Groups**.
3. On the toolbar, click the + icon.

   The *Output Group* window opens.



Description: Output Group 1

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



Description: Output Group 1

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

   The window closes and the new output group appears in the display area.

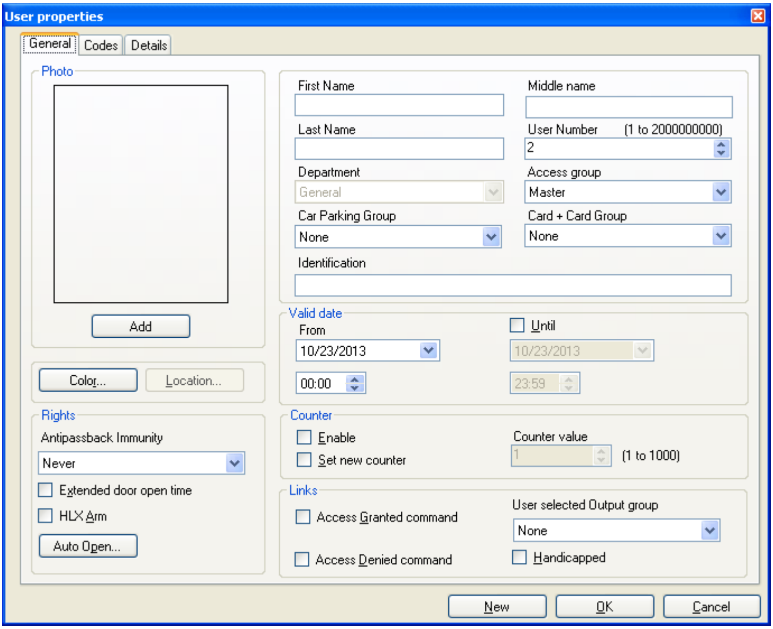
5.11.3.1 Auto Opening for Output Groups

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

To set up 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.

   The *Add User* window opens.



First Name:
Middle name:
Last Name:
User Number (1 to 2000000000): 2
Department: General
Access group: Master
Car Parking Group: None
Card + Card Group: None
Identification:

Valid date
From: 10/23/2013 00:00
□ Until: 10/23/2013 23:59

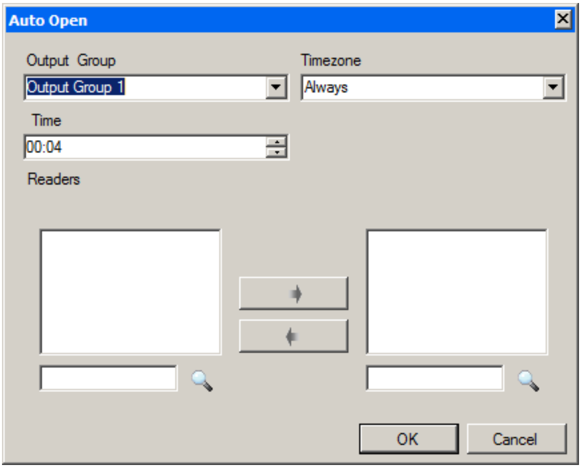
Rights
Antipassback Immunity: Never
□ Extended door open time
□ HLX Arm

Counter
□ Enable
□ Set new counter
Counter value: 1 (1 to 1000)

Links
□ Access Granted command
□ Access Denied command
User selected Output group: None
□ Handicapped

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

5. The *Auto Open* window opens.



Output Group: Output Group 1

Timezone: Always

Time: 00:04

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

5.11.4 Defining Card + Card Groups

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

> Note
> This feature is only available to Access Control panels AC-225, AC-425, and AC-525.

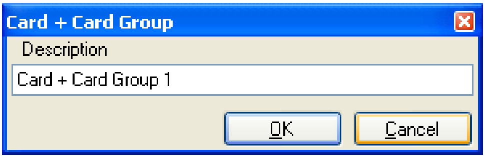
5.11.4.1 Adding a Card + Card Group

First, you must add a Card + Card group.

To add a Card + Card group:

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

   The *Card + Card Group* window opens.



Description: Card + Card Group 1

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.

5.11.4.2 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 Table View area.
3. On the toolbar, click the icon.
4. In 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.

5.12 Adding Users and Cards

The AxTraxNG database maintains a list of every user card or PIN that has ever been assigned. The *Add Users and Cards* window is used to define:

- 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

The *Add Users and Cards* window contains the following fields:

Table 14: Cards > Add Users and Cards Window

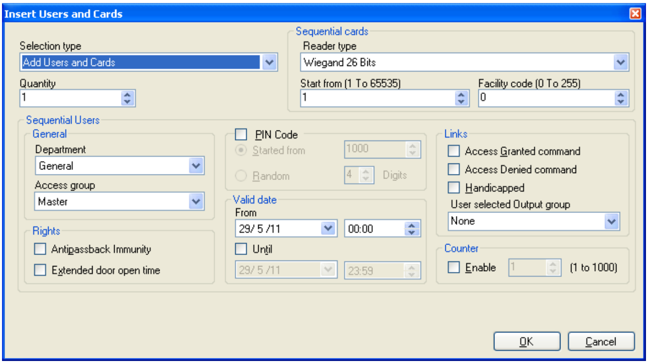
Field	Description
Selection Type	Select what will be added: Users and cards, Users only, or Cards only
Quantity	Type or select the number of cards/users to add
Sequential cards	Define the card properties: • **Reader Type:** Select the type of reader appropriate for the new cards being added • **Start from:** Type the number of the first card in the set • **Facility code:** Type the site code for these cards. This field is not available for all reader types
Sequential Users > General	Define the users general properties: • **Department:** Associate to the new user(s) created to a department • **Access Group:** Associate to the new user(s) created to an Access group

Field	Description
Sequential Users > Rights	Define the users right properties: • **Antipassback immunity:** Select the checkbox to override any antipassback restrictions • **Extended door open time:** Select the checkbox to activate the extended door option defined for each door
Sequential Users > PIN Code	Select the checkbox to define automatic pin codes, select between: • **Start from:** Sequential pin code starting from a predefined number based on a defined number of digits • **Random:** Random pin codes where the only definition is the number of PIN code digits
Sequential Users > Valid date	Define the access right validity: • **From:** Define the date and time to begin allowing access • **Until:** Select the checkbox to define an end date for the access right validity, then define the date and time
Sequential Users > Links	Select the checkbox to define associated link commands: • **Access Granted command:** Activate a user-defined set of inputs or outputs for access granted events • **Access Denied command:** 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. The operations, inputs, and outputs are defined in the Links window (see Section 5.10).
Sequential Users > Counter	Select *Enable* to use the counter option then type or select the counter number to be used for the first user

To add users and cards:

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

The *Add Users and Cards* window opens.



Insert Users and Cards

Selection type: Add Users and Cards

Quantity: 1

Sequential cards

Reader type: Wiegand 26 Bits

Start from (1 To 65535): 1

Facility code (0 To 255): 0

Sequential Users

General

Department: General

Access group: Master

Rights

□ Antipassback Immunity

□ Extended door open time

□ PIN Code

○ Started from 1000

○ Random 4 Digits

Valid date

From: 29/ 5 /11 00:00

□ Until 29/ 5 /11 23:59

Links

□ Access Granted command

□ Access Denied command

□ Handicapped

User selected Output group: None

Counter

□ Enable 1 (1 to 1000)

3. Configure the user and card properties as required, according to the field descriptions in Table 14 above.
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.

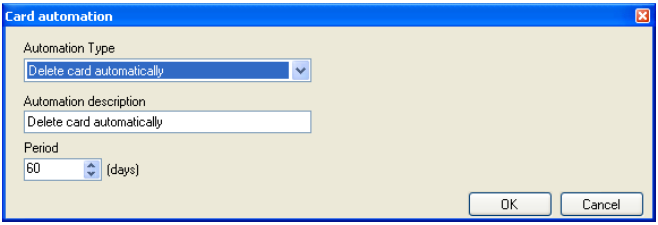
5.12.1 Setting Card Automation

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.



Card automation

Automation Type: Delete card automatically

Automation description: Delete card automatically

Period: 60 (days)

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
   - Report in System Event Log only

5. From the **Period** spin box, select the time period.
6. Click **OK**.

5.13 Card Design

See Chapter 6 for how to create and print card templates.

5.14 Adding Departments, Users, and Visitors

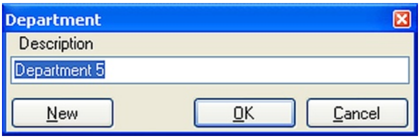
Every user is associated with a department. For each user, AxTraxNG stores contact details, associated card details, and access rights.

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.



Department

Description

Department 5

3. In the **Description** field, enter a name for the department and click **OK**.

   The window closes and a new department is created.

5.14.2 Adding Users

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

The *User Properties* window contains three main tabs (Figure 2):

- *General* tab – Displays identification and control information
- *Codes* tab – Displays card information associated with the user
- *Details* tab – Records user contact details

In addition, there are two content-oriented windows:

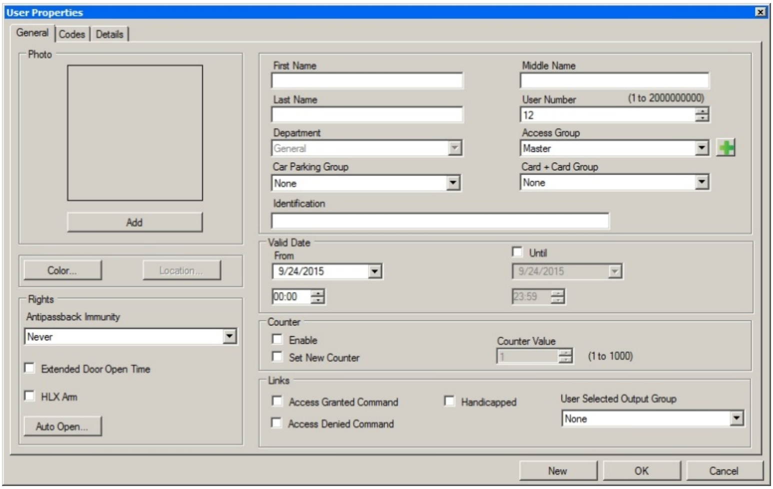
- *User Fields* – Stores user-defined data
- *Visitor* Tab – Appears when the user is defined as a visitor (Section 5.14.3)

5.14.2.1 General Tab

The General tab displays:

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

Figure 2: User Properties > General Tab



First Name
Middle Name
Last Name
User Number (1 to 2000000000): 12
Department: General
Access Group: Master
Car Parking Group: None
Card + Card Group: None
Identification

Valid Date
From: 9/24/2015 00:00
□ Until: 9/24/2015 23:59

Counter
□ Enable
□ Set New Counter
Counter Value: 1 (1 to 1000)

Rights
Antipassback Immunity: Never
□ Extended Door Open Time
□ HLX Arm
Auto Open...

Links
□ Access Granted Command
□ Access Denied Command
□ Handicapped
User Selected Output Group: None

The *General* tab contains the following fields:

Table 15: Departments/Users > Department > User Properties > General Tab

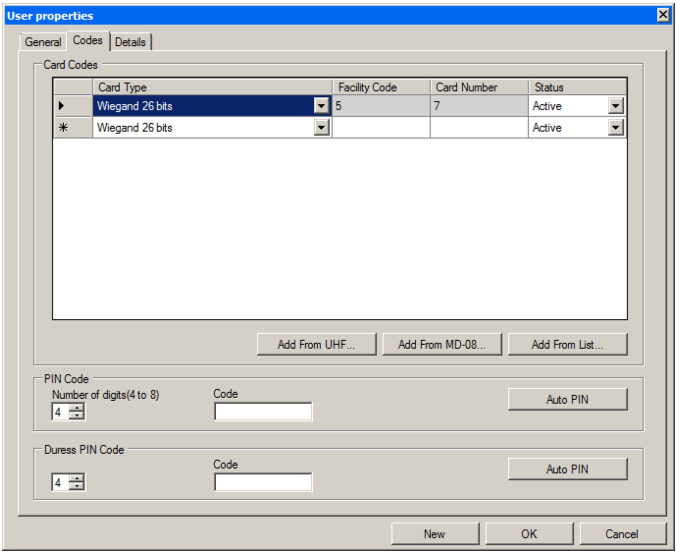
Field	Description
Photo > Add	Click to add a photo of the user, or to remove an existing photo. The selected photo aspect ratio should be 1.25 H x 1.00 L; otherwise, the photo may be distorted.
First Name	Type the user's first name.
Middle Name	Type the user's middle name.
Last Name	Type the user's last 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. Click ✚ to add the user to a custom access group within all available readers.
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.

Field	Description
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.
Counter > Enable	Select the checkbox 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 the checkbox 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 *Set new counter* checkbox is selected.
Rights > Antipassback immunity	Select the checkbox to override any Antipassback restrictions for this user.
Rights > Extended door open time	Select the checkbox to entitle this user to an extended unlocked door duration. The extended duration is set for each door (see Section 5.6).
Rights > HLX Am	Gives the user the right to arm/disarm an HLX panel (see the *AxTraxNG™ Intrusion Integration Manual*)
Rights > Auto Open	When defining user properties, you can define certain output groups to be active automatically. See Section 5.11.3.1
Links > Access Granted command	Select the checkbox to activate a link rule initiated by access granted commands for this user (see Section 5.10).
Links > Access Denied command	Select the checkbox to activate a link rule initiated by access denied commands for this user (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 *Links* window (see Section 5.10).
Links > Handicapped check-box	Select the checkbox to activate a dedicated output a short time after the door is unlocked (see Section 5.10).

5.14.2.2 Codes Tab

The *Codes* tab displays:

- The cards assigned to this user (up to 16 cards)
- The PIN code assigned to this user



	Card Type	Facility Code	Card Number	Status
▸	Wiegand 26 bits	5	7	Active
*	Wiegand 26 bits			Active

PIN Code: Number of digits(4 to 8): 4; Code:

Duress PIN Code: 4; Code:

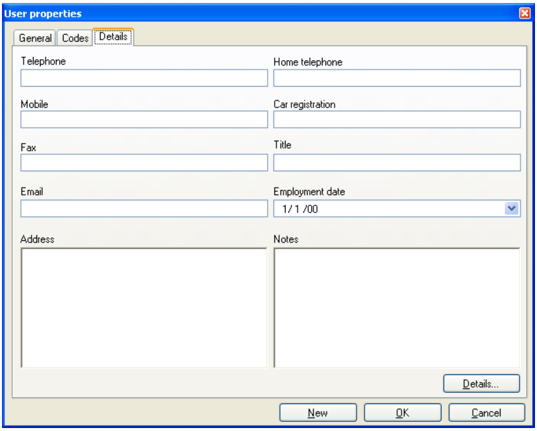
The *Codes* tab contains the following fields:

Table 16: Departments/Users > Department > User Properties > Codes Tab

Field	Description
Card Codes	Define card codes options: • **Card Type:** The card type used by the reader/user • **Facility Code:** The site code assigned to this card • **Card Number:** The unique number of this card • **Status:** Select the status of the card. Inactive cards cannot gain access to the facility
Add from UHF	Click to read card details using UHF Desktop Programmer
Add from MD-D08	Click to read card details using MD-D08 module
Add from list	Click to add a new card All cards within the user's specified Facility code, are listed
PIN/Duress PIN Code	Define PIN and Duress PIN code options: • **Number of digits:** Select the length of the PIN for this user • **Code:** The 4- to 8-digit PIN and/or Duress PIN code • **Auto PIN**: 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.



Employment date: 1/ 1 /00

The *Details* tab contains the following fields:

Table 17: 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.
Address	Type a postal address for the user.
Home telephone	Type a home telephone number for the user.
Car registration	Type the user's license plate number.
Title	Type the user's title (e.g. "Mr.").
Employment Date	Enter the date that the user joined the firm.
Notes	Type any additional information.
Details	Click to open the user's additional details folder.

5.14.2.4 User Fields Tab

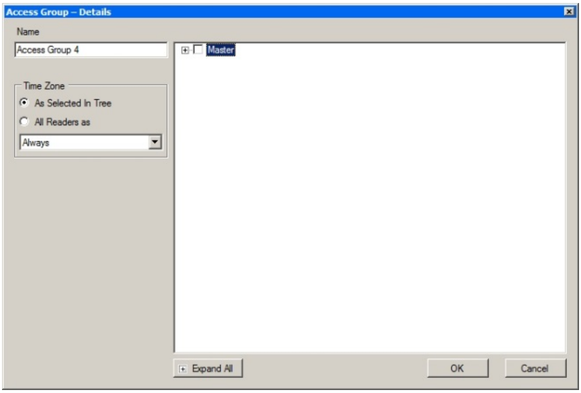
The User Fields tab can be used to store any information required by the system operator.

User fields are defined in the *Tools > Options > User Fields/Default* tab (see Section 11.5.2).

To add a 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 *Add User* window opens.
4. Enter the user details as needed using the tabs described in the above subsections.
5. In addition, you can click the ✚ next to Access Group to open the following window, where you can select to which access panels that access group is granted permission.



6. Click **OK**.

   The window closes and the added user is displayed.

5.14.3 Adding Visitors

AxTraxNG stores contact details for each visitor, associated card details, and visitor access rights.

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

Table 18: Departments/Users > Visitors > Add User > Visitor's Options Tab

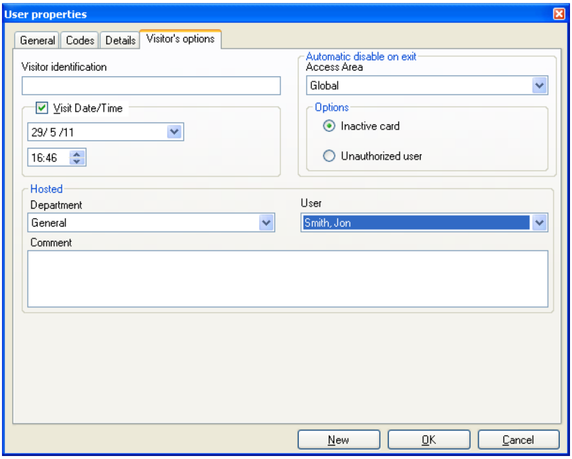
Field	Description
Visitor Identification	Type a unique visitor identification
Visit Date/Time	Select the checkbox and specify the date and time for the visit

Field	Description
Automatic disable on exit	Define automatic disable access right options: • **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: • **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 *Add User* window as before opens; however, now the *Visitor's Options* tab is available.



User properties

General | Codes | Details | Visitor's options

Visitor identification:

☑ Visit Date/Time: 29/ 5 /11, 16:46

Automatic disable on exit
Access Area: Global
Options: ● Inactive card ○ Unauthorized user

Hosted
Department: General
User: Smith, Jon
Comment:

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 added visitor is displayed.

> 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.

5.15 Adding Access Areas

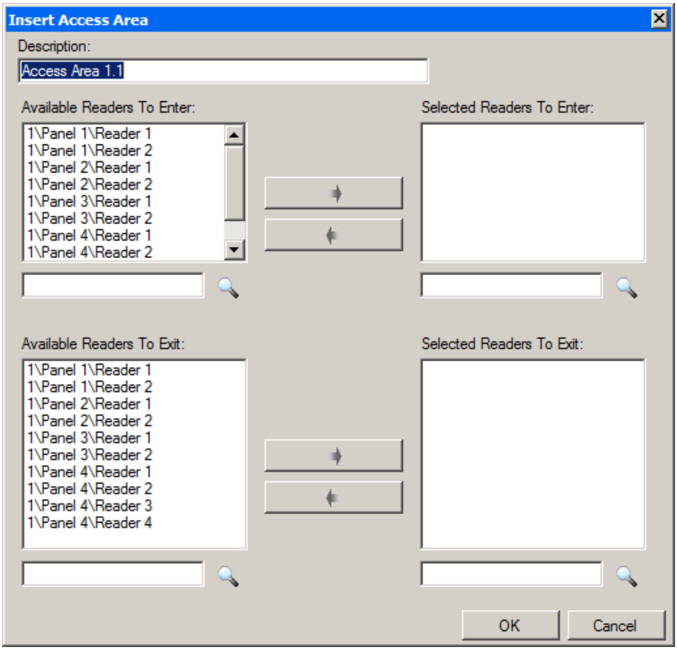
A large site can be divided into several smaller, more manageable access areas. Reports can be produced individually for each area. In addition, global Antipassback rules can be applied for each access area. When global Antipassback rules are in effect, users cannot re-enter an access area until they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

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

To add an access area:

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

   The *Add Access Area* window opens.



Insert Access Area

Description: Access Area 1.1

Available Readers To Enter:
1\Panel 1\Reader 1
1\Panel 1\Reader 2
1\Panel 2\Reader 1
1\Panel 2\Reader 2
1\Panel 3\Reader 1
1\Panel 3\Reader 2
1\Panel 4\Reader 1
1\Panel 4\Reader 2

Selected Readers To Enter:

Available Readers To Exit:
1\Panel 1\Reader 1
1\Panel 1\Reader 2
1\Panel 2\Reader 1
1\Panel 2\Reader 2
1\Panel 3\Reader 1
1\Panel 3\Reader 2
1\Panel 4\Reader 1
1\Panel 4\Reader 2
1\Panel 4\Reader 3
1\Panel 4\Reader 4

Selected Readers To Exit:

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.

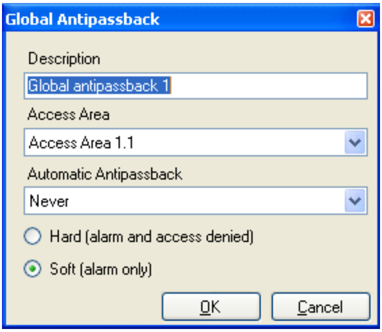
5.16 Adding Global Antipassback Rules

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

To create antipassback rules:

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

   The *Add Global Antipassback* window opens.



Global Antipassback

Description: Global antipassback 1

Access Area: Access Area 1.1

Automatic Antipassback: Never

○ Hard (alarm and access denied)

● Soft (alarm only)

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.

5.17 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.

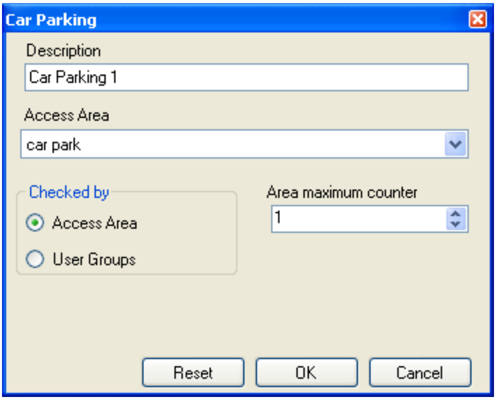
Note This feature is only available to access control panels AC-225, AC-425, and AC-525.

Note Only one car park area can be added per panel.

To define a car parking area:

1. Create an access area with Enter and Exit readers (see Section 5.15).
2. In the Tree View, select **Car Parking**.
3. On the toolbar, click the ✚ icon.

   The *Car Parking* window opens.



Car Parking

Description: Car Parking 1

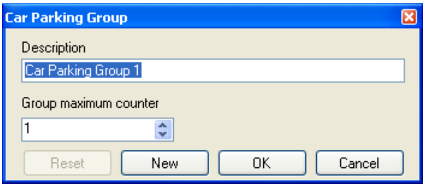
Access Area: car park

Checked by: ● Access Area ○ User Groups

Area maximum counter: 1

4. In *Description*, enter a name of the car parking element.
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, under **Car Parking**, select the car parking area you just created.
      iii. On the toolbar, click the ✚ icon.

      The *Car Parking Group* window opens.



Car Parking Group

Description: Car Parking Group 1

Group maximum counter: 1

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 Table View area.

ix. On the toolbar, click the icon.

x. In 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**.

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.

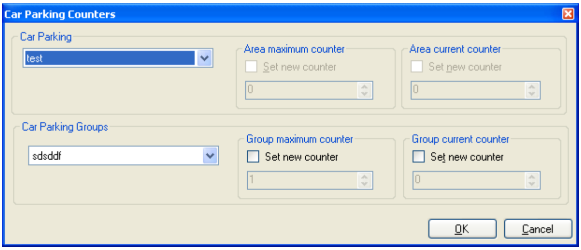
5.17.1 Viewing and Editing Car Parking Counters

Once you set up your various car parking groups and areas, 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.



Car Parking Counters

Car Parking: test

Area maximum counter: □ Set new counter 0

Area current counter: □ Set new counter 0

Car Parking Groups: sdsddf

Group maximum counter: □ Set new counter 1

Group current counter: □ Set new counter 0

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 5.17.

3. Click **OK**.

5.18 Adding Operators

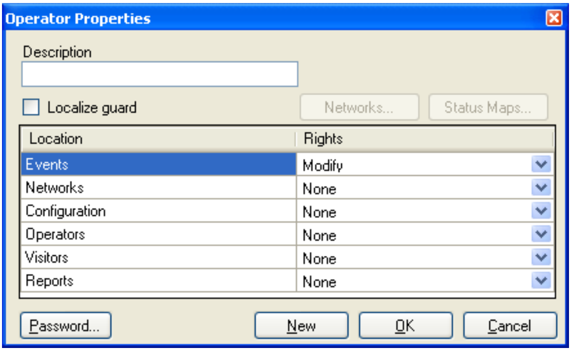
Operators are people with access to the AxTraxNG application. The default operator name is Administrator.

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 Add *Operator* window opens.

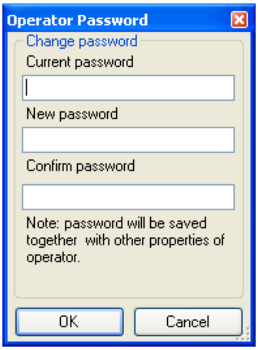


Description

□ Localize guard

Location	Rights
Events	Modify
Networks	None
Configuration	None
Operators	None
Visitors	None
Reports	None

3. In the *Description* field, enter the Operator's name.
4. Select **Localize guard** to define the operator with limited rights.
5. Click **Networks…** and **Status maps…** to define the associated operator's local rights.
6. Set the operators global permission rights for each of the screens in the *Location* list.
7. Click **Password…** to open the *Password* dialog.



Note: password will be saved together with other properties of operator.

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

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

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

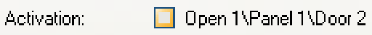
   The dialog closes and the operator is shown in the display area.

5.19 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 5.7) 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 5.11.3).

   Each output group represents a floor or several floors.

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

6. In 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.

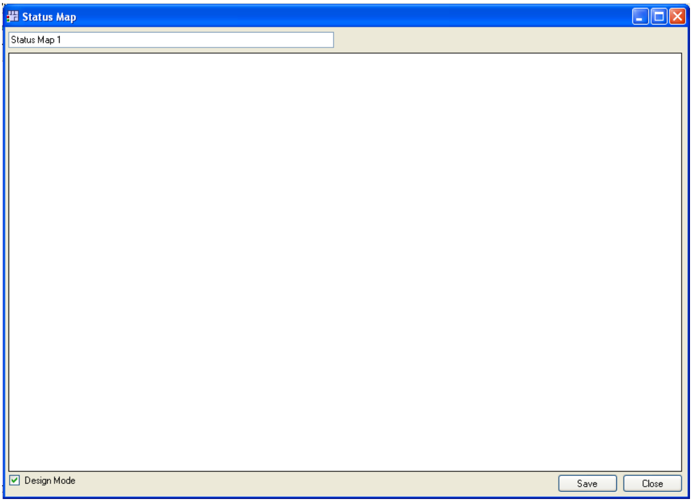
5.20 Creating Status Maps

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.

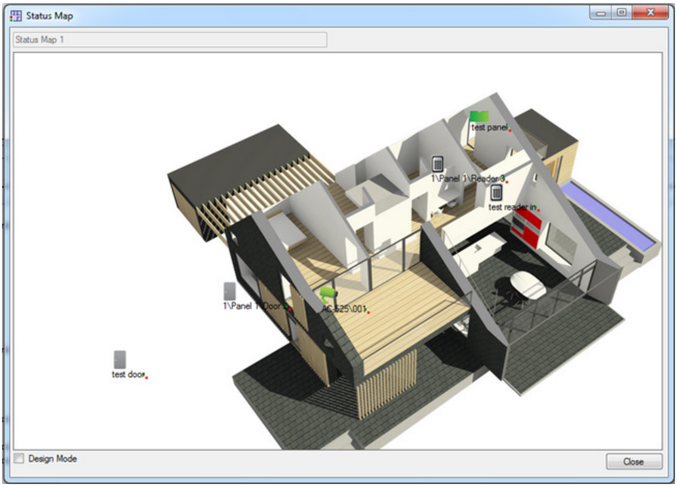


3. Right-click in the window and select **Set background** from the shortcut menu.

   The *Select Picture File* window opens.

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

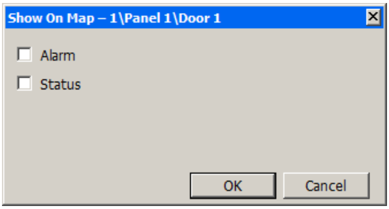
4. Select a graphic file (bmp, jpg, gif, or tiff) for the Status Map background.



5. Ensure that **Design Mode** is checked.
6. 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 position.
7. Right-click a map object and select **Show on Map** from the shortcut menu.

   The *Show on Map* window opens.

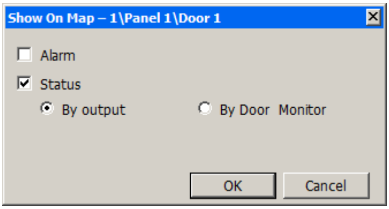


Show On Map – 1\Panel 1\Door 1

☐ Alarm

☐ Status

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



Show On Map – 1\Panel 1\Door 1

☐ Alarm

☑ Status

● By output ○ By Door Monitor

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.

> Note
>
> The alarm option is only available for panel elements where the alarm was already defined.

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.

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

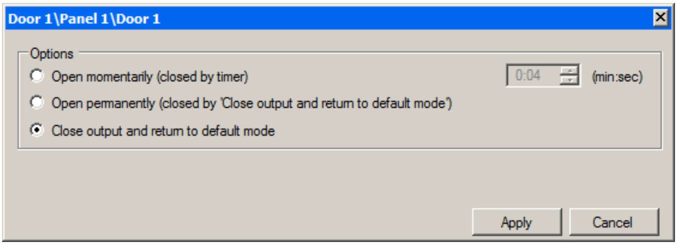
5.20.1 Manually Opening a Door from Status Map

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.



Door 1\Panel 1\Door 1

Options

○ Open momentarily (closed by timer) 0:04 (min:sec)

○ Open permanently (closed by 'Close output and return to default mode')

● Close output and return to default mode

   The available options are the same as those in Section 9.1.
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.

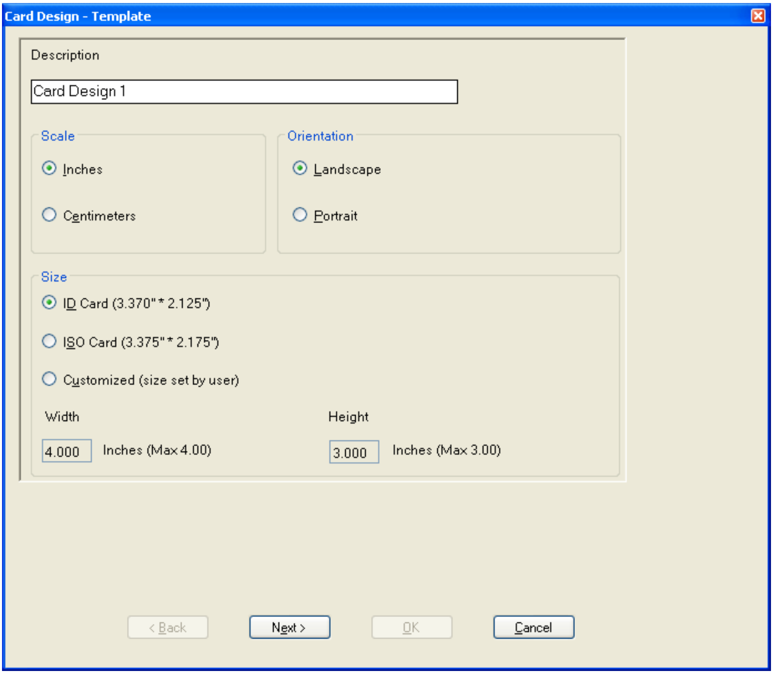
This chapter instructs installers and users how to use the Card Design element.

6.1 Creating a Card Template

To create a card template:

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

   The *Card Design - Template* screen opens.



Card Design - Template

Description

Card Design 1

Scale

● Inches

○ Centimeters

Orientation

● Landscape

○ Portrait

Size

● ID Card (3.370" * 2.125")

○ ISO Card (3.375" * 2.175")

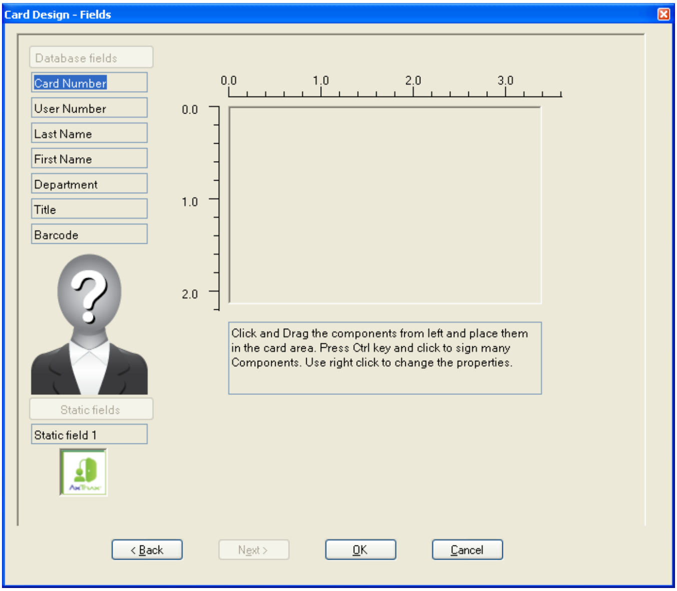
○ Customized (size set by user)

Width: 4.000 Inches (Max 4.00)

Height: 3.000 Inches (Max 3.00)

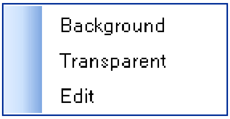
3. Enter a description for the template and define the scale, orientation, and size.
4. Click **Next**.

The *Card Design - Fields* screen opens.



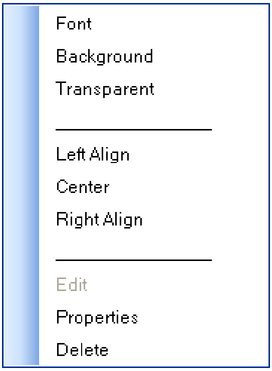
Click and Drag the components from left and place them in the card area. Press Ctrl key and click to sign many Components. Use right click to change the properties.

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

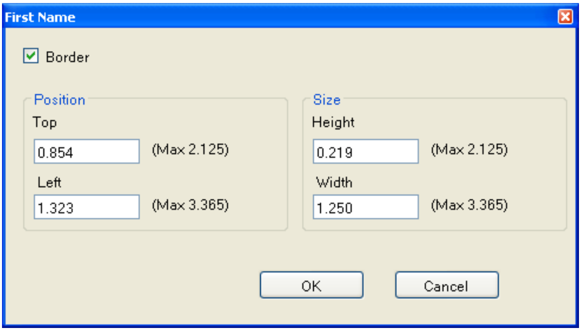


6. As desired, drag the fields on the left into the card area to create the layout of the card.

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



8. Select **Properties** to remove the border and change the field size.



First Name

☑ Border

Position

Top: 0.854 (Max 2.125)

Left: 1.323 (Max 3.365)

Size

Height: 0.219 (Max 2.125)

Width: 1.250 (Max 3.365)

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

6.2 Printing a Card

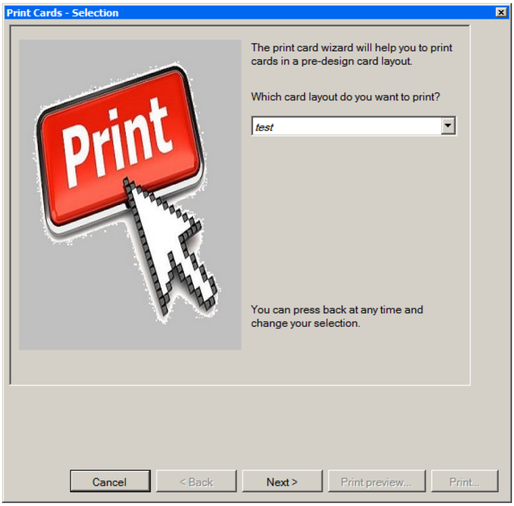
Once you have saved a card template, you can print cards using the template.

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 Table View area, select the template you wish to use and click the 🏷 icon.

   The *Print Card – Selection* window opens.



Print Cards - Selection

The print card wizard will help you to print cards in a pre-design card layout.

Which card layout do you want to print?

test

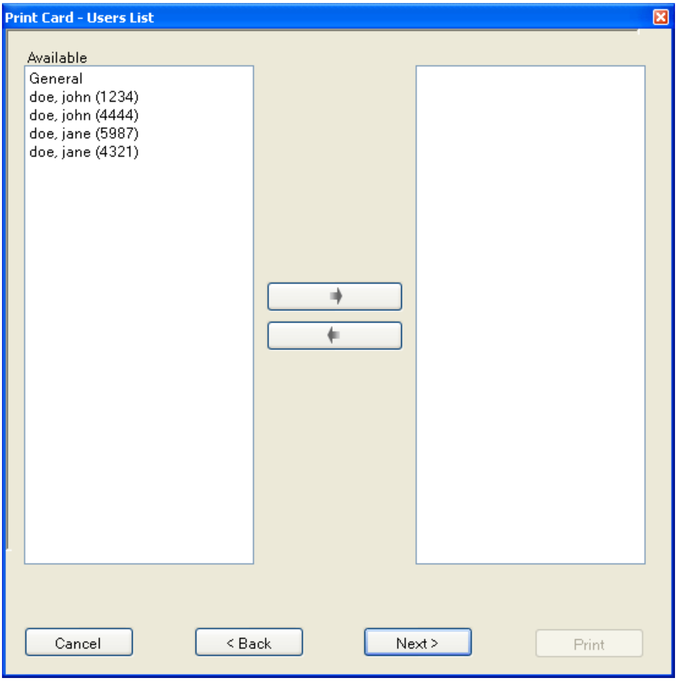
You can press back at any time and change your selection.

2. Select the layout you wish to use (if different than what you selected in

Step 1 from the corresponding dropdowns.

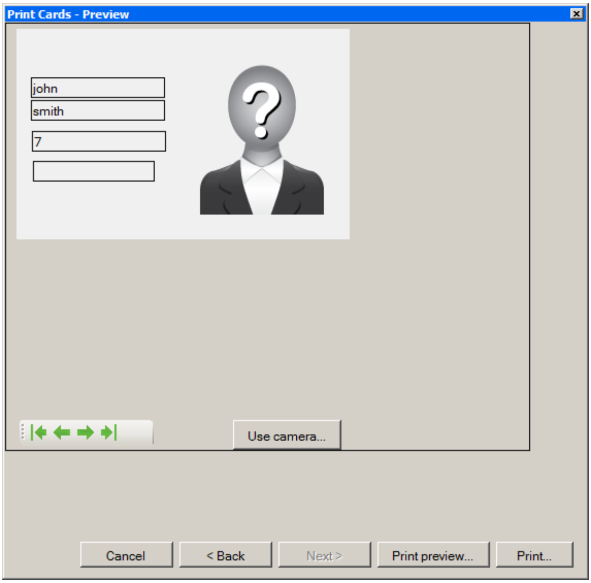
3. Click **Next**.

   The *Print Card – Users List* screen opens.



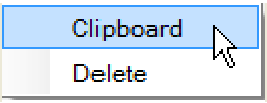
4. Select the users from the available list for whom you wish to print a card and move them to the right panel.
5. Click **Next**.

The *Print Card – Preview* screen opens.

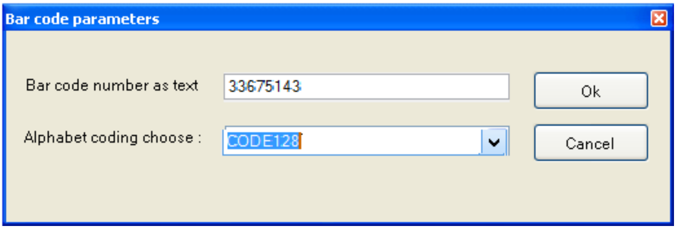


6. Set up the barcode:

   a. Right-click on the Barcode field and select **Clipboard**.



The *Barcode Parameters* window opens.



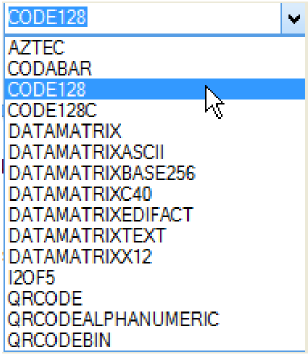
Bar code parameters

Bar code number as text: 33675143

Alphabet coding choose : CODE128

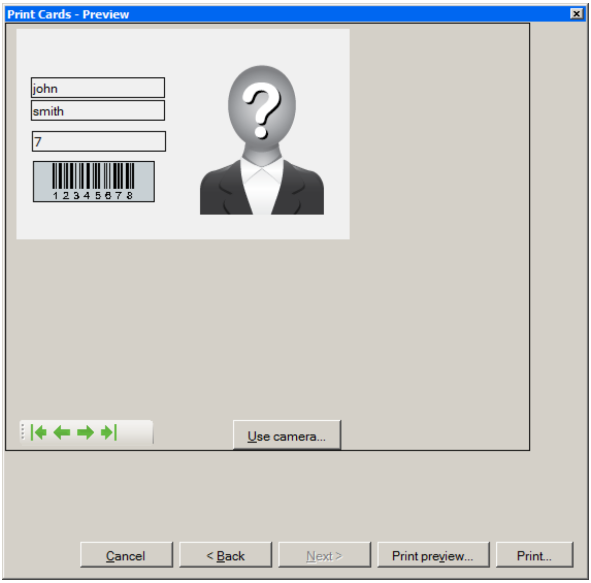
   b. You can use the barcode that is generated automatically or enter a numeric barcode manually.

c. From the **Alphabet coding** dropdown, select the kind of coding.



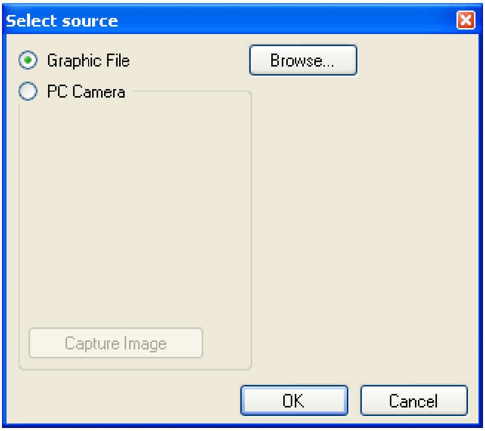
d. Click **OK**.

The barcode appears on the card template.



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

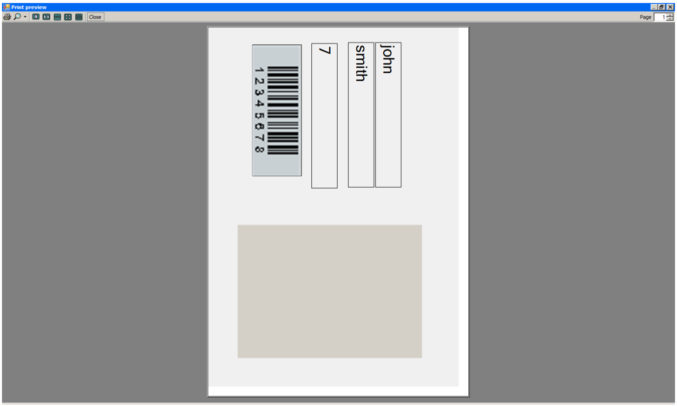
The *Select Source* window opens.



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.



10. Click **Print** to print a card.
11. Repeat the steps for each card to be printed.

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 AC-525, as well as 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.

Refer to the *ViTrax™ Software Installation Manual* for installation and user instructions.

8. Intrusion Integration

The intrusion integration allows you to integrate the intrusion panel into the AxTraxNG access control management software and to manage the intrusion panel (when available). In addition, the integration creates logical event links between the software and the access control system.

Refer to the *AxTraxNG™ Intrusion Integration Manual* for installation and user instructions.

9. Manual Operation

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

> Note
>
> Door Manual Operation can only control doors that have been set as “Manual Door Open Enabled” in the *Door Properties* window (see Section 5.4.2).

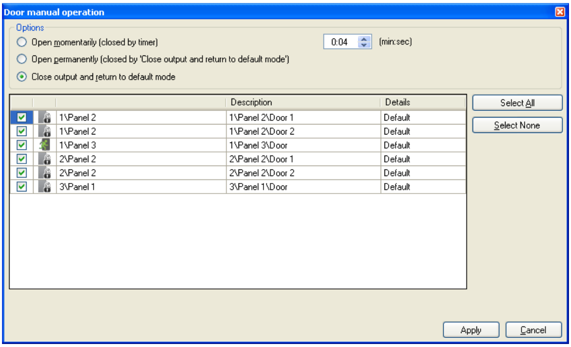
9.1 Controlling the Door Manually

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. In the Tree View, expand a network and expand a panel.
3. Select **Doors**.
4. On the toolbar, click the 🏃 icon.

   The *Manual Door Operation* window opens.



Options

○ Open momentarily (closed by timer) 0:04 (min:sec)

○ Open permanently (closed by 'Close output and return to default mode')

● Close output and return to default mode

			Description	Details
☑	🔒	1\Panel 2	1\Panel 2\Door 1	Default
☑	🔒	1\Panel 2	1\Panel 2\Door 2	Default
☑	🏃	1\Panel 3	1\Panel 3\Door	Default
☑	🔒	2\Panel 2	2\Panel 2\Door 1	Default
☑	🔒	2\Panel 2	2\Panel 2\Door 2	Default
☑	🔒	3\Panel 1	3\Panel 1\Door	Default

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 a**ll 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**.

9.2 Changing the Reader Mode

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

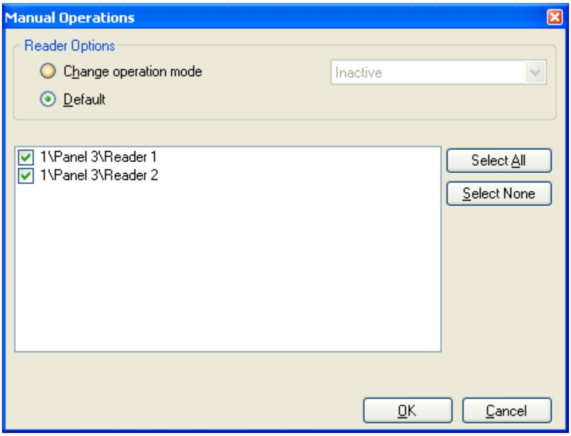
Readers have six possible operation modes:

- **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.
- **Secure (Card + PIN):** The reader requires first a card and then a PIN. The PIN must be entered within 10 seconds of the card.
- **No Access:** The reader does not grant access to users.

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.



Manual Operations

Reader Options

○ Change operation mode   Inactive

● Default

☑ 1\Panel 3\Reader 1

☑ 1\Panel 3\Reader 2

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**.

> Note
>
> For more information on secured (Card + PIN) time zones, see Section 5.7.1.

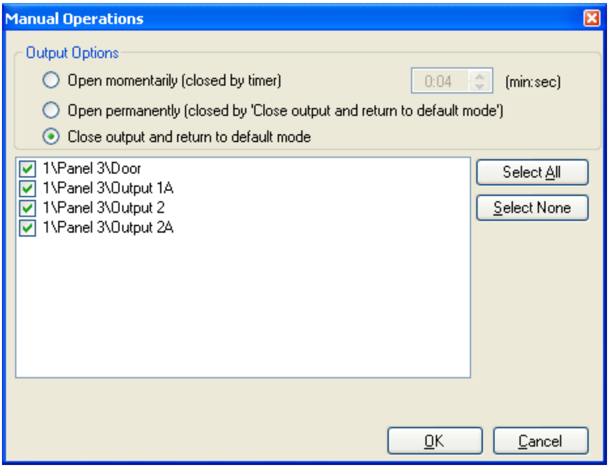
9.3 Controlling Outputs Manually

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.



Manual Operations

Output Options

○ Open momentarily (closed by timer) 0:04 (min:sec)

○ Open permanently (closed by 'Close output and return to default mode')

● Close output and return to default mode

☑ 1\Panel 3\Door

☑ 1\Panel 3\Output 1A

☑ 1\Panel 3\Output 2

☑ 1\Panel 3\Output 2A

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**.

9.4 Manually Disarming Inputs

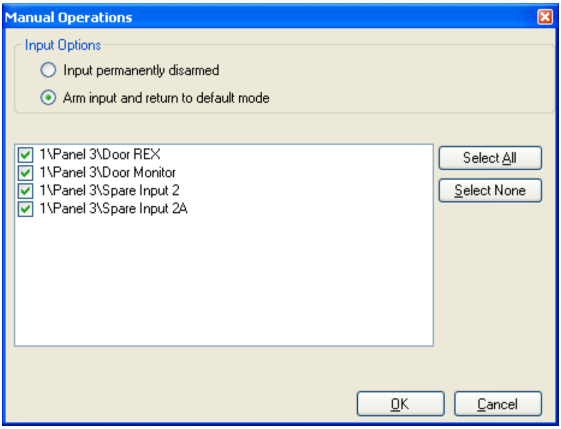
The *Manual Input Operation* window allows an operator to disarm a selected group of inputs directly on a panel.

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.



Manual Operations

Input Options

○ Input permanently disarmed

● Arm input and return to default mode

☑ 1\Panel 3\Door REX

☑ 1\Panel 3\Door Monitor

☑ 1\Panel 3\Spare Input 2

☑ 1\Panel 3\Spare Input 2A

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**.

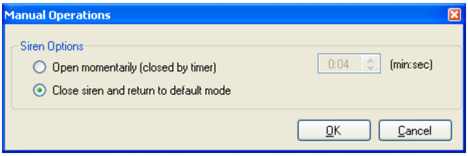
9.5 Controlling Sirens Manually

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.



○ Open momentarily (closed by timer) 0:04 (min:sec)

● Close siren and return to default mode

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**.

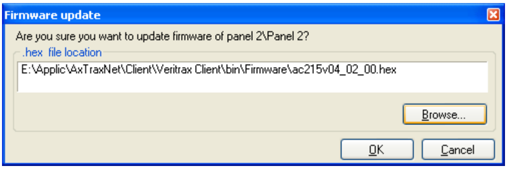
9.6 Manually Update Firmware

The *Update Firmware* window allows an operator to update the firmware version of the selected access control panel.

To perform a firmware update 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 *Update Firmware* window opens.



Are you sure you want to update firmware of panel 2\Panel 2?

E:\Applic\AxTraxNet\Client\Veritrax Client\bin\Firmware\ac215v04_02_00.hex

4. Click **Browse** and select the HEX file relevant to the panel's hardware type.
5. Click **OK**.

10. 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.

10.1 Types of Reports

AxTraxNG includes four main categories of reports and each category contains its

- Immediate Reports
- Panel Reports
- System Reports
- Interactive Report

10.1.1 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.

10.1.2 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.
- **Fingerprint Report** – Lists specific fingerprints readers' events, sorted by reader and date.
- **Visitors Report** – Lists visitors who have made a visit to a certain user or department, or lists all related visitors.

10.1.3 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.

10.1.4 Interactive Report

Interactive reports list details of users and their access activity.

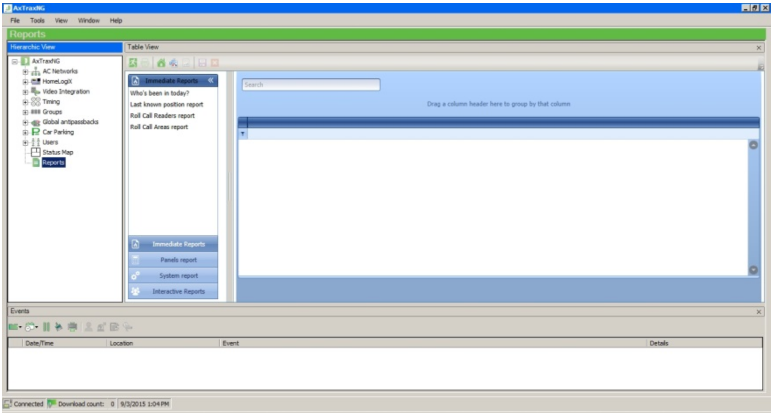
There are three available interactive reports:

- **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.

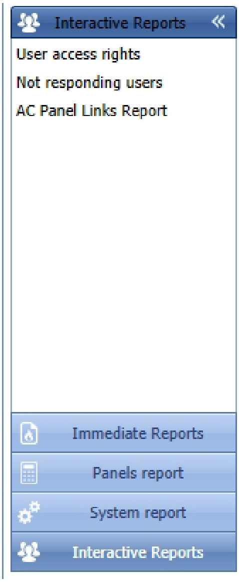
10.2 Generating a Report

To generate a report:

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



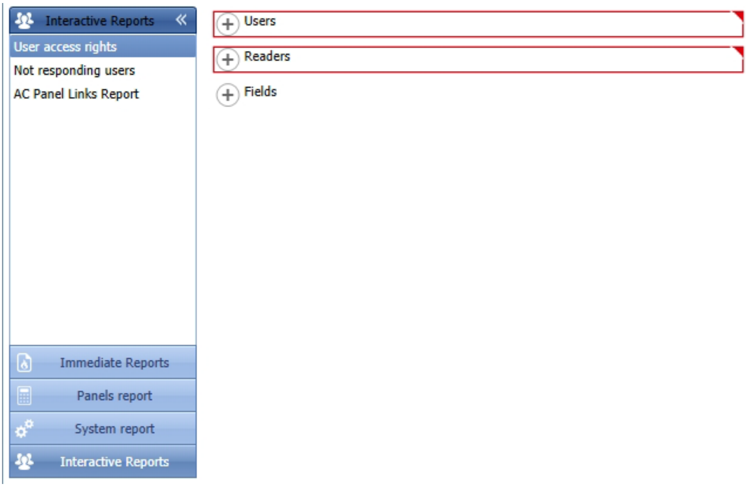
2. Select one of the four main report categories.



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.

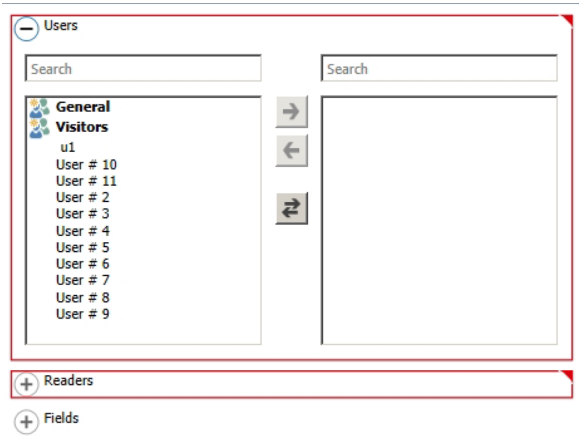
   For example, the parameters needed for the User Access Rights Report are displayed.



Note

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

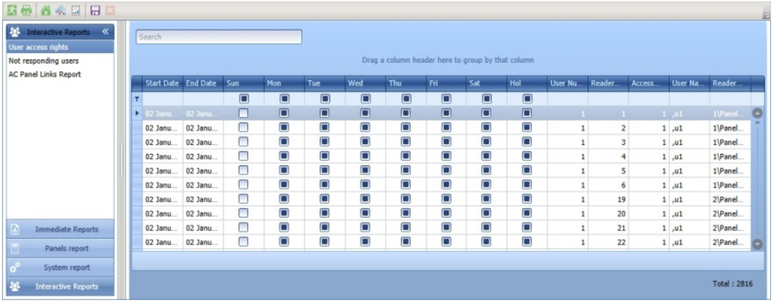
4. Click on a parameter to expand it.



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

6. Once all the entities in each parameter have been selected, click (run) in the Toolbar to generate a report.

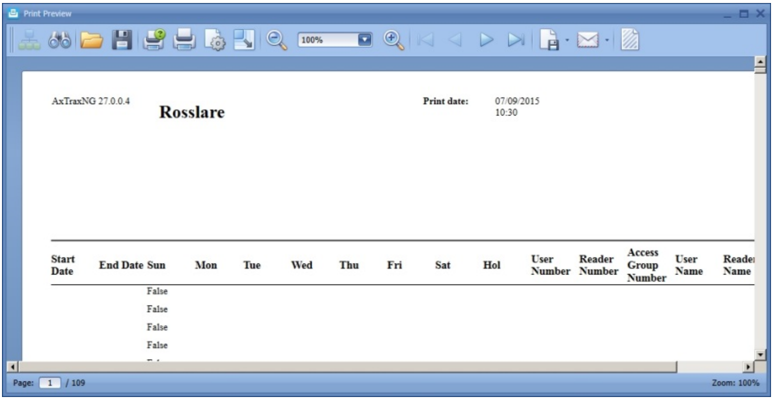
   The generated report, in this example the User Access Rights Report, appears in the Display Area.



Start Date	End Date	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol	User Nu...	Reader...	Access...	User Na...	Reader...
		☑	☑	☑	☑	☑	☑	☑	☑					
02 Janu...	02 Janu...	☐	☑	☑	☑	☑	☑	☑	☑	1	1	1	,u1	1\Panel...
02 Janu...	02 Janu...	☐	☑	☑	☑	☑	☑	☑	☑	1	2	1	,u1	1\Panel...
02 Janu...	02 Janu...	☐	☑	☑	☑	☑	☑	☑	☑	1	3	1	,u1	1\Panel...
02 Janu...	02 Janu...	☐	☑	☑	☑	☑	☑	☑	☑	1	4	1	,u1	1\Panel...
02 Janu...	02 Janu...	☐	☑	☑	☑	☑	☑	☑	☑	1	5	1	,u1	1\Panel...
02 Janu...	02 Janu...	☐	☑	☑	☑	☑	☑	☑	☑	1	6	1	,u1	1\Panel...
02 Janu...	02 Janu...	☐	☑	☑	☑	☑	☑	☑	☑	1	19	1	,u1	2\Panel...
02 Janu...	02 Janu...	☐	☑	☑	☑	☑	☑	☑	☑	1	20	1	,u1	2\Panel...
02 Janu...	02 Janu...	☐	☑	☑	☑	☑	☑	☑	☑	1	21	1	,u1	2\Panel...
02 Janu...	02 Janu...	☐	☑	☑	☑	☑	☑	☑	☑	1	22	1	,u1	2\Panel...

Total : 2816

7. In the Toolbar, click 📄 to preview the report.



AxTraxNG 27.0.0.4

Rosslare

Print date: 07/09/2015 10:30

Start Date	End Date	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol	User Number	Reader Number	Access Group Number	User Name	Reader Name
		False												
		False												
		False												
		False												

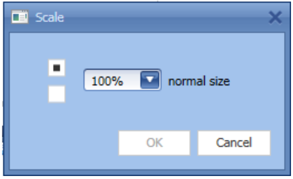
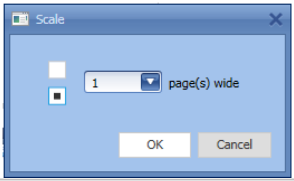
Page: 1 / 109

Zoom: 100%

Table 19 presents the icons that are available for each type of report preview:

Table 19: 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
🖨	**Quick Print**	Print the document with default settings
⚙	**Page Setup**	Adjust the documents settings

Icon	Name	Click button to…
↘	**Scale**	Adjust the scaling of the page Upon clicking on it the following screen opens:  Scale ■ 100% ▾ normal size □ Select the top box to then choose a zoom percentage from the dropdown. Select the bottom box to then choose page width from the dropdown.  Scale □ ■ 1 ▾ page(s) wide
⊖	**Zoom Out**	To view more of the page
⊕	**Zoom In**	To enlarge the script on the page
100% ▾	**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.

11. Administrator Operations

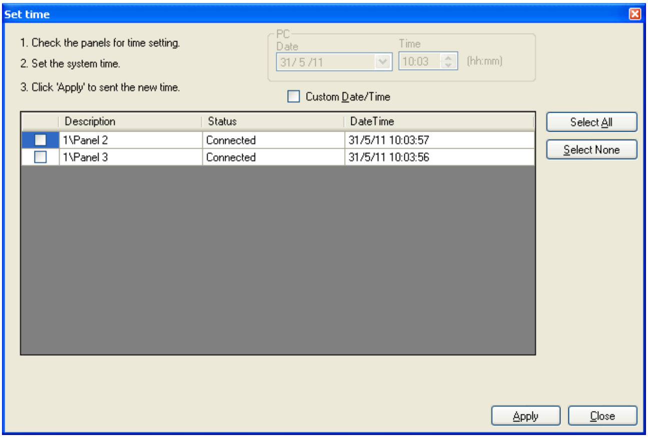
11.1 Setting the Time and Date

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.



Set time

1. Check the panels for time setting.
2. Set the system time.
3. Click 'Apply' to sent the new time.

PC — Date: 31/ 5 /11 — Time: 10:03 (hh:mm)

□ Custom Date/Time

	Description	Status	DateTime
□	1\Panel 2	Connected	31/5/11 10:03:57
□	1\Panel 3	Connected	31/5/11 10:03:56

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.

11.2 Downloading Failed Data

In the event that some data fails to download to the access control panels, it is possible to perform a download of the failed operations only. You can perform this operation on a single panel, on all the panels in a network, or on all the panels in the entire system.

Note: The Failed Data icon only appears if failed data exists in the database.

To download failed data:

1. In the Tree View, select a specific panel, a specific network, or all the networks.
2. On the toolbar, click the icon.

   The download data process begins.

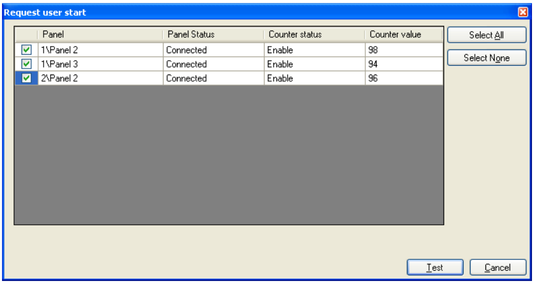
11.3 Testing User Counters

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 Count* window opens.



Request user start

	Panel	Panel Status	Counter status	Counter value
☑	1\Panel 2	Connected	Enable	98
☑	1\Panel 3	Connected	Enable	94
☑	2\Panel 2	Connected	Enable	96

5. Click **Test**.

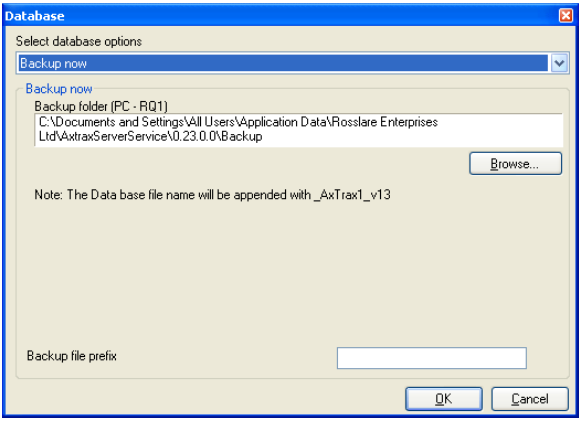
11.4 Maintaining the Database

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

To open the Database window:

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

The *Database* window opens.



Select database options: Backup now

Backup now

Backup folder (PC - RQ1)

C:\Documents and Settings\All Users\Application Data\Rosslare Enterprises Ltd\AxtraxServerService\0.23.0.0\Backup

Note: The Data base file name will be appended with _AxTrax1_v13

Backup file prefix

2. From the **Select database options** dropdown, select your desired option.

The following database operations are available:

Table 20: 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.
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 A user's photo can also be imported.
Import database versions earlier than AS-225 VeriTrax or AS-525 AxTrax*	Replace the current database with VeriTrax AS-225 or AxTrax databases A user's photo can also be imported.

Operation	Description
Import database versions earlier than 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.**

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

3. 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.

4. Click **OK**.

11.5 AxTraxNG Options and Preferences

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

To open the Options window:

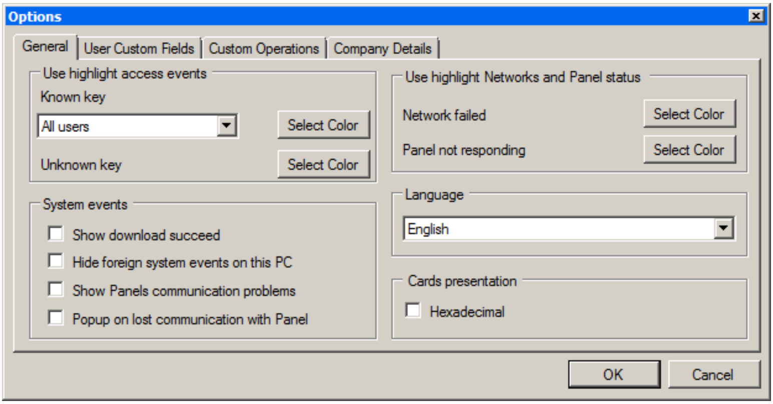
1. From the menu bar, select **Tools > Options**.

   The Options window has four tabs:

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

11.5.1 General Tab

The General tab includes presentation connection settings.



The *General* tab contains the following fields:

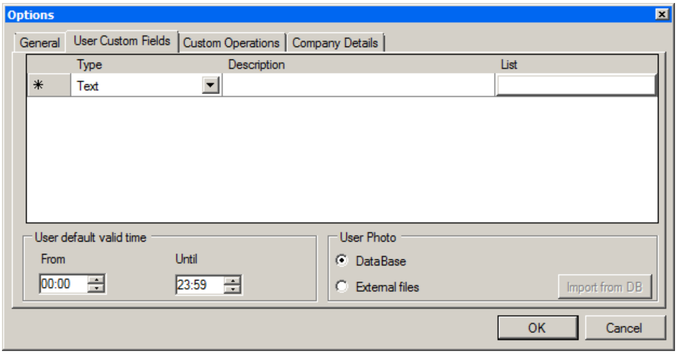
Table 21: Tools > Options > General Tab

Field	Description
Use highlight access events	From the **Known Key** 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 *Unknown key* to define the highlight color for unknown keys.
System events>Show download succeed	Select the checkbox 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 the checkbox to see only local administrator and AxTraxNG Server messages.
System events>Show panel communication problems	Select the checkbox to have status indicate panel communication problems
System events>Pop-up on lost communication with panel	Select the checkbox 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 *Network failed* to define the highlight color for network alarms. Click **Select Color** adjacent to *Panel not responding* to define the highlight color for panel communication errors.

Field	Description
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.

11.5.2 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).



Type	Description	List
Text		

User default valid time: From 00:00 Until 23:59

User Photo: ● DataBase ○ External files

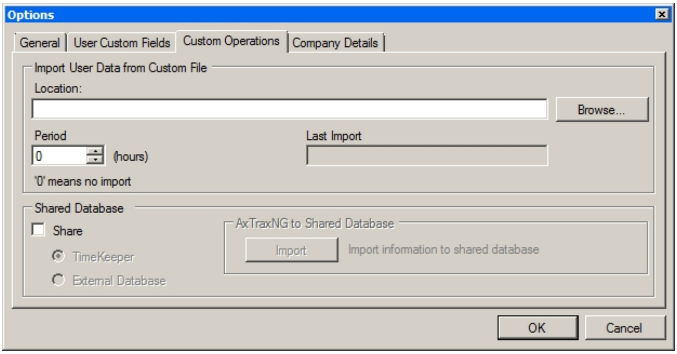
The *User Custom Fields* tab contains the following fields:

Table 22: Tools > Options > User Custom Fields Tab

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

11.5.3 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.



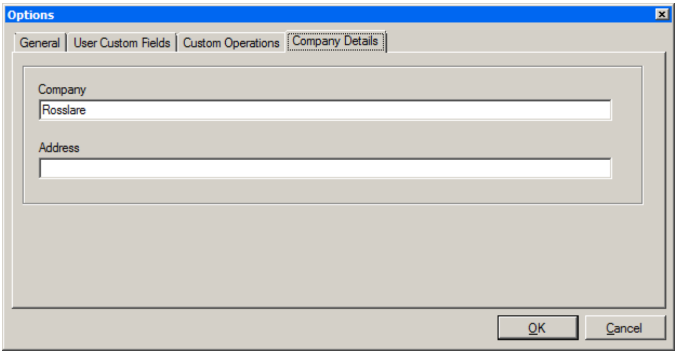
The *Custom Operations* tab contains the following fields:

Table 23: 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** spin box, select the time period. The period is the time between import processes in hours where ‘0’ means the import is only in manual operation.
Shared Database events>Share	Select the checkbox 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 radio button: TimeKeeper – Sets the DB sharing for the TimeKeeper program External Database – Sets the DB sharing for other generic formats
Shared Database events>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.

11.5.4 Company Details

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

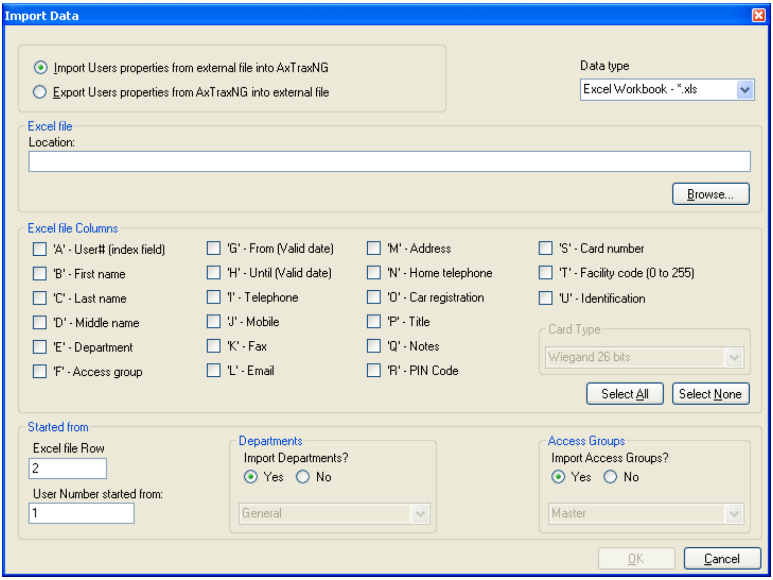


Company: Rosslare

Address:

11.6 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.



● Import Users properties from external file into AxTraxNG
○ Export Users properties from AxTraxNG into external file

Data type: Excel Workbook - *.xls

Excel file
Location:

Excel file Columns

□ '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' - Telephone
□ 'J' - 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 (0 to 255)
□ 'U' - Identification

Card Type: Wiegand 26 bits

Started from
Excel file Row: 2
User Number started from: 1

Departments
Import Departments? ● Yes ○ No
General

Access Groups
Import Access Groups? ● Yes ○ No
Master

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

Table 24: Tools > Import/Export Data

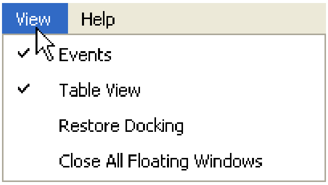
Field	Description
Import Users properties from external file into AxTraxNG	Select this option to import user properties
Export Users properties from AxTraxNG into external file	Select this option to export user properties
Data Type	Select the type of data file to import/export.
Location	Select the location 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.
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 *No* 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 *No* option is selected in the import access group option.

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 24.
3. Click **OK**.

11.7 AxTrax GUI View Options

The AxTraxNG Client main window GUI can be customized using the *View* menu.



- **Events** to make Events window visible/invisible.
- **Table View** to make Table View visible/invisible
- **Restore** docking to return to default GUI Setting
- **Close all floating Windows** to close all pop-up windows.

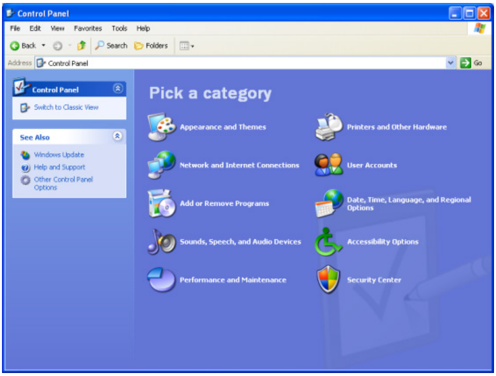
A. Firewall Configuration

A.1 For Windows XP

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

To configure the firewall:

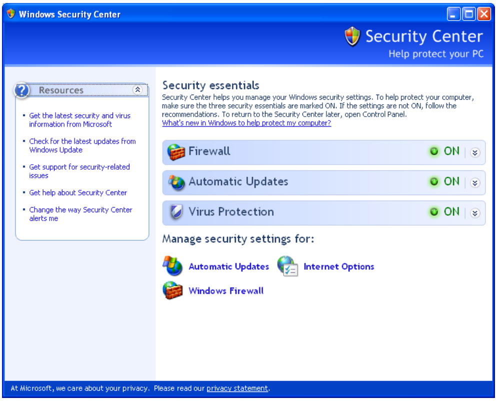
1. Open the Control Panel on your computer.



2. Click the **Security Center** category.

   The *Windows Security Center* window opens.

   (When in "Classic View", click the **Security Center** category in the top-left Control Panel preferences pane.)



- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.

What's new in Windows to help protect my computer?

Firewall ● ON

Automatic Updates ● ON

Virus Protection ● ON

Manage security settings for:

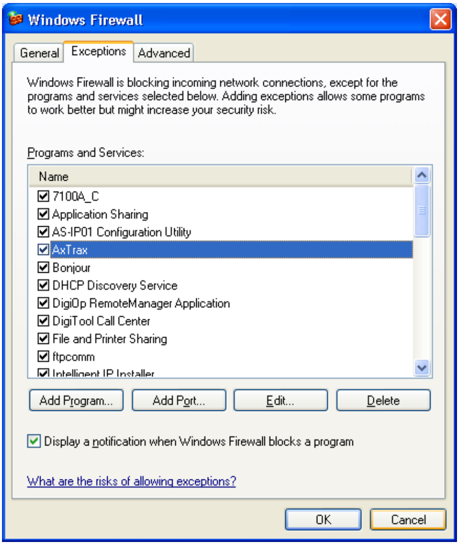
Automatic Updates Internet Options

Windows Firewall

At Microsoft, we care about your privacy. Please read our privacy statement.

3. Click **Windows Firewall**.

4. Select the *Exceptions* tab.



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

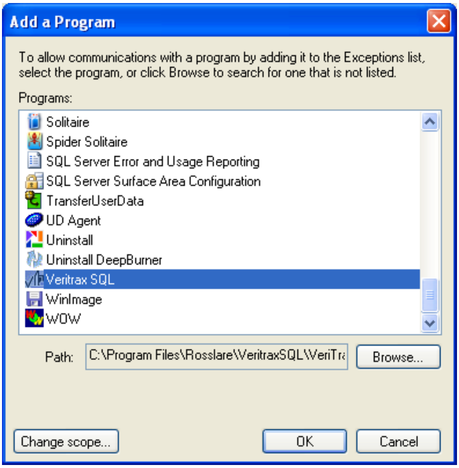
Name
☑ 7100A_C
☑ Application Sharing
☑ AS-IP01 Configuration Utility
☑ AxTrax
☑ Bonjour
☑ DHCP Discovery Service
☑ DigiOp RemoteManager Application
☑ DigiTool Call Center
☑ File and Printer Sharing
☑ ftpcomm
☑ Intelligent IP Installer

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

5. Click **Add Program**.

The *Add a Program* dialog appears.



To allow communications with a program by adding it to the Exceptions list, select the program, or click Browse to search for one that is not listed.

Programs:

- Solitaire
- Spider Solitaire
- SQL Server Error and Usage Reporting
- SQL Server Surface Area Configuration
- TransferUserData
- UD Agent
- Uninstall
- Uninstall DeepBurner
- Veritrax SQL
- WinImage
- WOW

Path: C:\Program Files\Rosslare\VeritraxSQL\VeriTra

6. Click **Browse**.

The *Browse* dialog appears.

7. In the **File Name** box, type:

“**C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\BINN\sqlservr.exe**” and click **Open**.

8. Click **OK**.

   The SQL Server program appears in the Add a Program dialog.

9. Repeat Steps 6 and 7.

10. In the **File Name** box, type:

    "**C:\Program Files\Microsoft SQL Server\90\Shared\sqlbrowser.exe**" and click **Open**.

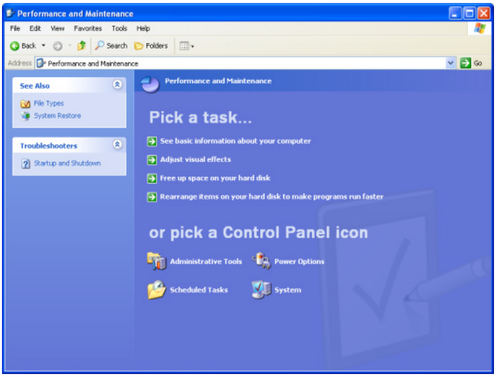
11. Click **OK**.

    The SQL Browser program appears in the Add a Program dialog.

12. In the Control Panel, click the **Performance and Maintenance** category.

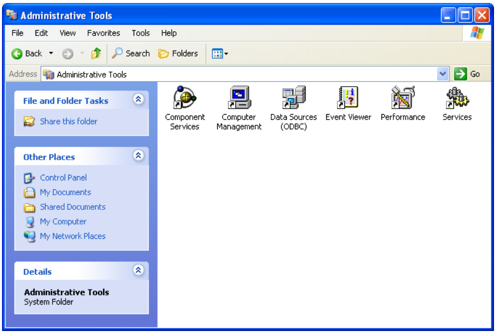
    (When in "Classic View", click **Switch to Category View** in the top-left Control Panel preferences pane, and then click the **Performance and Maintenance** category.)

    The *Performance and Maintenance* window opens.


Performance and Maintenance
File Edit View Favorites Tools Help
Back Search Folders
Address Performance and Maintenance
Go
See Also
File Types
System Restore
Troubleshooters
Startup and Shutdown
Performance and Maintenance
Pick a task...
See basic information about your computer
Adjust visual effects
Free up space on your hard disk
Rearrange items on your hard disk to make programs run faster
or pick a Control Panel icon
Administrative Tools
Power Options
Scheduled Tasks
System

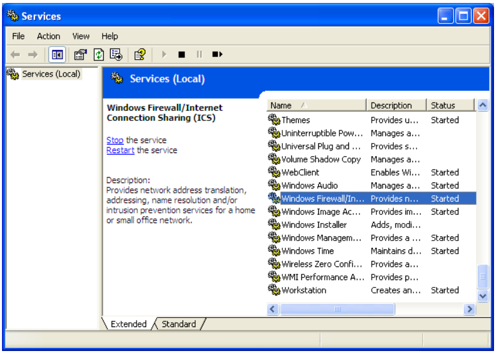
13. Click **Administrative Tools**.

    The Administrative Tools window opens.



14. Double-click *Services*.

    The Services Console opens.



Windows Firewall/Internet Connection Sharing (ICS)

Stop the service
Restart the service

Description:
Provides network address translation, addressing, name resolution and/or intrusion prevention services for a home or small office network.

Name	Description	Status
Themes	Provides u…	Started
Uninterruptible Pow…	Manages a…	
Universal Plug and …	Provides s…	
Volume Shadow Copy	Manages a…	
WebClient	Enables Wi…	Started
Windows Audio	Manages a…	Started
Windows Firewall/In…	Provides n…	Started
Windows Image Ac…	Provides im…	Started
Windows Installer	Adds, modi…	
Windows Managem…	Provides a …	Started
Windows Time	Maintains d…	Started
Wireless Zero Confi…	Provides a…	
WMI Performance A…	Provides p…	
Workstation	Creates an…	Started

15. Right-click **Windows Firewall/Internet Connection Sharing (ICS)** and click **Restart** from the pop-up menu.
16. Right-click **SQL Server** and click **Restart** from the pop-up menu.
17. Right-click **SQL Server Browser** and click **Restart** from the pop-up menu.

    The Firewall is now configured for AxTraxNG.

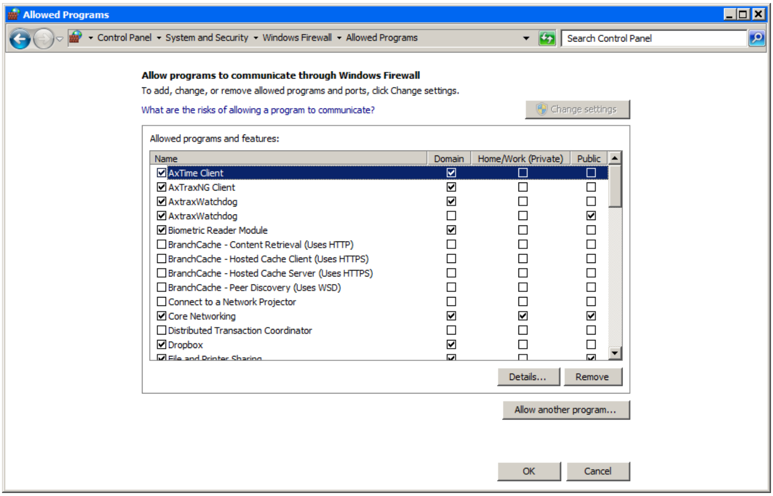
A.2 For Windows 7

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**.

The *Allowed Programs* window opens.



Allow programs to communicate through Windows Firewall

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

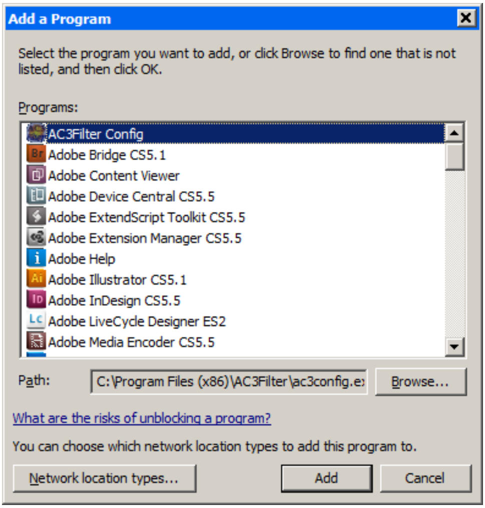
What are the risks of allowing a program to communicate?

Allowed programs and features:

Name	Domain	Home/Work (Private)	Public
☑ AxTime Client	☑	☐	☐
☑ AxTraxNG Client	☑	☐	☐
☑ AxtraxWatchdog	☑	☐	☐
☑ AxtraxWatchdog	☐	☐	☑
☑ Biometric Reader Module	☑	☐	☐
☐ BranchCache - Content Retrieval (Uses HTTP)	☐	☐	☐
☐ BranchCache - Hosted Cache Client (Uses HTTPS)	☐	☐	☐
☐ BranchCache - Hosted Cache Server (Uses HTTPS)	☐	☐	☐
☐ BranchCache - Peer Discovery (Uses WSD)	☐	☐	☐
☐ Connect to a Network Projector	☐	☐	☐
☑ Core Networking	☑	☑	☑
☐ Distributed Transaction Coordinator	☐	☐	☐
☑ Dropbox	☑	☐	☐
☑ File and Printer Sharing	☑	☐	☑

4. Click **Add Program**.

   The *Add a Program* dialog appears.



Select the program you want to add, or click Browse to find one that is not listed, and then click OK.

Programs:

AC3Filter Config
Adobe Bridge CS5.1
Adobe Content Viewer
Adobe Device Central CS5.5
Adobe ExtendScript Toolkit CS5.5
Adobe Extension Manager CS5.5
Adobe Help
Adobe Illustrator CS5.1
Adobe InDesign CS5.5
Adobe LiveCycle Designer ES2
Adobe Media Encoder CS5.5

Path: C:\Program Files (x86)\AC3Filter\ac3config.e:

What are the risks of unblocking a program?

You can choose which network location types to add this program to.

5. Click **Browse**.

   The *Browse* dialog 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:

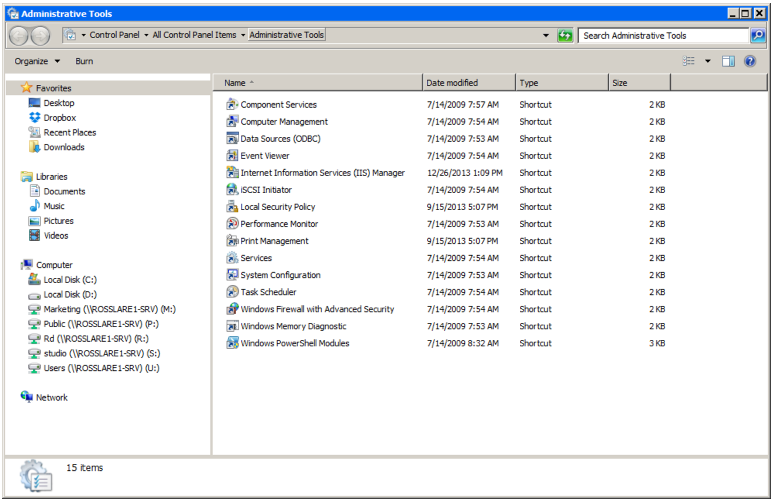
   "**C:\Program Files\Microsoft SQL Server\90\Shared\sqlbrowser.exe**" and click **Open**.

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.

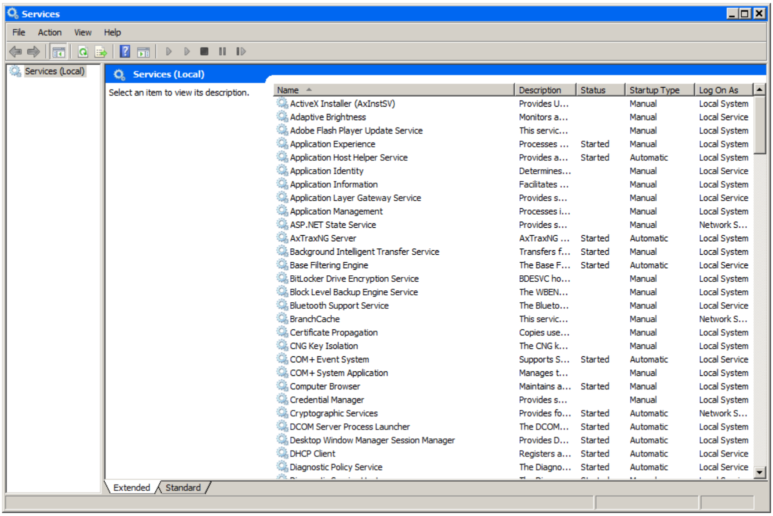

Administrative Tools
Control Panel ▸ All Control Panel Items ▸ Administrative Tools
Search Administrative Tools
Organize
Burn
Favorites
Desktop
Dropbox
Recent Places
Downloads
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Local Disk (D:)
Marketing (\\ROSSLARE1-SRV) (M:)
Public (\\ROSSLARE1-SRV) (P:)
Rd (\\ROSSLARE1-SRV) (R:)
studio (\\ROSSLARE1-SRV) (S:)
Users (\\ROSSLARE1-SRV) (U:)
Network

Name	Date modified	Type	Size
Component Services	7/14/2009 7:57 AM	Shortcut	2 KB
Computer Management	7/14/2009 7:54 AM	Shortcut	2 KB
Data Sources (ODBC)	7/14/2009 7:53 AM	Shortcut	2 KB
Event Viewer	7/14/2009 7:54 AM	Shortcut	2 KB
Internet Information Services (IIS) Manager	12/26/2013 1:09 PM	Shortcut	2 KB
iSCSI Initiator	7/14/2009 7:54 AM	Shortcut	2 KB
Local Security Policy	9/15/2013 5:07 PM	Shortcut	2 KB
Performance Monitor	7/14/2009 7:53 AM	Shortcut	2 KB
Print Management	9/15/2013 5:07 PM	Shortcut	2 KB
Services	7/14/2009 7:54 AM	Shortcut	2 KB
System Configuration	7/14/2009 7:53 AM	Shortcut	2 KB
Task Scheduler	7/14/2009 7:54 AM	Shortcut	2 KB
Windows Firewall with Advanced Security	7/14/2009 7:54 AM	Shortcut	2 KB
Windows Memory Diagnostic	7/14/2009 7:53 AM	Shortcut	2 KB
Windows PowerShell Modules	7/14/2009 8:32 AM	Shortcut	3 KB

15 items

12. Double-click *Services*.

    The *Services* console opens.



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides U…		Manual	Local System
Adaptive Brightness	Monitors a…		Manual	Local Service
Adobe Flash Player Update Service	This servic…		Manual	Local System
Application Experience	Processes …	Started	Manual	Local System
Application Host Helper Service	Provides a…	Started	Automatic	Local System
Application Identity	Determines…		Manual	Local Service
Application Information	Facilitates …		Manual	Local System
Application Layer Gateway Service	Provides s…		Manual	Local Service
Application Management	Processes i…		Manual	Local System
ASP.NET State Service	Provides s…		Manual	Network S…
AxTraxNG Server	AxTraxNG …	Started	Automatic	Local System
Background Intelligent Transfer Service	Transfers f…	Started	Manual	Local System
Base Filtering Engine	The Base F…	Started	Automatic	Local Service
BitLocker Drive Encryption Service	BDESVC ho…		Manual	Local System
Block Level Backup Engine Service	The WBEN…		Manual	Local System
Bluetooth Support Service	The Blueto…		Manual	Local Service
BranchCache	This servic…		Manual	Network S…
Certificate Propagation	Copies use…		Manual	Local System
CNG Key Isolation	The CNG k…		Manual	Local System
COM+ Event System	Supports S…	Started	Automatic	Local Service
COM+ System Application	Manages t…		Manual	Local System
Computer Browser	Maintains a…	Started	Manual	Local System
Credential Manager	Provides s…		Manual	Local System
Cryptographic Services	Provides fo…	Started	Automatic	Network S…
DCOM Server Process Launcher	The DCOM…	Started	Automatic	Local System
Desktop Window Manager Session Manager	Provides D…	Started	Automatic	Local System
DHCP Client	Registers a…	Started	Automatic	Local Service
Diagnostic Policy Service	The Diagno…	Started	Automatic	Local Service

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.

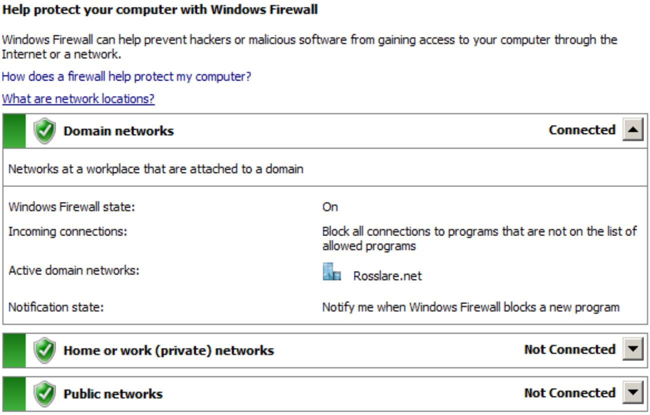
15. Right-click **SQL Server Browser** and click **Restart** from the pop-up menu.

    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. Select Windows Firewall.



Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Domain networks **Connected**

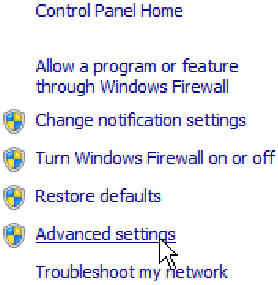
Networks at a workplace that are attached to a domain

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active domain networks:	Rosslare.net
Notification state:	Notify me when Windows Firewall blocks a new program

Home or work (private) networks **Not Connected**

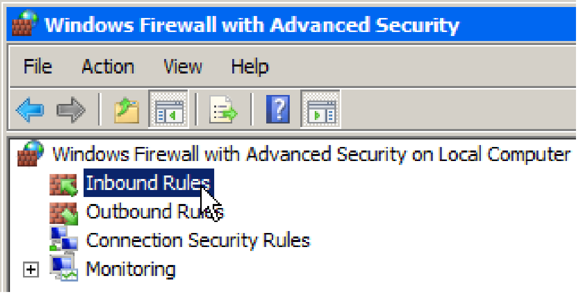
Public networks **Not Connected**

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

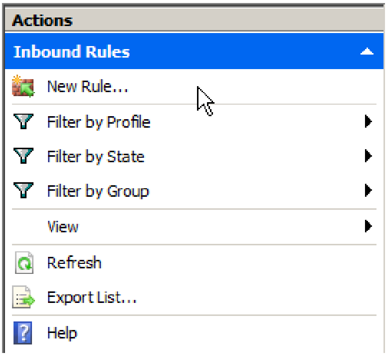


Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

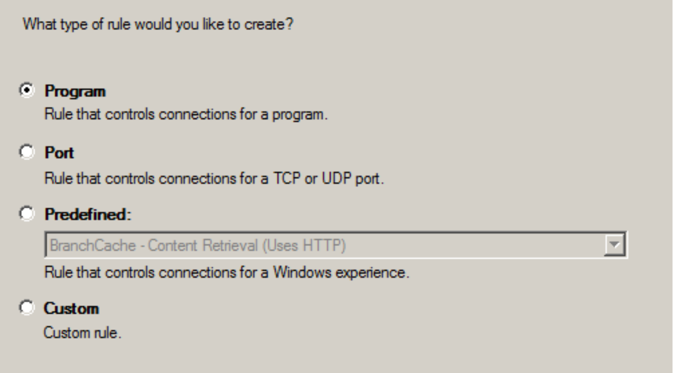
4. In the console tree on the left, click **Inbound Rules**.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanced Security on Local Computer
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

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



The following screen opens:



What type of rule would you like to create?

● **Program**
Rule that controls connections for a program.

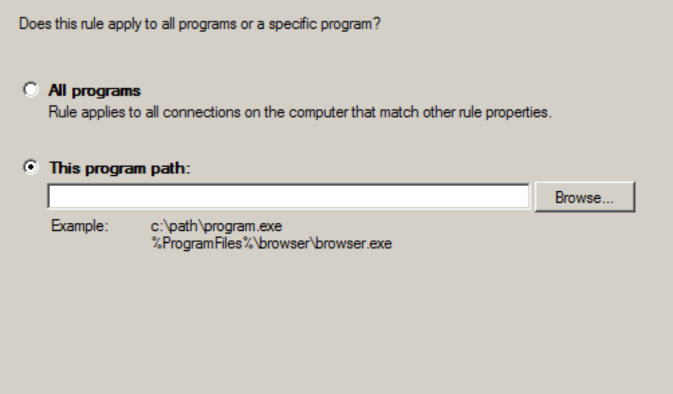
○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

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

The following screen opens:



Does this rule apply to all programs or a specific program?

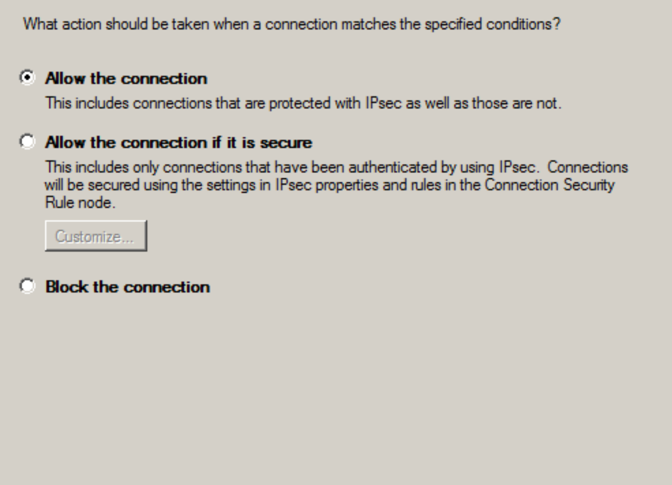
○ **All programs**
Rule applies to all connections on the computer that match other rule properties.

● **This program path:**

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

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:



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

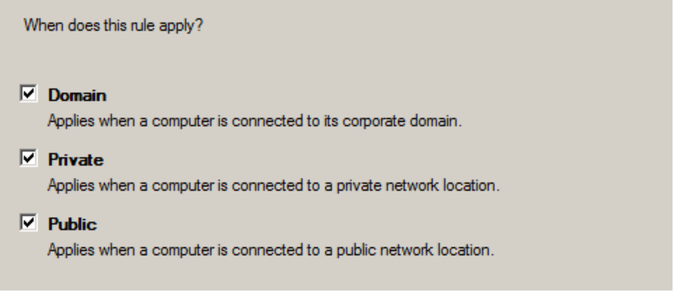
● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **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?

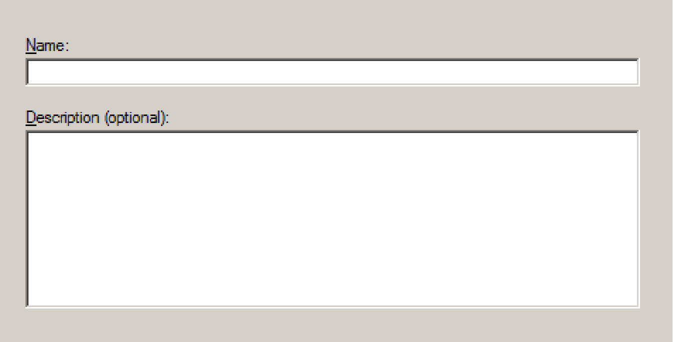
☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **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. Working with Windows 8 and 8.1

Although AxTraxNG Version 26.xx does not support use with Windows 8, it is possible to run the application with Windows 8 and 8.1 by performing the following workaround before upgrading AxTraxNG to version 24.03:

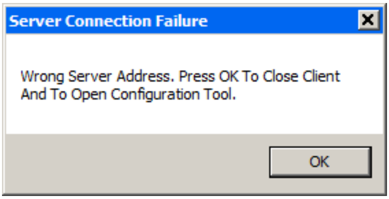
1. Run regedit.exe
2. Open HKEY_LOCAL_MACHINE/Software/Wow6432Node/Rosslare.
3. Right-click on each node and change permissions to Full.
4. Reboot the PC.
5. Perform the AxTraxNG upgrade.

D. WAN Connection Troubleshooting

This appendix presents three scenarios of a server connection problem.

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

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



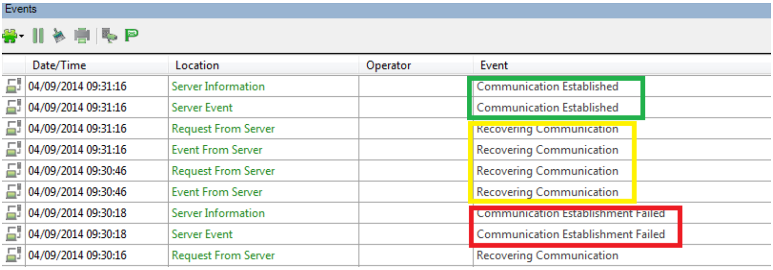
Server Connection Failure

Wrong Server Address. Press OK To Close Client And To Open Configuration Tool.

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

D.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.

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

Check the following possible firewall problems:

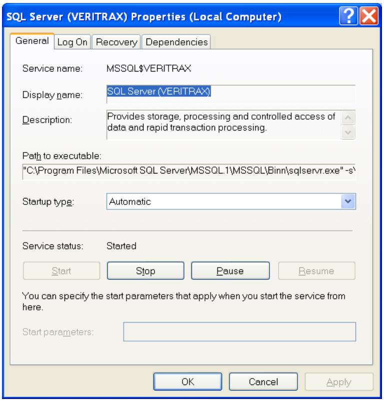
- Check firewall for server PC
- Check firewall for client PC
- Check firewall to Server network
- Check firewall to Client network

E. 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:



Service name: MSSQL$VERITRAX

Display name: SQL Server (VERITRAX)

Description: Provides storage, processing and controlled access of data and rapid transaction processing.

Path to executable:
"C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.exe" -s\

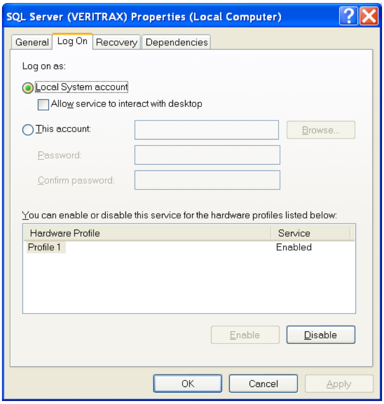
Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

3. Under the General tab, verify that the Startup type is “Automatic” and that the Service status is “Started”.



Log on as:

● Local System account

□ Allow service to interact with desktop

○ This account:

Password:

Confirm password:

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Profile 1	Enabled

4. In the Log On tab, verify that the *Local System Account* radio button is selected. If not, select **Local System Account** and restart the computer for the changes to take effect.

F. Network Configuration

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

TCP/IP and Modem-to-Modem connections must be configured for use, and require expert knowledge of the local network.

F.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 or AC-525).

Each TCP/IP connection can support up to 32 access control panels that are connected to each other using RS-485.

> 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 using the onboard converter of AC-225IP or AC-525.

To configure a TCP/IP Connection for AxTraxNG:

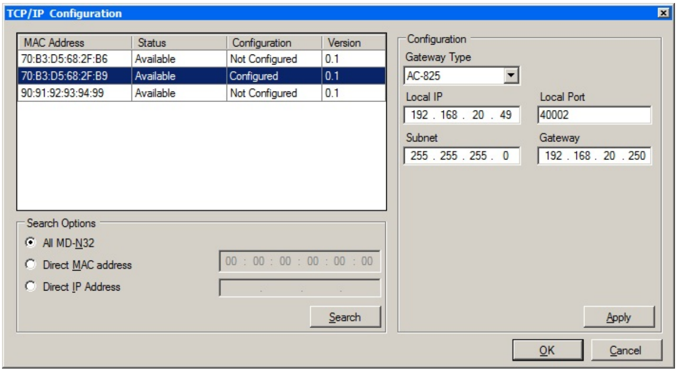
1. In the Tree View, click **AC Networks**.
2. On the toolbar, click the ☑ icon.

   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.

4. Click **Configuration**.

   The *TCP/IP Configuration* window opens.



TCP/IP Configuration

MAC Address	Status	Configuration	Version
70:B3:D5:68:2F:B6	Available	Not Configured	0.1
70:B3:D5:68:2F:B9	Available	Configured	0.1
90:91:92:93:94:99	Available	Not Configured	0.1

Search Options
● All MD-N32
○ Direct MAC address 00 : 00 : 00 : 00 : 00 : 00
○ Direct IP Address . . .

Configuration
Gateway Type: AC-825
Local IP: 192 . 168 . 20 . 49
Local Port: 40002
Subnet: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 20 . 250

   The upper left window lists all TCP/IP converters connected to the local network, identified by their MAC address, and indicates if they are available to be assigned to a new panel network or are already assigned.

5. From the MD-N32 list (the MD-N32's MAC address should be labeled on the TCP/IP converter), select the appropriate MAC address.
6. In **Gateway Type**, select the type of TCP/IP converter, MD-N32, MD-IP32 onboard, or any other valid option. Skip this selection if it is already valid.
7. For an AC-825, the IP module should be configured to the AxTraxNG server.

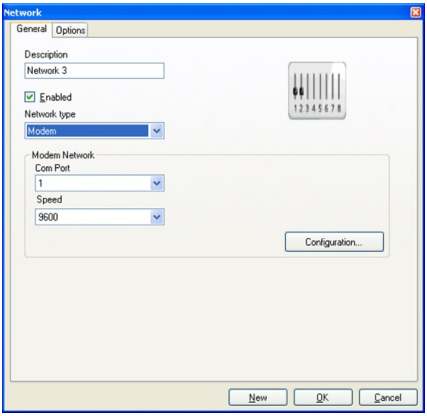
   Even if the IP module was configured before, you need to click **Apply** to configure with the server and then click **OK** to add the AC-825 network.
8. Type the **Local IP address** and **Subnet** for the computer's network.
9. Enter the **Local Port** number and select the **Speed** of your connection. 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.
10. Click **OK** to start the verification process.
11. Turn off the MD-N32 power (or panel power if using the onboard module, such as MD-IP32), and then turn the power on again. This step is necessary when using certain versions of MD-N32 or MD-IP32 models. Skip this step if not applicable.
12. If configuration applies to a WAN network, disconnect the configured unit from the local network, and reconnect to the WAN network and access control panels network working over the WAN.

F.2 Modem Connection (not for AC-825)

You can also use Rosslare's MD-N33 modem for a Modem-to-Modem connection. Refer to the hardware installation manuals of the desired panel for more details.

To configure MD-N33 in AxTraxNG:

1. In the AxTraxNG software, add a new network.
2. Under network type, select **Modem**.



Description: Network 3

☑ Enabled

Network type: Modem

Modem Network

Com Port: 1

Speed: 9600

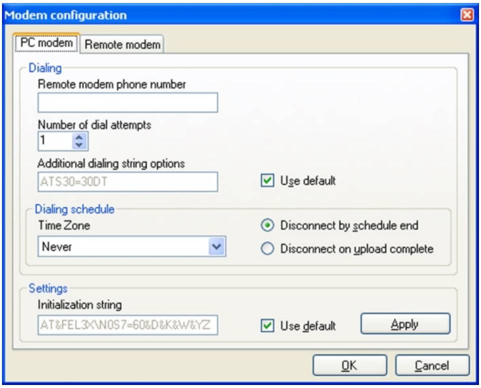
Note

Communication speed is limited to 9600, 19200, 57600, or 115200 bits per second.

To initialize and configure the computer modem:

1. In the Network window, click **Configuration**.

   The Modem Configuration window opens.



Dialing

Remote modem phone number:

Number of dial attempts: 1

Additional dialing string options: ATS30=30DT ☑ Use default

Dialing schedule

Time Zone: Never

● Disconnect by schedule end

○ Disconnect on upload complete

Settings

Initialization string: AT&FEL3X\N0S7=60&D&K&W&YZ ☑ Use default

2. In the **Dialing** area, under **Remote modem phone number**, type the destination telephone number to call.

3. Click to change the **Number of dial attempts** (if required).

   For most applications, the default dialing string is sufficient.

   The dialing string is displayed in the window.
4. Clear **Use default**. This allows adding or editing of the dialing string. Then, type the AT command in the **Dialing string** window.
5. From the **Dialing schedule** dropdown list, select the time zone.
6. Select the disconnecting condition: **Disconnect by schedule end** or **Disconnect on upload complete**.

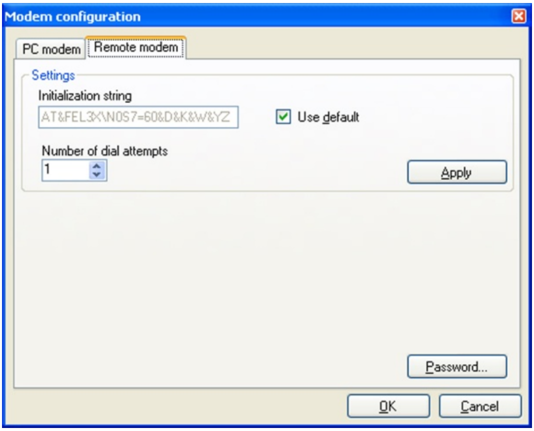
   This option is enabled when the selected time zone is different from the default time zone (Always and Never).
7. In the **Settings** area, the initialization string is displayed in the window. For most applications, the default initialization string is sufficient.
8. Clear **Use default** to allow adding or editing of the dialing string. Then, type the AT command in the **Dialing string** window.
9. Connect the modem to the PC via the selected COM port, and click **Apply** to initialize the PC modem.
10. Click **OK** to complete the initialization.
11. If the computer displays a failure message, check the modem connections and repeat the last steps.

Note

Remote modem initialization is at the PC side. When modem initialization fails through telephone line, a message appears.

To initialize and configure the remote modem:

1. In the Modem Configuration window, click the **Remote modem** tab.



Modem configuration

Settings

Initialization string: AT&FEL3X\N0S7=60&D&K&W&YZ

☑ Use default

Number of dial attempts: 1

2. In the **Settings** area, the initialization string is displayed in the window. For most applications, the default initialization string of is sufficient.
3. Clear **Use default** to allow adding or editing of the dialing string. Then type the AT command in the **Dialing string** window.
4. In **Number of rings to answer**, set the number of rings before the computer modem answers.
5. Connect the remote modem to the computer via the selected com port, and click **Apply** to initialize the computer modem.
6. Click **OK** to initialize.
7. If a failure message appears, check the modem connections and repeat the last steps.

Note

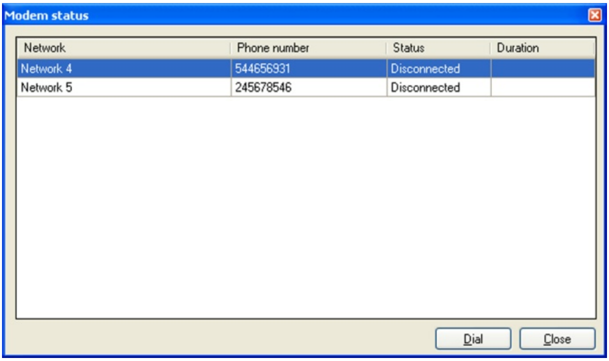
You must perform the action twice at the PC side, to Initialize two MD-N33s.

The MD-N33 and AxTraxNG software are now configured and ready.

You can now continue working using the AxTraxNG Adding New Panel procedure.

To check the remote modem status:

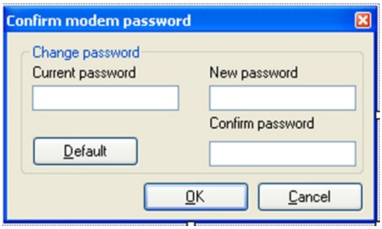
1. When a panel is connected in a modem network, you can see the status of the modem by clicking the *phone* icon in the toolbar.
2. There is a manual option to dial or disconnect the modem.



Modem status

Network	Phone number	Status	Duration
Network 4	544656931	Disconnected	
Network 5	245678546	Disconnected	

3. To prevent access to AxTraxNG data from non-authorized users, the AC-215, AC-225, AC-425 or AC-525 access control panels contain a password that can be changed only when the modem is connected and there is a link with the panel. You may be asked to enter the password during first data configuration, such as adding a new panel or downloading a new firmware.



G. Restoring Factory Default Settings

If the modem configuration password is lost or forgotten, reset the access control panel to the factory default settings, and use the default "VeriTrax" password.

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

To restore the factory default settings:

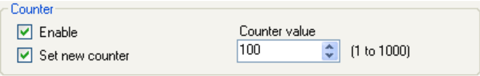
1. Turn off the supply power.
2. Disconnect all doors and readers wiring.
3. Connect Data 0, Data 1, and Tamper inputs to GND (-) in both reader 1 and 2 (total of six wires)
4. Power up the supply power for a few seconds. Wait for the "LED3" and "LED4" LEDs to flash alternately.
5. Turn off the supply 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.
9. Dial to the appropriate access control panel and click **password** in the modem status screen. Use **AxTraxNG** as the current password, and change the password to a new one.

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 2 in Section 5.14.2).

To configure user counters:

1. Go 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** spin box.



Counter

☑ Enable

☑ Set new counter

Counter value: 100 (1 to 1000)

5. Click **OK**.
6. Go the *General* tab of the *Reader Properties* (Section 5.7).
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

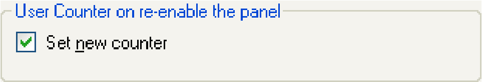
If this option is not used, then upon panel re-enable, the user counter continues with its previous value prior to having that panel disabled.

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. Click the *Options* tab.

5. Select **Set new counter**.



User Counter on re-enable the panel

☑ Set new counter

6. Click **OK**.

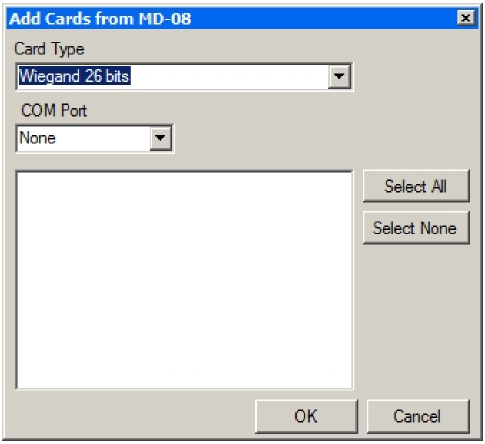
I. Enrolling Cards using the MD-08

This option is available for users with the connected MD-08 unit.

To enroll cards using an MD-08 unit:

1. Be sure the MD-08 is connected.
2. In the Tree View, expand the **Users** element and select the **Cards** element.
3. Click the **Insert card by MD-08** icon (✓) on the toolbar or click **Add from MD-08** in the *Codes* tab in the *Users Properties* window (Section 5.14.2.2).

   The *Add Cards from MD-08* window opens.



Add Cards from MD-08

Card Type: Wiegand 26 bits

COM Port: None

4. Select the Card type and Com Port from the respective dropdown lists.
5. Enroll cards using the reader. Each card enrolled appears in the screen.
6. Select the cards to add.
7. Click **OK**.

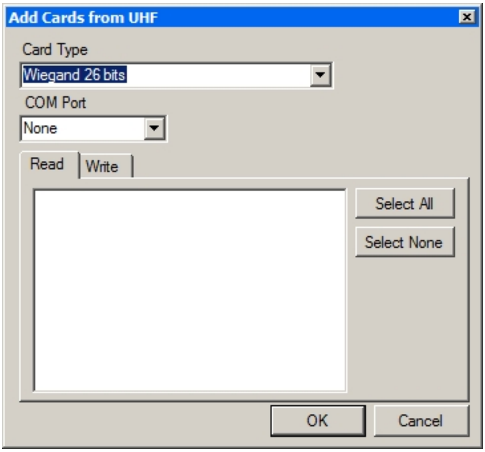
J. Enrolling Cards using a UHF Reader

This option is available for users with a connect UHF reader.

To enroll cards using a UHF reader:

1. In the Tree View, expand the **Users** element and select the **Cards** element.
2. Click the **Insert card by UHF** icon (➕) on the toolbar or click **Add from UHF** in the *Codes* tab in the *Users Properties* window (Section 5.14.2.2).

   The *Add Cards from MD-08* window opens.



Add Cards from UHF

Card Type: Wiegand 26 bits

COM Port: None

3. Select the Card type and Com Port from the respective dropdown lists.
4. Enroll cards using the reader. Each card enrolled appears in the screen.
5. Select the cards to add.
6. Click **OK**.

K. SQL Server Installation Troubleshoot

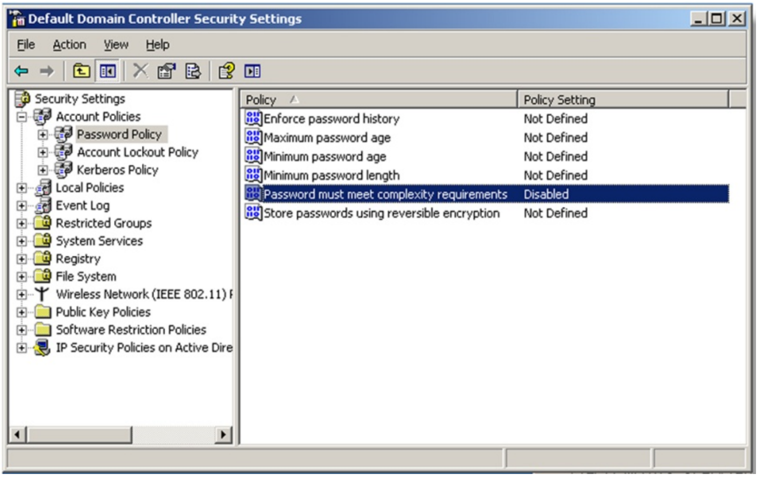
When installing the MS SQL Server 2005 Express component in a Windows Server (2003 or 2008) environment, you might get the following error message: " *The sa password must meet SQL Server password policy requirements.*"

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:



Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wireless Network (IEEE 802.11) P
Public Key Policies
Software Restriction Policies
IP Security Policies on Active Dire

Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	Not Defined
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Not Defined

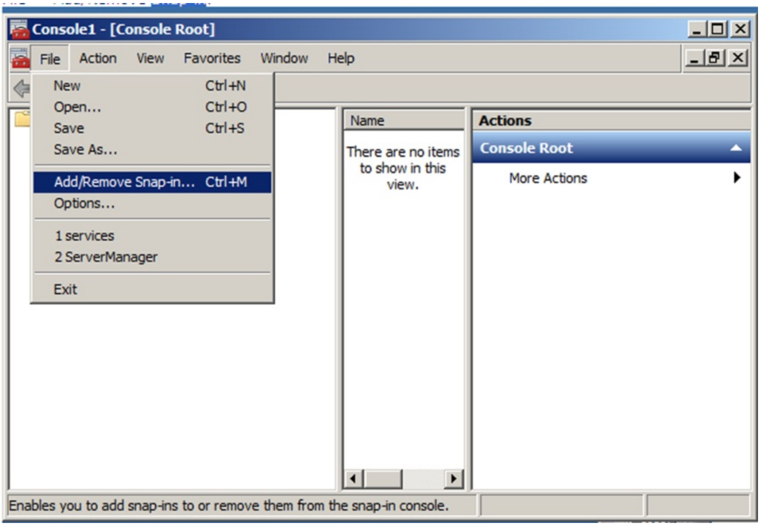
Note

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

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

To check the local security policy

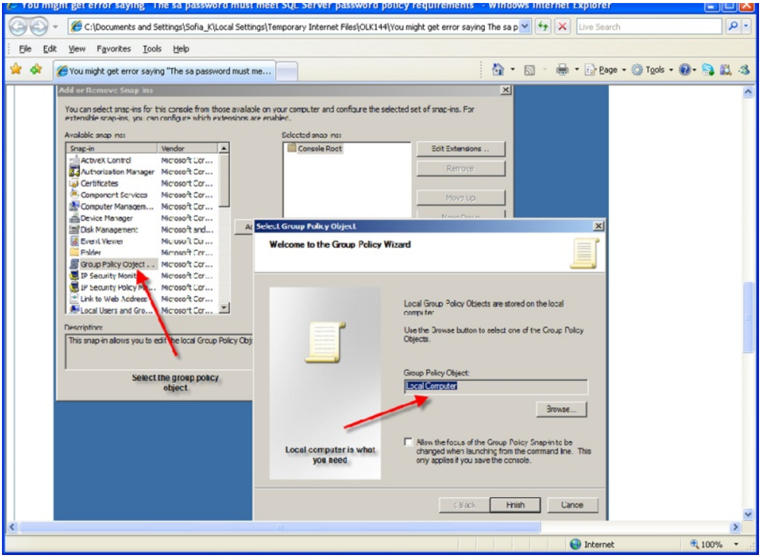
1. Open the MMC console: **Start -> Run -> mmc.exe**
2. Click **File -> Add/Remove Snap-in**:



There are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

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


You might get error saying "The sa password must meet SQL Server password policy requirements" - Windows Internet Explorer
C:\Documents and Settings\Sofia_K\Local Settings\Temporary Internet Files\OLK144\You might get error saying The sa p
Live Search
File
Edit
View
Favorites
Tools
Help
You might get error saying "The sa password must me...
Page
Tools
Add or Remove Snap-ins
Available snap-ins:
Selected snap-ins:
Console Root
Edit Extensions ...
Remove
Move Up
Move Down
Select Group Policy Object
Welcome to the Group Policy Wizard
Group Policy Object:
Browse...
< Back
Finish
Cancel
Internet
100%

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monit...	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...

Description:

This snap-in allows you to edit the local Group Policy Obj

Select the group policy object

Local Group Policy Objects are stored on the local computer.

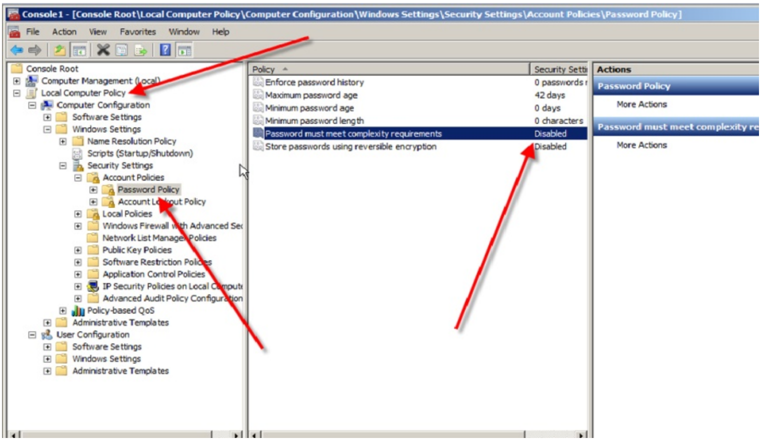
Use the Browse button to select one of the Group Policy Objects.

Group Policy Object: Local Computer

Local computer is what you need

□ Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

4. Disable (temporarily) the security policy:



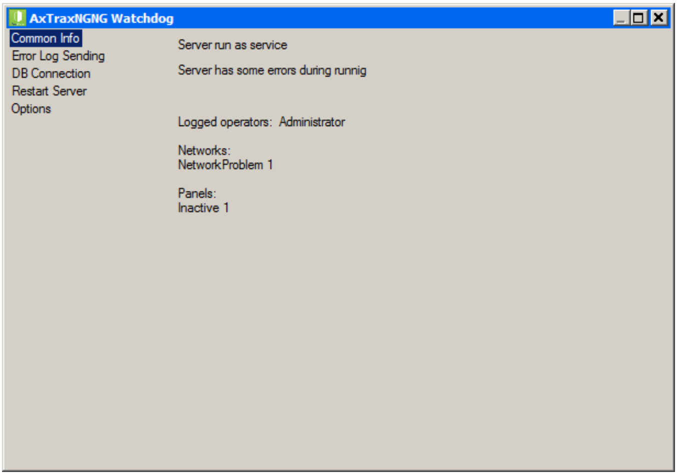
Console1 - [Console Root\Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy]
File
Action
View
Favorites
Window
Help
Console Root
Computer Management (Local)
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Sec
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Actions
Password Policy
More Actions
Password must meet complexity re
More Actions

Policy	Security Setti
Enforce password history	0 passwords r
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

L. AxTrax.NET Watchdog

The AxTrax.NET Watchdog is a program that monitors the AxTrax server.

Double-click the icon in the Window system tray to open the program.



Server run as service

Server has some errors during runnig

Logged operators: Administrator

Networks:
NetworkProblem 1

Panels:
Inactive 1

The main window contains the following five topics:

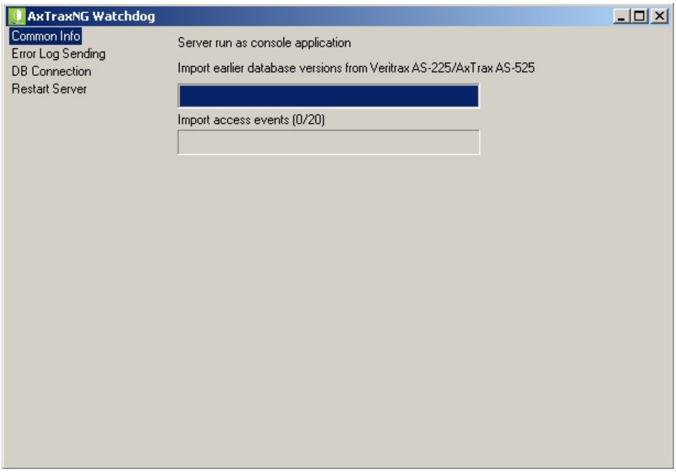
Parameter	Description
Common Info	Shows general system information
Error Log Sending	Sends error log to Rosslare Customer Support
DB Connection	Changes DB connection string **Note: Administrator password is required**
Restart Server	Restarts the AxTraxNG server **Note: Administrator password is required**
Options	• TimeKeeper synchronization • Use static IP option

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

L.1 Common Info

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

In addition, if you import an earlier database from VeriTrax AS-225/AxTrax AS-525, the progress of the import is displayed in Common Info.



Server run as console application

Import earlier database versions from Veritrax AS-225/AxTrax AS-525

Import access events (0/20)

L.2 Error Log Sending

If you are experiencing problems with the server, you can use this function to send a report to Rosslare Customer Support for help.

The *Error Log Sending* screen contains following fields:

Table 25: Watchdog > Error Log Sending Screen

Parameter	Description
Hardware Configuration	Select this checkbox if you want to sends Hardware configuration with Error log
Operating System	Sends OS version with Error log
List of Users	Sends Users list with Error log
List of Installed Programs	Sends List of installed programs with Error log
List of SQL Servers	Sends List of SQL Servers with Error log
Event Log Messages	Sends Windows Event Log with Error log
Ping Networks	Sends network ping result with Error log
Get connection string from server	Sends connection string of DB with error log This option is enabled when Ping Network checkbox is selected.

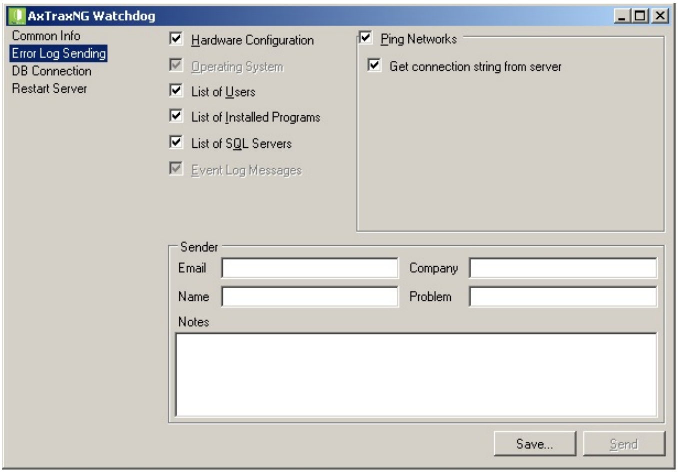
Parameter	Description
SQL Server*	PC address with SQL server installed
Database*	DB name
Username*	Username of DB
Password*	Password of DB
AxTraxNG/Old AxTrax radio buttons*	DB of AxTraxNG of Old AxTrax
Sender Section	
Email	Sender Email
Company	Sender Company
Name	Sender Name
Problem	Short description of problem
Buttons	
Save Button	Saves log to local machine
Send Button	Sends the log to Rosslare Customer Support

*These options are enabled when **Get connection string from server** is cleared.

To send an Error Log report:

1. Click the **Error Log Sending** topic.

   The *Error Log Sending* screen is displayed.



☑ Hardware Configuration
☑ Operating System
☑ List of Users
☑ List of Installed Programs
☑ List of SQL Servers
☑ Event Log Messages
☑ Ping Networks
☑ Get connection string from server

2. Select the relevant checkboxes.
3. In the Sender section, fill out the necessary fields.
4. Click **Send**.

L.3 DB Connection

This feature allows you to change the database connection string.

The *DB connection* screen contains following fields:

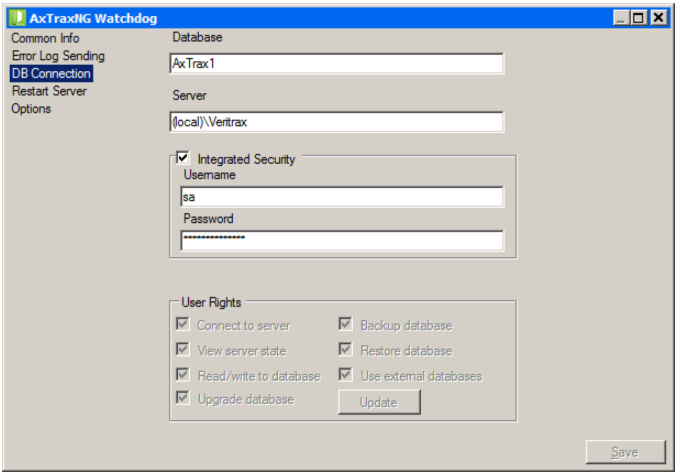
Table 26: Watchdog > DB Connection Screen

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.

To change the DB connection settings:

1. Click the **DB Connection** topic.
2. Enter the administrator password and click **OK**.

   The *DB Connection* screen is displayed.



Database: AxTrax1

Server: (local)\Veritrax

☑ Integrated Security

Username: sa

Password: ***************

User Rights

☑ Connect to server

☑ View server state

☑ Read/write to database

☑ Upgrade database

☑ Backup database

☑ Restore database

☑ Use external databases

3. Change the field parameters as desired.
4. Click **Save**.

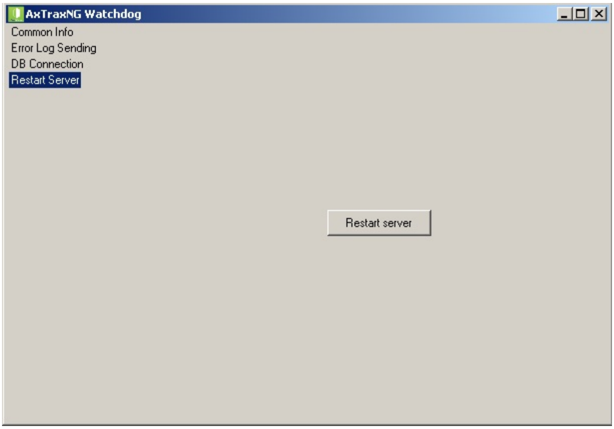
L.4 Restart Server

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* button appears.



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

   The server restarts within a few seconds.

L.5 Options

The *Options* screen contains following fields:

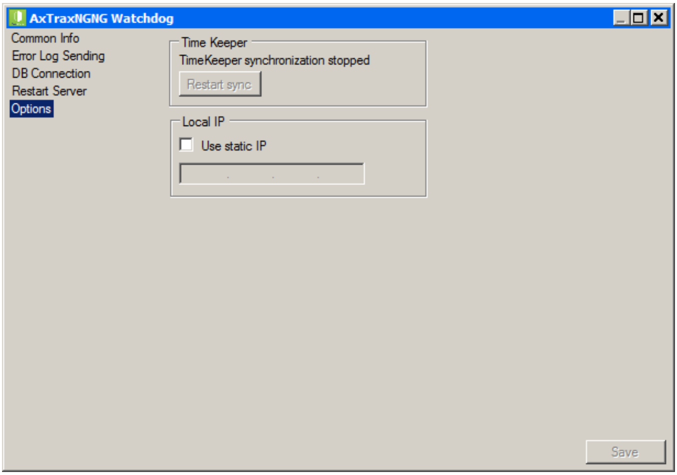
Table 27: Watchdog > Options Screen

Parameter	Description
TimeKeeper > Restart sync	The field shows the status of TimeKeeper synchronization (running, stopped, error, and so on) Click **Restart sync** to start the synchronization
Local IP > 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 Watchdog does not have permission to write in the server's directory, the option will fail. User the Readme.txt file to learn about Windows permissions.**

To change the DB connection settings:

1. Click the **DB Connection** topic.
2. Enter the administrator password and click **OK**.

   The *Options* screen is displayed.



TimeKeeper synchronization stopped

□ Use static IP

3. Change the field parameters as desired.
4. Click **Save**.

M. Adding Custom Wiegand Formats

The Wiegand protocol it 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.

M.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’.

M.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 M.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.

M.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’.
- 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’.

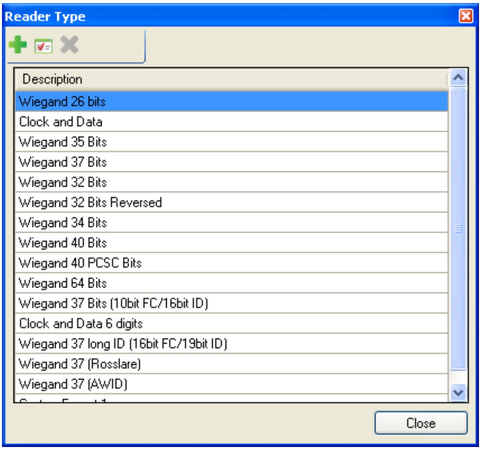
M.4 Creating New Rules

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.

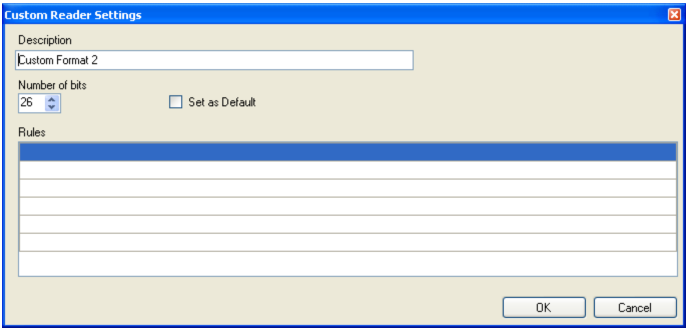
   The *Reader Type* window opens.



Description
Wiegand 26 bits
Clock and Data
Wiegand 35 Bits
Wiegand 37 Bits
Wiegand 32 Bits
Wiegand 32 Bits Reversed
Wiegand 34 Bits
Wiegand 40 Bits
Wiegand 40 PCSC Bits
Wiegand 64 Bits
Wiegand 37 Bits (10bit FC/16bit ID)
Clock and Data 6 digits
Wiegand 37 long ID (16bit FC/19bit ID)
Wiegand 37 (Rosslare)
Wiegand 37 (AWID)

3. Click the ✚ icon.

   The *Custom Reader Settings* window opens.



Description: Custom Format 2
Number of bits: 26
☐ Set as Default

4. Enter a description of the new rule.
5. Select the number of bits the new rule will use.
6. [Optional] Select **Set as Default**.
7. In the Rules section, enter the protocol rules according to the guidelines described in Sections M.1 through M.3 and as shown in the example below.

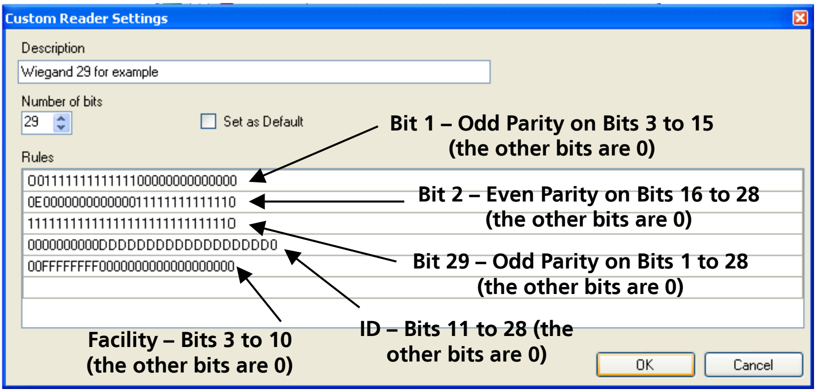
> **Note**
> The protocol definition is for the entire system and not per controller.

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.



Description: Wiegand 29 for example

Number of bits: 29

□ Set as Default

Rules

```
O01111111111111000000000000000
0E0000000000000111111111111110
1111111111111111111111111111O
0000000000DDDDDDDDDDDDDDDDDD0
00FFFFFFFF0000000000000000000
```

Bit 1 – Odd Parity on Bits 3 to 15 (the other bits are 0)

Bit 2 – Even Parity on Bits 16 to 28 (the other bits are 0)

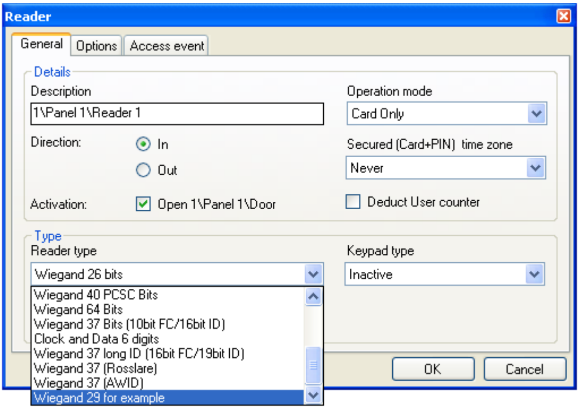
Bit 29 – Odd Parity on Bits 1 to 28 (the other bits are 0)

Facility – Bits 3 to 10 (the other bits are 0)

ID – Bits 11 to 28 (the other bits are 0)

> **Note**
> 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).

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



Description: 1\Panel 1\Reader 1

Operation mode: Card Only

Direction: ● In ○ Out

Secured (Card+PIN) time zone: Never

Activation: ☑ Open 1\Panel 1\Door

□ Deduct User counter

Reader type: Wiegand 26 bits

Keypad type: Inactive

```
Wiegand 40 PCSC Bits
Wiegand 64 Bits
Wiegand 37 Bits (10bit FC/16bit ID)
Clock and Data 6 digits
Wiegand 37 long ID (16bit FC/19bit ID)
Wiegand 37 (Rosslare)
Wiegand 37 (AWID)
Wiegand 29 for example
```

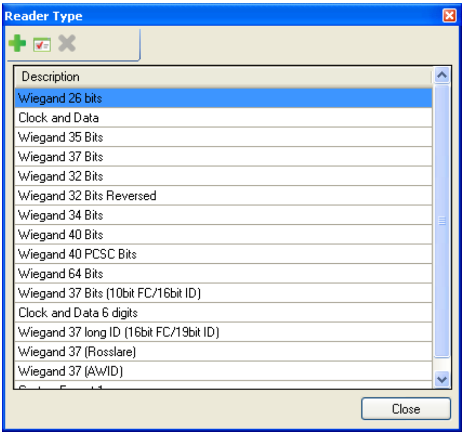
Adding Custom Wiegand Formats

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.

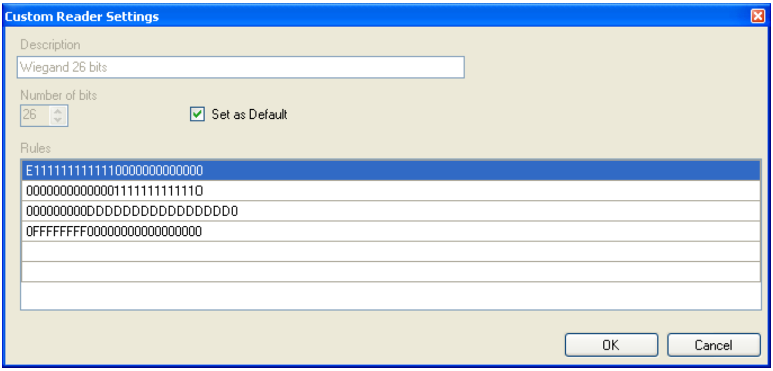


Description

- Wiegand 26 bits
- Clock and Data
- Wiegand 35 Bits
- Wiegand 37 Bits
- Wiegand 32 Bits
- Wiegand 32 Bits Reversed
- Wiegand 34 Bits
- Wiegand 40 Bits
- Wiegand 40 PCSC Bits
- Wiegand 64 Bits
- Wiegand 37 Bits (10bit FC/16bit ID)
- Clock and Data 6 digits
- Wiegand 37 long ID (16bit FC/19bit ID)
- Wiegand 37 (Rosslare)
- Wiegand 37 (AWID)

3. Double click 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.

   The *Custom Reader Settings* window opens.



Description: Wiegand 26 bits

Number of bits: 26

☑ Set as Default

Rules

```
E1111111111110000000000000
0000000000000111111111111O
000000000DDDDDDDDDDDDDDDD0
0FFFFFFFF00000000000000000
```

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

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

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.
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
Tel: +54-11-4001-3104
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
www.rosslaresecurity.com