AxTraxNG™
Access Control Management Software
Software Manual
Copyright © 2012 by Rosslare. All rights reserved.

This manual and the information contained herein are proprietary to REL, RSP Inc. and/or their related companies and/or subsidiaries’ (hereafter: “ROSSLARE”). Only ROSSLARE and its customers have the right to use the information.

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

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

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

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

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

1. Introduction ........................................................................... 13
   1.1 System Features ......................................................................... 13
   1.1.1 Access Control ........................................................................ 13
   1.1.2 Access Monitoring ................................................................. 14
   1.1.3 Software Security ................................................................. 14
   1.2 AxTraxNG™ Server and Client ............................................... 14
   1.3 Using this User Guide .............................................................. 14

2. Specifications and Requirements .................................. 16
   2.1 System Capabilities .................................................................. 16
   2.2 System Requirements .............................................................. 17
      2.2.1 AxTraxNG™ Server and Client Requirements ......................... 17
      2.2.2 SQL Express Server Requirements ........................................... 17

3. Installation ............................................................... 18
   3.1 Choosing an SQL Server ......................................................... 18
   3.2 Preparing the AxTraxNG™ Installation ...................................... 18
   3.3 Installing Prerequisite Software for the AxTraxNG™ Client .......... 20
   3.4 Installing AxTraxNG™ Client Software .................................... 22
   3.5 Installing AxTraxNG™ Network Server Software ....................... 25
   3.6 Installing AxTraxNG™ Watchdog .......................................... 30
   3.7 Video Enhancement for AC-525 Setup ..................................... 35
   3.8 Firewall Settings ...................................................................... 35
   3.9 SQL Server Settings ................................................................. 35

4. System Overview .......................................................... 36
   4.1 Starting the Software ............................................................... 36
   4.2 AxTraxNG™ Main Window ..................................................... 37
   4.3 Menu Bar ................................................................................ 38
      4.3.1 File Menu ........................................................................... 38
      4.3.2 Tools Menu ................................................................. 39
# Table of Contents

4.3.3 View Menu .................................................................................................................. 39  
4.3.4 Help Menu .................................................................................................................. 39  
4.4 Toolbar ............................................................................................................................. 39  
4.4.1 General Icons ............................................................................................................. 40  
4.4.2 General Network Icons ............................................................................................. 40  
4.4.3 Network Icons ............................................................................................................. 40  
4.4.4 Panel Icons ................................................................................................................... 41  
4.4.5 Card\Users Icons ........................................................................................................ 41  
4.4.6 Reports Icons ............................................................................................................. 41  
4.4.7 Events Icons ............................................................................................................... 42  
4.5 Tree View ......................................................................................................................... 43  
4.5.1 Networks ..................................................................................................................... 43  
4.5.2 Timing .......................................................................................................................... 43  
4.5.3 Groups ........................................................................................................................ 44  
4.5.4 Global Antipassback ................................................................................................. 44  
4.5.5 Users ........................................................................................................................... 44  
4.5.6 Status Map .................................................................................................................. 45  
4.5.7 Reports ........................................................................................................................ 45  

## 5. How to Set Up a Site .................................................................................................. 46  
5.1 Adding Time Zones ....................................................................................................... 47  
5.2 Adding Holidays ........................................................................................................... 48  
5.3 Adding a Network .......................................................................................................... 49  
5.4 Adding Access Control Panels ...................................................................................... 53  
5.4.1 General Panel Settings ............................................................................................... 54  
5.4.2 Adding a Panel ............................................................................................................. 54  
5.4.3 Editing the Panel ......................................................................................................... 57  
5.5 Configuring the Doors ................................................................................................... 61  
5.6 Configuring the Readers ............................................................................................... 62  
5.6.1 General Tab .................................................................................................................. 63  
5.6.2 Options Tab ................................................................................................................ 64  
5.6.3 Access Event .............................................................................................................. 66  
5.7 Configuring the Inputs ................................................................................................... 67  
5.8 Adding Panel Links ....................................................................................................... 68
# Table of Contents

5.9 Creating Groups ........................................................................................................... 72
  5.9.1 Adding Access Groups ......................................................................................... 72
  5.9.2 Adding Input Groups ......................................................................................... 73
  5.9.3 Adding Output Groups ....................................................................................... 74
5.10 Adding Users and Cards ......................................................................................... 76
5.11 Adding Departments, Users, and Visitors .............................................................. 78
  5.11.1 Adding Departments ......................................................................................... 78
  5.11.2 Adding Users .................................................................................................. 78
  5.11.3 Adding Visitors ............................................................................................... 83
5.12 Adding Access Areas ............................................................................................... 84
5.13 Adding Global Antipassback Rules ...................................................................... 85
5.14 Adding Operators .................................................................................................. 86
5.15 Creating Elevator Control ...................................................................................... 88
5.16 Creating Status Maps ............................................................................................. 88

6. ViTrax Video Integration ............................................................................................ 93
  6.1 Connecting to ViTrax Server .................................................................................. 93
  6.2 Adding a Camera to the AC-525 Panel ................................................................. 95
  6.3 Conditioned Recording via Panel Links ................................................................ 95
  6.4 Viewing Recorded Events ...................................................................................... 96
  6.5 Automated ViTrax Camera Activation Options .................................................. 99
    6.5.1 Reader Access ................................................................................................. 99
    6.5.2 Alarm Event ..................................................................................................100
    6.5.3 Camera Event ...............................................................................................101
    6.5.4 Door Warning Event ....................................................................................102

7. Manual Operation ........................................................................................................ 103
  7.1 Controlling the Door Manually .............................................................................103
  7.2 Changing the Reader Mode ....................................................................................104
  7.3 Controlling Outputs Manually ..............................................................................105
  7.4 Manually Disarming Inputs ...................................................................................106
  7.5 Controlling Sirens Manually ................................................................................107
  7.6 Manually Update Firmware ..................................................................................108
# Table of Contents

8. **AxTraxNG™ Reports** ......................................................... 109

8.1 Immediate Reports.............................................................. 109
8.2 Archive Reports .................................................................. 110
8.2.1 Panels Events Reports ...................................................... 110
8.2.2 System AxTraxNG™ Events Report ................................... 111
8.2.3 Interactive Report .............................................................. 111

9. **Administrator Operations** .............................................. 113

9.1 Setting the Time and Date ..................................................... 113
9.2 Downloading Failed Data ..................................................... 113
9.3 Testing User Counters .......................................................... 114
9.4 Maintaining the Database .................................................... 114
9.5 AxTraxNG™ Options and Preferences ................................... 116
9.5.1 General Tab ...................................................................... 116
9.5.2 User Custom Fields ........................................................... 117
9.6 Importing/Exporting User Data ............................................ 118
9.7 AxTrax GUI View Options .................................................... 119

A. **Firewall Configuration** ..................................................... 121

B. **SQL Service Settings** ..................................................... 125

C. **Network Configuration** .................................................... 127

D. **Restoring Factory Default Settings** .................................. 133

E. **Cross Platform Camera Setup** ........................................ 134

F. **Enrolling Cards using MD-08 Desktop Reader** ............... 137

G. **SQL Server Installation Troubleshoot** ............................. 138

H. **AxTrax.NET Watchdog** ................................................... 141

H.1 Common Info ..................................................................... 142
H.2 Error Log Sending .............................................................. 142
H.3 DB Connection ................................................................. 144
H.4 Restart Server .................................................................... 144
List of Figures

Figure 1: Installation Initiation Screen ............................................................ 19
Figure 2: AxTraxNG™ Elements Selection Screen ........................................... 19
Figure 3: Crystal Report Installation Start Installation ..................................... 20
Figure 4: Report Runtime Installation Progress .............................................. 21
Figure 5: Microsoft Visual C++ 2005 Redistributable – Start Installation ........ 21
Figure 6: Microsoft Visual C++ – License Agreement ..................................... 22
Figure 7: Microsoft Visual C++ 2005 Redistributable – Installation ............... 22
Figure 8: AxTraxNG™ Client – Welcome Screen ............................................. 23
Figure 9: AxTraxNG™ Client – Destination Folder Screen ............................... 23
Figure 10: AxTraxNG™ Client – Ready to Install Program Screen ................. 24
Figure 11: AxTraxNG™ Client – Installing AxTraxNG™ Client Screen ............. 24
Figure 12: AxTraxNG™ Client – InstallShield Wizard Completed Screen ......... 25
Figure 13: SQL Server Installation Requirements Screen .............................. 25
Figure 14: AxTraxNG™ Server – Wizard Welcome Screen .............................. 26
Figure 15: AxTraxNG™ Server – Setup Type Screen ........................................ 26
Figure 16: AxTraxNG™ Server – Destination Folder Screen ............................ 27
Figure 17: AxTraxNG™ Server – Database Server Screen ............................... 27
Figure 18: AxTraxNG™ Server – Selection Browse Window ............................ 28
Figure 19: AxTraxNG™ Server – Ready to Install the Program Screen ............. 29
Figure 20: AxTraxNG™ Server – Installing AxTraxNG™ Server Screen .......... 29
Figure 21: AxTraxNG™ Server – Install Shield Wizard Completed Screen ....... 30
Figure 22: AxTraxNG™ Watchdog – Preparing to Install Screen .................. 30
Figure 23: AxTraxNG™ Watchdog – Welcome Screen .................................... 31
Figure 24: AxTraxNG™ Watchdog – Destination Folder Screen ...................... 32
Figure 25: AxTraxNG™ Watchdog – Ready to Install the Program Screen ...... 32
Figure 26: AxTraxNG™ Watchdog – Installing AxTraxNG™ Watchdog Screen 33
Figure 27: AxTraxNG™ Watchdog – InstallShield Wizard Completed Screen . 34
List of Figures

Figure 28: AxTraxNG™ Watchdog – Install Shield Wizard Completed Screen 34
Figure 29: AxTraxNG™ Server is Connected ........................................................... 34
Figure 30: AxTraxNG™ Server Connection Dialog Box ......................................... 36
Figure 31: AxTraxNG™ Software Logon Dialog Box ............................................ 37
Figure 32: AxTraxNG™ Client Main Window ......................................................... 37
Figure 33: Add Time Zone Window ....................................................................... 47
Figure 34: Options Window .................................................................................. 48
Figure 35: Outlook Holidays Window .................................................................... 48
Figure 36: Holiday Properties Window .................................................................. 49
Figure 37: Available Networks ............................................................................. 50
Figure 38: Network Window – General Tab ........................................................... 50
Figure 39: Network Window – Options Tab ........................................................... 52
Figure 40: Network Options Tab – Network’s Time Zone Area .............................. 52
Figure 41: Door Controller > Panel Properties > General Tab ............................... 55
Figure 42: Panel Connection Test ......................................................................... 56
Figure 43: Find Panels Window ............................................................................. 57
Figure 44: Available Panel in a Network ................................................................. 59
Figure 45: Networks > Panel Properties > Antipassback Tab ................................. 60
Figure 46: Panel Properties window – Options Tab ................................................. 60
Figure 47: Door Properties Window ....................................................................... 62
Figure 48: Reader Properties Window – General Tab ............................................. 63
Figure 49: Reader Properties window – Options Tab ............................................. 65
Figure 50: Reader Properties window – Access Event Tab .................................... 66
Figure 51: Input Properties Window ...................................................................... 68
Figure 52: Add Link Window ................................................................................ 70
Figure 53: Alarm Handler Window ....................................................................... 70
Figure 54: Link Window ....................................................................................... 71
Figure 55: Open all Outputs of Selected Output Group Checkbox ........................... 72
Figure 56: Add Access Group Window ................................................................. 72
Figure 57: Access Group Properties Window ....................................................... 73
List of Figures

Figure 58: Add Input Group Window ............................................................ 74
Figure 59: Add Input Group – Network Expanded ......................................... 74
Figure 60: Add Output Group Window .......................................................... 75
Figure 61: Add Output Group – Network Expanded ...................................... 75
Figure 62: Add Users and Cards Window ...................................................... 77
Figure 63: Add Department Dialog ............................................................... 78
Figure 64: Add User Window – General Tab ................................................. 79
Figure 65: Add User Window – Codes Tab .................................................... 81
Figure 66: Add User Window – Details Tab ................................................... 82
Figure 67: User Properties Window – Visitor’s Options Tab ......................... 84
Figure 68: Add Access Area Window ............................................................ 85
Figure 69: Add Global Antipassback Window .............................................. 86
Figure 70: Add Operator Window ............................................................... 87
Figure 71: Operator Password Window ........................................................ 87
Figure 72: Add Status Map Window ............................................................. 89
Figure 73: Status Map with Image ............................................................... 90
Figure 74: Status Map with Door ................................................................. 91
Figure 75: Show on Map Window ............................................................... 91
Figure 76: ViTrax Servers Window ............................................................. 93
Figure 77: Server ViTrax window ............................................................... 94
Figure 78: ViTrax Servers List ................................................................. 94
Figure 79: Cameras Window ........................................................................ 95
Figure 80: Panel Link – Local Recording ..................................................... 96
Figure 81: Camera Properties Window ....................................................... 97
Figure 82: Available Camera List ............................................................... 98
Figure 83: Live Video Streaming ............................................................... 99
Figure 84: Enable Cameras Pop-Up Options by Events .............................. 100
Figure 85: Enable Cameras Pop-Up Options by Alarm Handler Events ........ 101
Figure 86: Video Popup and Snapshot Window .......................................... 101
Figure 87: Enable Cameras Options by Door Warning Events .................. 102
List of Figures

Figure 88: Manual Door Operation Window ................................................... 103
Figure 89: Manual Reader Operations Window .............................................. 105
Figure 90: Manual Output Operation Window ............................................. 106
Figure 91: Manual Input Operation Window .............................................. 107
Figure 92: Manual Siren Operation Window .............................................. 108
Figure 93: Manual Firmware Update Window ............................................ 108
Figure 94: Immediate Report Wizard (Step 1) ........................................... 110
Figure 95: Archives Report Wizard (Step 1) .......................................... 112
Figure 96: Set Time Window .................................................................. 113
Figure 97: Request User Count Window .................................................. 114
Figure 98: Database Window ................................................................. 115
Figure 99: General Tab ........................................................................ 116
Figure 100: User Custom Fields Tab ...................................................... 117
Figure 101: Import Data Window ............................................................ 118
Figure 102: Control Panel Window .......................................................... 121
Figure 103: Windows Security Center Window ........................................ 121
Figure 104: Windows Firewall ................................................................ 122
Figure 105: Add a Program Window ..................................................... 122
Figure 106: Performance and Maintenance Window .............................. 123
Figure 107: Administrative Tools Window ............................................. 124
Figure 108: Services Console ................................................................. 124
Figure 109: SQL Service Settings ........................................................... 125
Figure 110: SQL Service Log On ............................................................. 125
Figure 111: TCP/IP Configuration Window ............................................ 128
Figure 112: AxTraxNG™ Modem Network .......................................... 129
Figure 113: AxTraxNG™ Computer Modem Configuration ...................... 129
Figure 114: AxTraxNG™ Remote Modem Configuration ......................... 130
Figure 115: AxTraxNG™ Modem Status ............................................... 131
Figure 116: AxTraxNG™ Modem Security ........................................... 132
Figure 117: Camera List ....................................................................... 135
List of Figures

Figure 118: Add Cards from MD-08 Window ............................................. 137
Figure 119: Domain Controller Security Settings Window ......................... 138
Figure 120: Add/ Remove Snap-in Option .................................................. 139
Figure 121: Add a Group ............................................................................ 140
Figure 122: Domain Controller Security Options ........................................ 140
Figure 123: AxTraxNG Watchdog – Main Window .................................... 141
Figure 124: AxTraxNG Watchdog – Progress of Database Import Window... 142
Figure 125: AxTraxNG Watchdog – Error Log Sending Window ................. 143
Figure 126: AxTraxNG Watchdog – DB Connection Window ....................... 144
Figure 127: AxTraxNG Watchdog – Restart Server Button ......................... 145
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.
- REL, RSP Inc. and/or their related companies and/or subsidiaries’ (hereafter: "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.
- 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, and AC-525 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 00.12.00 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
Introduction

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
- Clients connect to the server using Serial communication (RS-485) or LAN remote communication technology
- The server runs as a Windows service by default
- The client software is based on dynamic docking technology

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, or AC-525 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
Introduction

- 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

<table>
<thead>
<tr>
<th>Software Architecture</th>
<th>Client-Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>SQL Server Express 2005, 2008</td>
</tr>
</tbody>
</table>
| Max. Number of Users  | • 30,000 per panel (AC225, AC425, AC525)  
                        | • 5000 (AC215)     |
| Max. Access Groups    | Based on the maximum number of users, 30,000 x the number of panels |
| Max. Number of Time Zones | 32         |
| Max. Cards per User   | 15            |
| Max. Number of Doors  | 8184          |
| Max. Access Control Panels | 1023       |
| Antipassback          | • Timed  
                        | • Door  
                        | • Global – across the entire facility |
| International Holiday Support | Up to 64 holidays |

#### Networks

<table>
<thead>
<tr>
<th>Max. Number of Networks</th>
<th>Unlimited</th>
</tr>
</thead>
</table>
| Supported Access Control Panel Models | • AC-215  
                                           | • AC-215 (SPV)  
                                           | • 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 |
| Panel Networks Communication Interface | • Serial (RS-232/485)  
                                                   | • TCP-IP  
                                                   | • Modem |
| Communication Speed     | 9600, 19200, 57600, and 115200 bps |
Specifications and Requirements

2.2 System Requirements

2.2.1 AxTraxNG™ Server and Client Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows XP SP2, Windows Server 2003, Windows Server 2008 (32/64 bits), Windows Vista, or Windows 7 (32/64 bits)</td>
</tr>
<tr>
<td>Processor</td>
<td>Pentium 4 or better</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
</tr>
<tr>
<td>Network</td>
<td>LAN card required for TCP/IP networking</td>
</tr>
<tr>
<td>Hard Disk Space</td>
<td>4 GB minimum</td>
</tr>
</tbody>
</table>

2.2.2 SQL Express Server Requirements

SQL Server Express is not always required. See Section 3.1 for further information.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Pentium 4 or better</td>
</tr>
<tr>
<td>Memory</td>
<td>2 GB</td>
</tr>
<tr>
<td>Hard Disk Space</td>
<td>4 GB</td>
</tr>
</tbody>
</table>
3. Installation

The AxTraxNG™ installation CD-ROM includes all the setup files required to install the AxTraxNG™ Access Control software on the system’s main computer. The software system consists of the following four main components:

- AxTraxNG™ Server – Manages the database linked to the access control panels
- AxTraxNG™ Client – Configures the system
  The AxTraxNG™ Client is only needed on the main computer; however, it can be installed on additional computers as needed to help monitor the system.
- ViTrax software – Enables video integration (if needed)
- AxTraxNG™ Watchdog
- Microsoft® .NET 3.5 Framework SP1

Microsoft® .NET Framework is prerequisite software. It must be installed on any Microsoft Windows® operating system older than Windows 7.

3.1 Choosing an SQL Server

The AxTraxNG™ Server operates using an SQL server 2005/2008 database. If there is already an SQL 2005/2008 server available on your computer network, use it to run the AxTraxNG™ database using your SQL login credentials.

Alternatively, install Microsoft SQL Server Express on the computer that uses the AxTraxNG™ server.

Note: Do not install the SQL server when installing additional AxTraxNG™ clients, which connect to the AxTraxNG™ Server database.

3.2 Preparing 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 installing the AxTraxNG™:

1. Insert the CD into your computer's CD drive.
2. Double-click the AxTraxNG™ setup file.
   The AxTraxNG Setup screen opens.
Installation

3. To select a new destination folder for the installation of the system, either type the destination in the Destination folder text box or click Browse… to browse to the required folder.

4. Click Install to start the installation process.

   Following the extraction of the installation package, the AxTraxNG™ elements selection screen appears:

   ![AxTraxNG™ Elements Selection Screen](image)

   **Note**
   
   If the AxTraxNG™ Server or Client setup detects a previous version of AxTraxNG, a prompt appears asking if you want to upgrade AxTraxNG™ to the newer version.

   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.

   ![AxTraxNG™ Installation Requirements Screen](image)

   **Figure 1: Installation Initiation Screen**

   **Figure 2: AxTraxNG™ Elements Selection Screen**
Installation

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

5. Check the configuration you wish to install.

When installing the ViTrax software for video integration, make sure to install it on every client PC as well as on the server PC.

6. Click **Start**.

The installation process of the prerequisite applications for the AxTraxNG™ Client begins.

The installation of the following prerequisite applications and subsequent AxTraxNG™ Client software installation can be performed on as many computers as you wish.

### 3.3 Installing Prerequisite Software for the AxTraxNG™ Client

The Crystal reports Business objects library application is the first prerequisite application to install.

The *Crystal Reports Basic Runtime for Visual Studio 2008* screen opens automatically.

![Crystal Reports Basic Runtime for Visual Studio 2008](image)

*Figure 3: Crystal Report Installation Start Installation*
Installation

To install the prerequisite software for AxTraxNG™ Client:

1. Wait while the Crystal Report Runtime installs.

![Figure 4: Report Runtime Installation Progress](image)

When the Crystal Report Runtime Installation finishes, the installation of Microsoft Visual C++ 2005 Redistributable automatically begins.


![Figure 5: Microsoft Visual C++ 2005 Redistributable – Start Installation](image)
Installation

3. Click **Yes** to agree to the License Agreement.

![License Agreement](image1.png)

**Figure 6: Microsoft Visual C++ – License Agreement**

The Microsoft Visual C++ installation begins.

![Installation](image2.png)

**Figure 7: Microsoft Visual C++ 2005 Redistributable – Installation**

Once the installation finishes, the AxTraxNG™ Client installation begins.

### 3.4 Installing AxTraxNG™ Client Software

The installation wizard opens automatically once the prerequisite software is installed.
To install the AxTraxNG™ Client application:

1. Click **Next** to begin the AxTraxNG™ Client installation process. The Destination Folder screen opens.

2. If you wish to select a new destination folder for the AxTraxNG™ client, click **Change** and browse to the required folder.

3. Click **Next**.
   The Ready to Install the Program screen opens.
Installation

4. Click **Install**.

   The *Installing AxTraxNG Client* screen opens.

   ![AxTraxNG Client – Installing AxTraxNG Client Screen](image)

   *Figure 11: AxTraxNG™ Client – Installing AxTraxNG™ Client Screen*

When the installation is complete, the *InstallShield Wizard Completed* screen opens.
5. Click **Finish** to complete installing the AxTraxNG™ Client software.

### 3.5 Installing AxTraxNG™ Network Server Software

Following the prerequisite software and AxTraxNG™ Client software installations, the AxTraxNG™ Install Shield Wizard for the AxTraxNG™ Server software installation appears.

If there is no SQL server installed, the Installation Requirements screen opens. Click **Install** and follow the steps to install the SQL server.

**To install the AxTraxNG™ Server:**

1. Wait while the AxTraxNG™ server prepares to install.
The Welcome to the Install Shield Wizard screen opens.

Figure 14: AxTraxNG™ Server – Wizard Welcome Screen

2. Click **Next**.
   The *Setup Type* screen opens.

   Figure 15: AxTraxNG™ Server – Setup Type Screen

3. Select the **Server** option, and then click **Next**.
   The *Destination Folder* screen opens.
4. To select a new destination folder for the AxTraxNG™ server, click Change, and browse for the required folder.

5. Click Next.

The Database Server screen opens.

6. For the Database Server field, do one of the following:
   a. Select the database server name from the dropdown list or use the default location (local)\VERITRAX.
   b. Click Browse... to choose the database server location.
The AxTraxNG™ Server and SQL Server databases must be installed on the same PC.

c. For database servers installed from the AxTraxNG™ Server setup program ("SQL Server express"), add the instance name "\VeriTrax" to the database computer name and click **OK**. You return to the previous window.

7. In **Connect using**, choose **Server authentication using the Login ID and password below**.

   The only condition for choosing the **Windows authentication credentials of current user** option is that you are using an existing SQL database installed using Windows authentication only and not from the VeriTrax Setup.

8. Click **Next**.

   The Ready to Install the Program screen opens.
Installation

9. Click **Install**.

The *Installing AxTraxNG Server* screen opens.

When the installation is complete, the *Install Shield Wizard Completed* screen opens.
10. Click **Finish** to complete installing the AxTraxNG™ Server software.

   ![Figure 21: AxTraxNG™ Server – Install Shield Wizard Completed Screen](image)

   **Figure 21: AxTraxNG™ Server – Install Shield Wizard Completed Screen**

   Turn off the Hard Disk Off option to avoid disconnecting panels from the server when a computer goes into Sleep mode.

3.6 **Installing AxTraxNG™ Watchdog**

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

![Figure 22: AxTraxNG™ Watchdog – Preparing to Install Screen](image)

**Figure 22: AxTraxNG™ Watchdog – Preparing to Install Screen**
Installation

To install the AxTraxNG™ Watchdog:

1. Wait for Preparing process to finish.
   The AxTraxNG™ Watchdog Installation Wizard opens.

   ![AxTraxNG Watchdog – Welcome Screen](image)

   **Figure 23: AxTraxNG™ Watchdog – Welcome Screen**

2. Click **Next** to initiate the AxTraxNG™ Watchdog installation process.
   The Destination Folder screen opens.
3. If you wish to select a new destination folder for the AxTraxNG™ Watchdog, click **Change** and browse for the required folder.

4. Click **Next**.

The Ready to Install the Program screen opens.
Installation

5. Click **Install**.
   The installation process begins.

![AxTraxNG™ Watchdog – Installing AxTraxNG™ Watchdog Screen](image)

**Figure 26: AxTraxNG™ Watchdog – Installing AxTraxNG™ Watchdog Screen**

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

6. Click **Finish** to complete the AxTraxNG™ Watchdog software installation. A window opens telling you to restart the computer.

7. Click **OK**.
   
   You return to the AxTraxNG™ Elements Selection Screen (Figure 2).

8. Click **Close** and then 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.
3.7 Video Enhancement for AC-525 Setup

AxTraxNG™ can connect with single or multiple ViTrax servers installed in a LAN or WAN configuration.

Make sure to check AxTraxNG™ and ViTrax version compatibility.

To install ViTrax Server and Client applications, refer to the ViTrax Software manual.

When installing AxTraxNG™ on a different PC, make sure that the ViTrax Server has already been installed (no license is required for that ViTrax Server).

To add cameras for AC-525:

1. Activate the ViTrax Server and Client (see ViTrax Software manual).
2. Define ViTrax Servers (see Section 6.1).
3. Define communication of AC-525 cameras to the ViTrax Server (see Section 6.2).
4. Activate AxTraxNG™ and configure it (see Chapters 4 and 5).

3.8 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.

3.9 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.

If SQL Express 2005 is being installed (part of the installation package), the installation must be on the same Windows user account that is being used for AxTraxNG™.
System 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.

4.1 Starting the Software

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.
   If the AxTraxNG™ server is installed on a different PC, the Server connection dialog box appears.

   ![Figure 30: AxTraxNG™ Server Connection Dialog Box](image)

   If the AxTraxNG™ server is installed on the same PC, skip to Step 5 (after the Logon AxTraxNG Client Dialog box appears).

2. Type the AxTraxNG™ server’s PC IP address in the IP Address text box.
3. Select the AxTraxNG™ server’s PC Port from the Port select box.
4. Click OK.
   The Server connection dialog box closes and the Logon AxTraxNG Client dialog box appears.
4.2 AxTraxNG™ Main Window

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

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

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

6. Click **OK**.

   The main AxTraxNG™ window opens.
System Overview

The AxTraxNG™ Client Main window is divided into six adjustable sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Menu Bar</td>
<td>The Menu bar controls the software’s general operation and setup. For more information, see Section 4.3.</td>
</tr>
<tr>
<td>2 Toolbar</td>
<td>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 4.4.</td>
</tr>
<tr>
<td>3 Tree View</td>
<td>The Tree View allows users to configure, monitor, and control every aspect of access control. For more information, see Section 4.5.</td>
</tr>
<tr>
<td>4 Event Log</td>
<td>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, including video stream archives that are saved to the ViTrax database.</td>
</tr>
<tr>
<td>5 Display Area</td>
<td>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.</td>
</tr>
<tr>
<td>6 Status Bar</td>
<td>The Status Bar displays server connection status, Downloads Counter, and the Firmware programming progress bar.</td>
</tr>
</tbody>
</table>

4.3 Menu Bar

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

4.3.1 File Menu

The File menu has three options:

<table>
<thead>
<tr>
<th>Menu</th>
<th>Select Menu item to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Connection</td>
<td>Log on to the AxTraxNG™ server</td>
</tr>
<tr>
<td>ViTrax Server</td>
<td>Log on to the ViTrax server</td>
</tr>
<tr>
<td>Exit</td>
<td>Exit the AxTraxNG™ software</td>
</tr>
</tbody>
</table>
4.3.2 Tools Menu

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

<table>
<thead>
<tr>
<th>Menu</th>
<th>Select Menu item to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>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</td>
</tr>
<tr>
<td>Options</td>
<td>Set software options and preferences, including national holidays, event highlighting, custom user information fields, and GUI language</td>
</tr>
<tr>
<td>Import/Export Data</td>
<td>Import/export user information from/to an Excel spreadsheet file.</td>
</tr>
</tbody>
</table>

4.3.3 View Menu

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

<table>
<thead>
<tr>
<th>Menu</th>
<th>Select Menu item to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>Check the option to show event logs</td>
</tr>
<tr>
<td>Table View</td>
<td>Check the option to show a detailed table view</td>
</tr>
<tr>
<td>Restore Docking</td>
<td>Restore the default GUI view</td>
</tr>
<tr>
<td>Close All Floating</td>
<td>Close all pop-up windows at once</td>
</tr>
</tbody>
</table>

4.3.4 Help Menu

The help menu has one option:

<table>
<thead>
<tr>
<th>Menu</th>
<th>Select menu item to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>About</td>
<td>View software, firmware, and database version information, as well as the current operator</td>
</tr>
</tbody>
</table>

4.4 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:
### 4.4.1 General Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Click icon to…</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Manual Door Operation" /></td>
<td>Manual Door Operation</td>
<td>Open the <em>Door Manual Operation</em> window (see Section 7.1)</td>
</tr>
<tr>
<td><img src="image" alt="Print" /></td>
<td>Print</td>
<td>Send the current display area view to the printer</td>
</tr>
<tr>
<td><img src="image" alt="Add" /></td>
<td>Add</td>
<td>Add a new element of the selected type</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Edit</td>
<td>Edit the selected element</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Delete</td>
<td>Delete the selected item</td>
</tr>
</tbody>
</table>

### 4.4.2 General Network Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Click icon to…</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add to Status Map" /></td>
<td>Add to Status Map</td>
<td>Add available panels and panel components to the Status Map (see Section 4.5.6)</td>
</tr>
<tr>
<td><img src="image" alt="Download Failed Data Manually" /></td>
<td>Download Failed Data Manually</td>
<td>Download the entire panels’ failed database (see Section 9.2)</td>
</tr>
</tbody>
</table>

### 4.4.3 Network Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Click icon to…</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Set Time" /></td>
<td>Set Time</td>
<td>Set the time on the selected access control panel (see Section 9.1)</td>
</tr>
<tr>
<td><img src="image" alt="Find Panels" /></td>
<td>Find Panels</td>
<td>Find and update panels within the network (see Section Error! Reference source not found.)</td>
</tr>
<tr>
<td><img src="image" alt="Manual Modem" /></td>
<td>Manual Modem</td>
<td>Open the <em>Modem Status</em> window to allow the operator to connect or disconnect the modem and change the connection password (see Appendix C)</td>
</tr>
<tr>
<td><img src="image" alt="Camera" /></td>
<td>Camera</td>
<td>View a list of connected cameras, and assign the cameras to panels (see Section 6.2)</td>
</tr>
</tbody>
</table>
## System Overview

### 4.4.4 Panel Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Click icon to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Reader</td>
<td>Change the operation mode of the readers on the selected panel (see Section 7.2)</td>
<td></td>
</tr>
<tr>
<td>Update Firmware</td>
<td>Send a firmware update to the selected access control panel (see Section 7.6)</td>
<td></td>
</tr>
<tr>
<td>Control Output Manually</td>
<td>Change the settings for the outputs on the selected panel (see Section 7.3)</td>
<td></td>
</tr>
<tr>
<td>Control Input Manually</td>
<td>Change the settings for the inputs on the selected panel (see Section 7.4)</td>
<td></td>
</tr>
<tr>
<td>Control Siren Manually</td>
<td>Test the siren for the selected panel (see Section 7.5)</td>
<td></td>
</tr>
</tbody>
</table>

### 4.4.5 Card/Users Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Click icon to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Counter</td>
<td>View the current user count value (see Section 9.3)</td>
<td></td>
</tr>
<tr>
<td>Add users</td>
<td>Create up to 1000 new users in one click (Section 5.10)</td>
<td></td>
</tr>
<tr>
<td>Add cards</td>
<td>Create up to 1000 new cards in one click (Section 5.10)</td>
<td></td>
</tr>
<tr>
<td>Assign cards</td>
<td>Add and assign cards to selected users or add cards from MD-08 (see Appendix F)</td>
<td></td>
</tr>
<tr>
<td>User Filter</td>
<td>Filter the list of users by various parameters, such as name and card number (see Section 4.5.5.3)</td>
<td></td>
</tr>
</tbody>
</table>

### 4.4.6 Reports Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Click icon to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Produce Report</td>
<td>Produce the selected report (Chapter 8)</td>
<td></td>
</tr>
<tr>
<td>Print</td>
<td>Send the current report to the printer</td>
<td></td>
</tr>
<tr>
<td>View Last Hour Access</td>
<td>Display relevant access events that occurred within the last hour (Chapter 8)</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This icon appears only when a Roll Call – Readers report is selected.</td>
<td></td>
</tr>
</tbody>
</table>
### System Overview

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Click icon to...</th>
</tr>
</thead>
</table>
| ![View Periodic Access](image) | View Periodic Access | Displays relevant access events that occurred within a selected time frame (Chapter 8)  
**Note:** This icon appears only when a Roll Call – Readers report is selected. |

#### 4.4.7 Events Icons

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Click icon to...</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Panel" /></td>
<td>Panel</td>
<td>Display all event types uploaded from the access control units</td>
</tr>
<tr>
<td><img src="image" alt="Access" /></td>
<td>Access</td>
<td>Display only access events uploaded from access control units</td>
</tr>
<tr>
<td><img src="image" alt="Alarm" /></td>
<td>Alarm</td>
<td>Display only alarm events uploaded from access control units</td>
</tr>
<tr>
<td><img src="image" alt="Archive" /></td>
<td>Archive</td>
<td>Display video stream archive events stored in either the ViTrax database, the USB key, or snapshots saved on PC</td>
</tr>
<tr>
<td><img src="image" alt="System" /></td>
<td>System</td>
<td>Display events related to the AxTraxNG™ Server operation and operators activity</td>
</tr>
<tr>
<td><img src="image" alt="Pause" /></td>
<td>Pause</td>
<td>Halt the display of events in the display area. New events are shown again when the Pause button is clicked a second time.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>Refresh</td>
<td>Manually refresh the event list</td>
</tr>
<tr>
<td><img src="image" alt="View Events within the last Hour" /></td>
<td>View Events within the last Hour</td>
<td>Display all events that occurred within the last hour. Click the dropdown arrow to change the view.</td>
</tr>
<tr>
<td><img src="image" alt="View Events within the last Day" /></td>
<td>View Events within the last Day</td>
<td>Display all events that occurred within the last day</td>
</tr>
<tr>
<td><img src="image" alt="View Events within the last Week" /></td>
<td>View Events within the last Week</td>
<td>Display all events that occurred within the last week</td>
</tr>
<tr>
<td><img src="image" alt="View Periodical Events" /></td>
<td>View Periodical Events</td>
<td>Display all events that occurred within a selected period</td>
</tr>
<tr>
<td><img src="image" alt="View All Events" /></td>
<td>View All Events</td>
<td>Display all events</td>
</tr>
</tbody>
</table>
System Overview

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Click icon to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>🛄</td>
<td>Clear</td>
<td>Clear the entire log and empty the current event list view</td>
</tr>
<tr>
<td>🚺</td>
<td>Show User</td>
<td>Open the User window for the selected user.</td>
</tr>
<tr>
<td>🚺</td>
<td>Clear Alarm</td>
<td>Open the Alarm Details window to allow the operator to reset the alarm.</td>
</tr>
<tr>
<td>🕵️♀️</td>
<td>Antipassback</td>
<td>Open the Antipassback Forgive window to allow the operator to cancel an</td>
</tr>
<tr>
<td>🝷</td>
<td>Forgive</td>
<td>Antipassback restriction for the selected user.</td>
</tr>
<tr>
<td>📸</td>
<td>Camera List</td>
<td>Open a list of all ViTrax cameras attached to the network</td>
</tr>
<tr>
<td>🎥</td>
<td>Archive</td>
<td>Open the Archive Camera Window for the selected video stream or snapshot.</td>
</tr>
</tbody>
</table>

4.5 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.

4.5.1 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.

4.5.2 Timing

The Timing tree branch consists of two elements: time zones and Holidays.

4.5.2.1 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.

For more information, see Section 5.1.

4.5.2.2 Holidays

This element defines annual holiday dates; it is possible to set special access behaviors for holiday time.
System Overview

For more information, see Section 5.2.

4.5.3 **Groups**

The Groups tree branch consists of three elements: Access groups, Input and Output Groups, and access areas.

4.5.3.1 **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 5.9.1.

4.5.3.2 **Input and Output Groups**

Input and Output groups define sets of outputs or inputs that should be managed together within a panel.

For more information, see Sections 5.7, 5.9.2, and 5.9.3.

4.5.3.3 **Access Areas**

A facility can be subdivided into several access areas to configure and manage it more effectively.

For more information, see Section 5.12.

4.5.4 **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.

For more information, see Section 5.13.

4.5.5 **Users**

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

4.5.5.1 **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 5.11.

4.5.5.2 **Visitors**

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

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

For more information, see Section 5.11.

4.5.5.3 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.

4.5.5.4 Cards

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

For more information, see Section 5.10.

4.5.5.5 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 5.14.

4.5.6 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 5.16.

4.5.7 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 8.
How to Set Up a Site

5. How to Set Up a Site

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Add Time Zones and Holidays</td>
<td>5.1 and 5.2</td>
</tr>
<tr>
<td>2</td>
<td>Add a Network</td>
<td>5.3</td>
</tr>
<tr>
<td>3</td>
<td>Add and Configure an Access Control Panel</td>
<td>5.4</td>
</tr>
<tr>
<td>4</td>
<td>Configure the Doors</td>
<td>5.5</td>
</tr>
<tr>
<td>5</td>
<td>Configure the Readers</td>
<td>5.6</td>
</tr>
<tr>
<td>6</td>
<td>Configure the Inputs</td>
<td>5.7</td>
</tr>
<tr>
<td>7</td>
<td>Add Panel Links</td>
<td>5.8</td>
</tr>
<tr>
<td>8</td>
<td>Create Groups: Access Groups, Input Groups, and Output Groups</td>
<td>5.9.1, 5.9.2, and 5.9.3</td>
</tr>
<tr>
<td>9</td>
<td>Add New Users and Cards</td>
<td>5.10</td>
</tr>
<tr>
<td>10</td>
<td>Add Departments, Users and Visitors</td>
<td>5.11</td>
</tr>
<tr>
<td>11</td>
<td>Add Access Areas and Add Global Antipassback Rules</td>
<td>5.12 and 5.13</td>
</tr>
<tr>
<td>12</td>
<td>Add a Status Map</td>
<td>5.16</td>
</tr>
</tbody>
</table>

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.

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 9.2).
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. Click the + icon on the toolbar.
   
   The Add *Time Zone* properties window opens.

3. In **Name**, type a name for the time zone.
4. Click and drag the mouse button 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. In the main *Time zone* window, click **New** to create a new time zone.
8. Click **OK** when all of the time zones are defined.

---

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: national (existing) holidays are added using the **Tools>Options** menu, while a new holiday is added using the **Holiday** element in the Tree view.

**To add a national holiday:**

1. From the Menu Bar, click **Tools>Options**.
   The Options window opens.

   ![Figure 34: Options Window](image)

   **Figure 34: Options Window**

2. In the Holidays area, click the **Select Holiday** button.
   The **Outlook Holidays** window opens.

   ![Figure 35: Outlook Holidays Window](image)

   **Figure 35: Outlook Holidays Window**
How to Set Up a Site

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 choose 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. Click the icon on the toolbar.
   The Add Holiday window opens.

   Figure 36: Holiday Properties Window

3. In Description, type a name for the holiday.
4. Check the Enabled checkbox to enable the holiday.
5. Use the Date dropdown to select the holiday’s date.
6. Check the Every Year checkbox 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
- The type of network connection and the connection settings

To add a network:

1. In the Tree view, select Networks.
2. Expand the Networks element to view available networks.
3. On the *Network* toolbar, click the + icon. The Add *Network* window opens.

![Network Window – General Tab](image)

*Figure 38: Network Window – General Tab*
How to Set Up a Site

The General tab contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Name for the network. The network address appears to the right of the network name.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Checkbox is selected when the network is connected and operational.</td>
</tr>
<tr>
<td>Network Type</td>
<td>Network type: Serial, TCP/IP, or Modem. For TCP/IP connection, set the TCP/IP network (see Appendix C).</td>
</tr>
<tr>
<td>Configuration Button</td>
<td>Configuration window to set communication preferences. This button appears when selecting a Modem or TCP/IP LAN network. For more information, see Appendix C.</td>
</tr>
</tbody>
</table>

4. In Description, type a name for the new network and select the Enabled checkbox.

5. In Network type, select the network type and set the connection settings:
   a. For serial, select the correct COM port.
   b. For a TCP/IP LAN, click Configuration to locate the hardware on the local network.
   c. For a modem, 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 C. Check with your system administrator for more information, or contact Rosslare technical support. Clear the Enabled checkbox if you want to halt communication to panels on the network.

6. 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.

7. In the Add Network window, click the Options tab.
8. To use the time zone of the AxTraxNG™ Server for the panel network, select the option `Panel network using AxTraxNG™ Server time zone` (default), and then continue to Step 12.

9. To select a different time zone for the panel network, select the `Panel network using different time zone` option.

The Network Time Zone area opens.
How to Set Up a Site

The Network Time Zone area contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Time Zone (Windows Date and Time)</td>
<td>From the dropdown list, select the desired time zone.</td>
</tr>
<tr>
<td>Custom Daylight saving</td>
<td>Select the checkbox to define custom settings.</td>
</tr>
<tr>
<td>Daylight Time</td>
<td>Select the new hour at the time that daylight saving time begins.</td>
</tr>
<tr>
<td>Start DST (time)</td>
<td>Select the hour that daylight saving time begins.</td>
</tr>
<tr>
<td>Stop DST (time)</td>
<td>Select the hour that daylight saving time ends.</td>
</tr>
<tr>
<td>Every year</td>
<td>Select the Every year checkbox to set a day in one of the weeks of a defined month to automatically begin and end daylight saving time every year. Clear the Every year checkbox 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.</td>
</tr>
<tr>
<td>Start DST (date)</td>
<td>If Every year is not selected, select the commence date for daylight saving time.</td>
</tr>
<tr>
<td>Month, Week, Day of Week</td>
<td>These fields are enabled when the Every year checkbox is selected. Select the month, week within the month, and day of the week when daylight saving time is to begin every year.</td>
</tr>
<tr>
<td>Stop DST (date)</td>
<td>If Every year is not selected, select the end date for daylight saving time.</td>
</tr>
<tr>
<td>Month, Week, Day of Week</td>
<td>These fields are enabled when the Every year checkbox is selected. Select the month, week within the month, and day of the week when daylight saving time is to end every year.</td>
</tr>
</tbody>
</table>

10. Set the Daylight Saving Time definitions according to the field descriptions in the table.
11. Click New from within Network tab to add a new network.
12. Click OK to exit the Network’s Time Zone setup window.

5.4 Adding Access Control Panels

Every network is a cluster of access control panels. In its standard form, each access control panel can be configured as either one or two readers per door. Each of the AC-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.
How to Set Up a Site

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 REX switch or a mechanical door handle only).

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

5.4.1 General Panel Settings

The General tab of the Door Controller Panel Properties window displays the following:

- The panel’s address and status
- The DIP switch settings for the panel

If panel expansion boards are installed, the tab also displays:

- The input and output connections for the panel
- The panel’s hardware version

Refer to AC-525 Hardware manual for further details.

5.4.2 Adding a Panel

You can add an individual panel using the Tree View.

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 add an individual panel:

1. In the Tree View, click Networks.
2. Expand a network in the Tree View and select an available network.
3. On the toolbar, click the icon.
   The Add Panel window opens.
The *General* tab of the Door Controller *Panel properties* window contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Type a description for the panel</td>
</tr>
<tr>
<td>Panel Address</td>
<td>Type an address number for the panel</td>
</tr>
<tr>
<td></td>
<td>The network’s address appears to the left of the panel address. Valid entries are 1-32.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the checkbox to activate this panel</td>
</tr>
<tr>
<td></td>
<td>Clear the checkbox if the panel is not connected</td>
</tr>
<tr>
<td>Hide events on this PC</td>
<td>Select the checkbox to hide events originating from this PC</td>
</tr>
<tr>
<td>Type</td>
<td>Select one or two readers per door</td>
</tr>
<tr>
<td>Hardware Version</td>
<td>Select the appropriate panel hardware type</td>
</tr>
<tr>
<td>Firmware version</td>
<td>Upon selection of the hardware version, the field displays the current firmware version</td>
</tr>
<tr>
<td>Boot loader version</td>
<td>Upon selection of the hardware version, the field displays the current boot loader version</td>
</tr>
<tr>
<td>Inputs</td>
<td>Displays the input connections for the panel</td>
</tr>
<tr>
<td>Outputs</td>
<td>Displays the output connections for the panel</td>
</tr>
</tbody>
</table>
How to Set Up a Site

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

4. Click Test.

The Hardware Test window opens with the complete panel details.

![Figure 42: Panel Connection Test]

The test screen displays the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware version</td>
<td>Displays the firmware version of the board</td>
</tr>
<tr>
<td>Bootloader version</td>
<td>Displays the boot loader version of the board</td>
</tr>
<tr>
<td>Hardware</td>
<td>Displays the hardware name</td>
</tr>
<tr>
<td>Supervised Inputs</td>
<td>Displays the panel is secure in case of tampering</td>
</tr>
<tr>
<td>MD-IO84</td>
<td>Indicates whether or not MD-IO84 exists</td>
</tr>
<tr>
<td>MD-D02</td>
<td>Indicates whether or not MD-D02 exists</td>
</tr>
<tr>
<td>MD-D04</td>
<td>Indicates whether or not MD-D04 exists</td>
</tr>
<tr>
<td>MD-IPAV1</td>
<td>Displays the AC-525 Video board version number</td>
</tr>
</tbody>
</table>

5. Click Close.

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

To search for existing panel on the network:

1. In the Tree View, expand the Networks element and select a network.
2. Click the icon. The Find Panels window opens.

3. Click **Find Panels** to search for all connected panels in the network. Once the detection process is complete (this may take 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.

**5.4.3 Editing the 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.
# How to Set Up a Site

The Antipassback tab contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Antipassback</td>
<td>From the <em>Automatic Antipassback</em> dropdown menu, select the time zone for door Antipassback rules to apply.</td>
</tr>
<tr>
<td>Antipassback severity</td>
<td>Choose the antipassback severity:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hard</strong> – When hard Antipassback is selected, an event is generated and the door does not open.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Soft</strong> – When soft Antipassback is selected, an event is generated and the door opens.</td>
</tr>
<tr>
<td>In/Out reader list</td>
<td>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.</td>
</tr>
</tbody>
</table>

The *Options* tab contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Communication event (min:sec)</td>
<td>Select a period of time in minutes and seconds to determine when the system generates a No Communication event. If there is no communication from the AxTraxNG™ server for a period longer than the setting defined, the <em>No communication with server</em> event is generated in the panel.</td>
</tr>
<tr>
<td>Events filter</td>
<td>Click <em>Select</em> to open the Events Filter and select the events that this panel should record. Set the filter's operation method:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Always Active</strong> – Only the selected events are recorded by the panel</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active when panel disconnected</strong> – 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.</td>
</tr>
</tbody>
</table>

**Note:** In the default configuration, some events are filtered and may not be seen in the display area Events view

| Door Interlock                | Select the *Enabled* checkbox to enable Door Interlock. Select the Door 1-8 checkboxes to apply the Door Interlock restrictions to Doors 1-8. |
|                               | The Door Interlock function is only enabled when the *Enable* checkboxes and a minimum of two doors are selected.                        |
## Field Description

**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.

## To edit a panel:

1. In the Tree View, click **Networks**.
   The available networks are listed in the display area.
2. In the Tree View, expand a network and select a panel to configure.

![Figure 44: Available Panel in a Network](image)

3. Click **Edit**.
   The **Panel Properties** window appears.
4. Click the **Antipassback** tab.
   The panel properties of the Antipassback tab opens.
How to Set Up a Site

60 AxTraxNG™ Software Installation and User Guide

5.  Set the Antipassback behavior, according to the field descriptions in the table.
6.  Click the Options tab.

   The panel properties of the Options tab opens.

7.  Set the event filtering options for this panel.
8.  Click OK.

   The window closes and the configured panel is displayed.
5.5 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

The *Door Properties* window contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Type a name for the door.</td>
</tr>
<tr>
<td><strong>Auto-Relock</strong></td>
<td>Select the event that causes the door to relock automatically.</td>
</tr>
<tr>
<td><strong>REX enabled</strong></td>
<td>A Request to Exit unlocks the door for a user-defined duration. Select the checkbox to allow Requests to Exit for this door. The location of the door REX input depends on panel configurations; it can be seen in the Panel properties window.</td>
</tr>
<tr>
<td><strong>First person delay on automatic unlock</strong></td>
<td>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 5.8).</td>
</tr>
<tr>
<td><strong>Door output polarity is Normal Closed</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Manual Door Open Enabled</strong></td>
<td>Select this checkbox to allow operators to adjust the door manually (see Section 5.8).</td>
</tr>
<tr>
<td><strong>Door open time</strong></td>
<td>Set the duration for which the door stays unlocked.</td>
</tr>
<tr>
<td><strong>Extended door open time</strong></td>
<td>Set the duration for which the door stays unlocked for users with Extended door open rights.</td>
</tr>
</tbody>
</table>
| **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 5.7) feature for that door must be set to 0.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door forced open</td>
<td>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 5.7) feature for that door must be set to 0.</td>
</tr>
</tbody>
</table>

**To edit the door properties:**

1. In the Tree View, click **Networks**.
2. Select a network and expand a panel in the Tree View.
3. Select **Doors**.
   The available doors are listed in the display area
4. Select a door in the display area and click **Edit**.
   The Door Properties window opens.

![Door Properties Window](image)

**Figure 47: Door Properties Window**

5. Configure the door as required.
6. Click **OK**.

### 5.6 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
How to Set Up a Site

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

**To configure a reader:**

1. In the Tree View, click **Networks**.
2. Select a network and expand a panel in the Tree View.
3. Select **Readers**.
   - The available readers are listed in the display area
4. Select a reader in the display area and click **Edit**.
   - The **Reader Properties** window opens to the **General** tab.

**5.6.1 General Tab**

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

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

![Reader Properties Window – General Tab](image)

**Figure 48: Reader Properties Window – General Tab**
How to Set Up a Site

The General tab in the Reader window contains the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Type the name of the reader.</td>
</tr>
<tr>
<td>Operation Mode</td>
<td>Select how the reader operates.</td>
</tr>
<tr>
<td>- Inactive:</td>
<td>The reader is not in use.</td>
</tr>
<tr>
<td>- Card Only:</td>
<td>The reader uses RFID cards only.</td>
</tr>
<tr>
<td>- PIN Only:</td>
<td>The reader uses PIN inputs only.</td>
</tr>
<tr>
<td>- Card or PIN:</td>
<td>The reader uses both cards and PIN codes.</td>
</tr>
<tr>
<td>- Desktop:</td>
<td>The reader is inactive, but is being used to record new cards on the computer.</td>
</tr>
<tr>
<td>- No Access Mode:</td>
<td>The reader does not grant access to any users.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction</td>
<td>Select whether the reader is allowing entry into the area or exit out of the area.</td>
</tr>
</tbody>
</table>

| 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. |

| Open Door                  | Select the checkbox to allow the reader to unlock the door.                 |
| Deduct User Counter        | Select the checkbox to record this entry against the user’s entry allowance counter. See Section 5.11.2.1. |

| Reader type                | Select the data transmission type for the reader hardware.                  |
| Keypad type                | Select the data transmission type for the type of keypad hardware.          |
| 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. |
| AYC-W6500 Biometric Reader | Select the checkbox to interface with the AYC-W6500 biometric reader and its PC application, BioTrax. |

5.6.2 Options Tab

The Options tab in the Reader window displays:

- Timed antipassback settings for the reader
- Restricted site access settings
The *Options* tab in the *Reader* window contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatic Antipassback</strong></td>
<td>Select whether to apply antipassback rules.</td>
</tr>
<tr>
<td></td>
<td>To set Time Zones, see Section 5.1.</td>
</tr>
<tr>
<td><strong>Hard</strong></td>
<td>When hard antipassback is selected, an event is generated and the door does not open.</td>
</tr>
<tr>
<td><strong>Soft</strong></td>
<td>When soft antipassback is selected, the door opens but an event is generated.</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>Set the number of minutes before a user can reenter using this reader.</td>
</tr>
<tr>
<td><strong>Facility Codes</strong></td>
<td>Click and type the facility code (between 0-255). Up to four different facility codes can be entered.</td>
</tr>
</tbody>
</table>
5.6.3 Access Event

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

It contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Granted</td>
<td>Mark to checkbox to enable a pop-up window for Access Granted event type alerts.</td>
</tr>
<tr>
<td>Access Denied</td>
<td>Mark to checkbox to enable a pop-up window for Access Denied event type alerts.</td>
</tr>
<tr>
<td>Access Recorded</td>
<td>Mark to checkbox to enable a pop-up window for Access Recorded event type alerts.</td>
</tr>
<tr>
<td>Close window Options</td>
<td>Once a pop-up is enabled, the close window options are available. Select one of two options:</td>
</tr>
<tr>
<td></td>
<td>• Manually: The operator is required to manually close the pop-up window.</td>
</tr>
<tr>
<td></td>
<td>• By timer: The pop-up window closes automatically based on the predefined timer.</td>
</tr>
<tr>
<td>Camera Available only with AC-525</td>
<td>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.</td>
</tr>
</tbody>
</table>
5.7 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>A display field showing the input name</td>
</tr>
<tr>
<td>Description</td>
<td>Type a name for the input.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of input to be monitored.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Normally Open/Close</strong>: An input either in an open or closed state</td>
</tr>
<tr>
<td></td>
<td>- <strong>Normally Open/Close 1 Resistor</strong>: An input in an open, closed, or trouble state. This option is only available for supervised inputs.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Normally Open/Close 2 Resistors</strong>: 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.</td>
</tr>
<tr>
<td>Activity start delay</td>
<td>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.</td>
</tr>
</tbody>
</table>

To configure an input:

1. In the Tree View, click **Networks**.
2. Select a network and expand a panel in the Tree View.
3. Select **Inputs**.
   The available inputs are listed in the display area
4. Select an input from the display area and click **Edit**.
   The Input Properties window opens.
5. Select an input and configure it as required.

5.8 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 element 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Type</td>
<td>Select the panel element type, input, output, reader, and so on which is the event source</td>
</tr>
<tr>
<td>Source</td>
<td>Select the specific panel element that raises the event based on the source type selected.</td>
</tr>
<tr>
<td>Event</td>
<td>Select the event type for the panel element</td>
</tr>
<tr>
<td>Event Description</td>
<td>Type the link or event description</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the checkbox to enable the link rule</td>
</tr>
<tr>
<td>Generate Alarm</td>
<td>Select the checkbox to generate an alarm event in addition to the link rule activity</td>
</tr>
<tr>
<td>Destination Type</td>
<td>Select the panel element type, which is to be activated by the link rule trigger event</td>
</tr>
<tr>
<td>Destination</td>
<td>Select the specific panel element, which is to be activated by the link rule trigger event</td>
</tr>
<tr>
<td>Operation</td>
<td>Select the operation performed by the destination panel element</td>
</tr>
<tr>
<td>Time</td>
<td>Define a duration timeframe for the operation. This box is only available when a time-bound operation is selected</td>
</tr>
</tbody>
</table>
### How to Set Up a Site

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Zone</strong></td>
<td>Select the time zone for which the link rule applies</td>
</tr>
</tbody>
</table>
| **PTZ Preset position** | Set the default preset PTZ (Pan, Tilt, Zoom) camera position  
\*Note: To activate this feature, you must set the preset on Vitrax.* |
| **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 the *Generate Alarm* checkbox is selected. |

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, click **Networks**.
2. Select a network and expand a panel in the Tree View.
3. Select **Links**.
4. On the *Network* toolbar, click the **Add** icon.  
The *Add Link* window opens.
5. Configure the link rule as required, according to the field descriptions in the table.
6. Select the Generate Alarm checkbox to activate the Alarm Handler button.
7. Click Alarm Handler. The Alarm Handler window opens.
8. Configure the alarm handler as required, according to the field descriptions in the table 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.
How to Set Up a Site

To create a fire alarm input:

1. In the Tree View, click **Networks**.
2. Select a network and expand a panel in the Tree View.
3. Select **Links**.
4. On the **Network** toolbar, click the **+** icon.
   The Add Link window opens.

![Figure 54: Link Window](image)

5. Configure the link rule as follows:
   a. In Source Type, select **Input**.
   b. In Destination, select **Output Group**.
   c. In Operation, select **Timer**.
   d. Select the **Generate Alarm** checkbox.
6. Click **Alarm Handler**.
   The Alarm handler window opens.
7. Configure the alarm handler as required, according to the field descriptions in the table above.
8. Select the *Open all Outputs of selected Output group* checkbox.
9. Click OK to close the *Alarm handler* window and return to the Add Link window.
10. Click OK.

### 5.9 Creating Groups

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

#### 5.9.1 Adding Access Groups

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

*To add an access group:*

1. In the Tree View, expand the *Groups* element and select *Access Groups*.
2. On the toolbar, click the **+** icon.
   The *Add Access Group* window opens.
3. In the *Description* field, enter a name for the access group and click **OK**. The new access group appears in the View Tree.

4. Select the access group from the View Tree and click the ✅ icon. The *Access Group Properties* window opens.

![Figure 57: Access Group Properties Window](Image)

5. From the *Time zone* dropdown, select a time.

6. Select and move the desired readers from *Available* to *Selected* using the arrows.

7. Click **OK**. The window closes and the new access group appears in the Display Area.

### 5.9.2 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** and click the ✪ icon. The *Input Group* window opens.
3. In the **Description** field, enter a name for the input group.

4. Expand a network to see its panels.

5. Select the checkboxes of all relevant inputs.
   You can also use the **Select All** and the **Select None** buttons.

6. Click **OK**.
   The window closes and the new input group appears in the display area.

### 5.9.3 Adding Output Groups

Output groups are a collection of outputs from panel that can be used in panel links to perform advanced operations, such as Elevator control.
To add an output group:

1. In the Tree View pane, expand the Groups element.
2. Select Outputs Groups and click the + icon. The Output Group window opens.

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

5. Select the checkboxes of all relevant outputs. You can also use the Select All and the Select None buttons.
6. Click OK.
5.10 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection Type</td>
<td>Select what will be added: Users and cards, Users only, or Cards only</td>
</tr>
<tr>
<td>Quantity</td>
<td>Type or select the number of cards/users to add</td>
</tr>
<tr>
<td>Sequential cards</td>
<td>Define the card properties:</td>
</tr>
<tr>
<td></td>
<td>- Reader Type: Select the type of reader appropriate for the new cards being added</td>
</tr>
<tr>
<td></td>
<td>- Start from: Type the number of the first card in the set</td>
</tr>
<tr>
<td></td>
<td>- Facility code: Type the site code for these cards. This field is not available for all reader types</td>
</tr>
<tr>
<td>Sequential Users – General</td>
<td>Define the users general properties:</td>
</tr>
<tr>
<td></td>
<td>- Department: Associate to the new user(s) created to a department</td>
</tr>
<tr>
<td></td>
<td>- Access Group: Associate to the new user(s) created to an Access group</td>
</tr>
<tr>
<td>Sequential Users – Rights</td>
<td>Define the users right properties:</td>
</tr>
<tr>
<td></td>
<td>- Antipassback immunity: Select the checkbox to override any antipassback restrictions</td>
</tr>
<tr>
<td></td>
<td>- Extended door open time: Select the checkbox to activate the extended door option defined for each door</td>
</tr>
<tr>
<td>Sequential Users – Pin Code</td>
<td>Select the checkbox to define automatic pin codes, select between:</td>
</tr>
<tr>
<td></td>
<td>- Start from: Sequential pin code starting from a predefined number based on a defined number of digits</td>
</tr>
<tr>
<td></td>
<td>- Random: Random pin codes where the only definition is the number of PIN code digits</td>
</tr>
<tr>
<td>Sequential Users – Valid date</td>
<td>Define the access right validity:</td>
</tr>
<tr>
<td></td>
<td>- From: Define the date and time to begin allowing access</td>
</tr>
<tr>
<td></td>
<td>- Until: Select the checkbox to define an end date for the access right validity, then define the date and time</td>
</tr>
</tbody>
</table>
## How to Set Up a Site

### Field | Description
--- | ---
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 5.8.

Sequential Users – Counter | Select the *Enable* checkbox 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, select **Cards**.
2. On the toolbar, click the ![Card icon](images/card_icon.png) icon.
   The *Add Users and Cards* window opens.

   ![Figure 62: Add Users and Cards Window](images/figure62.png)

   **Figure 62: Add Users and Cards Window**

3. Configure the user and card properties as required, according to the field descriptions in the table 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.
5.11 Adding Departments, Users, and Visitors

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

5.11.1 Adding Departments

**To add a department:**

1. In the Tree View, select the **Departments, Users and visitors** element.
2. To create a new department, click the icon. The Add **Department** dialog appears.

![Add Department Dialog](image)

3. In the **Description** field, enter a name for the department and click **OK**. The window closes and a new department is created.

5.11.2 Adding Users

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

The **Add User** window contains three main tabs:

- **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

5.11.2.1 General Tab

The General tab displays:

- User identification information
- User validity settings
- Access rights for the user
The General tab contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photo – Add</td>
<td>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.</td>
</tr>
<tr>
<td>First name</td>
<td>Type the user's first name.</td>
</tr>
<tr>
<td>Middle name</td>
<td>Type the user's middle name.</td>
</tr>
<tr>
<td>Last name</td>
<td>Type the user's last name.</td>
</tr>
<tr>
<td>User number</td>
<td>Type a unique user number to identify the user.</td>
</tr>
<tr>
<td>Department</td>
<td>Select the user's associated department.</td>
</tr>
<tr>
<td>Access group</td>
<td>Select the user's access group.</td>
</tr>
<tr>
<td>Select color</td>
<td>Click to select which color to use to highlight this user when the user generates access events. User highlighting must be activated in Tools &gt; Options &gt; General tab.</td>
</tr>
<tr>
<td>Location</td>
<td>Click to display a log of doors accessed by this user.</td>
</tr>
</tbody>
</table>
### How to Set Up a Site

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid date/time from</td>
<td>Select the date/time from when the user’s access rights begin.</td>
</tr>
<tr>
<td>Valid date/time until (checkbox)</td>
<td>Select the checkbox to set the date/time on which the user’s access rights end.</td>
</tr>
<tr>
<td>Valid date/time until (field)</td>
<td>Select the date/time on which the user’s access rights end.</td>
</tr>
<tr>
<td></td>
<td>This field is only available when the checkbox is enabled.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the checkbox to set an access rights countdown counter for this user.</td>
</tr>
<tr>
<td></td>
<td>When the counter reaches zero, the user’s access rights end.</td>
</tr>
<tr>
<td>Set new counter</td>
<td>Select the checkbox to set a new countdown counter value for this user.</td>
</tr>
<tr>
<td>Counter Value</td>
<td>Select a new countdown counter value for this user.</td>
</tr>
<tr>
<td></td>
<td>This field is only enabled when the Set new counter checkbox is selected.</td>
</tr>
<tr>
<td>Rights &gt; Antipassback immunity</td>
<td>Select the checkbox to override any Antipassback restrictions for this user.</td>
</tr>
<tr>
<td>Rights &gt; Extended door open time</td>
<td>Select the checkbox to entitle this user to an extended unlocked door duration. The extended duration is set for each door. See Section 5.5.</td>
</tr>
<tr>
<td>Links &gt; Access Granted command</td>
<td>Select the checkbox to activate a link rule initiated by access granted commands for this user. See Section 5.8.</td>
</tr>
<tr>
<td>Links &gt; Access Denied command</td>
<td>Select the checkbox to activate a link rule initiated by access denied commands for this user. See Section 5.8.</td>
</tr>
<tr>
<td>Links &gt; User selected Output group</td>
<td>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 5.8.</td>
</tr>
<tr>
<td>Links &gt; Handicapped checkbox</td>
<td>Select the checkbox to activate a dedicated output a short time after the door is unlocked. See Section 5.8.</td>
</tr>
</tbody>
</table>
How to Set Up a Site

5.11.2.2 Codes Tab

The Codes tab displays:

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

![Image of Codes Tab]

**Figure 65: Add User Window – Codes Tab**

The Codes tab contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Type</td>
<td>The card type used by the reader / user</td>
</tr>
<tr>
<td>Facility Code</td>
<td>The site code assigned to this card</td>
</tr>
<tr>
<td>Card Number</td>
<td>The unique number of this card</td>
</tr>
<tr>
<td>Status</td>
<td>Select the status of the card. Inactive cards cannot gain access to the facility</td>
</tr>
<tr>
<td>Number of digits</td>
<td>Select the length of the PIN for this user.</td>
</tr>
<tr>
<td>Code</td>
<td>Type a PIN.</td>
</tr>
<tr>
<td>Auto PIN</td>
<td>Click to automatically generate a random PIN.</td>
</tr>
<tr>
<td>Add from MD-D08</td>
<td>Click to read card details using MD-D08 module.</td>
</tr>
<tr>
<td>Add from list</td>
<td>Click to add a new card. All cards within the user’s specified facility code, are listed</td>
</tr>
</tbody>
</table>

5.11.2.3 Details Tab

The Details tab contains detailed contact and identification details about the user.
How to Set Up a Site

The *Details* tab contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td>Type an office telephone number for the user.</td>
</tr>
<tr>
<td>Mobile</td>
<td>Type a cell phone number for the user.</td>
</tr>
<tr>
<td>Fax</td>
<td>Type a fax number for the user.</td>
</tr>
<tr>
<td>Email</td>
<td>Type an email address for the user.</td>
</tr>
<tr>
<td>Address</td>
<td>Type a postal address for the user.</td>
</tr>
<tr>
<td>Home telephone</td>
<td>Type a home telephone number for the user.</td>
</tr>
<tr>
<td>Car registration</td>
<td>Type the user’s license plate number.</td>
</tr>
<tr>
<td>Title</td>
<td>Type the user’s title (e.g. “Mr.”).</td>
</tr>
<tr>
<td>Employment Date</td>
<td>Enter the date that the user joined the firm.</td>
</tr>
<tr>
<td>Notes</td>
<td>Type any additional information.</td>
</tr>
<tr>
<td>Details</td>
<td>Click to open the user’s additional details folder.</td>
</tr>
</tbody>
</table>

5.11.2.4  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 9.5.2).

*To create a user:*

1. In the Tree View, expand the *Departments/Users* element and select a department for the new user.
2. On the toolbar, click the icon. 
   The Add User window opens.
3. Enter the user details in the various tabs as explained in detail in the following sections.
4. Click OK. 
   The window closes and the added user is displayed.

5.11.3 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visitor Identification</td>
<td>Type a unique visitor identification</td>
</tr>
<tr>
<td>Visit Date/Time</td>
<td>Select the checkbox and specify the date and time for the visit</td>
</tr>
<tr>
<td>Automatic disable on exit</td>
<td>Define automatic disable access right options</td>
</tr>
<tr>
<td></td>
<td>• Access Area: Select the Access Area to disable access to</td>
</tr>
<tr>
<td></td>
<td>• Inactive card: The designated card automatically becomes inactive upon exit</td>
</tr>
<tr>
<td></td>
<td>• Unauthorized user: the designated access group changes to Unauthorized upon exit</td>
</tr>
<tr>
<td>Hosted</td>
<td>Define the details for the hosting party:</td>
</tr>
<tr>
<td></td>
<td>• Department: Select the Department</td>
</tr>
<tr>
<td></td>
<td>• User: Select the hosting User</td>
</tr>
<tr>
<td></td>
<td>• Comment: Type any additional information</td>
</tr>
</tbody>
</table>

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.
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.

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.

Select a user or a visitor row using the mouse and drag & drop it into the relevant Tree View icon.

### 5.12 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.
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.

### 5.13 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.

   ![Add Global Antipassback Window](image)

   **Figure 69: Add Global Antipassback Window**

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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Antipassback applies an Antipassback event only on &quot;Enter&quot; readers to the defined &quot;Area&quot;. To implement Antipassback on Exit readers as well, you must define a new area with opposite reader directions: Readers defined &quot;Enter&quot; in the first area need to be defined again in the new area as &quot;Exit&quot; readers, and &quot;Exit&quot; readers in the first area should be defined as &quot;Enter&quot; readers in the second area.</td>
</tr>
</tbody>
</table>

5.14 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.

![Operator Properties](image)

**Figure 70: Add Operator Window**

3. In the Description field, enter the Operator’s name.
4. Select the Localize guard checkbox to define the operator with limited rights.
5. Click the Networks... and Status maps... buttons 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.

![Operator Password](image)

**Figure 71: Operator Password Window**
8. Enter the operators’ password in the **Password** field and re-enter the password in the **Confirm Password** field.

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

9. Click **OK** to save your settings.
   The dialog closes and the operator is shown in the display area.

### 5.15 Creating Elevator Control

Elevator control can be created by following four simple steps.

Normally, a reader is associated with a door. For elevator control, a selected reader should be associated with several outputs (floors).

*To create elevator control:*

1. Assign a reader to the Elevator Control.
2. In the **Reader Properties** window, clear the Open Door checkbox. See Section 5.6.
3. Create output groups (see Section 5.9.3).
   Each output group represents a floor or several floors.

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

4. Create a panel link (see Section 5.8). Only one panel link is required.
5. Associate Users with Elevator Control Rights
   Each user can be associated with the relevant access group to allow user access to specific floors, as needed.
6. In the General tab of the User window, associate a user with output groups (see Section 5.11.2.1).

### 5.16 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** and click the ![](icon) icon.
   The **Add Status Map** window opens.
2. Right-click in the window and select **Set background** from the shortcut menu.

The *Select Picture File* window opens.

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

**Figure 72: Add Status Map Window**

To change the map image and/or to add objects on the map, you must mark the Design Mode checkbox. The **Add Map** icon in the toolbar is enabled.
How to Set Up a Site

4. Ensure that the Design Mode checkbox is checked.
5. Select any Readers, Doors, Inputs, Outputs, additional Status Maps, Cameras, or Panels lost and click the Add to Map icon from the toolbar menu.

The object appears on the status map, and can be dragged to its correct position.
6. Right-click a map object and select Show on Map from the shortcut menu.
   The Show on Map window opens.

7. Select the Status checkbox to display the object’s state on the status map.
8. 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.
How to Set Up a Site

9. Select the *Alarm* checkbox to enable a visual alarm on the map for alarm events.

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

10. Repeat Steps 5 to 9 until all objects are shown on the status map, as required.

11. Repeats Steps 1 to 9 to set up additional status maps.

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

Perform the following steps to use cameras on your AC-525 panel:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connect to ViTrax Server</td>
<td>6.1</td>
</tr>
<tr>
<td>2</td>
<td>Add a Camera to AC-525 panel</td>
<td>6.2</td>
</tr>
<tr>
<td>3</td>
<td>Use Panel Links</td>
<td>5.8 and 6.3</td>
</tr>
<tr>
<td>4</td>
<td>View Recorded Events</td>
<td>6.4</td>
</tr>
<tr>
<td>5</td>
<td>Use Automated Activation Options</td>
<td>6.5</td>
</tr>
</tbody>
</table>

6.1 Connecting to ViTrax Server

Define the ViTrax Server database with which the AxTraxNG™ Software communicates.

*To connect to the ViTrax server:*

1. When the ViTrax Server is running, click **File > ViTrax Server**.
   
The **ViTrax Servers** window opens.

   ![Figure 76: ViTrax Servers Window](image)

2. On the toolbar, click the + icon.
   
The **Add ViTrax Server** window opens.
3. In **ViTrax IP Address**, enter either “**localhost**” or another IP address name.

4. In **ViTrax User Name**, enter the username.

5. In **ViTrax Password**, enter the password.

   The entered password must resemble the non-default password for the server.

6. Click **Connect**.

7. Click **OK**.

   When connected, the *Connected* status is displayed.

   The ViTrax server now appears in the ViTrax Servers window list.
ViTrax Video Integration

6.2 Adding a Camera to the AC-525 Panel

Once a camera is physically installed, the system reads the camera on the network and displays it in the tree.

Defining communication of AC-525 cameras to the ViTrax server is performed physically between the camera and the AC-525 panel (see the AC-525 Installation Manual).

The cameras available on this network are displayed when clicking the Network in the tree and expanding it. When clicking the icon, the camera list is displayed (see Appendix E).

To view and add cameras to AxTraxNG™:

1. In the Tree View, click **Networks**.
   The available networks are listed in the display area.
2. Select a network and expand a panel in the Tree View.
3. Click the 📺 icon.
   The *Cameras* window opens.

   ![Figure 79: Cameras Window](image)

4. Select the **Attached to AxTraxNG** checkbox next to the camera you wish to add to the system.
5. Click **OK**.

6.3 Conditioned Recording via Panel Links

You can select the source, destination, and period of recordings using Conditioned Recording sequences programmed via the *Panel Links* screen.

To create a panel link:

1. In the Tree View, click **Networks**.
   The available networks are listed in the display area.
2. Select a network and expand a panel in the Tree View.
3. Select **Links**.
4. Click the + icon.
The Add Links window opens.

![Add Links window](image)

**Figure 80: Panel Link – Local Recording**

5. In the **Destination Type** dropdown list, select **Local recording**.
6. In the **Destination** dropdown list, select a camera (momentary recording or pre-event recording).
7. Click OK.

### 6.4 Viewing Recorded Events

In the **Camera Properties** window, you can view live streaming and edit various camera properties.

The **Camera Properties** window includes the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Displays the camera name</td>
</tr>
<tr>
<td>Enable ViTrax Motion Detector</td>
<td>Select this checkbox to enable motion detection in ViTrax. Enabling motion detection enables Record Motion features. It is possible to get motion detection events from ViTrax and use them to initiate recording, by first setting the Motion Detection section on this window, and then setting motion detection properties in ViTrax in the <strong>Sensitivity</strong>, <strong>Exclusion</strong>, <strong>Format</strong>, and <strong>Source</strong> tabs.</td>
</tr>
<tr>
<td>Time Lapse</td>
<td>This checkbox is automatically enabled due to the camera recording settings. Time Lapse refers to the periodic recording of single frames. AxTraxNG™ automatically enables the Time Lapse option in ViTrax when setting recording by AxTraxNG™.</td>
</tr>
<tr>
<td>Frame rate</td>
<td>Select the Time Lapse period. By default, the Time Lapse period is 0.005 frames per second (1 frame every 200 seconds).</td>
</tr>
<tr>
<td>Live Audio Volume</td>
<td>Select the live audio volume</td>
</tr>
</tbody>
</table>
ViTrax Video Integration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio to Camera</td>
<td>Select the checkbox to indicate when a microphone is connected to the camera.</td>
</tr>
<tr>
<td>Microphone Device</td>
<td>Enabled when the Audio to Camera checkbox is selected. From the dropdown list, select a microphone.</td>
</tr>
<tr>
<td>Properties</td>
<td>Camera properties</td>
</tr>
<tr>
<td>Options</td>
<td>Video pop-up window and snapshot options.</td>
</tr>
<tr>
<td>PC Archive</td>
<td>Streams saved in the PC</td>
</tr>
<tr>
<td>Local Archive</td>
<td>Streams saved in the USB-key</td>
</tr>
<tr>
<td>Snapshot</td>
<td>Opens the images list stored on the PC</td>
</tr>
<tr>
<td>Activation buttons</td>
<td>Start/Stop Recording, initiate Audio to camera, and Save current snapshot.</td>
</tr>
</tbody>
</table>

To access camera properties:

1. In the Tree View, click **Networks**. The available networks are listed in the display area.
2. Select a network and expand a panel in the Tree View.
3. Click the **icon**. The list of available camera appears in the display area.
4. Double-click the desired camera row within the camera list. The **Camera Properties** window opens.

   ![Camera Properties Window](image)

   **Figure 81: Camera Properties Window**

5. Click **OK**.
ViTrax Video Integration

ViTrax Server must be running to view recordings.

Note

For more information on camera properties, see the ViTrax Software Manual.

To access Live Video:

1. In the Events toolbar (above the Event Log area), click the icon. A list of all available cameras appears.

![Available Camera List](image)

**Figure 82: Available Camera List**

2. Double-click the desired camera row. The Live Video Streaming window opens.
The Live Video Streaming window includes the following buttons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Click icon to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>🎥</td>
<td>Recording</td>
<td>Starts/stops recordings that are saved as streams to the archive</td>
</tr>
<tr>
<td>🎧</td>
<td>Audio to Camera</td>
<td>Use the PC microphone by utilizing the panel RAM</td>
</tr>
<tr>
<td>📸</td>
<td>Snapshot</td>
<td>Save the current snapshot.</td>
</tr>
</tbody>
</table>

3. Click OK to close.

6.5 Automated ViTrax Camera Activation Options

The following automated camera activation options are available in networks utilizing the ViTrax camera.

The automated camera activation turns on the camera and opens a video pop-up and a snapshot window on the locally used PC in response to predefined events occurring in the system as described in the following sections:

6.5.1 Reader Access

Create reader-access event based automatic camera activation on the local PC.

To create reader-access camera activation:

1. Open the Reader window (see Section 5.6).
2. Click the Access event tab.
3. Under *Enable Camera options by events*, select the **Access Granted**, **Access Denied**, or **Access Recorded** checkbox.

4. Select a camera from the *Camera* dropdown.

5. Select a video option from the *Options* dropdown.

6. Select the **Popup Enabled** checkbox to enable local pop-up messages.

7. Under *Close window options*, select either **Manually** or **By timer**.

8. Click **OK**.

### 6.5.2 Alarm Event

Create alarm handler event based automatic camera activation.

*To create alarm handler camera activation:*

1. Open the *Alarm handler* window (see Section 5.8).
Figure 85: Enable Cameras Pop-Up Options by Alarm Handler Events

2. Select a camera from the **Camera** dropdown.
3. Select a video option from the **Options** dropdown.
4. Select the **Popup Enabled** checkbox to enable local pop-up messages.
5. Under **Close window options**, select either **Manually** or **By timer**.
6. Click **OK**.

### 6.5.3 Camera Event

Create camera event based automatic camera activation.

**To create camera event based camera activation:**

1. Open the **Camera Properties** window (see Section 6.4).
2. Click **Options**.
   - The **Video Popup and Snapshot** window opens.

   ![Video Popup and Snapshot Window](image)

   **Figure 86: Video Popup and Snapshot Window**

3. Select the **Popup Camera Window on ViTrax recording** checkbox to enable window pop-up on the PC during camera’s ViTrax recording.
4. Select the **Popup Window on Motion detected start** checkbox to enable window pop-up on the PC following an activation of the ViTrax Motion detection.

5. Under **Close window options**, select either **Manually** or **By timer**.

6. Click **OK**.

### 6.5.4 Door Warning Event

Create a door-warning event based automatic camera activation.

The available door warnings in the system are **Door held open** and **Door forced open**.

To create *door-warning event based camera activation*:

1. Open the *Door* window (see Section 5.5).
2. Select the **Door held open** and/or the **Door forced open** options, and define their associated timer.

   The *Enable Cameras Options by Door Warning Events* pane opens within the *Door* window.

![Figure 87: Enable Cameras Options by Door Warning Events](image)

3. Select a camera from the **Camera** List.
4. Select a video option from the **Options** list.
5. Enable local pop-up messages by checking the **Popup Enabled** checkbox.
6. Under **Close window options**, select either **Manually** or **By timer**.
7. Click **OK**.
Manual Operation

7. Manual Operation

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

Door Manual Operation can only control doors that have been set as “Manual Door Open Enabled” in the Door Properties window (see Section 5.5).

7.1 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 Networks element and expand a selected network.
2. Expand a panel and select Doors.
3. On the toolbar, click the icon.
   The Manual Door Operation window opens.

   Figure 88: Manual Door Operation Window

4. Sort the listed panels/doors in regular or reverse order, by clicking the column header with the left mouse button.
Manual Operation

5. Select an option:
   - **Open momentarily** – Open all selected doors for the time set in the timer box
   - **Open permanently** – Opens all selected doors
   - **Close output** – Closes all selected doors and returns control to AxTraxNG™

6. Select the checkboxes of those doors to which to apply the operation.

7. Click **Apply**.

7.2 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 **Networks** element and expand a selected network.
2. Select a panel.
3. Click the icon.
   - The *Manual Reader Operation* window opens.
4. Select an option:
   - **Change operation mode** – Resets all selected readers to the selected operation mode.
   - **Default** – Returns control of the readers to the system.
5. Select the checkboxes of those readers to which to apply the operation.
6. Click **OK**.

   *For more information on secured (Card + PIN) time zones, see Section 5.6.1.*

### 7.3 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 **Networks** element and expand a selected network.
2. Select a panel.
3. Click the **Obama** icon.

   The *Manual Output Operations* window appears.
4. Select an option:
   - Open momentarily – Opens all selected outputs for the time set in the timer box.
   - Open permanently – Opens all selected outputs.
   - Close output and return to default mode – Closes the selected outputs and returns control to default.

5. Select the checkboxes of the outputs to which to apply the operation.

6. Click OK.

7.4 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 Networks element and expand a selected network.

2. Select a panel.

3. Click the icon.

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**.

### 7.5 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 **Networks** element and expand a selected network.
2. Select a panel.
3. Click the 🎧 icon.
   
   The *Manual Siren Operations* window opens.
Manual Operation

Figure 92: Manual Siren Operation Window

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**.

7.6 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 **Networks** element and expand a selected network.
2. Select a panel.
3. Click the **icon**.
   - The *Update Firmware* window opens.

4. Click **Browse**… and select the HEX file relevant to the panel’s hardware type.
5. Click **OK**.
8. AxTraxNG™ Reports

AxTraxNG™ supports two types of reports.

- Immediate Reports – List details of recent movements (within the last few hours).
  They are shown in the display area and can be exported.
- Archive Reports – List all events in the database.

8.1 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.

To show an immediate report, select it from the Reports element of the tree-view, under Immediate.

**To create a new immediate report:**

1. In the Tree View, expand the Reports element and select Immediate.
2. On the toolbar, click the **+** icon.
   The Report Wizard opens.
3. From the dropdown list, select a report type
4. Click Next.
   Follow the on-screen wizard instructions until the wizard has completed. The display area lists the new report.

8.2 Archive Reports
You can produce three types of reports:
- Panels Event Reports
- System AxTraxNG™ Events Reports
- Interactive Reports

8.2.1 Panels Events Reports
Panel event reports display details of all recorded panel events.

There are six 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.
- Panels Report – Lists all the events recorded by the selected 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.
AxTraxNG™ Reports

- **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.

### 8.2.2 System AxTraxNG™ Events Report

System AxTraxNG™ events 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.

### 8.2.3 Interactive Report

Interactive reports list details of users and their access activity.

There are two 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.

To create a new archive report:

1. In the Tree View, expand the **Reports** element and select **Archives**.
2. On the toolbar, click the 📒 icon.
   The Report Wizard opens.
3. From the first dropdown list, select a report type.
4. From the second dropdown list, select which report you wish to produce.
5. Click **Next**.
   Follow the on-screen wizard instructions until the wizard has completed. The display area lists the new report.
9. Administrator Operations

9.1 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 Networks element and select a network.
2. Click the icon.
   The Set Time window opens.
3. Select the panels to reset.
4. Click Apply.
   The server connects to the panels and sets the time as requested. A dialog confirms the operation.

![Figure 96: Set Time Window](image)

9.2 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.

To download failed data:
1. In the Tree View, select a specific panel, a specific network, or all the networks.
2. Click the icon.
   The download data process begins.

9.3 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 Users > Department/Users or Users or Visitors.
2. Select one user or visitor in the display area.
3. Click the icon.
   The Request User Count window opens.

4. Click Test.

9.4 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 following database operations are available:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Periodic Backup</td>
<td>Run a scheduled backup every specified number of days at the specified time.</td>
</tr>
<tr>
<td>Backup now</td>
<td>Run a one-time backup immediately.</td>
</tr>
<tr>
<td>Export Configurations and Events*</td>
<td>Copy the contents of the database to the selected folder.</td>
</tr>
<tr>
<td>Import Configurations*</td>
<td>Replace the current configuration based on the imported file.</td>
</tr>
<tr>
<td>Import Configurations and Events</td>
<td>Replace the current configuration and events based on the imported file.</td>
</tr>
<tr>
<td>Erase Configuration and Events*</td>
<td>Erase the current database configuration and all events.</td>
</tr>
<tr>
<td>Limit Panel Events Period</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> It is recommended to set the value to no more than 91 days.</td>
</tr>
<tr>
<td>Erase Panel Events</td>
<td>Erase all events that are older than a specified number of days.</td>
</tr>
<tr>
<td>Import database versions earlier than AS-225 VeriTrax or AS-525 AxTrax *</td>
<td>Replace the current database with VeriTrax AS-225 or AxTrax databases</td>
</tr>
</tbody>
</table>
Administrator Operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import database versions earlier than AxTraxNG™</td>
<td>Replace the current database. <strong>Note:</strong> This option does not allow importing a database from a current AxTraxNG™ version.</td>
</tr>
</tbody>
</table>

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

The Backup and Export functions add the “_AxTrax1_vX” prefix at the end of exported or backed-up database. The Import database function executes only with the 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.

9.5 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 two tabs:

- **General** – General startup and presentation settings
- **User Custom Fields** – Additional user-defined fields for the User Properties window

9.5.1 General Tab

The General tab includes presentation connection settings.

![Figure 99: General Tab](image)

The General tab contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>

A AxTraxNG™ Software Installation and User Guide
### Field Description

**Use highlight access events**
Select the desired option from the **Known Key** dropdown and click the adjacent **Select Color** button to display selected user information in a custom picked colored highlight. Click the **Select Color** button adjacent to **Unknown key** to define the highlight color for unknown keys.

**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.

**Hide foreign system events on this PC**
Select the checkbox to see only local administrator and AxTraxNG™ Server messages.

**Select Holiday**
Click the button to select Microsoft Outlook™ holidays to load into AxTraxNG™

**Use highlight networks and panel status**
Click the **Select Color** button adjacent to **Network failed** to define the highlight color for network alarms. Click the **Select Color** button adjacent to **Panel not responding** to define the highlight color for panel communication errors.

**Language**
Select the system interface language. **Note:** Setting the language to Farsi also changes the date format to the Farsi date format.

### 9.5.2 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 5.11.2.4.

![User Custom Fields Tab](image)

**Figure 100: User Custom Fields Tab**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Firewall Configuration

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

9.6 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.

![Figure 101: Import Data Window](image)
The Import/Export Data window contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Users Properties from external file into AxTraxNG™</td>
<td>Select this option to import user properties</td>
</tr>
<tr>
<td>Export Users Properties from AxTraxNG™ into external file</td>
<td>Select this option to export user properties</td>
</tr>
<tr>
<td>Data Type</td>
<td>Select the type of data file to import/export.</td>
</tr>
<tr>
<td>Location</td>
<td>Select the location of the file to import/export.</td>
</tr>
<tr>
<td>Browse</td>
<td>Click to select the file to import/export.</td>
</tr>
<tr>
<td>Excel File Columns</td>
<td>Select the checkboxes of the columns to be imported/exported. Data in each column (A–T) are imported/exported as listed.</td>
</tr>
<tr>
<td>Excel file Row</td>
<td>Enter the first row of user data in the spreadsheet.</td>
</tr>
<tr>
<td>User number started from</td>
<td>Enter the number from which to start assigning unique system user numbers.</td>
</tr>
<tr>
<td>Import Departments?</td>
<td>Select Yes to import new departments into the AxTraxNG™ database. Select No to import users without their departments.</td>
</tr>
<tr>
<td>Department</td>
<td>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.</td>
</tr>
<tr>
<td>Import Access Groups?</td>
<td>Select Yes to import new access groups into the AxTraxNG™ database. Select No to import users without their access groups.</td>
</tr>
<tr>
<td>Access Groups</td>
<td>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.</td>
</tr>
</tbody>
</table>

To open the Import/Export Data window:

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

9.7 AxTrax GUI View Options

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

- Select View > Events to make Events window visible/invisible.
- Select View > Table View to make Table View visible/invisible
- Select View > Restore docking to return to default GUI Setting
Firewall Configuration

- Select **View > Close all floating Windows** to close all pop-up windows.
A. Firewall Configuration

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.)

3. Click Windows Firewall.
Firewall Configuration

4. Select the *Exceptions* tab.

![Figure 104: Windows Firewall](image)

5. Click **Add Program**.
   The *Add a Program* dialog appears.

![Figure 105: Add a Program Window](image)

6. Click **Browse**.
   The *Browse* dialog appears.
7. In the **File Name** box, type:
   “C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\BIN\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.

13. Click **Administrative Tools**.
    The Administrative Tools window opens.

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™.
B. 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:

   ![SQL Service Settings](image)

   **Figure 109: SQL Service Settings**

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

   ![SQL Service Log On](image)

   **Figure 110: SQL Service Log On**
SQL Service Settings

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.
C. Network Configuration

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

To connect access control panels to AxTraxNG™ over a TCP/IP LAN (Local Area Network) or WAN (Wide Area Network), 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.

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.

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.

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

To configure TCP-IP Connection for AxTraxNG™:

1. In the Tree View, click **Networks**. On the toolbar, click the ![Networks](icon) icon. The Networks window opens.
2. Set the Network type as **TCP/IP**.

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

3. Click the **Configuration** button.

   The TCP/IP Configuration window opens.
Figure 111: TCP/IP Configuration Window

The upper left window lists all TCP/IP converters attached on 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.

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

5. In **Gateway Type**, select the type of TCP/IP converter, MD-N32, MD-IP32 On board, or any other valid option. Skip this selection if it is already valid.

6. Type the **Local IP address** and **Subnet** for the computer's network.

7. 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.

8. Click **OK** to start the verification process.

9. 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.

10. 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.

**To configure MD-N33 in AxTraxNG™:**

1. In the AxTraxNG™ software, add a new network.

2. Under network type, select **Modem**.
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 the Configuration button. The Modem Configuration window opens.

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 the **Use default** checkbox. 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. Choose 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 the **Use default** checkbox to allow adding or editing of the dialing string. Then, type the AT command in the **Dialing string** window.

9. Connect the computer’s 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.

   ![Remote modem initialization is at the PC side. When modem initialization fails through telephone line, a message appears.](image)

   **To initialize and configure the remote modem:**
   1. In the Modem Configuration window, click the **Remote modem** tab.

   ![Figure 114: AxTraxNG™ Remote Modem Configuration](image)
Network Configuration

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 the **Use default** checkbox 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 setting 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.

---

**Figure 115: AxTraxNG™ Modem Status**

3. In order 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...
Network Configuration

during first data configuration, such as adding a new panel or downloading a new firmware.

![AxTraxNG™ Modem Security](image)

*Figure 116: AxTraxNG™ Modem Security*
D. 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.

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 the Enable panel checkbox in the panel screen. Click OK.
8. Select the Enable panel checkbox 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.
E. Cross Platform Camera Setup

This section describes the complete process of adding cameras to the AC-525 panels as defined both in AxTraxNG™ and ViTrax applications, as well as emphasizes some of the important steps to help ensure proper camera operation.

This process is essentially a two-step procedure that needs to be defined in both applications.

First, you need to add the installed camera in the ViTrax software, only then is it possible to assign the camera to the relevant AC-525 panel defined in the AxTraxNG™ application.

To add a camera to the system:

1. Install the AC-525 panel and connect the cameras (see AC-525 installation manual)
2. Add the camera in the ViTrax application by either:
   a. Performing a camera search using the **Automatically discover network devices** option.
   b. Manually add a camera using the **Camera setup wizard > Add new device – AC-525**.
3. [Optional] Configure Motion Detection in the ViTrax application if motion detection is used.
   If Motion Detection is required, first define Motion analysis via the ViTrax application:
   a. Select the **Use Motion Detector for the Stream Being Used** checkbox.
   b. Click **Properties** to adjust motion detection properties.

   ![Note](image)

   The Motion Detection feature consumes a large amount of CPU power, resulting in a high overall CPU power usage by the application. This may reduce the overall number of cameras that can be managed by the ViTrax Server application.

4. Add the camera in the AxTraxNG™ application:
   a. In AxTraxNG™, ensure that the ViTrax Server is configured and is "Connected" with AxTraxNG™.
   b. In the AxTraxNG™ Tree menu, select the relevant AC-525 Network item.
   c. Click the ![icon](image) icon.

   On the left, you see the names of the cameras connected with this network as previously defined in ViTrax.
Cross Platform Camera Setup

Figure 117: Camera List

d. Select the **Attached to AxTraxNG™** checkbox next to the camera you wish to add to the system.
e. Click **OK**.

5. Set the camera properties in the AxTraxNG™ application:
   a. In the Tree View, click **Networks**.
   b. Expand a network and select a panel to configure.
   c. Click the panel’s 🔄 icon. The available cameras are listed in the display area.
   d. Select a camera row.
e. Click the 🔄 Icon. The **Camera Properties** window appears.

6. Set the camera’s time zone and daylight savings behavior from the **Camera screen** in the AxTraxNG™ application (Step 1):
   a. In the **Camera Properties** screen, click the **Time** tab.
   b. Select the local Time Zone from the dropdown list.
   c. If Daylight Saving Time is now active, select the **Enable Daylight Saving Time** checkbox.

   This advances the local time selected by 1 hour.
   d. Click **Apply** or **OK**.

   Daylight savings is currently not updated automatically by Windows. It is therefore the user’s responsibility to enable or disable the daylight saving time checkbox as necessary.

7. Set the camera’s time zone and daylight savings behavior from the **Camera screen** in the AxTraxNG™ application (Step 2):
   a. In the Tree menu double click a Panel item and Select the **Options** tab.
   b. In the Time Zone section, define the time zone and Daylight Saving Time to match that of the **Camera properties** from Step 6).
8. Test time synchronization in both application:
   a. In the Tree menu, select your network and click the ⏰ icon and verify that it matches the AxTraxNG™’s Server PC time.
   b. Select the panel and click **Apply** (1 or 2 seconds difference is acceptable).
   c. In the tree menu, double-click the ⏰ icon and click **Properties**.
   d. Click the **Time** tab and verify that it matches the AxTraxNG™ Server PC time.
   e. If the ViTrax Server application and the AxTraxNG™ Server application are running on different PCs, ensure that both of the PCs are synchronized. It is advised that both PCs are assigned with the same time server.
F. Enrolling Cards using MD-08 Desktop Reader

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

To define the MD-08:

1. Select Cards in the Tree View.
2. Click the Insert card by MD-08 icon on the toolbar or click Add from MD-08 on the User form Codes tab.

The Add Cards from MD-08 window opens.

![Figure 118: Add Cards from MD-08 Window](image_url)

3. Select the Card type and Com Port from the respective dropdown lists.
4. Enroll cards using the reader.
5. Click Add.
G. 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 hit the "Retry" button 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:

![Domain Controller Security Settings Window](image)

**Figure 119: Domain Controller Security Settings Window**

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:

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

   ![Add/Remove Snap-in Option]

   Figure 120: Add/ Remove Snap-in Option

3. Add the Group policy object for the Local Computer:
4. Disable (temporarily) the security policy:
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.

![AxTraxNG Watchdog – Main Window](image)

**Figure 123: AxTraxNG Watchdog – Main Window**

The main window contains the following four topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common Info</strong></td>
<td>Shows general system information</td>
</tr>
<tr>
<td><strong>Error Log Sending</strong></td>
<td>Sends error log to Rosslare Customer Support</td>
</tr>
<tr>
<td><strong>DB Connection</strong></td>
<td>Changes DB connection string</td>
</tr>
<tr>
<td><strong>Restart Server</strong></td>
<td>Restarts the AxTraxNG server</td>
</tr>
</tbody>
</table>

**Note:** Administrator password is required

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

H.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.

Figure 124: AxTraxNG Watchdog – Progress of Database Import Window

H.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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Configuration</td>
<td>Sends OS version with Error Log</td>
</tr>
<tr>
<td>List of Users</td>
<td>Sends Users list with Error Log</td>
</tr>
<tr>
<td>List of Installed Programs</td>
<td>Sends List of Installed programs with Error Log</td>
</tr>
<tr>
<td>List of SQL Servers</td>
<td>Sends List of SQL Servers with error log</td>
</tr>
<tr>
<td>Event Log Messages</td>
<td>Sends Windows Event Log with error log</td>
</tr>
<tr>
<td>Ping Networks</td>
<td>Sends network ping result with error log</td>
</tr>
<tr>
<td>Get connection string from server</td>
<td>Sends connection string of DB with error log</td>
</tr>
<tr>
<td></td>
<td>This option is enabled when Ping Network checkbox checked.</td>
</tr>
</tbody>
</table>
AxTrax.NET Watchdog

<table>
<thead>
<tr>
<th>SQL Server*</th>
<th>PC address with SQL server installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database*</td>
<td>DB name</td>
</tr>
<tr>
<td>Username*</td>
<td>Username of DB</td>
</tr>
<tr>
<td>Password*</td>
<td>Password of DB</td>
</tr>
<tr>
<td>AxTraxNG/Old AxTrax radio buttons*</td>
<td>DB of AxTraxNG of Old AxTrax</td>
</tr>
</tbody>
</table>

**Sender section**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Sender Email</td>
</tr>
<tr>
<td>Company</td>
<td>Sender Company</td>
</tr>
<tr>
<td>Name</td>
<td>Sender Name</td>
</tr>
<tr>
<td>Problem</td>
<td>Short description of problem</td>
</tr>
</tbody>
</table>

**Buttons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save Button</td>
<td>Saves log to local machine</td>
</tr>
<tr>
<td>Send Button</td>
<td>Sends the log to Rosslare Customer Support</td>
</tr>
</tbody>
</table>

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

**To send an error log report:**

1. Click the **Error Log Sending** topic. The **Error Log Sending** screen is displayed.

![AxTraxNG Watchdog – Error Log Sending Window](image)

2. Check the relevant checkboxes.
3. In the Sender section, fill out the necessary fields.
4. Click **Send**.
H.3  DB Connection

This feature allows you to change the database connection string.

The DB connection window contains following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>Database name</td>
</tr>
<tr>
<td>Server</td>
<td>DB Server path</td>
</tr>
<tr>
<td>Integrated security checkbox</td>
<td>Select this option to sends username and password of database</td>
</tr>
<tr>
<td>Username</td>
<td>Database username</td>
</tr>
<tr>
<td>Password</td>
<td>Database Password</td>
</tr>
</tbody>
</table>

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.

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

H.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 is displayed.

![AxTraxNG Watchdog - Restart Server Button](image.png)

**Figure 127: AxTraxNG Watchdog – Restart Server Button**

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

The server restarts within a few seconds.
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
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

www.rosslaresecurity.com