PART 3 – GENERAL CONFIGURATION

Contents

PART 3 – GENERAL CONFIGURATION 1

CONTENTS 3

CONFIGURATION OVERVIEW 7

Using the IXP220 Base Application 7

Common Interface Controls 10

SYSTEM CONFIGURATION PARAMETERS 13

SITE CONFIGURATION 15

Opening the Software 15

Database Version Check 16

Hardware Auto-ID..... 16

Firmware Version Confirmation..... 18

Configuring the Site 19

Add a Site..... 21

Delete a Site..... 21

CONTROLLER CONFIGURATION.....22

IXP220.properties Configuration..... 22

General Configuration..... 23

Changing the Communications Channel 24

Controller UDP Broadcast Configuration 25

Disconnecting the GSM Module 25

Full Upload 26

Upgrade 26

DOOR CONFIGURATION 27

Add a Door 27

Edit a Door 31

Edit a Zone..... 34

Edit Door Mode Patterns..... 35

Edit Advanced Door Configuration..... 35

Delete a Door 37
Delete a Zone 37
Delete a Door Mode Pattern 38

ACCESS GROUP CONFIGURATION 39

Configure Tagholder Access Groups 39

TAGHOLDER CONFIGURATION 42

Add a Tagholder 42
Add a Tagholder by E-mail 44
Assign Tags to Tagholders 45
Delete an Assigned Tag 48
Delete a Tagholder 49
Set the Default Card Template 49
Batch Enrollment of Tags 49
Advanced Search 51

HOLIDAYS 52

MESSAGES 53

Message Display 53

REASON CODES 55

MODES OF OPERATION 56

Power Control (Emergency) Mode 56
Power Control (Lockdown) Mode 56
Alarm Arming Mode 57
Intrusion Mode 57
Bell Button Mode 58
Action Mode 58

PREFERENCE CONFIGURATION 59

Setting Your Preferences 59

BROADCAST TRANSACTIONS BY UDP 66

NOTIFICATION CONFIGURATION 67

FULL UPLOAD 70

Full Upload Procedure 70

OPERATOR MANAGEMENT 71

COMMUNICATION SCHEDULE CREATOR 73

Communication Schedule Setup 73

Edit a Communication Schedule 75

Delete a Communication Schedule 75

SCHEDULED REPORTS CREATOR 76

Scheduled Reports Setup 76

Edit a Report Schedule 78

Delete a Scheduled Report 78

HARDWARE REPLACEMENT 79

LOCALISATION AND TRANSLATION 82

Choose Locale 82

Translating the Software Interface 82

CLEARING THE TRANSACTION BUFFER 84

DATABASE MAINTENANCE 85

Firebird General 85

Firebird Utilities 86

Database Backups 89

Database Restore 92

Database Corruption 94

Configuration Overview

Using the IXP220 Base Application

The following parts comprise the IXP220 Base Application's interface:

- **A**—Menu Bar
- **B**—Page Tabs
- **C**—Configuration Pane
- **D**—Viewer Pane

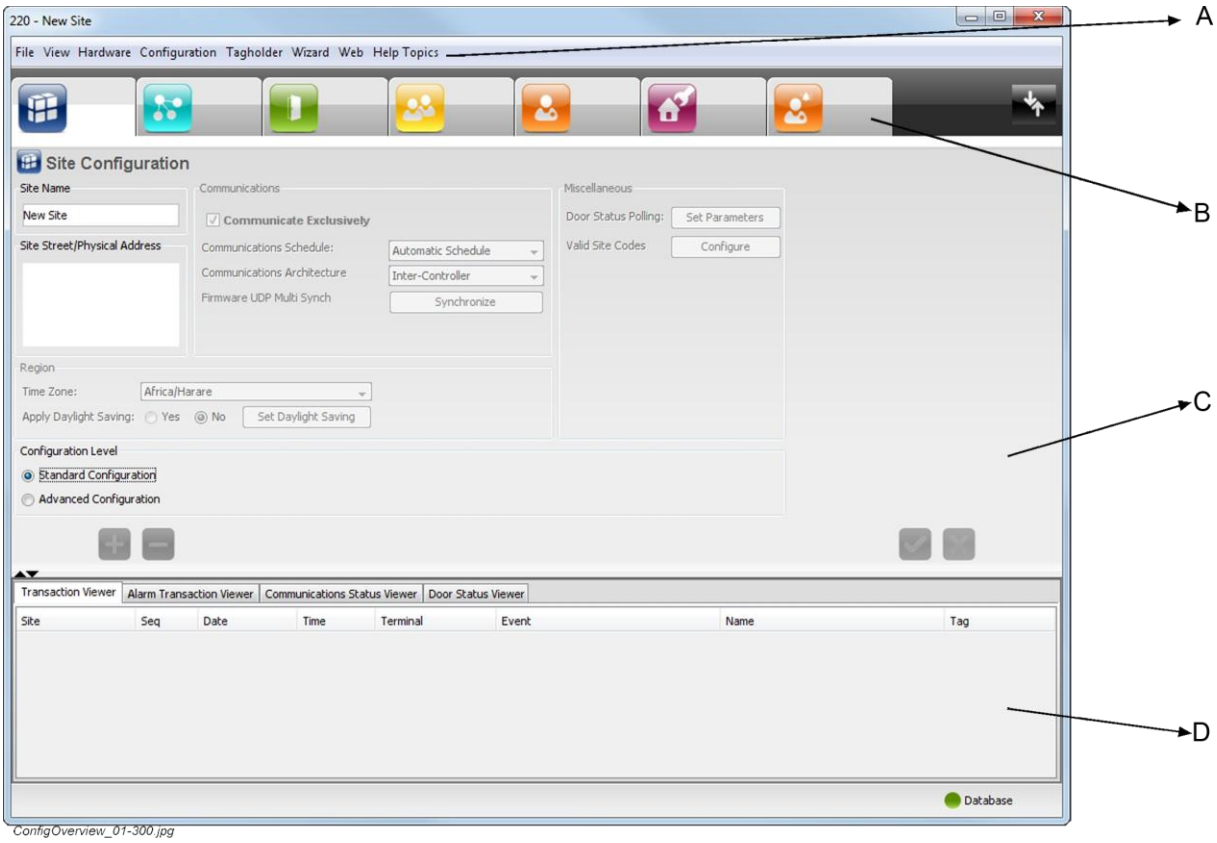


Figure 1 – IXP220 Base Application User Interface

The IXP220 Base Application only displays as shown in Figure 1 where you select the standard Windows® 7 (Professional, Enterprise or Ultimate), Windows® Vista (Business or Ultimate) and XP Professional themes. Using other non-standard themes results in IXP220 displaying incorrectly.

Menu Bar

The Menu Bar contains drop-down menus that let you navigate between different operations in the IXP220 Base Application. These menus include: File, View, Hardware, Configuration, Tagholder, Wizard, Web and Help Topics.

Page Tabs

The Page Tabs let you switch between the different configuration settings, for example:

- Site Configuration
- Controller Configuration
- Door Configuration
- Access Group Configuration
- Tagholder Configuration
- Building Management Configuration
- Notification Configuration

Configuration Pane

The Configuration Pane lets you adjust various settings based on your selection from the Page Tabs or Menu Bar.

Viewer Pane

Click the button (placed alongside the Page Tabs) to adjust the Base Application's layout:

- ***First Click**—Closes the Viewer Pane, opening the Configuration Pane in Full Screen Mode.*
- ***Second Click**—Opens the Viewer Pane in Full Screen Mode.*
- ***Third Click**—Returns the Base Application to Split-screen Mode, showing both the Configuration Pane and the Viewer Pane.*

Alternatively, adjust the layout as follows:

1. *From the Main Menu, select **View**.*
2. *Make your selection from the following:*
   - ***Split Display**— shows both the Configuration Pane and the Viewer Pane.*
   - ***Configuration View**—closes the Viewer Pane, opening the Configuration Pane in Full Screen Mode.*
   - ***Monitoring View**—opens the Viewer Pane in Full Screen Mode.*

The Viewer Pane consists of Tabs showing the following information:

- **Transaction Viewer**—gives a live real-time view of all types of transactions in the System. It displays the names of the Doors (Locations) and details of Tagholders who have entered or exited these Doors (Locations).
- **Alarm Transaction Viewer**—gives a live real-time view of all *alarm* transactions in the System. It displays the names of the Doors (Locations) and details of Tagholders who have entered or exited these Doors (Locations).
- **Communications Status Viewer**—indicates the status of the IXP220 Controllers communicating with the IXP220 System.
- **Door Status Viewer**—indicates the status of the Doors (Locations) forming part of the Site. You may physically unlock Doors (Locations) displayed here, using the IXP220 Software.

Using WebHelp

The IXP220 System has integrated WebHelp. Information not covered in this guide is covered in detail in the WebHelp. Activate the WebHelp from the Menu Bar as follows:

1. In Windows®, go to **Start**>**Programs**>**IXP220**>**IXP220**.
2. From the Menu Bar select **Help Topics**>**Online Help**.

The **Context Sensitive WebHelp provided with the IXP220 Software works with your positioned Mouse Pointer (or cursor) on your screen**. For example if you place your Mouse Pointer in the Viewer Pane, WebHelp opens Context Sensitive WebHelp specific to the Viewer Pane. If, however, you want WebHelp specific to the active Configuration Pane, continue as follows:

1. Move your Mouse Pointer into the Configuration Pane.
2. Anchor your Mouse Pointer by clicking the left-hand mouse button giving the Pane focus.
3. Press the **F1** key on your keyboard.

Key Assist

The IXP220 Base Application also includes Key Assistance. Selecting the **Key Assist** option opens an area on the right-hand side of the Base Application's desktop. This area displays a list of keyboard shortcuts letting you quickly move between the Page Tabs. The final option in the Key Assist Area (**System Navigation**) opens the System Navigation dialog. This dialog allows quick navigation through System related functions.

Get Key Assistance as follows:

1. In Windows®, go to **Start**>**Programs**>**IXP220**>**IXP220**.
2. From the Menu Bar select **Help Topics**>**Key Assist**.

Support Diagnostics

The Support Diagnostics Bundle assists you by supplying Technical Support Staff with information about your System. This helps them to solve your problems quickly and efficiently.

Create a Support Diagnostic Bundle as follows:

1. From the Main Menu, select **Help Topics**>**Support Diagnostics**.
2. Select the **Included in Bundle** tab.
3. The Diagnostics Bundle includes the following information by default. Customize the information sent by de-selecting the checkbox alongside:
   - **Transactions (Last 500**)—selecting this sends the last 500 transactions in the System including access, status and alarm transactions.
   - **System Log Files**—sends the System Log files.
   - **Firebird Log (Database Server)**—sends the Database server log if the Database is installed on the default directory.
   - **Site Summary**—includes information such as the number of Tagholders with access and the number of Doors configured on a Site. Also provides hardware configuration data like how the Base Application communicates to the Controller as well as information about connected terminals and their configuration.
   - **Holiday Data**—sends information about Holiday configuration.

- **Host PC Information**—includes information such as PC specifications, processes running on the PC and results from a netstat (a command-line tool providing information on network connections, routing and other network interface statistics).

4. Select the **Contact Information** tab.
5. Fill in your contact information as necessary.
6. Create the Diagnostic Bundle using one of the following methods:

Sites WITH Pre-configured Notifications

For e-mail setup information please refer to the section Preference Configuration (System Notification Tab) on page 63.

1. Click the **Generate Bundle** button.
2. If you have an existing reference number, complete the **Reference No.** textbox.
3. Complete the **Support E-mail Address** textbox.
4. Click the **E-mail Bundle** button.
5. Click the button.

Sites WITHOUT Pre-configured Notifications

1. Click the **Generate Bundle** button.
2. Click the button.
3. Browse to **C:\IXP220**.
4. Locate the zip file **diagnosticBundle_(date generated)_(time generated)**.
5. Attach the zip file to an e-mail.
6. Send the e-mail to the Technical Support Staff.

Common Interface Controls

The following types of controls let you interact with the IXP220 Base Application interface:

Buttons

Carries out a role when clicked on, these roles could include for example adding or deleting information, searching, opening or closing a dialog or window. As a rule Buttons normally appear in dialogs, or on the Configuration Pane. Button examples include:

Icons

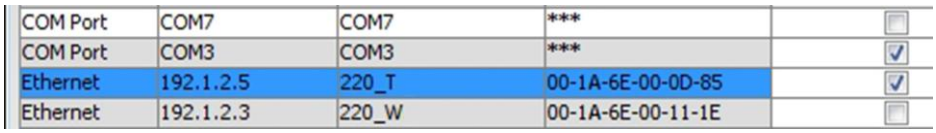
Icons are similar in function to buttons except that Icons are located in the Page Tabs. Icon examples include:

Radio Buttons

Use Radio Buttons when selecting an option. You may only select one radio button at a time. Click to enable or disable.

Checkboxes

Use Checkboxes to select multiple options. Any number of checkboxes in a group can be selected. Click to enable or disable.



COM Port	COM7	COM7	***	☐
COM Port	COM3	COM3	***	☑
Ethernet	192.1.2.5	220_T	00-1A-6E-00-0D-85	☑
Ethernet	192.1.2.3	220_W	00-1A-6E-00-11-1E	☐

Textboxes

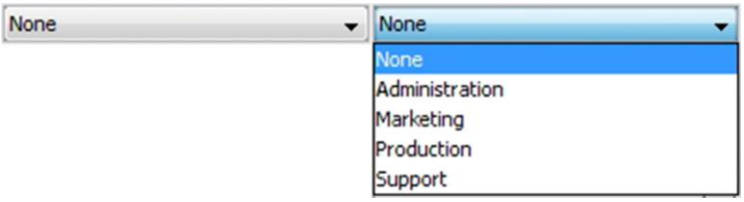
Textboxes let you enter text such as a name. Click the checkbox and type some text.

Text Areas

Same role as a textbox, except a text area displays multiple lines of text.

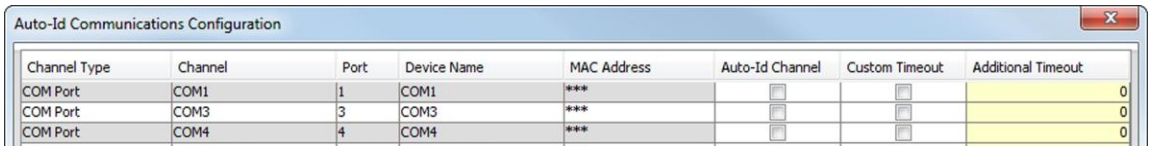
Drop-down Lists

Use Drop-down Lists to select an option from a list. Click the button with the arrow to display the list. Then, click a list item to make your selection.



Records

Records are *rows* of information displayed in a grid format. A record is a collection of fields compatible with a *column* name.



Channel Type	Channel	Port	Device Name	MAC Address	Auto-Id Channel	Custom Timeout	Additional Timeout
COM Port	COM1	1	COM1	***			0
COM Port	COM3	3	COM3	***			0
COM Port	COM4	4	COM4	***			0

This Manual displays screenshots of various screens in the IXP220 Base Application Software. Some of the details displayed in a screenshot may not be available in your copy of the IXP220 Software. This is because some details are dependent on the hardware installed and licenses activated.

System Configuration Parameters

System Parameters

Description	IXP220-1 Single APB Door or 2 non-APB Door System	IXP220-2 4 APB Door System	IXP220-3 256 APB Door System	IXP220-4 Multi-site System (256 Doors per Site)
Total Number of Tags	1 000	2 000	10 000	10 000
Total Buffered Transactions	100 000	100 000	100 000	100 000
Sites per System	1	1	1	1 000
Controllers per Site	1	4	64	64
Terminal Fixed Addresses per Controller	2	2	2	2
Terminal Fixed Addresses per Door (Location)	2	2	2	2
Doors (Locations) per Zone	1	4	32	32
Zones per Site	1	4	32	32
Doors (Locations) per Controller	2	4	32	32
Tags per Tagholder	4	4	4	4
Tagholder Access Groups (per Site)	64	64	64	64
Operating Voltage	18 V DC – 32 V DC 16 V AC – 24 V AC	18 V DC – 32 V DC 16 V AC – 24 V AC	18 V DC – 32 V DC 16 V AC – 24 V AC	18 V DC – 32 V DC 16 V AC – 24 V AC
Controller Communications Baud Rate	100 Mbps when using TCP/IP	100 Mbps when using TCP/IP	100 Mbps when using TCP/IP	100 Mbps when using TCP/IP
Terminal Communications Baud Rate	NA	38 400	38 400	38 400
Digital Inputs – per Controller (not used for Access Control)	1	1	1	1
Digital Inputs – per Controller (used for Access Control)	4	4	4	4
Onboard Relays – per Controller	3	3	3	3
Lift (Elevator) Control (per Site) (up to 32 floors per Lift (Elevator))	NA	NA	8 (Unlock Code Required)	8 (Unlock Code Required)
Maximum Fixed Addresses Supported (per Site)	2	8	512	512
Maximum Fixed Addresses Supported - APB Doors (per Site)	2	4	256	256
Host PC Communications	RS232, RS485, USB or TCP/IP	RS232, RS485, USB or TCP/IP	RS232, RS485, USB or TCP/IP	RS232, RS485, USB or TCP/IP
Controller Bus Communications	No	RS485	RS485	RS485
Terminal Bus Communications	No	RS485	RS485	RS485
Input or Output Devices (per Site)	NA	NA	18	18
Actions	1	1	300	300

Description	IXP220-1 Single APB Door or 2 non-APB Door System	IXP220-2 4 APB Door System	IXP220-3 256 APB Door System	IXP220-4 Multi-site System (256 Doors per Site)
Tag Registration	USB Registration Reader or Any Reader	USB Registration Reader or Any Reader	USB Registration Reader or Any Reader	USB Registration Reader or Any Reader
Maximum Number of Holidays (per Site)	40	40	40	40
Access Time Patterns to each Access Group	8	8	8	8
Access Groups per Tag	1	1	1	1
Reason Codes (per Site)	99	99	99	99
Maximum Number of Tagholder Messages (per Site)	100	100	100	100
Maximum Number of Messages on Building Management	150	150	150	150
Database	Firebird 2.1	Firebird 2.1	Firebird 2.1	Firebird 2.1

Table 1 – System Configuration Parameters

IXP220-3 and IXP220-4 Systems are restricted to 10 000 Tags per System regardless of the number of Sites. In addition these Systems are also restricted to 10 000 Tags per Site. This restriction includes Tagholders (Tags) from other Sites with access to the original Site. In other words, Site A can have up to 10 000 Tags, Tagholders from Site B with access to Site A are therefore included in Site A's total Tag count.

In IXP220-3 and IXP220-4 the Input or Output Devices (per Site) figure represents the total number of input or output devices for use across Lift (Elevator) Control and Building Management.

In IXP220-1 and IXP220-2 the Actions figure represents the input and output available on the IXP220 Controller Printed Circuit Board (PCB).

In IXP220-3 and IXP220-4 of the 300 Actions allowed, you may only allocate 100 of these as Time Triggered Actions.

A Terminal with two Fixed Addresses, such as the ImproX iTT, is treated as two separate Terminals. In the same way, a Terminal with 3 Fixed Addresses (that is the ImproX MfT), is treated as three Terminals by the Software.

All figures provided are the maximum. In some cases interdependence between parameters; that is the maximum number of Zones per Controller depends on how many Terminals are used per Location.

Unlock System IXP220-3 for up to 1 000 Sites per System and 8 Lifts (Elevators) using the Multi-site and Elevator Control Licences. The Multi-Site License allows for a maximum of 1 seat, and the Elevator Control License allows for a maximum of 1 seat.

1 Site Configuration

To set up a Site, you need to configure the following items:

- Host PC
- IXP220 Controllers
- Terminals
- Zones and Doors (Locations)

Opening the Software

To open the IXP220 Base Application, proceed as follows:

1. In Windows®, click **Start**>**All Programs**>**IXP220**>**IXP220**.
2. Enter your **Username** (**SYSDBA**) and **Password** (**masterkey**).

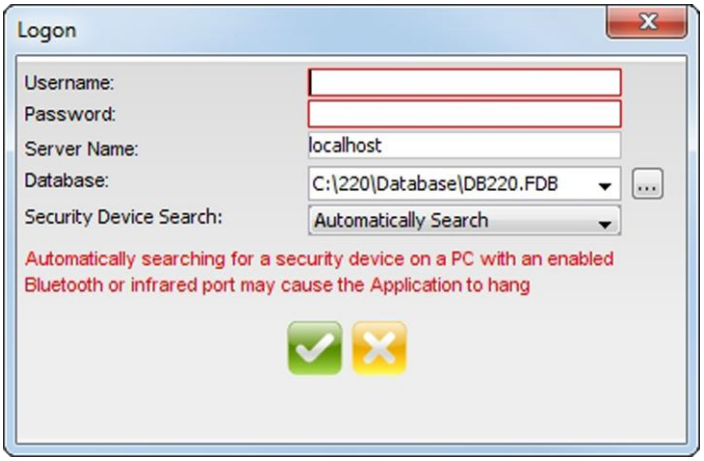


Figure 2 – Logon Dialog (Enter Username and Password)

3. From the **Security Device Search** drop-down list, make your selection from the following choices:

*On first time installation of the IXP220 Software, the **I do NOT Have One** choice is by default selected. In this case, if the site has an ImproX RS connected that's unlocked for a System 3 or System 4 then the IXP220 Software starts up as a **System 1**. This means no search is performed for the ImproX RS.*

- **Automatically Search**—for *IXP220-3* and *IXP220-4* installations where an ImproX RS is connected but you are unsure of the COM Port number in use by the ImproX RS. Automatically searching on a computer that has an enabled Bluetooth or Infrared Port may result in the IXP220 application freezing.
- **Enter the COM Port Name**—for *IXP220-3* and *IXP220-4* installations where an ImproX RS is connected and you know the COM Port number in use by the ImproX RS. *Recommended when you have an enabled Bluetooth or Infrared Port*. If you select this choice, enter the COM Port number in the supplied textbox. If your installation does

NOT use the default Database Server Port of 3050, enter the server name and port number (that is *server:port*). An example could include *localhost:3051*, that is with *3051* being the port used.

– **I do NOT Have One**—for *IXP220-1* and *IXP220-2* installations with no ImproX RS.

4. Click the button.

Do NOT disconnect the ImproX RS while still connected to the IXP220 Software.
Should you unintentionally disconnect the ImproX RS while the Software's running, close the IXP220 Software, reconnect the ImproX RS and then restart the Software.

*When using **separate PC's for the Base Application (Host PC) and Database (Server PC)** installation, start the IXP220 Base Application as follows:*

1. *On the Host PC, start the IXP220 Base Application Software.*
2. *At the Login dialog, in the **Server Name** textbox, enter the actual name (or IP Address) of the Server PC.*
3. *In the **Database** textbox, enter the local path to the database file as it resides on the Server PC.*
4. *Enter the **Username (SYSDBA)** and **Password (masterkey)**.*
5. *Click the button.*

Database Version Check

After completing the login action, the **Automatic Database Upgrade Utility** checks the database version. If the Utility confirms the Database is older than that needed by the Software, a Warning dialog tells you an upgrade is needed. Perform the upgrade as follows:

1. At the Warning dialog, click the **OK** button.
2. In the Database Updater dialog, click the **Upgrade** button.
3. At the Message dialog, click the **OK** button.

If you do not upgrade the Database immediately, the IXP220 Software closes.

Hardware Auto-ID

Hardware detected for the first time receives a Logical Address. This Logical Address does not change, thus ensuring continuity in the Database.

During an Auto-ID, the Base Application searches for and configures ImproX hardware for use with the IXP220 System. Perform an Auto-ID after physically connecting and powering up the Hardware. The Auto-ID process differs across the different communication mediums; therefore continue with one of the following:

Controller Connected to Host PC using RS485 (ImproX RS)

1. At the **Auto-ID is Recommended for New Sites** dialog, click the **Yes** button.
2. At the **Confirm Auto-ID** dialog, click the **OK** button.

3. From the Auto-ID Communications Configuration dialog, select the appropriate **Com Port** record.
4. From the list of devices displayed, in the **Auto-ID Channel** column, make your selection.
5. Click the button.
6. At the Firmware Revision dialog, click the button.

Controller Connected to the Host PC using TCP/IP

1. At the **Auto-ID is Recommended for New Sites** dialog, click the **Yes** button.
2. At the **Confirm Auto-ID** dialog, click the **OK** button.
3. If your Controller does NOT appear in the **Auto-ID Communications Configuration** dialog continue as follows:

When using IP Terminals, do not use the button. Instead, make use of the button.

   a. Click the button.
   b. In the **Channel** column, replace the default IP Address details with the IP Address of your Controller.
   c. Press **Enter**.

   Or alternatively continue as follows:

   a. Click the button.
   b. In the Input dialog, enter the **Subnet Mask** details for your Network.
   c. Click the button.

*The **IP Door Controllers (Advanced)** tab provides a list of the IP Terminals in the System as well as the IP Address of the Controllers they connect to. When using IP Terminals over a WAN, change the Controller IP Address to the IP Address of the Router to ensure that the IP Terminal communicates correctly. To do this, continue as follows:*

1. *On the Auto-ID Channel tab, click the button.*
2. *In the Input dialog, enter the **Subnet Mask** details for your network.*
3. *Click the button.*
4. *Select the **IP Door Controllers (Advanced)** tab.*
5. *In the **Address** column, enter the Public Static IP Address of the Router the Controller will use to communicate with the Terminal.*
6. *In the **Respond To Address** column, enter the Public Static IP Address of the Router the Terminal will use to communicate with the Controller.*
7. *If necessary, edit the **Additional Timeout (0.1s)** value.*
8. *Continue with Auto-ID as normal. (See step 4 following).*

4. From the list of devices displayed, in the **Auto-ID Channel** column, make your selection.
5. Click the button.
6. At the Firmware Revision dialog, click the button.

Controller Connected over a Wide Area Network (WAN)

Controllers connected using a GSM Module do NOT support IP Terminals.

1. At the **Auto-ID is Recommended for New Sites** dialog, click the **Yes** button.
2. At the **Confirm Auto-ID** dialog, click the **OK** button.
3. In the Auto ID Communications Configuration dialog, click the **Import Channels** button.
4. Select the **Discovery.txt** file (originally exported from the Discovery Utility).
5. Click the **Open** button.

*The **IP Door Controllers (Advanced)** tab provides a list of the IP Terminals in the System as well as the IP Address of the Controllers they connect to. When using IP Terminals over a WAN, change the Controller IP Address to the IP Address of the Router to ensure that the IP Terminal communicates correctly. To do this, continue as follows:*

1. *On the Auto-ID Channel tab, click the **Import Channels** button.*
2. *Select the **Discovery.txt** file (originally exported from the Discovery Utility).*
3. *Click the **Open** button.*
4. *Select the **IP Door Controllers (Advanced)** tab.*
5. *In the **Address** column, enter the Public Static IP Address of the Router the Controller will use to communicate with the Terminal.*
6. *In the **Respond To Address** column, enter the Public Static IP Address of the Router the Terminal will use to communicate with the Controller.*
7. *If necessary, edit the **Additional Timeout (0.1s)** value.*
8. *Continue with Auto-ID as normal. (See step 6 following).*

6. From the list of devices displayed, in the **Auto-ID Channel** column, make your selection.
7. Click the button.
8. At the Firmware Revision dialog, click the button.

*You may carry out the Auto-ID process at any stage, by selecting **Hardware**>**Auto ID Units**.*

Connecting Controller A via the network and Controller B (connected to Controller A) by RS485, lets you configure both Controllers at the same time. This is not supported for Controllers connected using a GSM Module.

*After performing Auto-ID, review the log of identified units by selecting **Hardware**>**Latest Auto-ID Log** from the Menu Bar. This feature lets you check whether Auto-ID has missed any terminals, possibly because of a wrong DIP-switch setting or faulty communications.*

Firmware Version Confirmation

After physically connecting, powering up and identifying the ImproX Hardware, confirm whether a Firmware upgrade is required.

The Firmware Revisions dialog indicates the Unit Type along with the Latest Firmware revision available and the Current Firmware version in use by the unit. Access the Firmware Revisions dialog by selecting **Hardware**>**Firmware Version Check** from the Menu Bar.

*See **Part 7 – Utilities** for more information on the **Firmware Upgrade Utility**.*

Configuring the Site

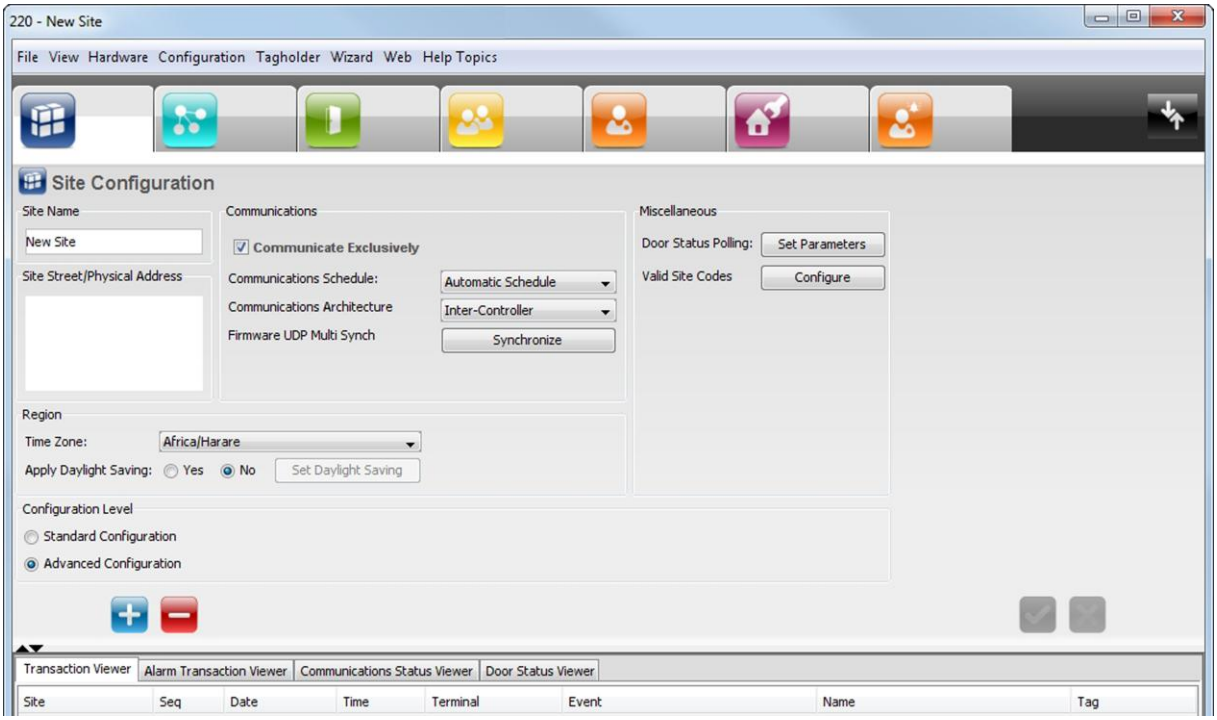


Figure 3 – Site Configuration Pane

Standard Site Configuration

1. If not already selected, select the Page Tab.
2. In the Configuration Pane, complete the **Site Name** textbox.
3. Complete the **Site Street/Physical Address** text area.

Advanced Site Configuration

Select the **Advanced Configuration** radio button.

Communications Group Options

1. If you wish to communicate only with the selected site, select the **Communicate Exclusively** checkbox.
2. From the **Communication Schedule** drop-down list select a Communication Schedule (see page 73 for information on setting up a Communication Schedule).
3. From the **Communications Architecture** drop-down list, select from the following options:
   - **Inter-controller**—this allows for communication to take place across Controllers. Inter-controller Communications is beneficial when used with Building Management and in maintaining Anti-passback (APB) status across Controllers.
   - **Fall-back**—this allows for configuration where TCP/IP is the default communications channel and RS485 being the secondary channel. Where your TCP/IP connection fails, the IXP220 Software falls back on RS485 and operations continue as normal (slightly slower than TCP/IP). When the TCP/IP connection restores, the Software automatically

resumes communication on the primary TCP/IP connection. *This configuration does NOT support inter-controller or pass-through communications.*

IXP220-1 and IXP220-2 Systems do NOT support Fall-back Communications.

The selection you make under point 3 above, determines the options available to you on the Controller Configuration Pane.

*Click the **Synchronize** button to write IP Mapping files to the IXP220 directory. These files are used on selection of **UDP Multi Controller** as the **communications type**. See Part 7– Utilities for more information.*

Region Group Options

1. From the **Time Zone** drop-down list, make your selection.
2. Set the **Apply Daylight Saving** option as follows:
   a. Alongside **Apply Daylight Saving**, click the **Yes** radio button.
   b. Click on the **Set Daylight Saving** button.
   c. In the Set Daylight Saving dialog, set the **Time Offset, Start Date, Start Time, End Date** and **End Time**.
   d. Click the button.

Miscellaneous Group Options

Door Status Polling

1. Click the **Set Parameters** button.
   – Set the **Polling Frequency** (seconds)—how often Doors (Locations) get polled for their status.
   – Set the **Door Open Time Limit** (seconds)—normal duration Doors (Locations) remain open.
2. Click the button.

Valid Site Codes

You may set up to **64** Site Codes per Site. For your convenience, Site Codes may be copied between sites using the **Copy Selected Codes (All Sites)** and **Copy Selected Codes (Selected Site)** buttons. Configure a list of accepted Site codes (affects HID® Tags only):

1. Click the **Configure** button.

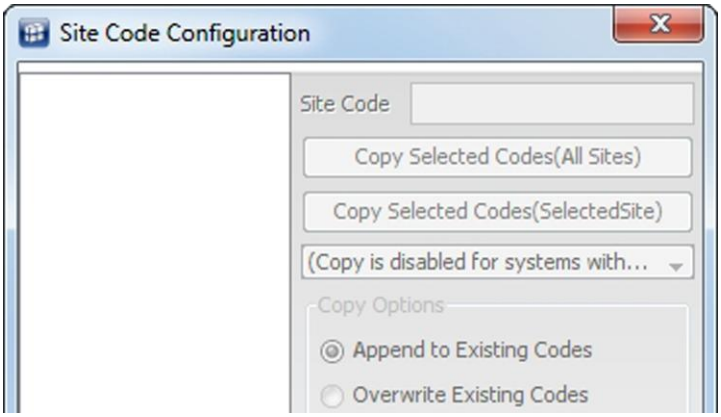


Figure 4 – Site Code Configuration

2. Click the button.
3. In the **Site Code** textbox, enter a suitable code.
4. Select either the **Append to Exiting Codes** or **Overwrite Existing Codes** radio button.
5. Click the button.

After updating the Site Configuration Pane, click the button.

Add a Site

On sites with an *unlocked Multi-site License*, add a new Site as follows:

1. Select the Page Tab.
2. In the Configuration Pane, select the **Advanced Configuration** radio button.
3. Click on the button.
4. In the IXP220 Site Creator dialog, complete the **Site Name** textbox.
5. Complete the **Site Street/Physical Address** textbox.
6. Click the button.

Refer to the section **Running Auto-ID** on page 16 for further information.

Delete a Site

Deleting a Site deletes all information (including Tagholder details and transactions) relating to the Site.

To delete a Site, proceed as follows:

1. Select the Page Tab.
2. In the Configuration Pane, select the **Advanced Configuration** radio button.
3. From the **Select Site** group, select the Site for deletion.
4. Click on the button.
5. At the **Confirmation of Site Deletion** warning dialog, click the **OK** button.
6. In the **Password** textbox, enter your administrator password.
7. Click the button.

2 Controller Configuration

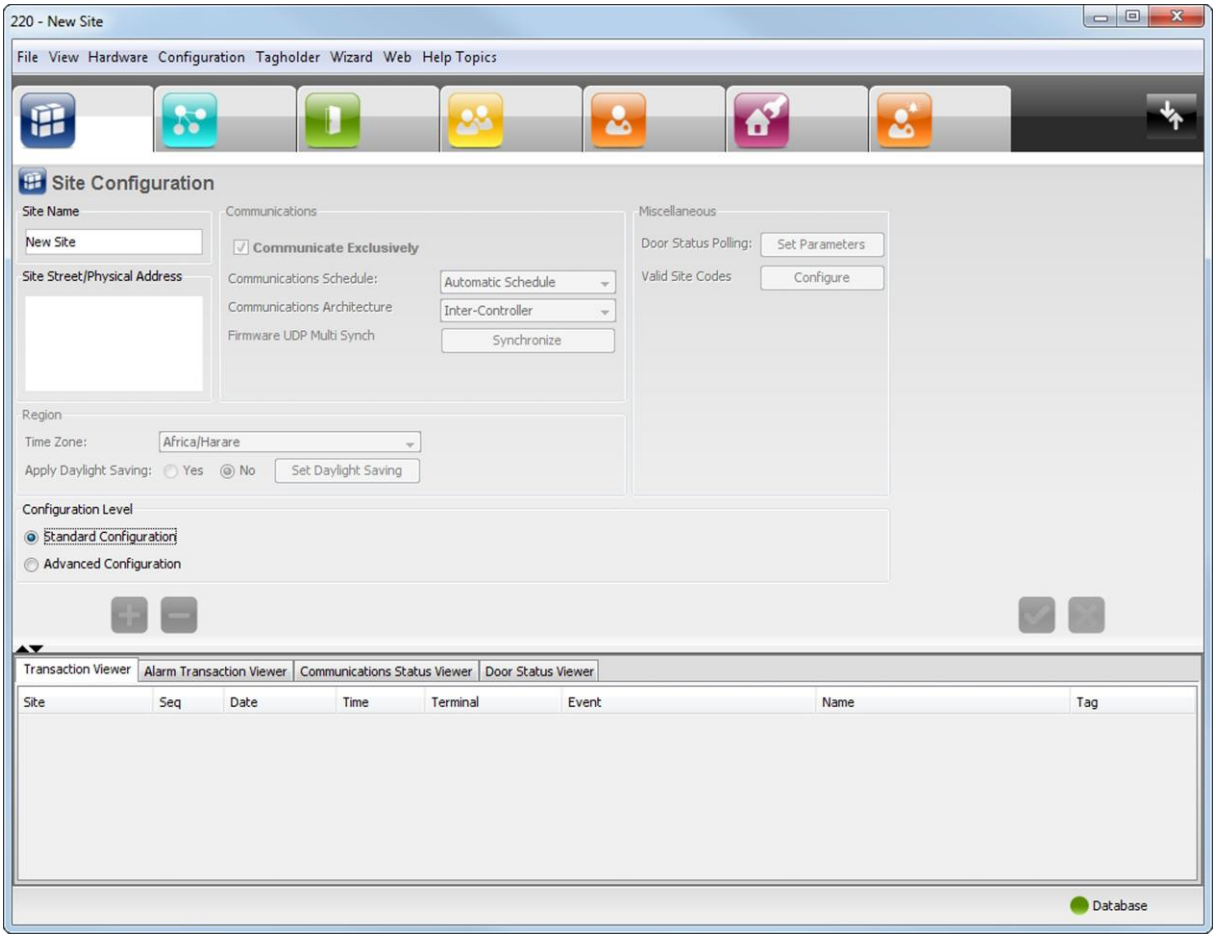


Figure 5 – Controller Configuration Pane – With Standard Controller Configuration Tab Selected

*The information displayed in the **Communications Channel** column varies according to your IXP220 Controllers installation:*

- *Using **TCP/IP**, the column displays the **IP Address** of the Controller.*
- *Using **USB, RS232 or RS485**, the column displays the **Communications Port** number.*
- *Using **GPRS**, the column displays the public static IP Address or the dynamic Host Name of the Controller.*

IXP220.properties Configuration

Where you have ImproX iTT or iTRT Ethernet Terminals connected to your Controller (using Firmware V4.00 or above), continue as follows:

1. Close the IXP220 Base Application.
2. From **C:\IXP220**, open the **IXP220.properties** file.
3. Set the **ixp220.controller.diagnostic.interval=0** setting.

*This is how often the Controller calculates the diagnostic statistics. The minimum value is **1** minute and the maximum **60** minutes (1 hour). This setting does not indicate how often the communications diagnostic transaction goes through. Rather the Controller recalculates the diagnostic transactions and compares the latest value to its last calculation. If there is a notable difference, the Controller sends a new transaction. Refer to Part 4 – Reports for information on the Communications Diagnostic Report.*

4. From the Main Menu, select **File**>**Save**.
5. From the Main Menu, select **File**>**Exit**.
6. Open the IXP220 Base Application. Refer to page 15 for more information on starting the Base Application.
7. Perform a **Full Upload**. Refer to page 70 for more information on performing a Full Upload.

General Configuration

Configure your Controller as follows:

1. Select the Page Tab.
2. In the **Controller Name** textbox, assign your Controller a suitable name.
3. From the **Mode Configuration** drop-down list, make your selection. See page 56 for more information on Modes of Operation.

The instructions that follow continue as for an Advanced Configuration. For a Standard Configuration ignore references made to fields that appear greyed out.

4. Select the **Advanced Configuration** radio button.
5. Enable or disable Controllers as per your requirements, by selecting or de-selecting the **Controller Enabled** checkbox.
6. From the **APB Configuration** group, adjust the following settings:
   - Set the **APB Lockout Delay on Entry** (minutes)—the same Tagholder may not pass the same anti-passback (APB) entry access point within the specified time period.
   - Set the **APB Lockout Delay on Exit** (minutes)—the same Tagholder may not pass the same anti-passback (APB) exit access point within the specified time period.

Site Configuration Set to Inter-controller Communications

With your site setup to use inter-controller communications, continue with the following Controller configuration options:

1. From the **Primary Communications** drop-down list, make your selection.
2. From the **Communications Mode** drop-down list, make your selection from the following choices:
   - **Standard Controller**—this is the default choice. This configuration associates to Controller configurations preceding V1.82, including all configuration choices offered in IXP220 Software V1.80. In addition, support includes inter-controller communications (for IP Controllers only).
   - **Controller Forwards Communications for RS485 Controllers**—this allows for inter-controller communications for Controllers daisy-chained from an IP Controller. For example, Controller A has a network cable connected to it and has Controller B and Controller C connected to its RS485 Controller bus. A Tagholder enters a Door

(Location) on Controller A, Controller A will update the anti-passback status of the Tagholder on Controller B and Controller C. This option DOES NOT affect pass through communications. The Software still communicates with the daisy-chained Controllers via Controller A.

*Activate the **Controller Forwards Communications for RS485 Controllers** option as follows:*

1. *In the Controller Configuration Pane, click the **Communications** button.*
2. *In the **Communication Configuration** dialog, click the button.*
3. *In the **Address** column of the new record, enter the Communication Port details for your ImproX RS.*
4. *Click the button.*
5. *From the **Communications Mode** drop-down, select the **Controller Forwards Communications for RS485 Controllers** option.*
6. *From the **Primary Communications** drop-down list, select the newly added Communication Port number.*

Site Configuration Set to Fall-back Communications

Fall-back Communications allows for configuration using TCP/IP as the primary communications channel and RS485 as the secondary channel. Where your TCP/IP connection fails, the IXP220 Software falls back on RS485 and operations continue as normal (slightly slower than TCP/IP). When the TCP/IP connection restores, the Software automatically resumes communication on the primary TCP/IP connection. *This configuration does NOT support inter-controller or pass-through communications.* With your site setup to use fall-back communications, continue with the following Controller configuration options:

1. From the **Primary Communications** drop-down list, make your selection.
2. From the **Secondary Communications** drop-down list, make your selection.

After updating the Controller Configuration Pane, click the button.

Changing the Communications Channel

Change your Controller's Communications Channel as follows:

1. Select the Page Tab.
2. Select the **Advanced Configuration** radio button.
3. Click the button.
4. In the **Communication Configuration** dialog, click the button.
5. In the **Address** column of the new record, enter the Communication Port number, IP Address or Hostname you wish to change to.

When entering a Communications Port, use the prefix COM.
*When entering an IP Address or Host Name, ensure that you enter Port number in the **Port** column.*

6. If the Controller has IP Terminals connected, in the **Respond Address** column of the associated IP Terminal records, enter the IP Address referred to in step 5.

7. Click the button.
8. From the **Primary Communications** drop-down list, select the newly added Communication Port number, IP Address or Hostname.
9. If the Controller has IP Terminals connected, perform a **Full Upload**. For more information on performing a Full Upload refer to page 70.

Controller UDP Broadcast Configuration

Controller UDP Broadcast will only work if the Primary Communication of your Controller is set to IP. Refer to page 24 for more information on changing the primary communication of your controller.

The IXP220 Controller can broadcast transactions as they happen to a defined IP Address. The Base Application lets you configure the IP Address the Controller broadcasts transactions to. Once this information uploads to the Controller, the Controller sends an ASCII string for each transaction to the IP Address as defined in the Base Application. This is a Controller specific setting. The format of the broadcast messages are:

*Where you see **<CR>** it stands for a carriage return. Where you see **<LR>** it stands for a line feed. Where you see **SSHHCCTT**, the SS stands for Site Address (hard-coded to 01), HH stands for Host Address (hard-coded to 01), CC stands for Controller Logical Address and TT stands for Terminal Logical Address.*

- **Heartbeat**—<site name>,,,,,,,,,,<CR><LF>
- **Status Transactions**—<site name>,<date>,<time>,<sequence number>,<event>,<address = SSHHCCTT>,<[door no]door name>,<zone>,,,, <CR><LF>
- **Access Transactions**—<site name>,<date>,<time>,<sequence number>,<event>,<address = SSHHCCTT>,<[door no]door name>,<zone>,<tagholder last name>,<tagcode>,<tag type>,<reason code><CR><LF>

This feature gives users direct access to transactions as they happen on the Controller. Users are therefore not forced to rely on the Base Application being on-line all the time.

1. Select the Page Tab.
2. Select the **Advanced Configuration** radio button.
3. In the **UPD Output** group, select the Enable UDP Broadcast checkbox.
4. In the **Address** textbox, enter the IP Address for the device receiving the broadcasted data.
5. In the **Port** textbox, enter the Port number of the device receiving the broadcasted data.
6. Set the time (in seconds) between notifications using the **Keep Alive Time** textbox. The default Keep Alive Time is **60** seconds.
7. Click the button.

Disconnecting the GSM Module

*The **Remove GSM Module** button only appears when configuring a Controller with a GSM Module connected.*

Clicking the **Remove GSM Module** button uninstalls the GSM Module from the selected Controller. This lets you disconnect the GSM Module safely.

Disconnect the GSM Module as follows:

1. Select the Page Tab.
2. Select the **Advanced Configuration** radio button.
3. Click the **Remove GSM Module** button.
4. At the Confirmation Required dialog, click the **OK** button.

Full Upload

Clicking the **Upload** button uploads the selected Controllers configuration information to the physical unit. Refer to page 70 for more information on performing a Full Upload.

Upgrade

The textbox situated alongside the **Upgrade** button, indicates the status of the Controller (either Stand-alone or System). The Stand-alone Controller has a locked Terminal Bus. You may unlock the Terminal Bus by purchasing an unlock code, thus upgrading your Controller to a System Controller.

Upgrade your Stand-alone Controller to a System Controller as follows:

1. Select the Page Tab.
2. Select the **Advanced Configuration** radio button.
3. Click the **Upgrade** button.
4. From the **Select Device XML File** dialog, select the downloaded XML (Webstore Unlock) File.

*The file name reflects the **Fixed Address** of the Controller for Upgrade.*

5. Click the **Open** button.
6. At the Unlock Successful dialog, click the **OK** button.
7. Click the **Upload** button.

When you return to the Controller Configuration Pane, you will notice that the textbox alongside the Upgrade button now reflects the Controllers new settings.

3 Door Configuration

The Door Configuration Pane lets you configure a Site's Doors (Locations) including Terminals, Readers, Zones and Door Mode Patterns.

See Part 5 – Advanced Configuration for details on Lift (Elevator) control.

*Editing Door settings or making changes to the Door Mode Patterns resets all Tags in the System to A**nti-passback (APB) neutral**. This ensures that Tagholders are not denied access because of Tags being in the wrong state. The Anti-passback (APB) state of all Tags again synchronizes correctly on first access.*

Add a Door

Doors are set up using the largely intuitive Door Configuration Wizard. This allows you to configure Doors quickly and easily. Once configured, use the Door Tab ( ) to edit your settings.

1. From the Main Menu, select **Wizard > Doors**.
2. From the **Assign Readers From** drop-down list, make your selection from:
   - **All Controllers**—assigns available Readers from all Controllers.
   - **Your Specific Controller**—assigns available Readers from a specific Controller.
3. From the **Reader Allocation** drop-down list, make your selection:
   - **Only Entry Reader**—only configures the Entry Reader for each Door.
   - **Entry + Exit Reader**—configures both the Entry and the Exit Reader for each Door.
4. From the **Door Naming Convention** drop-down list, make your selection:
   - **Use Template Name**—names all Doors according to the name entered in the Door Name textbox.
   - **Use Controller Name**—uses the Controller name for each Door.
5. If necessary, deselect the **Append Incremental Number to Door Name** checkbox.

Add Door Mode Patterns

*Making changes to the Door Mode Patterns resets all Tags in the System to **Anti-passback (APB) neutral**. This ensures that Tagholders are not denied access because of Tags being in the wrong state. The Anti-passback (APB) state of all Tags again synchronizes correctly on first access.*

The IXP220 Software supports a maximum of 8 Door Mode Patterns at each door. This setting regulates the Door's (location's) operating mode including the start and end time. Continue as follows to add a new Door Mode Pattern:

1. In the New Door Configuration Wizard, click the **Door Mode Pattern** button.
2. Click the button.
3. In the **Pattern Name** textbox, assign your Door Mode Pattern a suitable name.
4. Click the button.
5. From the records displayed on the left-hand side of the Configuration Pane, select the newly created Door Mode Pattern record.
6. Edit the following settings for the selected record:
   - **Start Time** and **End Time**—breaks the day into time slots. By selecting and changing the End Time figure, you effectively create extra records, breaking the day into parts. You may create a maximum of 8 time slots per Door Mode Pattern.
   - **Mode**—indicates the mode in which the Door (Location) operates.

Door (Location) operating mode examples include:

- ***Tag****—requires presentation of a Tag to gain access.*
- ***Supervisor Unlock****—requires that a Supervisor unlock the Door prior to normal employees gaining entrance.*
- ***Locked****—the Door is locked and cannot be overridden with any Tag.*
- ***Open on First Tag****—the door is opened when the first valid Tagholder presents their Tag.*
- ***No Entry****—only Administrators are granted access.*
- ***Door Entry Code****—requires entry of a Door Entry Code to gain access.*
- ***Open Now****—Door opens at specified time. A Tag is not required to open the Door.*
- ***Personal Access Code****—requires entry of a Personal Access Code to gain access. Your Personal Access Code may range from between **1 to 999999999** followed by a # symbol.*

   - **Finger (B-SHO)**—make a selection from the choices presented: No, “+Entry”, “+Exit”, “+Both”, “or Entry”, “or Exit”, “or Both”, “Finger only Entry”, “Finger only Exit” or “Finger only Both”. Selecting “+Entry”, “+Exit” or “+Both”, calls for Tagholders to present their Tag (MIFARE® or DESFIRE®) and their fingerprint at the ImproX B-SHO Fingerprint Terminal. Selecting “or Entry”, “or Exit” or “or Both”, calls for Tagholders to present either their Tag or fingerprint at the ImproX B-SHO Fingerprint Terminal. For the following options, “Finger only Entry”, “Finger only Exit” or “Finger only Both”, only fingerprint presentation is allowed (the tag reader is disabled).
   - **+PIN**—make a selection from the choices presented: No, Entry, Exit or Both. By selecting Entry, Exit or Both, you call for Tagholders to present their Tag and enter a PIN-code at the respective Keypad Reader.
   - **+Reason**—make a selection from the choices presented: No, Entry, Exit or Both. By selecting Entry, Exit or Both, you call for Tagholders to present their Tag and enter a Reason Code (see page 54 for information on Adding a Reason Code) at the respective Keypad Reader.
   - **+Dual Tag**—requires presentation of 2 individual Tags for access.
   - **Record**—log Transaction. If you select NO, the “Allowed In” and “Allowed Out” transactions do not appear in the Transaction Viewer and do not save to the Database. This affects any report using transactions.
   - **Denied Alarm**—by selecting Yes, you instruct the System to treat denied events as alarms. Set the Controller Mode Configuration to Intrusion or Alarm Arming for functionality of this feature.
   - **LED**—sets the LED’s behaviour during the stipulated time slot.

7. Click the button.
8. Click the button.

Add a Zone

To create and configure Zones, continue as follows:

1. In the New Door Configuration Wizard, click the **Zone** button.
2. Click the button.

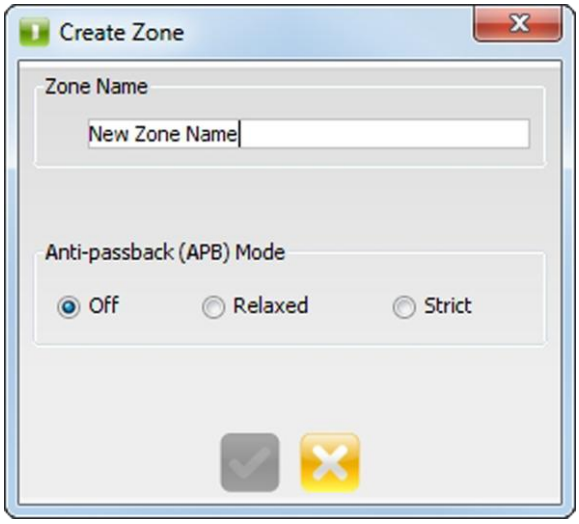


Figure 6 – Create Zone Dialog

3. In the **Zone Name** textbox, assign the Zone a suitable name.
4. Select one of the **Anti-passback (APB) Mode** radio buttons:
   - **Off**—Anti-passback (APB) not enforced.
   - **Relaxed**—after entering a Zone, the Tagholder must exit the Zone using their Tag *before* they can re-enter. However, Tagholders can use their Tags for multiple, consecutive exits in this Mode.
   - **Strict**—enforced Anti-passback (APB) Zone rules for **in** and **out** directions. A Tagholder cannot enter or exit a Zone consecutively.

*You may elect from time to time to **reset Anti-passback (APB)**, essentially giving ALL Tagholders a "free pass" on their next transaction. Carry out this task as follows:*

1. *From the Main Menu, select **Hardware**>**Reset Anti-passback**.*
2. *At the Reset Anti-passback dialog, click the **OK** button.*

Should you wish to reset Anti-passback (APB) on an individual Tagholder, refer to page 48, Miscellaneous Configuration for more information.

5. Click the button.

*Once the Zone record appears on the Zone tab, edit the **Zone Name** and **APB Mode** settings using the Configuration Pane.*

*Configure multiple Zone records at the same time, by holding down the **Ctrl** key and selecting multiple records. Alternately hold down the left mouse button and drag your mouse over the records, making your selection.*

6. Click the button.

Door Template Setup

1. Select the **Door** Tab.
2. In the **Door Name** textbox, assign the Door a suitable name up to 20 characters. If under Door naming Convention you selected Use Template Name, the name you assign becomes the door name template. Refer to page 27 for more information on the Door Naming Convention setting.
3. Under **Zone**, select a Zone from the drop-down list.
4. In the **Door Entry Code** textbox, enter a **5-digit** number for use in gaining access. Refer to Door Mode Patterns page 27 for more information on setting Modes.

*Using a **Door Entry Code** allows Tagholders to enter or exit a Door using a numeric code. Note, however, Tags with access permissions for the Door (Location) are still acknowledged by the Reader. Activate the Door Entry Code feature, as follows:*

1. *On the Door Configuration Pane, select the **Door Mode Pattern** Tab.*
2. *Click the button.*
3. *In the **Pattern Name** textbox, assign your Door Mode Pattern a suitable name.*
4. *Click the button.*
5. *From the records displayed on the left-hand side of the Configuration Pane, select the newly created Door Mode Pattern record.*
6. *Edit the following settings for the selected record:*
   - ***Start Time**, **End Time**, **+PIN**, **+Reason**, **+Dual Tag**, **Record**, **Denied Alarm** and **LED**.*
   - ***Mode**—select **Door Entry Code** from the drop-down list. (Door Entry Codes range from **1 to 65535**. After entering the Door Entry Code at the Reader or Terminal, complete the entry by pressing the # key).*
7. *Click the button.*
8. *On the Door Configuration Pane, select the **Door** Tab.*
9. *In the **Door Entry Code** textbox, enter a **5-digit** numeric code.*

5. In the **Daily Door Mode Patterns** group, make your selections from the Day's Door Mode Pattern drop-down lists.

Entry or Exit Reader Configuration

1. Select the **Entry** or **Exit** Tab.
2. From the **Configuration Level** group, select one of the following radio buttons:
   - **Standard Configuration**—activates only the basic features.
   - **Advanced Configuration**—activates extra advanced features.
3. From the **RTE Mode** drop-down list, make your selection from the following:
   - **Normally Open**—use this option when connecting Normally Open switches.
   - **Normally Closed**—use this option when connecting Normally Closed switches.
4. From the **Reader Function** drop-down list, make your selection from the following:
   - **Access Control**—sets a flag in the Database alerting third-party time and attendance applications that the door is used for Access Control purposes only.

- **Access Control + Time & Attendance**—sets a flag in the database alerting third-party time and attendance applications that the Door is used for Time and Attendance and Access Control functions.

5. From the **DOS Mode** group, from the DOS Mode drop-down list, make your selection:
   - **Normally Closed**—use this option when connecting Normally Closed Door Sensors.
   - **Normally Open**—use this option when connecting Normally Open Door Sensors.
6. From the **DOS Usage** drop-down list, make your selection from the following:
   - **Normal**—alarm sounds if the Door remains open too long or if the Door is forced. Use this feature for monitoring real Door open states.
   - **Terminate Strike**—deactivates the relay if Door is opened and closed or forced. Use this feature where the lock must re-engage once the Door is closed.
   - **Inhibit**—deactivates the Reader as long as the Door is open; also there is no alarm for Doors forced open. Used when the Door is opened, the Reader disables while the Door remains open.
7. Edit the **Strike Duration (0.1s)** textbox, the default value is **40** (0.1s). Setting the Strike Duration to 55555 toggles the Relay.
8. Edit the **Open Duration(s)** textbox. By default, the Open Duration is set to **0**, disabling the Door Open Sensor (DOS).
9. Enable End-of-line Sensing by selecting the **Enable End-of-line Sensing** checkbox.

End-of-line Sensing lets the System raise an alarm when somebody bypasses the Door Open Sensor. That is, the System distinguishes between tampering on the circuit and closure of the Door Open Sensor. End-of-line sensing on the IXP220 Controller, ImproX iTT (input 1 and 3 only) and iTRT (input 1 and 3 only) is only possible if Door Open Sensing is configured. Set End-of-line Sensing per Door.

10. From the **ON VALID Tag** group, from the LED Action drop-down list, select the required LED colour state and Duration.
11. From the **Buzzer Volume** drop-down list, select the Buzzer volume and Duration.
12. From the **On INVALID Tag** group, from the LED Action drop-down list, select the required LED colour state and Duration.
13. From the **Buzzer Volume** drop-down list, select the Buzzer volume and Duration.
14. Click the button.
15. Review the Door configuration settings selected. If you accept the settings, click the button.

Edit a Door

Configuration of multiple Doors (Locations) is allowed. Configure multiple Doors (Locations), by holding down the **Ctrl** key and selecting multiple records. Alternatively, hold down the left mouse button and drag your mouse over the records. Multi-selecting Doors (Locations) loads the default values for all Doors and Readers, only the changed settings save to the individual Doors.

1. Select the Page Tab. Within the previously selected Door Tab, you will notice a new set of Tabs activate. These include a new **Door** Tab, an **Entry** Tab and an **Exit** Tab.
2. Select the Door you wish to edit.

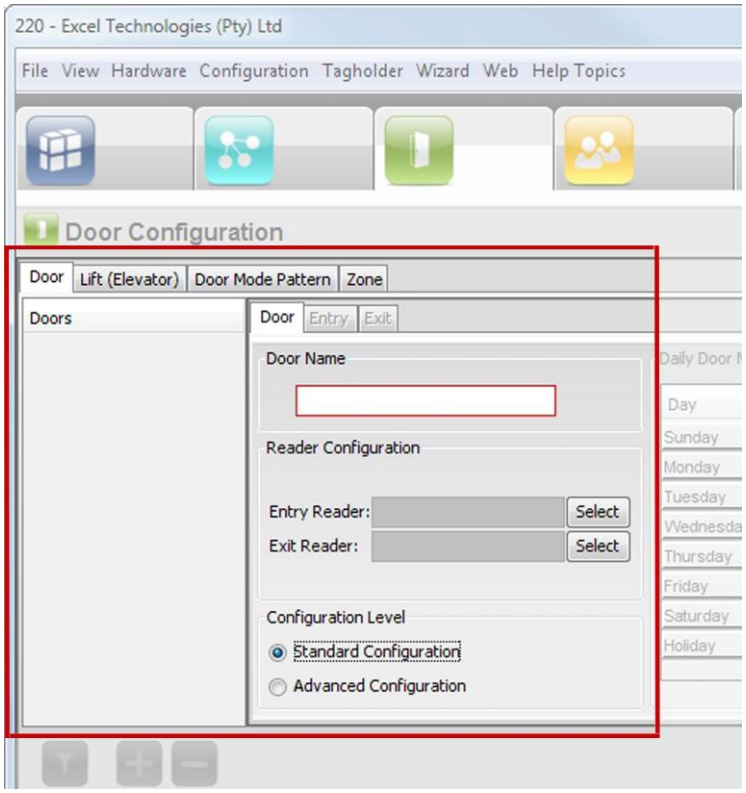


Figure 7 – Left-hand Side of the Door Configuration Pane

3. From the **Configuration Level** group, select one of the following radio buttons:
   - **Standard Configuration**—activates only the basic Access Control features.
   - **Advanced Configuration**—activates extra advanced features, for sites that need Daily Door Mode Patterns, Zones, Door Entry Codes and Alarm Arming.

*The **Enable Bell** checkbox only activates on Doors using ImproX (KMA) Keypad Mullion Antenna Readers. Selecting this checkbox activates the Bell button (situated at the bottom of the Antenna Reader's Keypad).*

Edit Readers

To edit and configure Readers, continue as follows:

Reader Selection

1. In the **Reader Configuration** group (see Figure 7), alongside the **Entry Reader** textbox, click the **Select** button.
2. In the **Unassigned Readers** dialog, from the list of displayed records, select a Reader.

In the Unassigned Readers dialog, reduce the number of Readers displayed by selecting a specific Controller from the Controller Filter drop-down list.

3. Click the button.
4. Alongside the **Exit Reader** textbox, click the **Select** button.
5. In the **Unassigned Readers** dialog, from the list of displayed records, select a Reader.
6. Click the button.

*Select a single Reader by double-clicking the Reader's record. Alternatively **multi-select Readers** as follows:*

1. *Click the Entry Reader's **Select** button.*
2. *In the Unassigned Readers Dialog, select both your **Entry** and **Exit** Readers.*
3. *Click the button.*

*The IXP220 Software automatically assigns the **top selected Reader as the Entry Reader** and the **bottom selected Reader as the Exit Reader**.*

7. Click the button.

Entry or Exit Reader Configuration

1. Select the **Entry** or **Exit** Tab.

The settings displayed on the Entry or Exit Tabs depend on the type of Terminal connected. Ignore references made below to fields that do not display.

2. From the **Configuration Level** group, select one of the following radio buttons:
   - **Standard Configuration**—activates only the basic features.
   - **Advanced Configuration**—activates extra advanced features.
3. From the **Miscellaneous** group, from the RTE Mode drop-down list, make your selection from the following:
   - **Normally Open**—use this option when connecting Normally Open switches.
   - **Normally Closed**—use this option when connecting Normally Closed switches.
4. From the **Reader Function** drop-down list, make your selection from the following:
   - **Access Control**—sets a flag in the Database alerting third-party time and attendance applications that the door is used for Access Control purposes only.
   - **Access Control + Time & Attendance**—sets a flag in the database alerting third-party time and attendance applications that the Door is used for Time and Attendance and Access Control functions.
5. From the **Message Display Supervisor** drop-down list, make your selection.
6. From the **Enable Off-line Validation** drop-down list, make your selection from the following:
   - **Disabled**—disables off-line validation.
   - **Enabled**—enables off-line validation.

ImproX iTT and ImproX iTRT units connected by IP will always run in Full Off-line Validation Mode. ImproX iTT and ImproX iTRT units connected by RS485 will run in Full Off-line Validation Mode when there are 1 000 Tags or less in the System. Once this threshold is exceeded, it will switch over to Cached Off-line Validation Mode. Cached Off-line Validation Mode relies on transactions in the ImproX iTT and ImproX iTRT Transaction Buffer to make access control decisions.

7. From the **DOS Mode** group, from the **DOS Mode** drop-down list, make your selection from the following:
   - **Normally Closed**—use this option when connecting Normally Closed Door Sensors.
   - **Normally Open**—use this option when connecting Normally Open Door Sensors.
8. From the **DOS Usage** drop-down list, make your selection from the following:
   - **Normal**—alarm sounds if the Door remains open too long or if the Door is forced. Use this feature for monitoring real Door open states.

- **Terminate Strike**—deactivates the relay if Door is opened and closed or forced. Use this feature where the lock must re-engage once the Door is closed.
- **Inhibit**—deactivates the Reader as long as the Door is open; also there is no alarm for Doors forced open. Used when the Door is opened, the Reader disables while the Door remains open.

9. Edit the **Strike Duration (0.1s)** textbox, the default value is **40** (0.1s). Setting the Strike Duration to 55555 toggles the Relay.
10. Edit the **Open Duration(s)** textbox. By default, the Open Duration is set to **0**, disabling the Door Open Sensor (DOS).
11. Enable End-of-line Sensing by selecting the **Enable End-of-line Sensing** checkbox.

End-of-line Sensing lets the System raise an alarm when somebody bypasses the Door Open Sensor (DOS). That is, the System distinguishes between tampering on the circuit and closure of the Door Open Sensor (DOS). End-of-line sensing on the IXP220 Controller, ImproX iTT (input 1 and 3 only) and iTRT (input 1 and 3 only) is only possible if Door Open Sensing is configured. Set End-of-line Sensing per Door.

12. From the **ON VALID Tag** group, from the LED Action drop-down list, select the required LED Colour State and Duration.
13. From the **Buzzer Volume** drop-down list, select the Buzzer Volume and Duration.
14. From the **ON INVALID Tag** group, from the LED Action drop-down list, select the required LED Colour State and Duration.
15. From the **Buzzer Volume** drop-down list, select the Buzzer Volume and Duration.
16. Click the button.

Edit a Zone

To edit and configure Zones, continue as follows:

1. On the Configuration Pane, select the **Zone** Tab.
2. Select the Zone you wish to edit.
3. On the right-hand side of the Configuration Pane, in the **Zone Name** textbox, edit the name of your Zone.
4. Select one of the **Anti-passback (APB) Mode** radio buttons:
   - **Off**
   - **Relaxed**
   - **Strict**

*You may elect from time to time to **reset Anti-passback (APB)**, essentially giving ALL Tagholders a "free pass" on their next transaction. Carry out this task as follows:*

1. *From the Main Menu, select **Hardware**>**Reset Anti-passback**.*
2. *At the Reset Anti-passback dialog, click the **OK** button.*

Should you wish to reset Anti-passback (APB) on an individual Tagholder, refer to page 48, Miscellaneous Configuration for more information.

5. Click the button.

*Configure multiple Zone records at the same time, by holding down the **Ctrl** key and selecting multiple records. Alternately hold down the left mouse button and drag your mouse over the records, making your selection.*

Edit Door Mode Patterns

*Making changes to the Door Mode Patterns resets all Tags in the System to **Anti-passback (APB) neutral**. This ensures that Tagholders are not denied access because of Tags being in the wrong state. The Anti-passback (APB) state of all Tags again synchronizes correctly on first access.*

The IXP220 Software supports a maximum of 8 Door Mode Patterns at each Door. This setting regulates the Door's (Location's) operating mode including the start and end time.
Continue as follows to edit a Door Mode Pattern:

1. On the Configuration Pane, select the **Door Mode Pattern** Tab.
2. From the records displayed on the left-hand side of the Configuration Pane, select the Door Mode Pattern record you wish to edit.
3. In the **Pattern Name** textbox, edit the name of your Door Mode Pattern.
4. Edit the following settings for the selected record:
   - **Start Time** and **End Time**
   - **Mode**

Door (Location) operating mode examples include:

- ***Tag**—requires presentation of a Tag to gain access.*
- ***Supervisor Unlock**—requires that a Supervisor unlock the Door prior to normal employees gaining entrance.*
- ***Locked**—the Door is locked and cannot be overridden with any Tag.*
- ***Open on First Tag**—the Door is opened when the first valid Tagholder presents their Tag.*
- ***No Entry**—only Administrators are granted access.*
- ***Door Entry Code**—requires entry of a Door Entry Code to gain access.*
- ***Open Now**—Door opens at specified time. A Tag is not required to open the Door.*
- ***Personal Access Code**—requires entry of a Personal Access Code to gain access. Your Personal Access Code may range from between **1 to 999999999** followed by a # symbol.*

   - **Finger (B-SHO)**
   - **+PIN**
   - **+Reason**
   - **+Dual Tag**
   - **Record**
   - **Denied Alarm**
   - **LED**
5. Click the button.

Edit Advanced Door Configuration

On selecting the **Advanced Configuration** radio button, additional advanced settings activate.

Continue as follows to edit these settings:

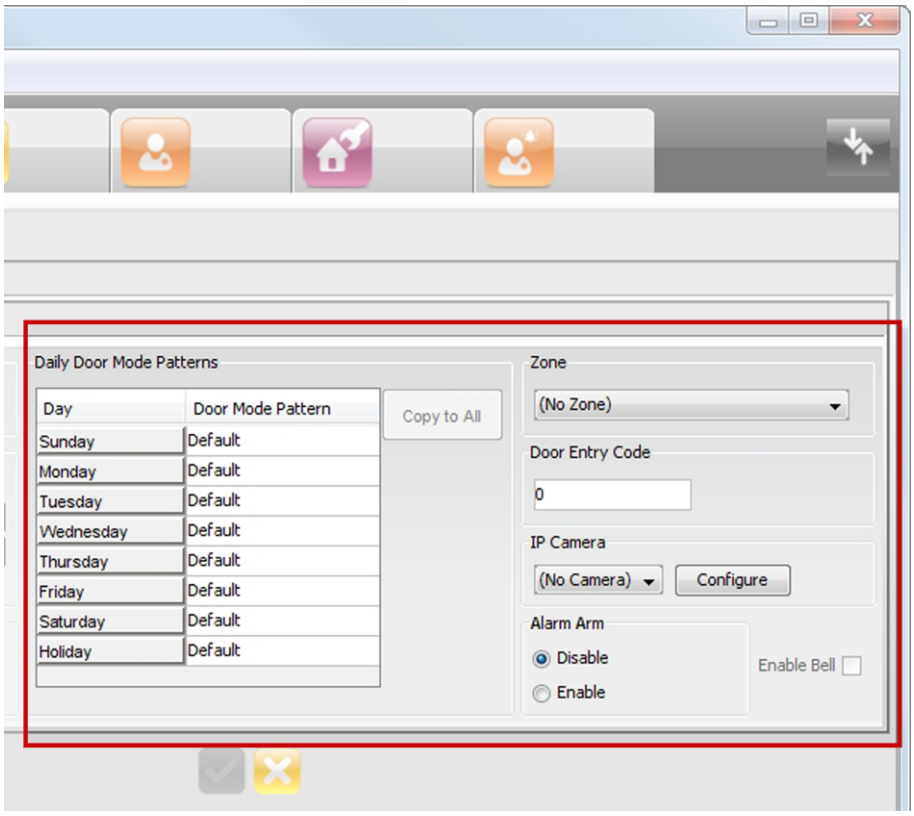


Figure 8 – Right-hand Side of the Door Configuration Pane

1. On the Door Configuration Pane, select the **Door** Tab.
2. In the **Daily Door Mode Patterns** group (see Figure 8), make your selections from the Day's Door Mode Pattern drop-down lists.
3. In the **Zone** group, select a Zone from the drop-down list.

*Using a **Door Entry Code** allows Tagholders to enter or exit a Door using a numeric code. Note, however, Tags with access permissions for the Door (Location) are still acknowledged by the Reader. Activate the Door Entry Code feature, as follows:*

1. *On the Door Configuration Pane, select the **Door Mode Pattern** Tab.*
2. *Click the button.*
3. *In the **Pattern Name** textbox, assign your Door Mode Pattern a suitable name.*
4. *Click the button.*
5. *From the records displayed on the left-hand side of the Configuration Pane, select the newly created Door Mode Pattern record.*
6. *Edit the following settings for the selected record:*
   - ***Start Time**, **End Time**, **+PIN**, **+Reason**, **+Dual Tag**, **Record**, **Denied Alarm** and **LED**.*
   - ***Mode**—select **Door Entry Code** from the drop-down list. (Door Entry Codes range from **1 to 65535**. After entering the Door Entry Code at the Reader or Terminal, complete the entry by pressing the # key).*
7. *Click the button.*
8. *On the Door Configuration Pane, select the **Door** Tab.*
9. *In the **Door Entry Code** textbox, enter a **5-digit** numeric code.*

*Refer page 57 for details on **Alarm Arming**.*

CCTV integration allows for better end user site management, that is in areas with rising crime, your receptionist can from a safe location monitor and control up to 4 Doors (Locations) (4 Cameras) at a time per site. Configure your IP Camera (Axis 210 or 213D range only) as follows:

1. *On the Door Configuration Pane, select the **Door** Tab.*
2. *Click the **Advanced Configuration** radio button.*
3. *Within the IP Camera group, click the **Configure** button.*
4. *In the IP Camera Configuration dialog, click the button.*
5. *In the **Name** textbox, assign your camera a meaningful name.*
6. *In the **Lookup** textbox, enter the **IP Address** for your camera.*
7. *Click the button*
8. *Exit the dialog by clicking the button.*
9. *Select the Door from the list of available Door records.*
10. *From the **IP Camera** drop-down list, select a Camera record, thus associating the Door and IP Camera.*
11. *Click the button*

4. Click the button.

Delete a Door

Deleting a Door automatically deletes reference to assigned Readers. Thus, these Readers return to the Unassigned Readers list ready for you to reallocate to a new Door. Continue as follows to delete a Door (Location):

1. Select the Page Tab.
2. On the Configuration Pane, select the **Door** Tab.
3. From the Doors Table on the left-hand side of the Configuration Pane, select the Door record for deletion.
4. Click the button.
5. At the Warning dialog, click **Yes**.

Delete a Zone

1. Select the Page Tab.
2. On the Configuration Pane, select the Zone Tab.
3. From the Zone records displayed, select the Zone for deletion.
4. Click the button.
5. Click the button.

*You may delete multiple Zones at the same time, by holding down the **Ctrl** key and selecting multiple records. Alternately hold down the left mouse button and drag your mouse over the records, making your selection.*

Delete a Door Mode Pattern

1. Select the Page Tab.
2. On the Configuration Pane, select the **Door Mode Pattern** Tab.
3. From the Door Mode Pattern Table on the left-hand side of the Configuration Pane, select the Door Mode Pattern record for deletion.
4. Click the button.
5. At the Confirmation Warning dialog, click **Yes**.

4 Access Group Configuration

Each Tagholder in a Site is assigned to at least one Tagholder Access Group. The purpose of Access Groups is to grant Tagholder access permissions in bulk. This saves you the trouble of configuring Tagholders one-at-a-time.

Configure Tagholder Access Groups

Create a Tagholder Access Group

For information on setting a Lift (Elevator) Access Group, see Part 5 – Advanced Configuration.

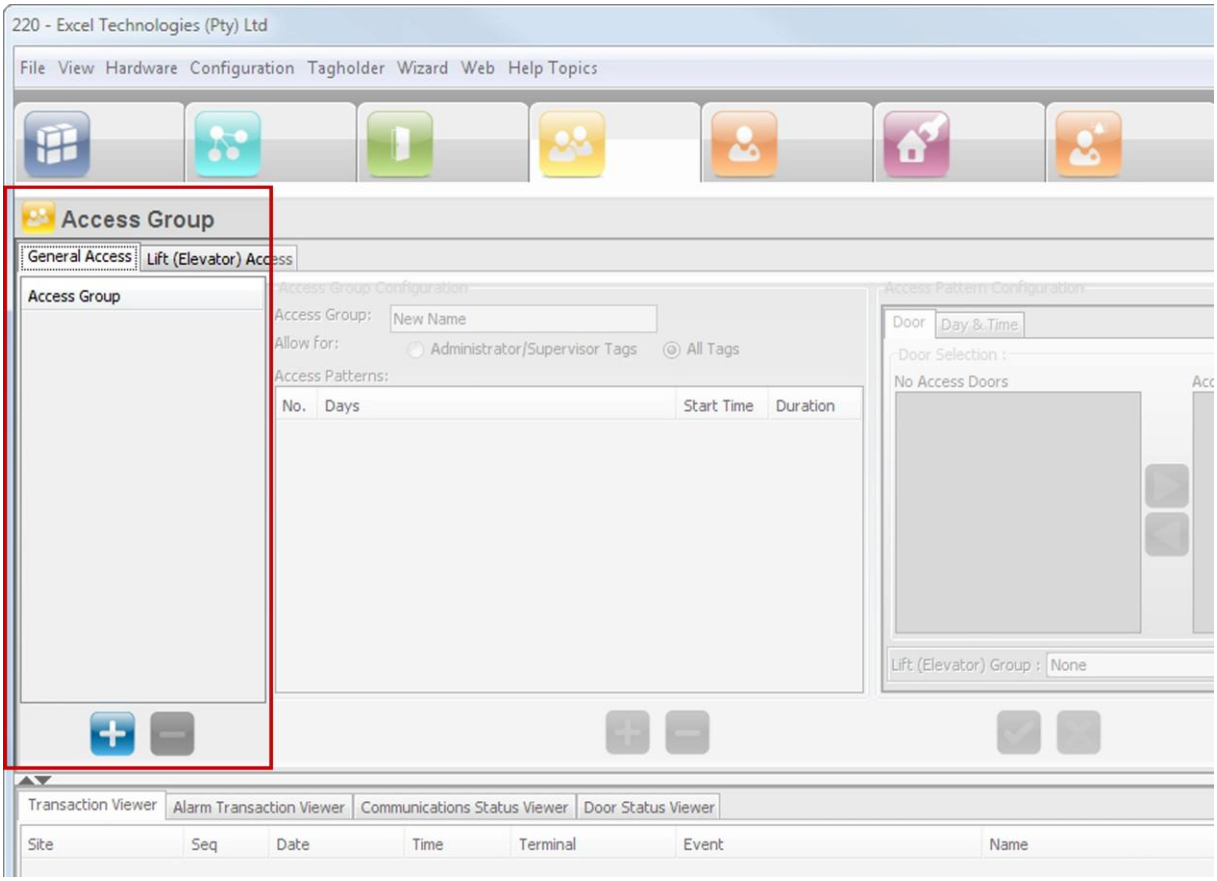


Figure 9 – Left-hand Side of the Access Group Pane (General Access Tab Selected)

To create a Tagholder Access Group, proceed as follows:

1. Select the Page Tab.
2. Select the **General Access** Tab.
3. As highlighted in Figure 9, click the button.
4. In the **Access Group** textbox, assign your Access Group a suitable name.

5. From the **Allow For** radio buttons, select either of the following choices:
   - **Administrator/Supervisor Tags**
   - **All Tags**—Visitor and Employee Tagholders.
6. Click the button.

Only the SYSDBA user can give a Tagholder access to a Tagholder Access Group categorized as Administrator or Supervisor.

Create an Access Time Pattern

*You may add a **maximum of 8** Access Time Patterns to each Access Group.*

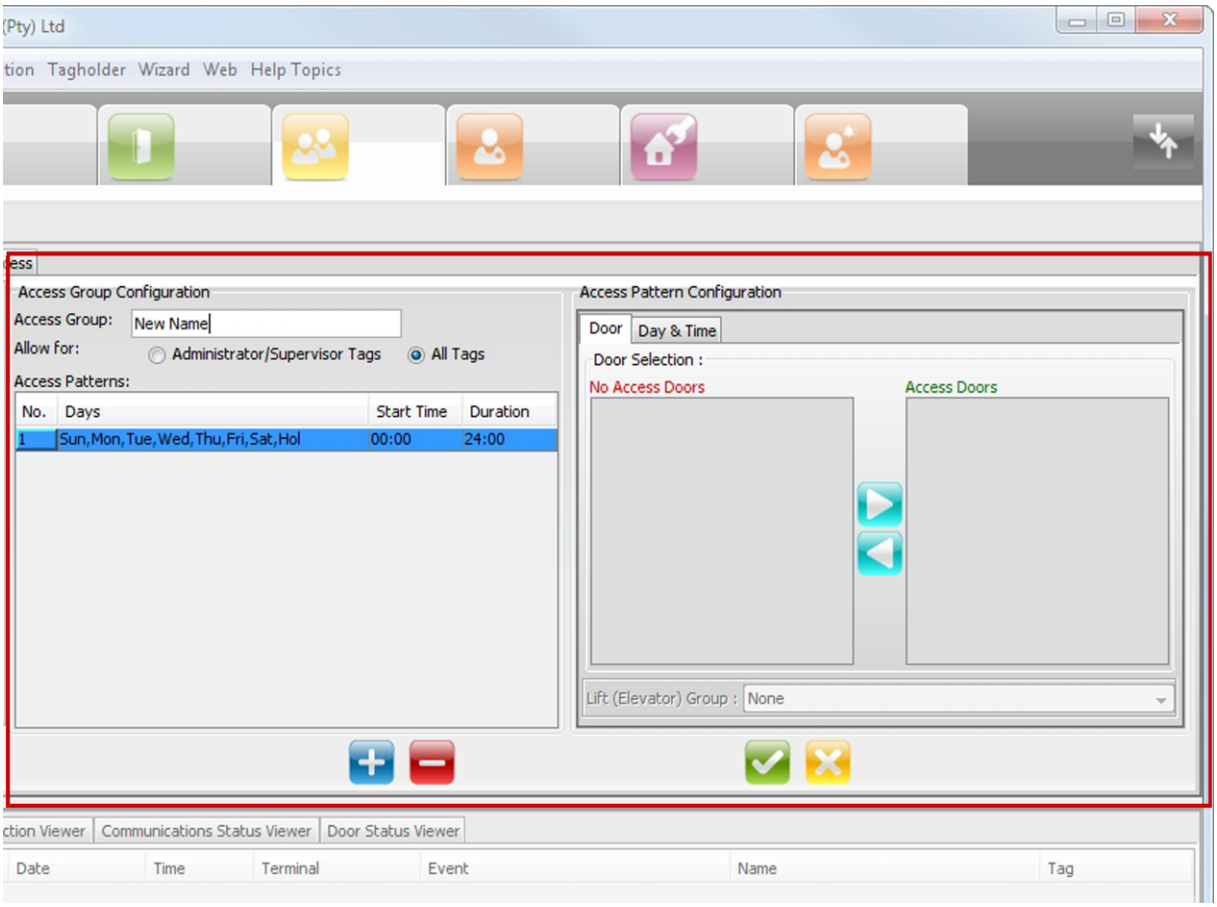


Figure 10 – Right-hand Side of the Access Group Pane (General Access Tab Selected)

To create an Access Time Pattern, proceed as follows:

1. As highlighted in Figure 10, click the button.
2. In the **Access Pattern Configuration** group, select the **Door** Tab.
3. In the **No Access Doors** text area, select the **Door** you want the Access Pattern applied to.

*From the No Access Doors text area, select multiple Doors (Locations), by holding down the **Ctrl** key and selecting multiple records.*

4. Click the button.

5. In the **Access Pattern Configuration** group, select the **Day & Time** Tab.
6. From the **Select Day Pattern** group, deselect checkboxes where NOT applying the Pattern.
7. In the **Start Time** textbox, enter a suitable start time.
8. In the **End Time** textbox, enter a suitable end time.

The Duration automatically calculates based on the information you capture into the Start and End Time textboxes.

9. Click the button.

Select an Access Group

To select an existing Tagholder Access Group, proceed as follows:

1. Select the Page Tab.
2. Select the **General Access** Tab.
3. From the list of Access Group records (see the highlighted area in Figure 9 for more information) select a record.

The selected Access Group's details display on the right-hand side of the Access Groups Configuration Pane. See Figure 10 for more information.

Delete Access Group and Access Time Pattern Details

To delete a Tagholder Access Group, proceed as follows:

1. Select the Page Tab.
2. Select the **General Access** Tab.
3. From the list of Access Group records (see the highlighted area in Figure 9 for more information) select a record.
4. Click the button.
5. Click **Yes**.

Edit Access Group and Access Time Pattern Details

To edit a Tagholder Access Group, proceed as follows:

1. Select the Page Tab.
2. Select the **General Access** Tab.
3. From the list of Access Group records (see the highlighted area in Figure 9 for more information) select a record.
4. Edit the Access Time Pattern details as required.
5. Click the button.
6. When using distributed templates along with biometrics, after editing the Lift (Elevator) Group, ensure you perform a full upload. Refer to page 70 for more information on performing a full upload.

5 Tagholder Configuration

A Tagholder is any person who uses a Tag in accessing a Site. Visitors are Tagholders with restricted access rights. Before assigning access to a Tag, first assign the Tag to a Tagholder.

Add a Tagholder

To add a Tagholder, proceed as follows:

1. Select the Page Tab.
2. Click the button.

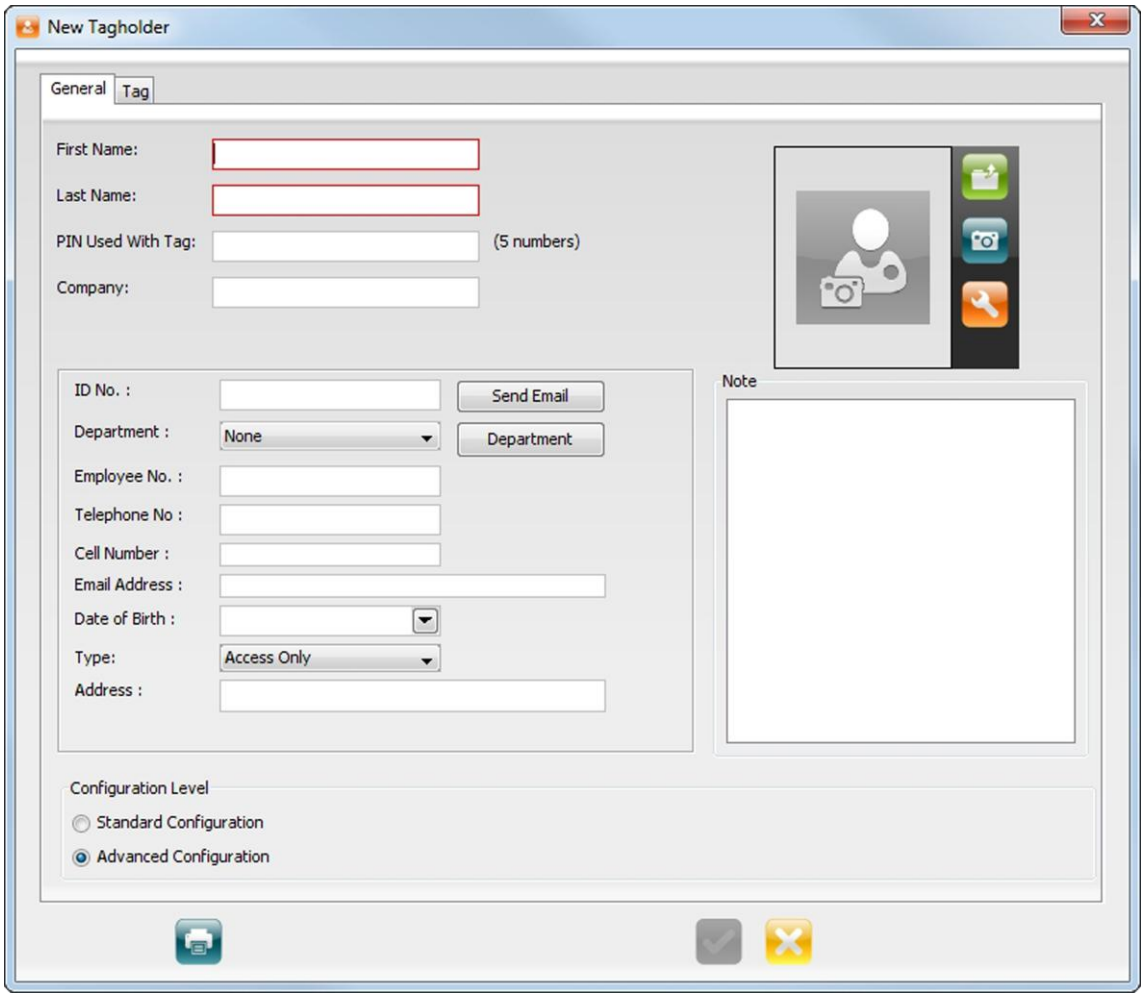


Figure 11 – Tagholder Dialog (Showing the General Tab)

*To add a Tagholder through the **Transaction Viewer**:*

1. *Present an un-enrolled tag to a Reader.*
2. *In the **Transaction Viewer**, right click on the unidentified Tag.*

3. *Select **Enroll Tag**.*
4. *Continue with either of the following processes:*

   Tagholders without Tags

   a. *At the **Tagholders without Tags** dialog, select a Tagholder.*
   b. *Click the button.*
   c. *Within the **Tagholder** dialog, on the **General** tab, complete the fields as required.*
   d. *Continue with step 5.*

   New Tagholders

   a. *At the **Tagholder** dialog, enter the Tagholder's **First Name**.*
   b. *Enter the Tagholder's **Last Name**.*
   c. *Complete the remaining fields as required.*
   d. *Continue with step 5.*

5. *Select the **Tag** tab.*
6. *Within the **Access Rights** group, from the **Access Group** drop-down list, make your selection.*
7. *Complete the remaining fields as required.*
8. *Click the button.*

The **Tagholder** dialog consists of two tabs namely General and Tag. The **General** Tab allows addition of a Tagholder's information, while the **Tag** Tab allows Tag assignment. On the General Tab, only the **First Name** and **Last Name** fields are required. However, we recommend entering as much information as possible.

3. In the Tagholder dialog, select the **General** Tab.
4. Enter the Tagholder's **First Name**.
5. Enter the Tagholder's **Last Name**.
6. From the **Configuration Level** group, select from the following radio buttons:
   - **Standard Configuration**—displays standard Tagholder details.
   - **Advanced Configuration**—displays extra advanced Tagholder details.

The instructions below continue as for an Advanced Configuration. For a Standard Configuration ignore references made to fields that appear greyed out.

7. In the **PIN Used with Tag** textbox, enter a PIN-code of up to 5 digits. (PIN-codes range from **2 to 65534**. After entering the PIN-code at the Reader or Terminal, complete the entry by pressing the # key).
8. Enter the Tagholders **Company** name details.
9. From the **Department** drop-down list, select a department name.

*Add extra **Departments** as follows:*

1. *Click the **Department** button.*
2. *Click the button.*
3. *In the **Department** textbox, enter a suitable name for the Department.*
4. *Click the button.*
5. *Click the button.*

Click the button to edit a Department or the button to delete a Department.

*The **Send E-Mail** button lets you send Tagholder details to interested parties. The **To** textbox is mandatory, thus requiring data entry for successful e-mail transmission. For e-mail setup information please refer to the section Preference Configuration (System Notification Tab) on page 63.*

10. From the **Type** drop-down list make your selection. The value selected, once captured in the master table, lets the third-party Time and Attendance Software determine who to calculate and who not to calculate. For Sites using third-party Time and Attendance Software we therefore recommend selecting the **Access and Time** option, for all other installations select the **Access Only** option.
11. Complete other personal information as necessary.

*Add a Tagholder **Image** as follows:*

1. *Click the button.*
2. *At the Open dialog, select the image file. Image formats supported include: jpg, jpeg, gif, tif and tiff. The recommended resolution is 640 x 480 pixels.*
3. *Click the **Open** button.*

For more information on the Live Video Image Capture feature ( ) please see Part 5 – Advanced Configuration.

Clicking the button opens the Edit dialog, allowing image cropping, rotation, resizing and use of an image mirror effect.

*To change the **Tagholder Image** back to the default image:*

1. *Right click on the Tagholder Image.*
2. *Select **Default Image**.*

12. Use the **Note** text area when entering further information about the Tagholder.
13. Click the button.

*To view a **Transaction Image**:*

1. *From the Main Menu, Select **View**.*
2. *Select **Enable Transaction Image**.*

*Once **Enable Transaction Image** is selected, a dialog window will open. This dialog window will display the image for the last Tagholder to have a transaction.*

Add a Tagholder by E-mail

Requesting the Available Subject Line List

You do not need to perform step 1 every time you want to add a Tagholder by e-mail.

1. Using your preferred e-mail client, create an e-mail message.

2. In the **To** textbox, enter the E-mail Address you configured in **E-mail Account Configuration** (see page 63 for more information).
3. In the **Subject** textbox, enter the phrase **HELP**.
4. In the body of the E-mail Message, enter the **Password** you configured in **Incoming Configuration** (see page 64 for more information).
5. Click the **Send** button.

Requesting the Enrollment Form

1. Using your preferred e-mail client, create an e-mail message.
2. In the **To** textbox, enter the E-mail Address you configured in **E-mail Account Configuration** (see page 63 for more information).
3. In the **Subject** textbox, enter the phrase **ENROLLMENT**.
4. In the body of the E-mail message, enter the password you configured in **Incoming Configuration** (see page 64 for more information).
5. Click the **Send** button.

Completing the Enrollment Request Form

*The **Enrollment Request Form** expires after 1 hour, or if the base Application closes. Each template can only be used once.*

1. In your e-mail client, select the e-mail with **ENROLLMENT TEMPLATE REQUEST** in the subject.
2. Open the message attachment.

*If the **ENROLLMENT TEMPLATE REQUEST** form does not display correctly, save the attachment to your PC and then open it.*

3. From the **Tagholder Details** group, fill in the following required textboxes:
   - **First Name**—fill in the Tagholder's first name.
   - **Last Name**—fill in the Tagholder's last name.
   - Complete other personal information as necessary.
4. From the **Tag** group, select from the following drop-down lists:
   - **Tag**—Select either **Issue on Arrival** or **Generate Personal Access Code**.
   - **Tag Level**—option activates when you select the Generate Personal Access Code option on the Tag drop-down list. Your Tag Level options include **Visitor** or **Normal**.
   - **Site**—select the site the Tagholder belongs to.
5. Click the **Generate Request** button.
6. Click the **OK** button at the Windows Internet Explorer dialog.
7. Click the **Allow** button at the Microsoft Office dialog.

Assign Tags to Tagholders

A Tagholder can have up to 4 Tags assigned to them. To assign Tags to a Tagholder, proceed as follows:

1. In the Tagholder dialog, select the **Tag** Tab.
2. Click any of the **Create New Tag** buttons.

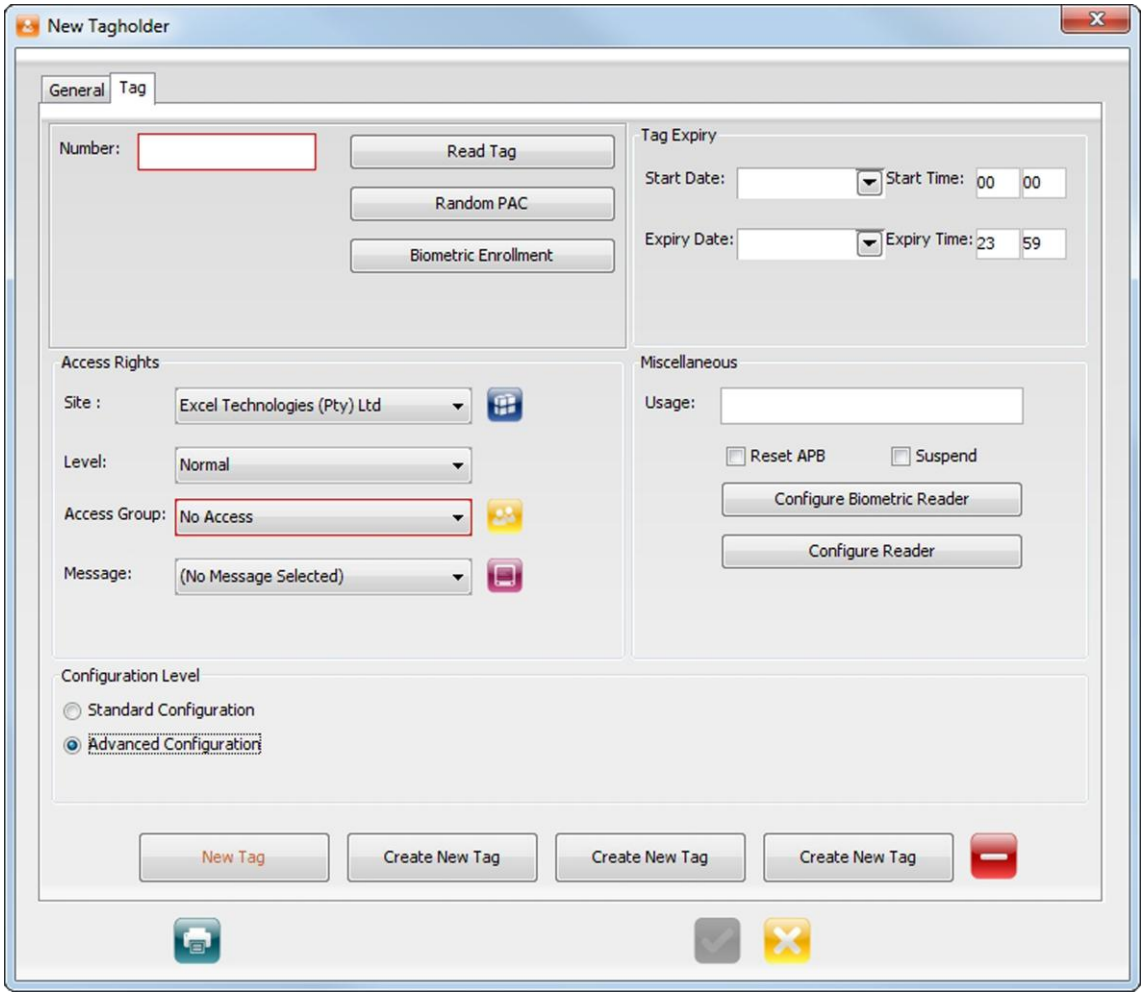


Figure 12 – Tagholder Dialog (Showing the Tag Tab)

3. From the **Configuration Level** group, select from the following radio buttons:
   - **Standard Configuration**—disables advanced configuration options.
   - **Advanced Configuration**—enables advanced configuration options.

The instructions below continue as for an Advanced Configuration. For a Standard Configuration ignore references made to fields that appear greyed out.

Selecting a Registration Reader

1. From the **Miscellaneous** group, select the **Configure Reader** button.
2. In the **Configure Tag Reader** dialog, from the Use Registration Reader radio buttons, select one of the following:
   - **Yes**—when selected, the **Registration Reader Port** drop-down list activates. Select the **Port Number** to which you connected your Registration Reader.
   - **No**—selected by default, activates the **Select Reader** drop-down list. Select the **Reader** you intend using as the Registration Reader from the list of available Readers.
3. Click the button.

Tag Enrollment

1. Present a Tag to an Enrollment Reader.
2. On the Tag tab, click the **Read Tag** button.

*When the IXP220 Software detects the Tag, the Tag number displays in the **Number** textbox.*

*When the Software is set to ignore the Tag type, the Tag type updates automatically. When the Tag type is taken into consideration, select the Tag type from the **Type** drop-down list. Your Tag Type options include:*

- ***Standard (125 kHz)**—previously described as Slim Tag 5 Bytes.*
- ***Read/Write (125 kHz, 2048 bits)**—previously described as WriTag 2048.*
- ***Read/Write (125 kHz, 128 bits)**—previously described as WriTag 128.*
- ***3rd Party (Other)**—previously described as ASCII/Barcode/Magstripe.*
- ***Personal Access Code**—create a Personal Access Code (PAC) by selecting the **Personal Access Code** choice from the **Type** drop-down list and entering the Personal Access Code (PAC) in the **Tag Code** textbox. Your Personal Access Code may range from between **1 to 999999999**. After entering the Personal Access Code at the Reader or Terminal, complete the entry by pressing the # key).*
- ***RF/Infrared**—previously described as RF/Infrared Tag.*
- ***Mifare**—previously described as Mifare Tag.*
- ***HID (125 kHz)**—previously described as HID Tag.*
- ***13.56 MHz (General)**—previously described as General 13.56 MHz.*
- ***FeliCa**—previously described as FeliCa Tag.*

Access Rights Configuration

1. From the **Site** drop-down list, select the Site name.

Alternatively, click the button to select the Access Group for the Tagholder across all Sites.

2. From the **Level** drop-down list make your selection from the following choices:
   - **Visitor**—restricted access, valid for day of issue only.
   - **Normal**—employee Tagholder. Access restricted by Door Mode.
   - **Supervisor**—opens Doors (Locations) in Supervisor Mode, overrides Anti-passback (APB) and may cancel alarms.
   - **Administrator**—opens Doors (Locations) in Supervisor Mode and ignores No Entry Mode.
3. From the **Access Group** drop-down list, make a selection.

Alternatively, click the button to create a new Access Group.

You must assign a Tagholder Access Group for the Tag to have any access rights.

Tag Expiry Configuration

For temporary Tagholders, proceed as follows:

1. From the **Start Date** drop-down list, select a suitable start date.
2. In the **Start Time** textboxes, enter a suitable start time.
3. From the **Expiry Date** drop-down list, select a suitable expiry date.
4. In the **Expiry Time** textboxes, enter a suitable expiry time.

Message Configuration

*For information on adding Messages, refer to the **Messages** section on page 53.*

From the Message drop-down list, select a Message for display.

Alternatively, click the button to create a new Message.

Miscellaneous Configuration

- **Reset APB**—resets the Anti-passback (APB) status for an individual Tagholder.
- **Suspend**—suspends the Tag in the event the Tag is lost or no longer required.
- **Copy Tag**—copies the Tag code for use in sites with Tags and biometric facilities, thus upholding Anti-passback (APB) rules.
- **Usage**—stores a description of the Tag's usage.
- **Configure Reader**—select the Reader for use as the Registration Reader for the site.
- **Configure Biometric Reader**—opens the Tagholder biometric configuration and enrollment settings. See Part 8 – Integration Modules for more information.

General Details

1. Click the button.
2. Click the button.

If necessary, repeat the **Assign Tags to Tagholders** procedure for any extra Tags.

Delete an Assigned Tag

To delete an assigned Tag, proceed as follows:

1. Select the Page Tab.
2. From the list of Tagholder records displayed, double-click the Tagholder record for editing.
3. In the **Tagholder** dialog, select the **Tag** Tab.
4. Click the assigned Tag button (that is **Tag 1**, **Tag 2**, **Tag 3** *or* **Tag 4**) for deletion.
5. Click the button.
6. Click the button.
7. Click the button.

Delete a Tagholder

Before deleting a Tagholder, first delete all Tags assigned to the Tagholder.

To delete a Tagholder from the IXP220 System, proceed as follows:

1. Select the Page Tab.
2. From the list of Tagholder records displayed, select the Tagholder record for deletion.
3. Click the button.
4. At the Warning dialog, click the **OK** button.

Set the Default Card Template

When configuring a Tagholder, this facility allows you to select, from a library of Card Templates, the template to be used as the default when printing Credit Card Tags for that Tagholder.

*For information on setting the **Default Card Template**, see the Card Designer chapter of Part 6 – IXP220 Software Modules.*

Batch Enrollment of Tags

The Batch Enrollment feature lets you rapidly assign multiple Tags to a Site, without entering Tagholder details.

Start Batch Enrollment

1. From the Main Menu, select **Tagholder**>**Batch Tagholders**.

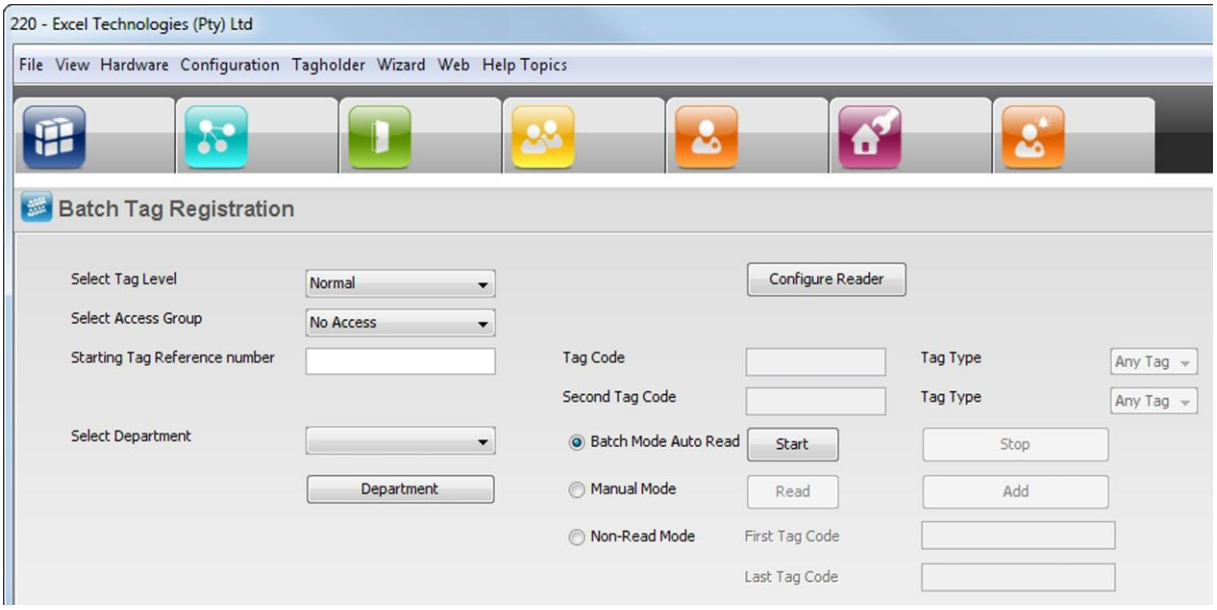


Figure 13 – Batch Tag Registration Configuration Pane

2. From the **Select Tag Level** drop-down list, select from the following choices:
   - **Visitor**—restricted access, valid for day of issue only.
   - **Normal**—employee Tagholder. Access restricted by Door Mode.
   - **Supervisor**—opens Doors in Supervisor Mode, overrides Anti-passback (APB) and may cancel alarms.
   - **Administrator**—opens Doors in Supervisor Mode and ignores No Entry Mode.
3. From the **Select Access Group** drop-down list, select an Access Group.
4. Enter a **Starting Tag Reference Number**. The Starting Tag Reference Number is any number that you can use temporarily in identifying the Tags.
5. From the **Select Department** drop-down list, select a Department.

*Add extra **Departments** as follows:*

1. *Click the **Department** button.*
2. *Click the button.*
3. *In the **Department** textbox, enter a suitable name for the Department.*
4. *Click the button.*
5. *Click the button.*

Click the button to edit a Department or the button to delete a Department.

6. Select one of the following to start the Batch Enrollment process:
   - **Batch Mode Auto Read**
   - **Manual Read**

Batch Mode Auto Read

This Mode lets you scan a batch of Tags in quick succession:

1. Select the **Batch Mode Auto Read** radio button.
2. Click the **Start** button.
3. Present Tags to the Enrollment Reader one at a time.
4. Click the **Stop** button.
5. On enabling, click the button.

Manual Read Mode

Manual Mode lets you scan a batch of Tags one at a time. It is useful if the Enrollment Reader is away from the Host PC.

1. Select the **Manual Mode** radio button.
2. Present a Tag to the Enrollment Reader.
3. Click the **Read** button. On reading the Tag, its numbers display in the **Tag Code** and **Second Tag Code** (if applicable) textboxes along with their **Tag Types**.
4. Click the **Add** button.
5. Repeat steps 1 to 4 for further Tags.
6. After you've scanned all the Tags, click the button.

Non-read Mode

This Mode lets you load a range of Tags without physically scanning the Tags. You may load up to **1 000** Tags at a time.

1. Select the **Non-read Mode** radio button.
2. In the **First Tag Code** textbox, enter the first tag code in the range.
3. In the **Last Tag Code** textbox, enter the last tag code in the range.
4. On enabling, click the button.

Advanced Search

To search for a Tagholder, continue as follows:

1. Select the Page Tab.
2. Enter a suitable keyword in the **Search By** textbox.

As you type, the Software automatically matches the keyword, highlighting the Tagholder record with the closest match.

6 Holidays

This feature lets you assign different access rights on holidays than on normal working days. If the **Holiday** checkbox in an Access Pattern is selected, then Tagholders assigned to that Access Pattern have access to a Site on or during Holidays. The IXP220 Software supports a maximum of 40 holidays per Site.

Add, Edit, or Delete a Holiday

To add, edit, or delete a Holiday, continue as follows:

1. From the Main Menu, select **Configuration**>**Holidays**.
2. In the Configuration Pane, do one of the following:
   – Click the button to **Add** a Holiday.
   – Click the button to **Delete** a Holiday.
   – Double-click the appropriate record to **Edit** a Holiday's details.
3. In the Holiday Configuration Pane, click the button.

Configure Holidays

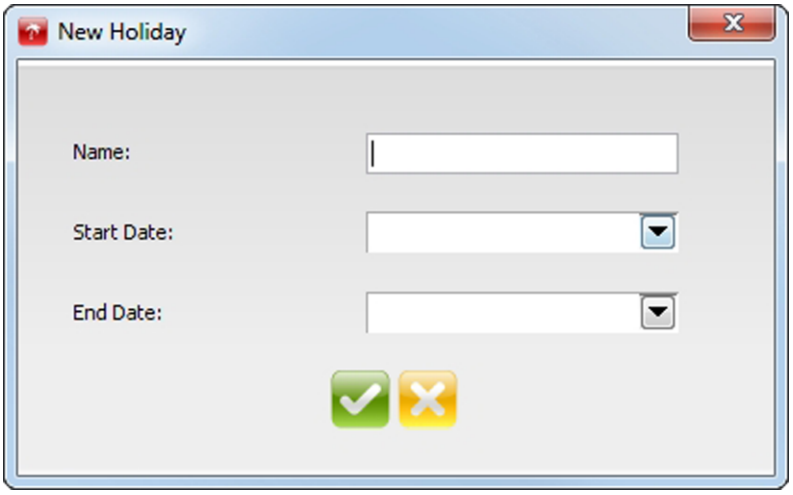


Figure 14 – New Holiday Dialog

The **New Holiday** dialog lets you specify selected dates as Holidays. To do this, continue as follows:

1. In the **Name** textbox, enter a Holiday name.
2. From the **Start Date** drop-down list, select a start date.
3. From the **End Date** drop-down list, select an end date.
4. Click the button.

Messages

Messages are brief strings of text that display on the ImproX (MDTA) Multi-discipline Time Attendance Terminal and the ImproX (TA) Time Attendance Terminal or Remote. The ImproX MDTA supports messages of up to 100 characters. The ImproX TA supports messages of up to 16 characters. The IXP220 System supports **up to 100 Messages**.

The IXP220 Message feature currently only supports ASCII character sets.

Add, Edit, or Delete a Message

To add, edit, or delete a Message, continue as follows:

1. From the Main Menu, select **Configuration**>**Messages**.
2. In the Configuration Pane, do one of the following:
   – Click the button to **Add** a Message.
   – Click the button to **Delete** a Message.
   – Double-click the appropriate record to **Edit** a Messages details.
3. In the Messages Configuration Pane, click the button.

Configure Messages

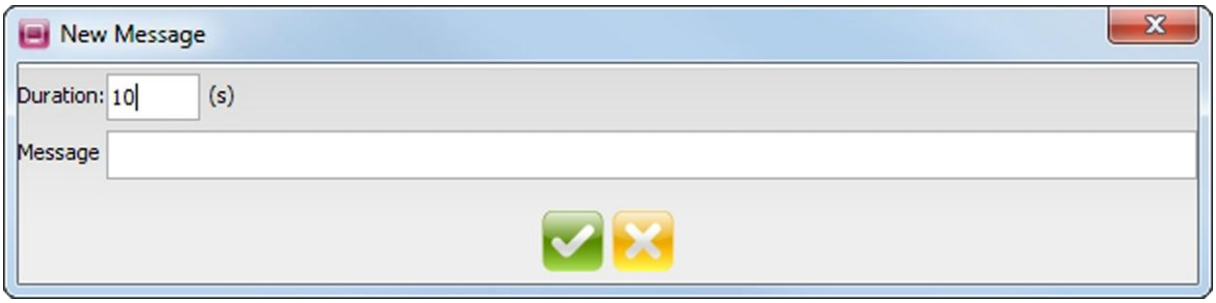


Figure 15 – New Message Dialog

The **New Message** dialog lets you specify Message details. To do this, continue as follows:

1. In the **Duration** textbox, enter the display duration, in seconds, for the Message. The default duration is **10**. The maximum duration is **3 000**.
2. In the **Message** textbox, enter the Message text.
3. Click the button.

Message Display

1. Select the Page Tab.
2. From the Doors table, select the Door record (with the Display Device).

3. Depending on whether the Display Device is installed on the Entry or Exit point, select either the **Entry** or **Exit** Tab.
4. From the **Configuration Level** group, select the **Advanced Configuration** radio button.
5. From the **Miscellaneous** group, from the **Message Display Supervisor** drop-down list, select the record that best represents your setup requirements.
6. Click the button.

Displaying Personalized Messages per Tagholder

1. Select the Page Tab.
2. From the list of Tagholder records displayed, double-click the Tagholder record for editing.
3. In the Tagholder dialog, select the **Tag** Tab.
4. Click the assigned Tag button (that is **Tag 1**, **Tag 2**, **Tag 3** or **Tag 4)** for which you want the message displayed.
5. From the **Configuration Level** group, select the **Advanced Configuration** radio button.
6. From the **Message** drop-down list, select a Message for display.
7. Click the button.

Reason Codes

A code normally used by Tagholders on exit that describes the reason for requesting access at a given Terminal. Reason codes are specific and should be used for access control out of ordinary limits. In other words, allowing access in restricted areas and during uncommon times. The IXP220 System allows **up to 99 Reason Codes**.

Add, Edit, or Delete a Reason Code

To add, edit, or delete a Reason Code, continue as follows:

1. From the Main Menu, select **Configuration**>**Reason Codes**.
2. In the Configuration Pane, do one of the following:
   – Click the button to **Add** a Reason Code.
   – Click the button to **Delete** a Reason Code.
   – Double-click the appropriate record to **Edit** a Reason Code's details.
3. In the Reason Codes Configuration Pane, click the button.

Configure Reason Codes

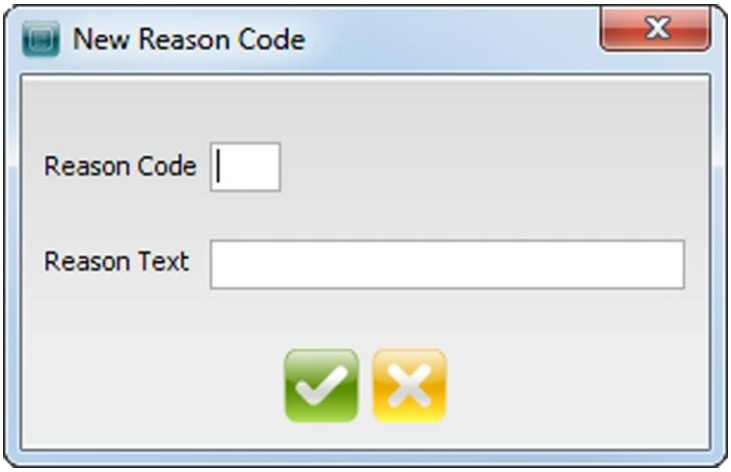


Figure 16 – New Reason Code Dialog

The **New Reason Code** dialog lets you specify Reason Code details. To do this, continue as follows:

1. In the **Reason Code** textbox, enter the Reason Code's number.

*Reason Codes range from **1 to 99**. When using the Reason Code at a Terminal or Reader, complete the entry by pressing the # symbol.*

2. In the **Reason Text** textbox, enter the Reason Code's text. This message must not exceed **15** alpha numeric characters.
3. Click the button.

Modes of Operation

Refer to the IXP220 Controller's Hardware Installation Manual for connection details relating to these Modes.

The IXP220 System provides the following Software selectable "Modes of Operation":

Power Control (Emergency) Mode

This Mode, on Sites configured for Inter-controller Communications, Power Control (Emergency) Mode allows you to unlock all Doors (Locations). Essentially, the Alarm Signal input on the Controller unlocks all Doors (Locations) on the Site. That is, where you have 2 Controllers with Inter-controller Communications, and both Controllers set to Power Control (Emergency) Mode, the unlock instruction passes from Controller 1 to Controller 2. All Doors (Locations) connected to these Controllers unlock.

Alternatively, on Sites without Inter-controller Communications, Power Control (Emergency) Mode only affects the single Controller's Doors (Locations).

Activating Power Control (Emergency) Mode

1. Select the Page Tab.
2. Select the **Advanced Configuration** radio button.
3. From the **Mode Configuration (Optional)** drop-down list, select the **Power Control/Emergency Mode** option (default).
4. Click the button.

Power Control (Lockdown) Mode

This Mode, on Sites configured for Inter-controller Communications, Power Control (Lockdown) Mode allows you to lockdown all Doors (Locations) denying Tagholders entry. Essentially, the Alarm Signal input on the Controller locks down all Doors (Locations) on the Site. That is, where you have 2 Controllers with Inter-controller Communications, and both Controllers set to Power Control (Lockdown) Mode, the lockdown instruction passes from Controller 1 to Controller 2. All Doors (Locations) connected to these Controllers enter lockdown.

Alternatively, on Sites without Inter-controller Communications, Power Control (Lockdown) Mode only affects the single Controller's Doors (Locations).

Activating Power Control (Lockdown) Mode

1. Select the Page Tab.
2. Select the **Advanced Configuration** radio button.

3. From the **Mode Configuration (Optional)** drop-down list, select the **Power Control/Lockdown** option.
4. Click the button.

Alarm Arming Mode

In this Mode, the Controller interfaces with an Alarm Panel to either, arm or disarm, or trigger the Alarm Panel.

The IXP220 Software does not currently support alarm arming on an ImproX MfT and Wiegand Keypad Reader combination.

Activating Alarm Arm Mode

1. Select the Page Tab.
2. Select the **Advanced Configuration** radio button.
3. From the **Mode Configuration (Optional)** drop-down list, select the **Alarm Arming** option.
4. Click the button.
5. Select the Page Tab.
6. From the Doors column, select a **Door**, designating a Reader as an “Alarm Arming Reader”.
7. If not already selected, select the **Advanced Configuration** radio button.
8. From the **Alarm Arm** group, select **Enable**.
9. Click the button.

Arming the Alarm

1. Present an **Administrator** or **Supervisor Tag** to the “Alarm Arming Reader”.
2. Within 10 seconds of presenting the Tag, on the Keypad Reader, press the # key.

The Reader beeps for 30 seconds, before activating the Alarm Relay, giving you sufficient time to vacate the Alarm Zone. The “Armed” Input detects that the Alarm Panel is armed in turn setting the “Alarm Arming Readers” Status LED to blink, indicating that the Alarm is armed. When the System is armed, the “Alarm Arming Reader” denies Normal or Visitor Tags access.

A “door forced” alarm triggers the alarm panel.

Disarming the Alarm

Present an **Administrator** or **Supervisor Tag** to the “Alarm Arming Reader”.

The Alarm Relay deactivates, signalling the Alarm Panel to disarm.

Intrusion Mode

In this Mode, there is no installed Alarm Panel and merely a simple alarm sensor is required.

Activating Intrusion Mode

1. Select the Page Tab.
2. Select the **Advanced Configuration** radio button.
3. From the **Mode Configuration (Optional)** drop-down list, select the **Intrusion** option.
4. Click the button.

Bell Button Mode

In this Mode, the Bell Button on the ImproX (KMA) Mullion Keypad Antenna Reader, when pushed, drives Relay 3 on the IXP220 Controller.

Activating Bell Button Mode

1. Select the Page Tab.
2. Select the **Advanced Configuration** radio button.
3. From the **Mode Configuration (Optional)** drop-down list, select the **Bell Button** option.
4. Click the button.
5. Select the Page Tab.
6. From the Doors column, select the **Door** using the ImproX (KMA) Mullion Keypad Antenna Reader.
7. If not already selected, select the **Advanced Configuration** radio button.
8. Select the **Enable Bell** checkbox.
9. Click the button.

Action Mode

Use this Mode when you setup actions making use of your Controller's Inputs and Relays. Use, for example could include switching on or off various building devices, such as lights or air conditioners.

See Part 5 – Advanced Configuration for more information on implementing Building Management.

Activating Action Mode

1. Select the Page Tab.
2. Select the **Advanced Configuration** radio button.
3. From the **Mode Configuration (Optional)** drop-down list, select the **Action** option.
4. Click the button.

Preference Configuration

The Preferences Dialog features various page tabs that let you set the following:

- **General Tab**—lets you select the IXP220 Software's default Configuration Level, Transaction Priority and System Seed (used to encrypt communications. The value is generated randomly on first startup of a new IXP220 V1.80 or later System).
- **Enrollment Tab**—select from either **Tag Type is Ignored when Validating a Tag** or **Tag Type is Taken into Consideration when Validating a Tag**. By selecting **Tag Type is Ignored when Validating a Tag**, you activate the AnyTag Mode. In this Mode, the IXP220 Software stores the Tag Code and not the Tag Type. Pre IXP220 V1.80 you enrolled each ImproX (QT) Quad Transmitter Tag twice (once for RF and once for the Passive Tag), using AnyTag Mode, you only enroll the Tag once.
- **Web Tab**—select either **Anyone can View Web Reports** or **Username and Password is Required to View Web Reports**. Also allows you to select the Port used by the Web Server. The default is Port **80**.
- **System Notifications Tab**—lets you configure your E-mail and Twitter account settings, set up Incoming Requests and customise the Tagholder V-Card.
- **Maintenance Tab**—lets you perform System maintenance including the deletion of expired Tagholders, Notifications or Tagholders without Tags.

Setting Your Preferences

From the Main Menu, select **File**>**Preference**.

General Tab

1. Select the **General** Tab.

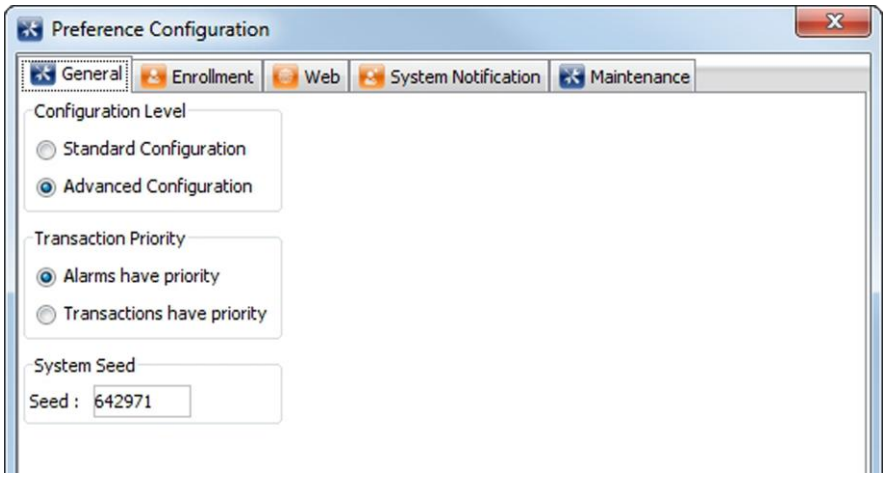


Figure 17 – Preference Configuration Dialog – General Tab Selected

2. From the **Configuration Level** group, select either the **Standard Configuration** or **Advanced Configuration** radio button. By selecting the Advanced Configuration radio button, you elect that the IXP220 Software automatically display all advanced settings.
3. From the **Transaction Priority** group, select either the **Alarms have Priority** or **Transactions have Priority** radio button. By selecting the Alarms have Priority radio button, you elect that the IXP220 Software give Alarms the highest priority. Likewise, by selecting the Transactions have Priority radio button, you elect that Transactions have the highest priority.

Enrollment Tab

Select the **Enrollment** Tab.

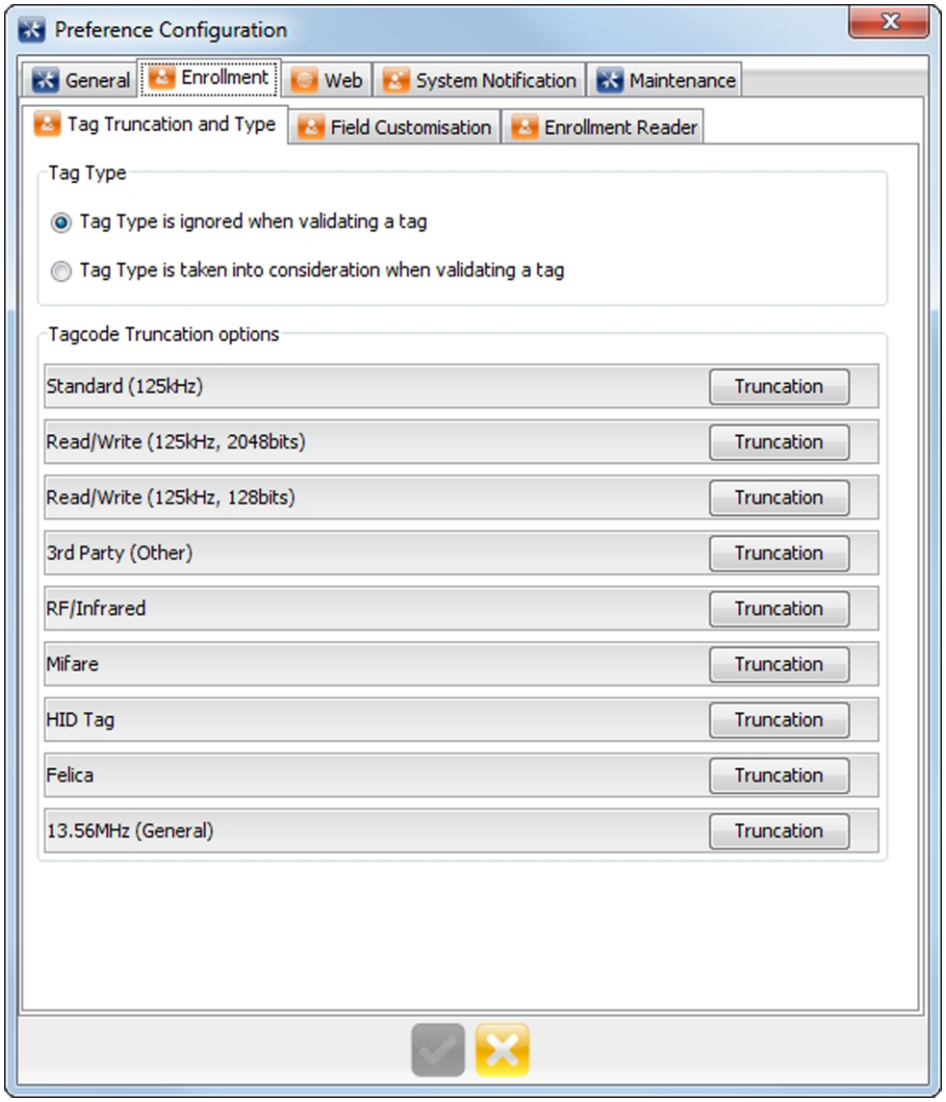


Figure 18 – Preference Configuration Dialog – Enrollment Tab Selected

Tag Truncation and Type Tab

Tag Type Group

Selecting the **Tag Type is Ignored when Validating a Tag** radio button, activates the AnyTag Mode. In this Mode, the IXP220 Software stores the Tag Code and not the Tag Type. Pre

IXP220 V1.80 you enrolled each ImproX (QT) Quad Transmitter Tag twice (once for RF and once for the Passive Tag), using AnyTag Mode, you only enroll the Tag once.

1. By default, **Tag Type is Ignored when Validating a Tag** is selected. To change this setting, select the **Tag Type is Taken into Consideration when Validating a Tag** radio button.
2. From the **Select Tag Type to Convert Existing Tags to** drop-down list, make your selection.

Tag Code Truncation Options Group

Set the **Tag Code Truncation**, in effect, allowing enrollment of the Tag using the same truncation rules as applied by the Reader (using DIP-switch settings) out in the field, as follows:

1. Select a Tag for editing and click the Tag's **Truncation** button.
2. From the **Tag Format** drop-down list, make your selection from the following:
   - **Full Tag Code**.
   - **Standard 16-bit**.
   - **Standard 24-bit**.
   - **Standard 32-bit**.
   - **26-bit Normal**.
   - **26-bit Raw**.
   - **37-bit Normal (UK)**.
   - **37-bit Raw (UK)**.
   - **H10302 37-bit Raw 35-bit Tagcode (US)**.
   - **H10304 37-bit Raw 19-bit Tagcode (US)**.
   - **Custom**—in most cases on selection of the Custom option, the **Tag Code Masking** and **Drop Zero Bits** options activate. However, for **3rd Party (Other)** or **HID Tag**, selecting the Custom option lets you set **Site Code Masking** allowing you to set a custom mask.
3. Click the button.

Field Customisation

1. Select the **Field Customisation** Tab.
2. The information displayed in the **Additional Fields** group refers to the extra fields displayed on the Tagholder dialog. Customise these fields by selecting from the following:
   - **Display Details**—by selecting this checkbox, you add fields for ID Number, PIN Used with Tag, Address, Company, Employee Number, Telephone Number, Cell Number, E-mail Address, Department and Date of Birth to the Tagholder dialog. Where information MUST be provided, select the Mandatory checkbox alongside the field name.
   - **Display Additional Info**—by selecting this checkbox, you add fields for Reports To, Destination and Reason for Visiting to the Tagholder dialog. Where information MUST be provided, select the Mandatory checkbox alongside the field name.
   - **Display Contractor Info**—by selecting this checkbox, you add fields for Occupation, Emergency Contact Person, Emergency Contact Details, Working For, Expected Departure Date and Date Employed to the Tagholder dialog. Where information MUST be provided, select the Mandatory checkbox alongside the field name.

- **Display Vehicle Info**—by selecting this checkbox, you add fields for Number Plate, Make, Number of Occupants, Weight and Additional Details to the Tagholder dialog. Where information MUST be provided, select the Mandatory checkbox alongside the field name.
- **Display Custom Info**—by selecting this checkbox, you can add up to 5 Custom Fields to the Tagholder dialog as well as customise the name of the tab. Where information MUST be provided, select the Mandatory checkbox alongside the field name.

Re-order the Tagholder Details, Additional Tagholder Details, Contractor Details, Vehicle Details and Custom Fields tabs using the and buttons.

Enrollment Reader

Automatic Enrollment is not supported on Systems using an ImproX RS for fall-back communications or where the Controller connects using an ImproX RS.

1. Select the **Enrollment Reader** Tab.
2. From the **Automatic Tag Reader** drop-down list, make your selection:
   - **From Anywhere**—this option opens the Tagholder dialog automatically on presentation of a Tag to the Registration Reader. Enrollment therefore takes place without opening the Page Tab.
   - **From Tagholder Configuration**—enrollment takes place from the Page Tab only.
   - **Disable Automatic Reading**—by selecting this option, enrollment takes place in the Tagholder dialog, from the Tag tab only.
3. From the **Multi-discipline Enrollment Reader** drop-down list, make your selection:
   - **Enroll 125 kHz and 13.56 MHz**—when enrolling dual tags, this option automatically saves both the 125 kHz and 13.56 MHz Tag codes to the Tag 1 and Tag 2 positions. This is the default setting.
   - **Enroll 125 kHz Only**—when enrolling dual tags, this option automatically saves only the 125 kHz Tag code.
   - **Enroll 13.56 MHZ Only**—when enrolling dual tags, this option automatically saves only the 13.56 MHz Tag code.

Web Tab

1. Select the **Web** Tab.
2. From the **Web Report Security** group:
   - Select either the **Anyone can View Web Reports** radio button.
   - Or **User Name and Password is Required to View Web Reports** radio button.

*By selecting the **User Name and Password is Required to View Web Reports** users must enter the **Username** (**SYSDBA**) and **Password** (**masterkey**) before viewing Web Reports.*

3. In the **Webserver Port** textbox, enter a new port number. By default the Web Server uses **Port 80**. In the event that Port 80 is already in use, change the port number.

System Notification Tab

Select the **System Notification** Tab.

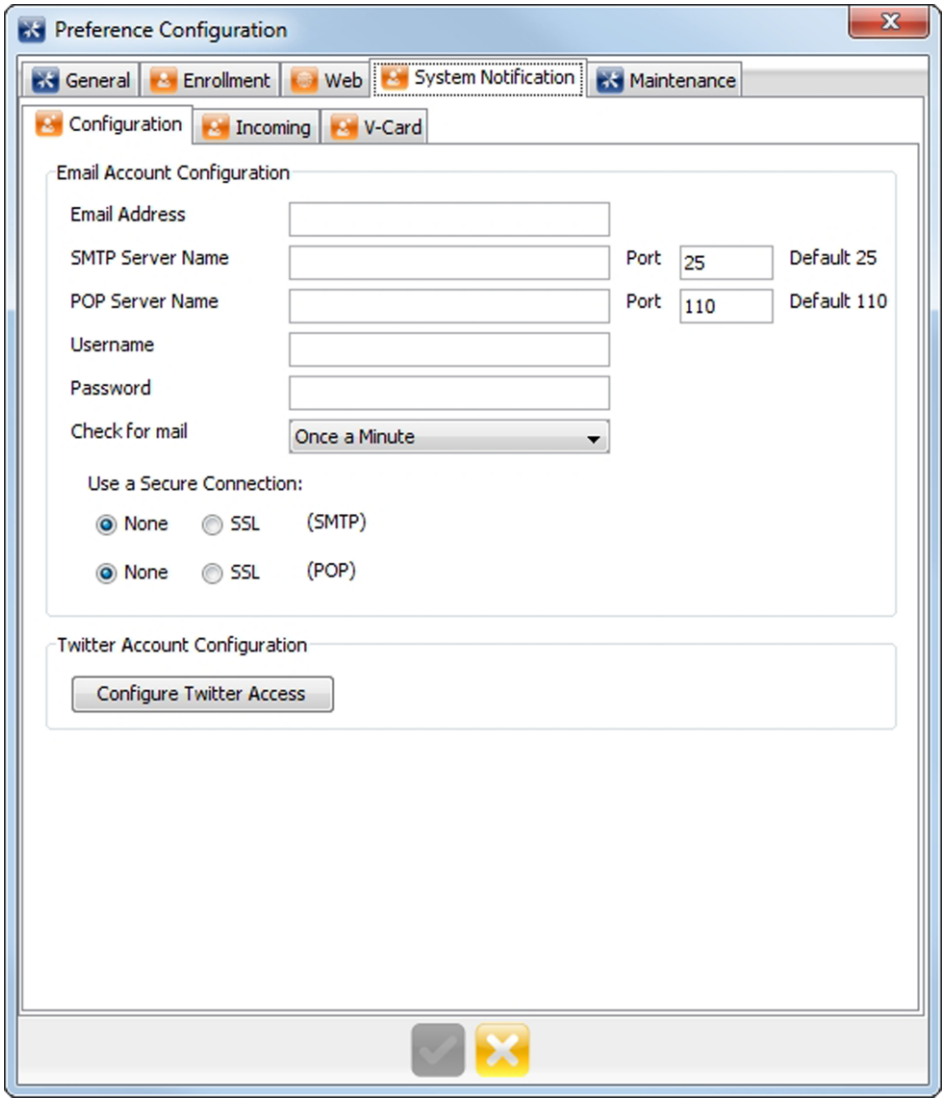


Figure 19 – Preference Configuration Dialog – System Notification Tab Selected

Configuration Tab

E-mail Account Configuration Group

This works on the following e-mail clients:

- *Thunderbird*
- *Outlook*
- *Outlook Express*
- *Gmail*

1. In the **E-mail Address** textbox, enter your e-mail account details.
2. Complete the **SMTP Server Name** field by entering your mail server's name or IP Address details.
3. In the **Port** textbox enter a Port number. The default Port number is **25**.

4. Complete the **POP Server Name** field by entering your mail server's name or IP Address details.
5. In the **Port** textbox enter a Port number. The default Port number is **110**.
6. Enter your E-mail **Username** and **Password** details.
7. From the **Check for Mail** drop-down list make your selection:
   - **Once a Minute**—checks for e-mail once a minute. This is the default setting.
   - **Once Every 5 Minutes**—checks for e-mail every 5 minutes.
   - **Once Every 10 Minutes**—checks for e-mail every 10 minutes.
   - **Once Every 30 Minutes**—checks for e-mail every 30 minutes.
   - **Once an Hour**—checks for e-mail once an hour.
8. Indicate whether to **Use a Secure Connection** for the SMTP and POP servers by selecting either of the following radio buttons:
   - **None**—unsecured message transmission on the Internet.
   - **SSL**—managed security of message transmission on the Internet.

Continue as follows where specifying a pre-configured Gmail™ account:

1. *In the **Account Name** textbox, enter your Gmail™ account name (for example **username@gmail.com**).*
2. *In the **SMTP Server Name** textbox, use **smtp.gmail.com**.*
3. *In the **Port** textbox, use either **465** or **587**.*
4. *In the **POP Server Name** textbox, use **pop.gmail.com**.*
5. *In the **Port** textbox, use **995**.*
6. *In the **Username** and **Password** textboxes enter your pre-configured Gmail™ Username and Password details.*
7. *Indicate whether to **Use a Secure Connection** by selecting either the **None** or **SSL** radio button.*

*Once you have configured this section, a **Notification Viewer** Tab appears in the **Monitoring View** section of the Software. This displays all the incoming and outgoing e-mails.*
*An **E-mail Enrollment** drop-down list also appears on the **Site Configuration** Tab under the **Miscellaneous** group. This allows you to set the access group you want to use for **E-mail Enrollment**. The **E-mail Enrollment** drop-down list only works if Generate Personal Access Code is selected under **Tag**, see **Add a Tagholder by E-mail** on page 44.*

Twitter Account Configuration Group

1. Click the **Configure Twitter Access** button.
2. Enter your Twitter **Username** or **Email**.
3. Enter your Twitter **Password**.
4. Click the **Authorize App** button.
5. Enter the Twitter generated PIN-Code in the **PIN** textbox.
6. Click the **OK** button.

Incoming Tab

1. Select the **Incoming** Tab.
2. From the **Enrollment** drop-down list make your selection:
   - **Disabled**—disables the E-mail Enrollment feature. This is the default setting.
   - **Password Authentication**—requires a password to make use of the E-Mail Enrollment feature.

3. From the **Report Request** drop-down list, make your selection:
   - **Disabled**—disables the Report Request feature. This is the default setting.
   - **Password Authentication**—requires a password to make use of the Report Request feature.
4. In the **Enrollment Password** textbox, enter a suitable alpha-numeric password.
5. In the **Report Password** textbox, enter a suitable alpha-numeric password.
6. Check the **SMS Personal Access Code** checkbox if you want to enable this feature. This feature only works if a GSM unit is connected.

*For more information on enrolling Tagholders by E-mail, see **Add a Tagholder by E-mail** on page 44.*
For more information on requesting Reports by E-mail, see Part 4 – Reports.

V-Card Tab

This tab allows you to customise the Tagholder V-Card sent out when using the E-mail Feature (For Tagholder setup information please refer to the section Tagholder Configuration (General Tab) on page 42). The tab is split into two parts, a Preview Area and a Configuration Table.

1. Select the **V-Card** tab.
2. If required, remove the Tagholder image by deselecting the **Insert Image** checkbox.
3. In the Configuration Table, select or deselect the **Enabled** checkboxes alongside each field as required.
4. For each enabled field, assign a layout position in the **Layout** column using the supplied drop-down lists.

Maintenance Tab

1. Select the **Maintenance** Tab.
2. From the **Delete Expired Tags** drop-down list, make your selection:
   - **Disabled**—enabled by default, this option disables automatic deletion of expired Tagholders.
   - **Enabled**—automatically deletes expired Notifications.

A Tag will only be deleted once it expires in all the time zones the Tag has access to.

3. From the **Delete Expired Notifications** drop-down list, make your selection:
   - **Disabled**— enabled by default, this option disables automatic deletion of expired Tagholders.
   - **Enabled**—automatically deletes expired Notifications.

A Notification will only be deleted once it expires in the time zone of the Site it was created for.

4. Delete Tagholders without Tags by clicking the **Delete Now** button.

After setting your preferences, close the Preference Configuration dialog by clicking the button.

Broadcast Transactions by UDP

This feature allows broadcast of real-time transaction data as a UDP comma separated packet to an IP Address and Port Number named by you, the user. The purpose of this is to allow third parties to pick up transactions and use the transactions as they wish (for example for Time Attendance or Alarms). During broadcast (to either the Host PC or another named PC), the transactions still go into the Database as usual.

Enable this feature as follows:

1. From **C:\IXP220**, open the **IXP220.properties** file.
2. Set the **ixp220.broadcast.udp.ip=<IP Address>:<Port>** setting.

*In place of the **<IP Address>** placeholder fill in the IP Address of the Host PC or other named PC picking up the transactions.*

*In place of the **<Port>** placeholder fill in the Port number of the Host PC or other named PC picking up the transactions. Switch the UDP Broadcast feature off by setting the Port number to **0**.*

3. From the Main Menu, select **File**>**Save**.
4. From the Main Menu, select **File**>**Exit**.

The Base Application collects and sends the broadcasted transactions as a list of comma separated values, in this order:

Site Number,yyyy-mm-dd,hh:mm:ss,Transaction Sequence Number,Transaction Event Number,Terminal Super Logical Address,Terminal Name,Tag Code,Tag Type,Tagholder Name,Employee Number followed by a carriage return and new line.

Where no value exists, integer values appear as 0 and string values appear as a space.

7 Notification Configuration

Ensure that you unlock your Registration Interface before using the Notification Module. This unlock allows a maximum of 1 seat.

Ensure that you have a GPRS Module fitted to your IXP220 Controller before using SMS Notifications. E-mail and Twitter Notifications require an internet connection.

The Notification feature is a combination of Hardware and Software providing a huge leap in the management of Tagholders. Notifications are setup using the largely intuitive Notification Creation Wizard. Thereafter, notifications take place at the time of a specified event, offering a retrospective view. Notifications take place by SMS, E-mail or Tweets via the Twitter micro-blogging network.

Adding, Editing or Deleting Notifications

1. Select the Page Tab.
2. In the Configuration Pane, do one of the following:
   - Click the button to **Add** Notifications.
   - Click the button to **Edit** Notifications.
   - Click the button to **Delete** Notifications.
3. In the Notification Configuration Pane, click the button.

Notification Configuration

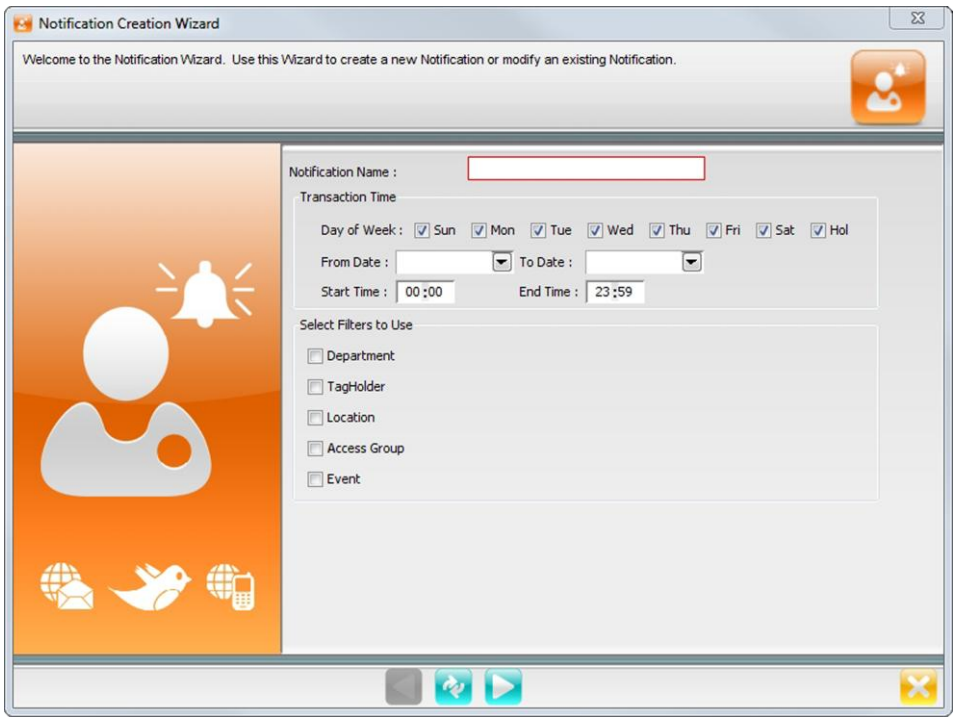


Figure 20 – Notification Creation Wizard

1. In the **Notification Name** textbox, enter a name for your Notification.
2. In the **Transaction Time** group, from the **Day of Week** checkboxes make your selection.
3. From the **From Date** drop-down list, make your selection.
4. From the **To Date** drop-down list, make your selection.
5. In the **Select Filters to Use** group, make your selection from the filter options supplied
   - **Department**—by selecting this option the following Wizard page asks for a Department selection. This selection triggers the Department filter part of the notification trigger.
   - **Tagholder**—by selecting this option the following Wizard page asks for a Tagholder selection. This selection triggers the Tagholder filter part of the notification trigger.
   - **Location**—by selecting this option the following Wizard page asks for a Location (Door) selection. This selection triggers the Location (Door) filter part of the notification trigger.
   - **Access Group**—by selecting this option the following Wizard page asks for an Access Group selection. This selection triggers the Access Group filter part of the notification trigger.
   - **Event**—by selecting this option the following Wizard page asks for an Event selection. This selection triggers the Event filter part of the notification trigger.
6. After completing the opening Wizard page, click the button.
7. Navigate through the Filter Wizard pages by clicking the button.
8. From the **Actions** group, make your selection from the following options:
   - **Send an E-mail for this Notification**—after selecting this option the following Wizard page confirms the E-mail details. This includes selection of the *E-mail Recipients* ( ) and details of the actual E-mail for sending. Currently you may only send E-mail Notifications from the Host PC. The GSM Module *DOES NOT* support sending of E-mail Notifications. Refer to the section Preference Configuration (E-mail Account Configuration Group) on page 63 for more information.

*Add a **Report Attachment** to your E-mail Notification, as follows:*

1. *Click the button.*
2. *From the Select Report drop-down list, make your selection from the following options:*
   - ***Absenteeism**—details a list of Employees absent on a specified date.*
   - ***Person**—displays a detailed record for a selected individual Tagholder.*
   - ***Hours Worked**—calculates hours worked from the IN and OUT Transactions of all Zones.*
   - ***Timesheet**—calculates hours worked from the IN and OUT Transactions of all Zones.*
   - ***Access Pattern**—displays a summary of an individual employee's time in, average time in, time out, average time out and average hours worked (grouped by Department).*
   - ***Zone Occupancy**—displays a summary of Tagholders within a specific Zone.*
   - ***Tagholder Transaction**—displays all transactions for a Tagholder.*
   - ***Transactions**—displays all transactions for a Tagholder.*
3. *From the **Filters** group, make your selection from the following available filters: **From** and **To Date**, **From** and **To Time**, **Site**, **Zone**, **Door** (Location), **Department** and **Tagholder**.*
4. *Click the button.*

   - **Send an SMS for this Notification**—after selecting this option the following Wizard page confirms the SMS details. This includes selection of the *SMS Recipient* ( ) and details of the actual SMS for sending. The *Enter SMS* text area supports entry of up to 160 characters (including spaces). Refer to Part 7 – Utilities for more information on configuring the Controller's mobile settings (GPRS).

- **Send a Tweet for this Notification**—after selecting this option the following Wizard page asks you to enter a Tweet. The *Enter Tweet* text area supports text-based posts of up to 140 characters. These Tweets display on the author's profile page while also being delivered to the author's followers. Refer to the section Preference Configuration (Twitter Account Configuration Group) on page 64 for more information.

9. After making your selection above, click the button.

Clicking the button lets you quickly select fields, from a shortcut menu, for use in your SMS or E-mail notification.

10. After capturing your E-mail, SMS or Tweet information, continue by clicking the button.
11. Review the summary information.
12. Click the button.

8 Full Upload

A Full Upload writes data from the Site Database to the IXP220 Controller.

Full Upload Procedure

After configuring your IXP220 Software, ensure that you perform a full upload as follows:

1. Select the Page Tab.
2. Select the Controller for upload.

You may perform a full upload per Controller, or elect to multi-select the desired Controllers for upload as a group.

3. Click the **Upload** button.

*Alternately, from the Main Menu, select **Configuration**>**Start Full Upload**.*

Operator Management

The Manage Operator feature allows you to create extra Users and customise their System Rights. This allows you to restrict access to Site definition and configuration tools without limiting access to day-to-day operations.

Operators do NOT have permission to edit a Supervisor or Administrator's Tagholder settings.

Add an Operator

To add an Operator, continue as follows:

1. From the Main Menu, select **File**>**Manage Operators**.
2. In the **Tagholders with Login Privileges** dialog, click the button.
3. In the **Tagholders without Login Privileges** dialog, select a Tagholder.
4. Click the button.

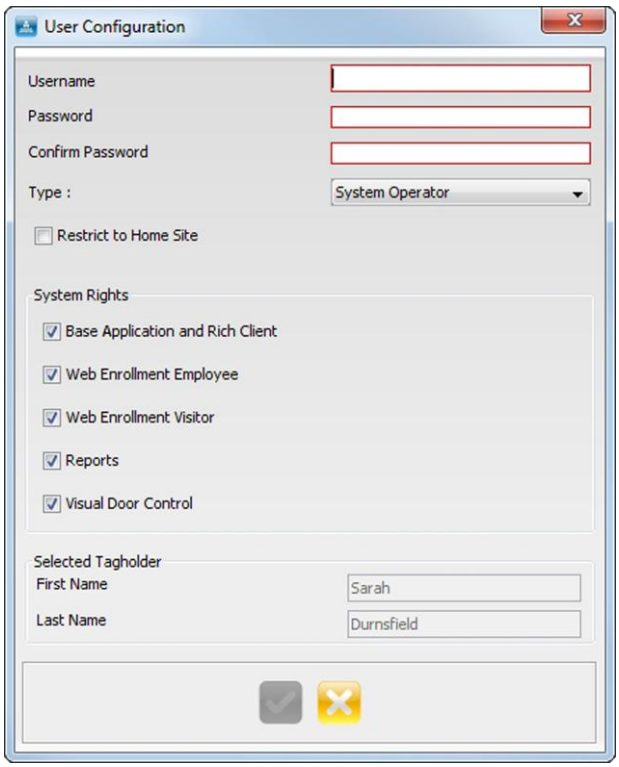


Figure 21 – User Configuration Dialog

5. In the User Configuration dialog, enter a suitable **User Name** and **Password** (not exceeding 20 characters).
6. Confirm your chosen Password in the **Confirm Password** textbox.
7. From the **Type** drop-down list, make your selection:
   - **System Operator**—only has access to the day to day operations of the IXP220 System. By default, a System Operator has access to the following System Rights:

Rich Client, Web Enrollment Employee, Web Enrollment Visitor, Reports and Visual Door Control. However, you may remove privileges by deselecting the associated checkbox.

- **User**—cannot log into the IXP220 Base Application. By default, a User only has access to Reports.
- **Administrator**—has access to Site definition and configuration tools (the same rights as the SYSDBA user). An Administrator has access to the following System Rights: Rich Client, Web Enrollment Employee, Web Enrollment Visitor, Reports and Visual Door Control. This User Type is not customisable.

8. Select the checkbox next to **Restrict to Home Site** if you want the person to only be able to configure changes for or view the site they belong to.

Restrict to Home Site *does not apply to anyone logged in through the Base Application.*

9. Remove System Rights from an Operator by deselecting the associated checkboxes in the **System Rights** group.
10. Click the button.
11. Click the button.

Edit an Operator

To edit an Operator, continue as follows:

1. From the Main Menu, select **File**>**Manage Operators**.
2. Click the button.
3. In the User Configuration dialog, enter a new suitable **User Name** and **Password**.
4. Click the button.
5. Click the button.

Delete an Operator

To delete an Operator, continue as follows:

1. From the Main Menu, select **File**>**Manage Operators**.
2. Select the Operator for deletion.
3. Click the button.
4. Click the button.

Communication Schedule Creator

This feature lets you set up a Site communication Schedule, essentially dictating when Site communication takes place. Schedules may run at a specified time on any day of the week, or on any combination of days in a month.

Ensure the IXP220 Software is running for the scheduled Site communication to take place.

Communication Schedule Setup

Adding a Communication Schedule

To add a communication Schedule, continue as follows:

1. From the Main Menu, select **Configuration**>**Schedule Creator**.

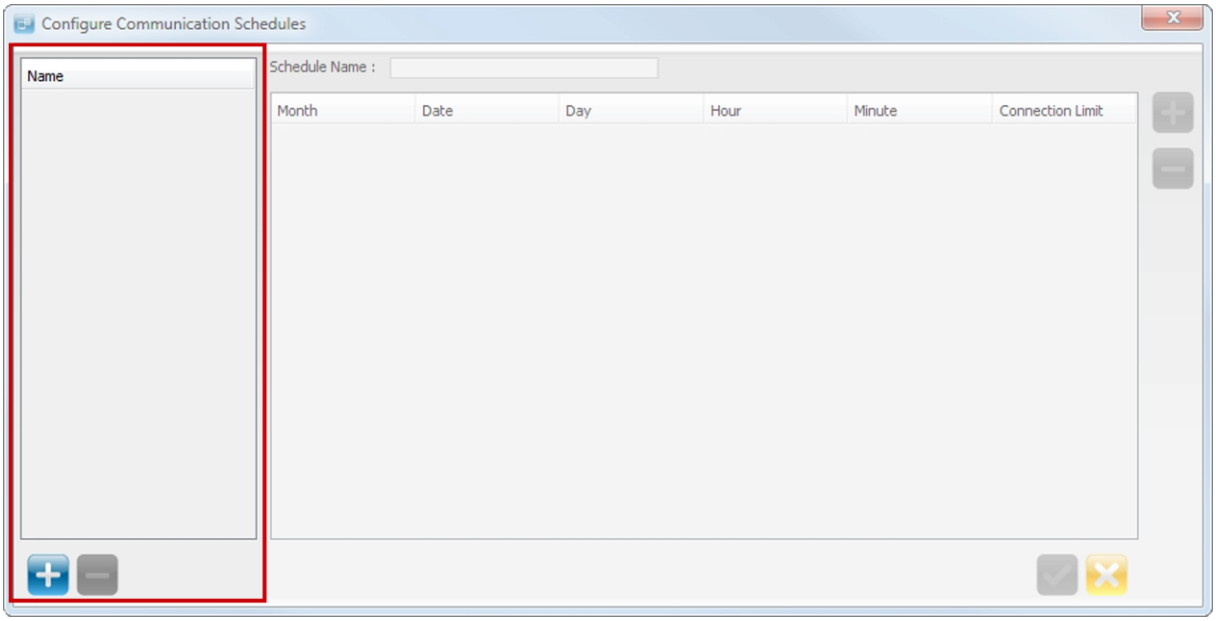


Figure 22 – Configure Communication Schedules Dialog

2. Click the button (as highlighted in Figure 22).
3. In the **Schedule Name** textbox, assign your new Schedule a name.
4. Click the button (as highlighted in Figure 23).

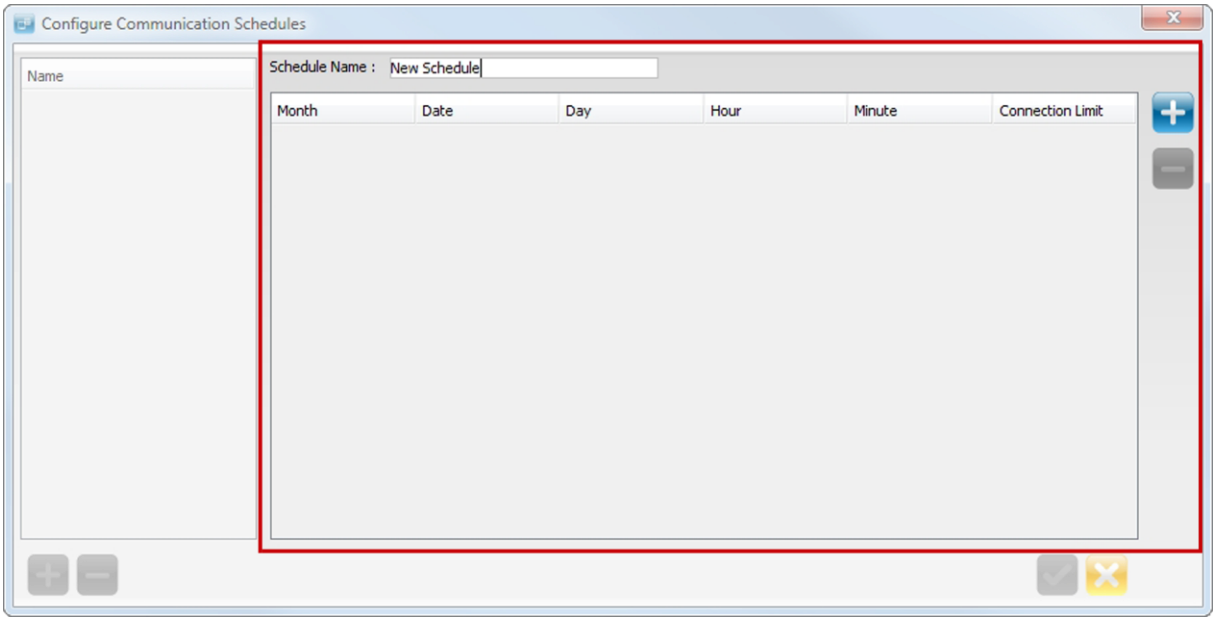


Figure 23 – Configure Communication Schedules Dialog

5. Make your selection by selecting values from each of the following drop-down menus:
   - **Month**—select from the range **January** to **December** for Site communication to take place on a given month. Else select the **Monthly** alternative for Site communication to take place monthly.
   - **Date**—select from the range **1st** to **31st** for Site communication to take place on a given date. Else select (**Every)** for Site communication to take place daily.
   - **Day**—select from the range **Sunday** to **Saturday** for Site communication to take place on a given day. Else select the **Daily** alternative.
   - **Hour**—select from the range **00:00** to **23:00** for Site communication to take place at a given hour. Else select (**Every)** for Site communication to take place hourly.
   - **Minute**—select from the range **00:00** to **00:59** for Site communication to take place.
   - **Connection Limit**—select from **00:00** to **00:59**, limiting the connection duration.
6. Click the button.
7. Click the button.

Implement a Communication Schedule

1. Select the Page Tab.
2. Select the **Advanced Configuration** radio button.
3. From the **Communication Schedule** drop-down list, select the Schedule created earlier.
4. Click the button.

Ensure the IXP220 Software is running for the scheduled Site communication to take place.

Edit a Communication Schedule

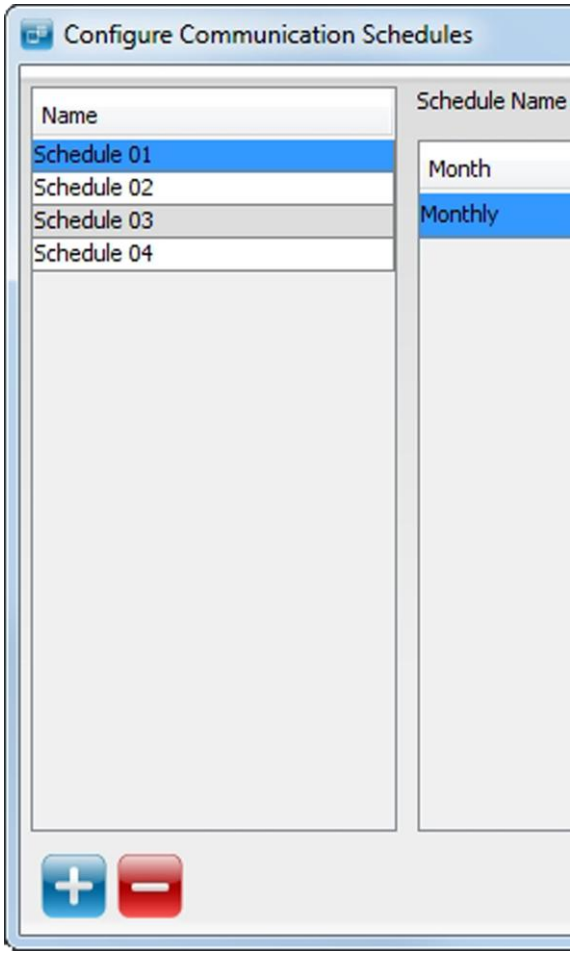


Figure 24 – Left-hand Side of the Configure Communication Schedules Dialog

To edit a communication Schedule, continue as follows:

1. From the Main Menu, select **Configuration**>**Schedule Creator**.
2. From the list of displayed Schedules, select a Schedule record (see Figure 24 for clarification).
3. Edit the Schedule's details as per your requirements.
4. Click the button.
5. Click the button.

Delete a Communication Schedule

To delete a Communication Schedule, continue as follows:

1. From the Main Menu, select **Configuration**>**Schedule Creator**.
2. From the list of displayed Schedules, select a Schedule record (see Figure 24 for clarification).
3. Click the button.
4. Click the button.

Scheduled Reports Creator

This feature lets you set up schedules that automatically run the Reports you request. These scheduled Reports may run at a specified time on any day of the week, or on any combination of days in a month.

Ensure the IXP220 Software is running for the scheduled Report to run.

Scheduled Reports Setup

Adding a Scheduled Report

To add details of a Scheduled Report, continue as follows:

1. From the Main Menu, select **Configuration**>**Scheduled Reports**.
2. Click the button.

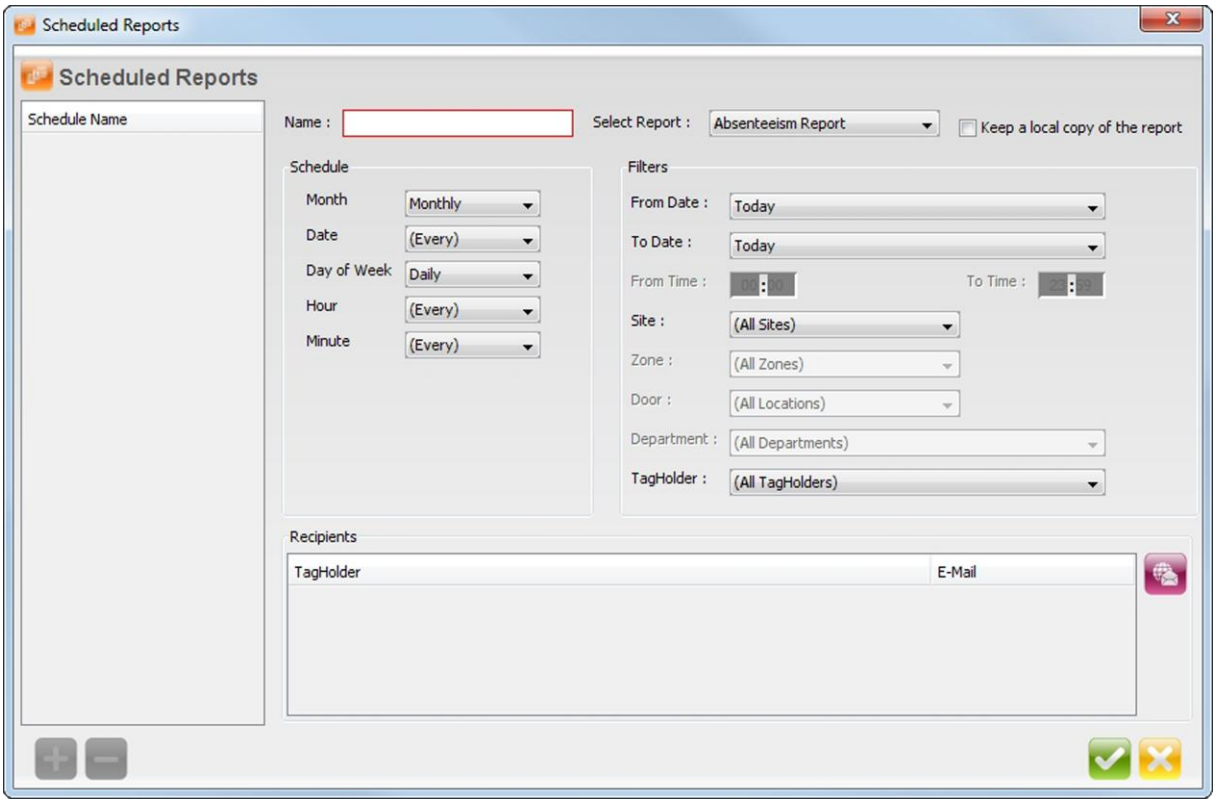


Figure 25 – Scheduled Reports Dialog

3. In the **Name** textbox, assign your new Schedule a name.
4. From the **Select Report** drop-down list, make your selection:
   – **Absenteeism Report**— this Report details a list of Employees absent on a specified date. The Report includes information such as: Employee Name and Number.

- **Person Report**—this Report displays a detailed record for a selected individual Tagholder. The Report includes information such as: First Name and Last Name, ID Number, Company, Department, Employee Number, transaction Date and Time, Door Accessed, Event and Tag code. The Report also displays a photo of the employee.
- **Hours Worked Timesheet Report**—this Report calculates hours worked of all employees from the IN and OUT Transactions of all Zones. The Report includes information such as: Name, Employee Number, Date, Time, Event, Terminal, Zone and Reason.
- **Access Pattern Report**—this Report displays a summary of an individual employee's time in, average time in, time out, average time out and average hours worked. The Report includes information such as: Date, First Transaction, Last Transaction, Time (Last Transaction – First Transaction), Average Time In and Out, Average Hours at Work and Total Time at Work.
- **Zone Occupancy Report**—this Report displays a summary of Tagholders within a specific Zone. The Report includes information such as: First Name, Last Name, Employee Number, Department, Zone, Site, Time In, Date and Hours in Zone.
- **Tagholder Transaction Report**—this Report displays all transactions for a Tagholder. The Report includes information such as: Time, Name, Door, Event and Tag.
- **Transactions Report**—this Report displays all Tagholders transactions on a specific date. The Report includes information such as: Time, First Name, Last Name, Employee Number, Door, Event, Tag and Zone.
- **Tag Expiry Report**—this Report displays details of Tags either expired or due for expiry. The Report includes information such as: Site, Tag Code, Tag Type, First Name, Last Name, ID, Expiry Date and Expiry Time.

5. From the checkbox, indicate whether to **Keep a Local Copy of the Report**.
6. From the **Schedule** group, make your selection:
   - **Month**—select from the range **January** to **December** for the Report to run on a given month. Else select the **Monthly** alternative for the Report to run monthly.
   - **Date**—select from the range **1st** to **31st** for the Report to run on a given date. Else select (**Every)** for the Report to run daily.
   - **Day of Week**—select from the range **Sunday** to **Saturday** for the Report to run on a given day. Else select the **Daily** alternative.
   - **Hour**—select from the range **00:00** to **23:00** for the Report to run at a given hour. Else select (**Every)** for the Report to run hourly.
   - **Minute**—select from the range **00:00** to **00:59** for the Report to run at the specified interval. Else select (**Every)** for the Report to run on a per minute basis.
7. From the **Filters** group, make your selection from the available filters: From Date, To Date, From Time, To Time, Site, Zone, Door, Department and Tagholder. Filter availability is determined by the Report selected.
8. Click the button to configure e-mail recipients for the Report.
9. In the **Recipient Selection** dialog, make your selection from the listed Tagholders.
10. Click the button.
11. At the Scheduled Reports dialog, click the button.
12. Click the button.

Edit a Report Schedule

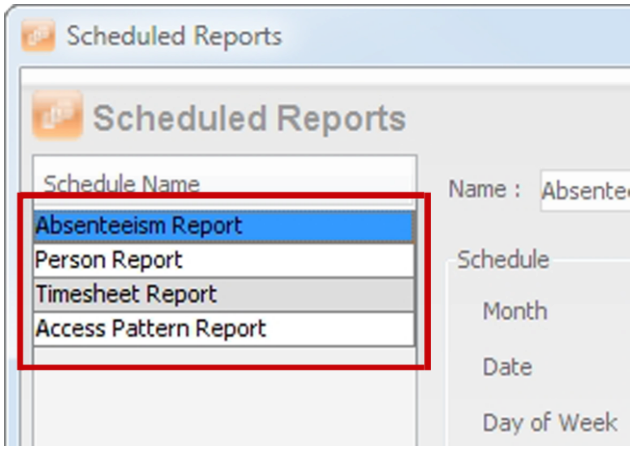


Figure 26 – Left-hand Side of the Scheduled Reports Dialog

To edit Scheduled Reports, continue as follows:

1. From the Main Menu, select **Configuration**>**Scheduled Reports**.
2. From the list of displayed Schedules, select a Schedule record (see Figure 24 for clarification).
3. Edit the Schedule's details as per your requirements.
4. Click the button.
5. Click the button.

Delete a Scheduled Report

To delete Scheduled Reports, continue as follows:

1. From the Main Menu, select **Configuration**> **Scheduled Reports**.
2. From the list of displayed Schedules, select a Schedule record (see Figure 24 for clarification).
3. Click the button.
4. Click the button.

Hardware Replacement

When you replace an old unit with a new one, ensure both units are of the same type.

*If Controllers are running on **Fallback Communications**, replacing hardware will fail. Therefore, only replace hardware running over primary communications.*

Using the IXP220 Software, continue as follows:

Uninstall OLD Hardware

1. From the Main Menu, select **Hardware**>**Device Management Wizard**.
2. In the **Device Maintenance Wizard**, select the **I Would Like to Uninstall a Device From This Site** radio button.
3. Click the button.
4. From the list of displayed hardware, make your selection using the checkbox alongside.
5. Click the button.
6. At the Uninstall Confirmation dialog, click the **Yes** button.

Uninstalling a device that has multiple Fixed Addresses, warns that uninstalling the selected device uninstalls other devices as well. For example, uninstalling a Controller that has its own Fixed Address and those of its Readers.

7. Click the button.

Install Replacement (NEW) Hardware

1. From the Main Menu, select **Hardware**>**Device Management Wizard**.
2. In the **Device Maintenance Wizard**, select the **I Would Like to Replace a Device On This Site** radio button.
3. Click the button.
4. From the list of displayed hardware, make your selection using the checkbox alongside.
5. Click the button.
6. At the Replace Confirmation dialog, click the **Yes** button.

Controllers or Terminals connected by RS485

1. In the activated **Replacement Device** group(s), enter the **Fixed Address(s)** of the replacement Controller or Terminal. When replacing Terminals, continue to step 4.
2. For Controllers connected by RS485, click the button.
3. From the Select Device dialog, double-click your chosen **COM Port** number.
4. Click the button.
5. At the Replace Unit dialog, connect the NEW hardware.

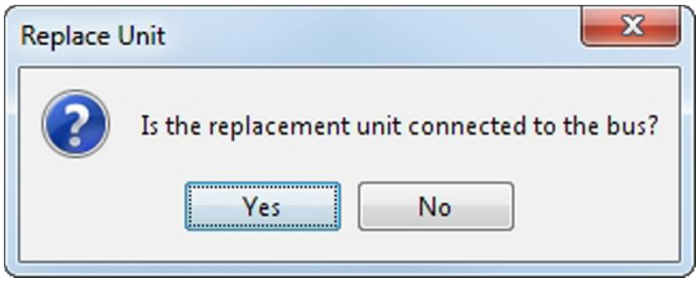


Figure 27 – Replace Unit Dialog

6. Click the **Yes** button.
7. Click the button.

Controllers or Terminals connected by Ethernet

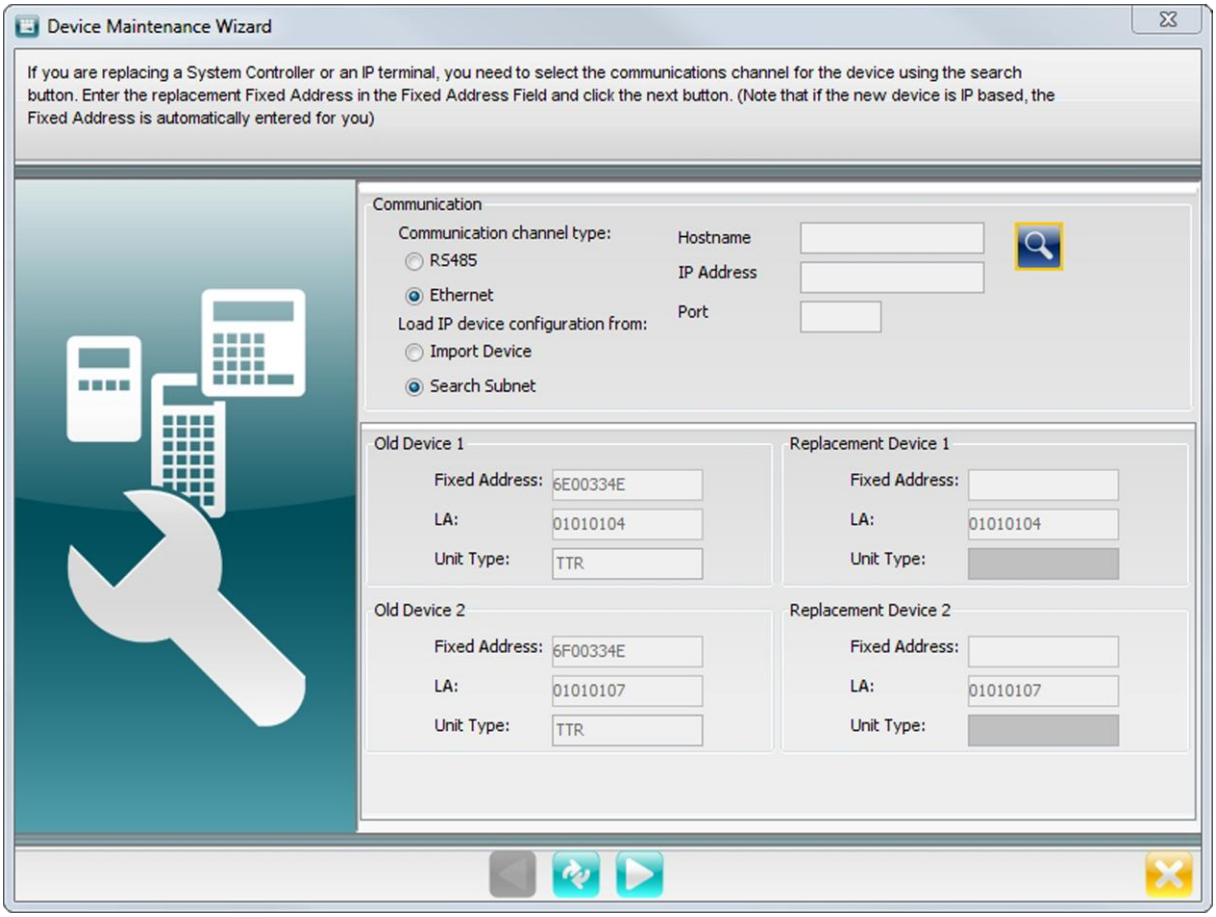


Figure 28 – Device Maintenance Wizard – Ethernet Settings

1. Under **Load IP Device Configuration From**, make your selection from the following:
   - **Import Device**—allows you to select the **Discovery.txt** file (originally exported from the Discovery Utility).
   - **Search Subnet**—selected by default, allows you to enter the **Subnet Mask details for your Network.**
2. Click the button.

Import Device

a. Select the **Discovery.txt** file (originally exported from the Discovery Utility).
b. Click the **Open** button.

Search Subnet

a. In the Input dialog, enter the **Subnet Mask details for your Network**.
b. Click the button.

3. From the Select Device dialog, double-click the replacement Controller or Terminal.
4. Click the button.
5. At the Replace Unit dialog, connect the NEW hardware.

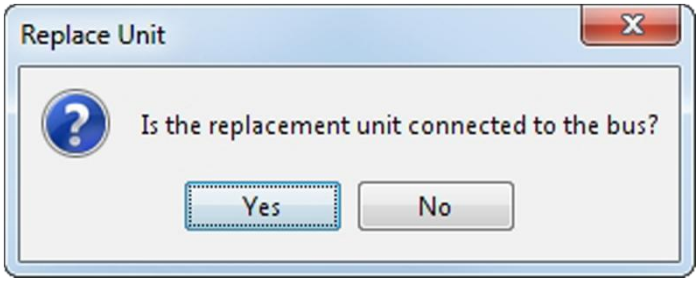


Figure 29 – Replace Unit Dialog

6. Click the **Yes** button.
7. Click the button.

After replacing an IP Terminal, ensure you group the new Terminal to the relevant Controller. See Part 7 – Discovery Utility for more information on Grouping Controllers and Terminals.

Localisation and Translation

Do not edit the same translation twice in the same session otherwise, your translation is overwritten.

Translation changes are permanent.

Localisation and Translation lets Users from different locales (countries and geographical locations), use the IXP220 Software in their own language. The IXP220 Software starts up in English unless a Locale is already set by the Operating System.

Choose Locale

1. From the Main Menu, select **File**>**Choose Locale**.

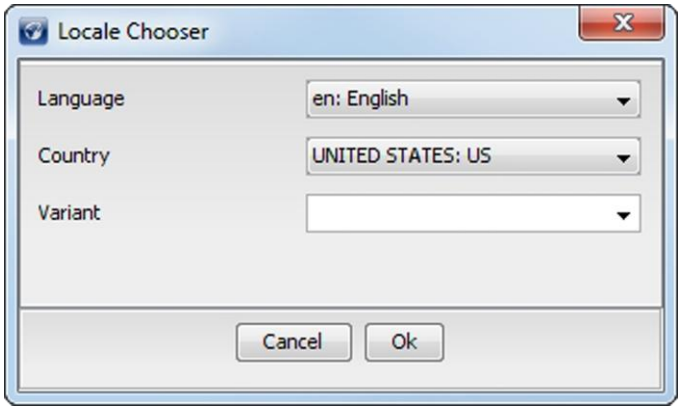


Figure 30 – Locale Chooser Dialog

2. In the **Locale Chooser** dialog, from the **Language** drop-down list, make your selection.
3. From the **Country** drop-down list, make your selection.
4. From the **Variant** drop-down list, select a language variant based on your previous selections.
5. Click the **OK** button.

Translating the Software Interface

1. From the Main Menu, select **File**>**Translate**.
2. In the Translation Selection dialog, from the **Text Group** drop-down list, select a group for editing.
3. Click the **OK** button.

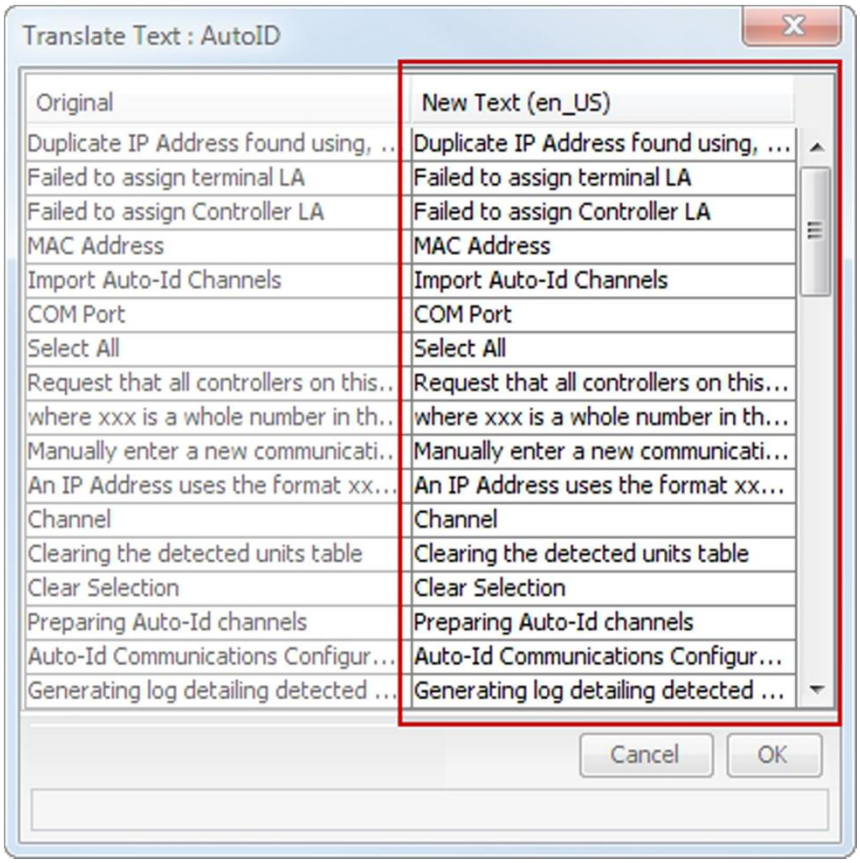


Figure 31 – Translate Text : Dialog

4. In the **Translate Text :** dialog, from the New Text column, select a phrase to translate.

*The **Original** column displays words in English. The **New Text** column displays a copy of the English words, but it is editable. This means you can substitute the default words in the **New Text** column for words in your own language.*

5. Press the **F2** key, thus opening the phrase for editing.
6. Enter a substitute phrase suitable for your Locale.
7. Press the **Tab** key to move to the next phrase.
8. Repeat steps 5 to 7 for each phrase you wish to edit.
9. Click the **OK** button.

Clearing the Transaction Buffer

The IXP220 Controller temporarily stores transactions in a buffer. Clearing the buffer on the Controller permanently erases this buffered transaction data. Transactions that have not been downloaded to the Host PC are lost, therefore only clear the buffer if you suspect that it has become corrupted.

In the event of corruption only, proceed as follows to clear the buffer:

1. From the Main Menu, select **Hardware**>**Clear Transaction Buffer**.
2. In the Clear Transaction Buffer dialog, click the **OK** button.

Database Maintenance

Firebird General

General

Firebird is a powerful, compact client or server SQL relational database management system offering many ANSI SQL standard features and can run on various server and client operating systems. Firebird's officially supported platforms are Windows and Linux. Firebird will, however, also run on operating systems, such as FreeBSD and Apple Macintosh OS/X. Firebird offers excellent concurrency, high performance, and powerful language support for stored procedures and triggers.

Firebird features a higher level of SQL standards compliance than most other industrial-strength client or server database management systems on the market today. Firebird also carries out some powerful language features in the vendor-specific sphere of procedure programming.

Firebird 2.1 is a full-featured SQL database engine. Firebird is powerful, yet lightweight, with the smallest possible configuration and administration needs. It's easily scalable from single-user, single-database use up to company-wide enterprise purposes. A single Firebird server can handle multiple independent databases, each with multiple client connections. And best of all: it's true Open Source, thus free of any license fees even for commercial use.

We publish all our Software with the Firebird Database as our standard offering. The purpose of this document is to aid you in running Systems on the Firebird Database.

This section will address the following topics:

- Firebird Utilities
- Database Backups
- Database Restore
- Database Corruption

Suggested Maintenance Schedule

We recommend regular database maintenance. The schedule of maintenance depends on how critical transactions are to the organisation, the size of the database, as well as the number of transactions written to the database daily. An organisation that uses the transactions for export to payroll may choose to make daily backups of the database. Whereas the small office with 20 employees may choose perform a backup once a month or even every 2 to 3 months. Irrespective of the above factors, carry out the following for database maintenance:

1. Perform regular backups using the tools and techniques described under the section Database Backups.
2. Perform regular test restores on the backup files, using the tools and techniques described under the section Database Restore.

3. At regular intervals, take the working database off-line and carry out a Backup and restore. This ensures the working database does not contain any corrupt data or tables. Refer to the section Recovering a Corrupt Database for more information.

Following these steps will not guarantee the Database will not corrupt in time, but they will lessen the odds of corruption occurring and ensure the least possible resulting data loss.

Figure 32 below shows an example of a monthly maintenance schedule: This organisation needs daily backups as data is critical.

September

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
	1	2	3	4	5	6
	Daily Backup	Daily Backup	Daily Backup	Daily Backup and Restore		
7	8	9	10	11	12	13
Daily Backup	Daily Backup	Daily Backup	Daily Backup	Daily Backup and Restore		
14	15	16	17	18	19	20
Daily Backup	Daily Backup	Daily Backup	Daily Backup	Daily Backup and Restore		
21	22	23	24	25	26	27
Daily Backup	Daily Backup	Daily Backup	Daily Backup	Daily Backup and Restore		
28	29	30				
Daily Backup	Daily Backup	Daily Backup and Restore of Working Database Backup and Restore				

Figure 32 – Example of a Monthly Maintenance Schedule

If the Database does not restore on the 25th, you have 2 choices:

1. Try to recover the Database using the steps described in the section Recovering a Corrupt Database, or
2. Resort to the previous day's backup and restore that file.

Firebird Utilities

There are many Database Management Utilities available for maintaining Firebird Databases. Many of these are open source utilities and are available at www.firebirdsql.org. These utilities include IBEasy (Freeware), IBExpert (commercial and open source personal editions), IBFirstAid (commercial) and IBConsole (open source). We ship IBConsole as the Database Management Utility.

An Introduction to IBConsole

IBConsole is a relational database management utility allowing connection to and administration of multiple Firebird Servers and Databases. The entire functionality of IBConsole is beyond the scope of this document; however administrators of Impro Access Control Databases may find the following roles within IBConsole useful:

- **Database maintenance** in the form of database sweeps and checking for errors
- **Backup and Restores** of the database
- **Review of the database structure**, allows addition of extra tables for third-party integration

The first step in connecting to an Impro Database is registering the Database Server. The following examples refer to the default Database **DB220.FDB** used by the IXP220 Software. The default locations for the Databases and the IBConsole Utility varies dependent on the Access Control System used.

Start the IBConsole Software

In Windows®, go to **Start**>**All Programs**>**IXP220**>**Utils**>**IBConsole**.

Register the Server

You need only perform these steps once. After registration, the settings remain and you need only login to the Server.

Figure 33 – Register Server and Connect Dialog

1. From the Server drop-down menu, select the **Register** choice.
2. In the Register Server and Connect dialog, click the **Remote Server** radio button.
3. In the **Server Name** textbox, assign the Server a name. In this example, we used **LOCALHOST**.

*Rather than assigning the Server a name in the **Server Name** textbox, you may use the PC's **IP Address**.*

4. In the Network Protocol textbox, select **TCP/IP** from the drop-down list.
5. In the **Alias Name** textbox, assign a suitable name.
6. Leave the remaining fields unchanged.
7. Click the **OK** button.

Login to the InterBase Server

1. From the Hierarchical Tree, select your InterBase Server (based on the example in Figure 33 select Local Server).
2. From the Server drop-down menu, select the **Login** choice.
3. In the Server Login dialog, enter the **Username** and **Password**.

*The default username is **SYSDBA**. The default password is **masterkey**.*

4. Click the **Login** button.

Register the Database

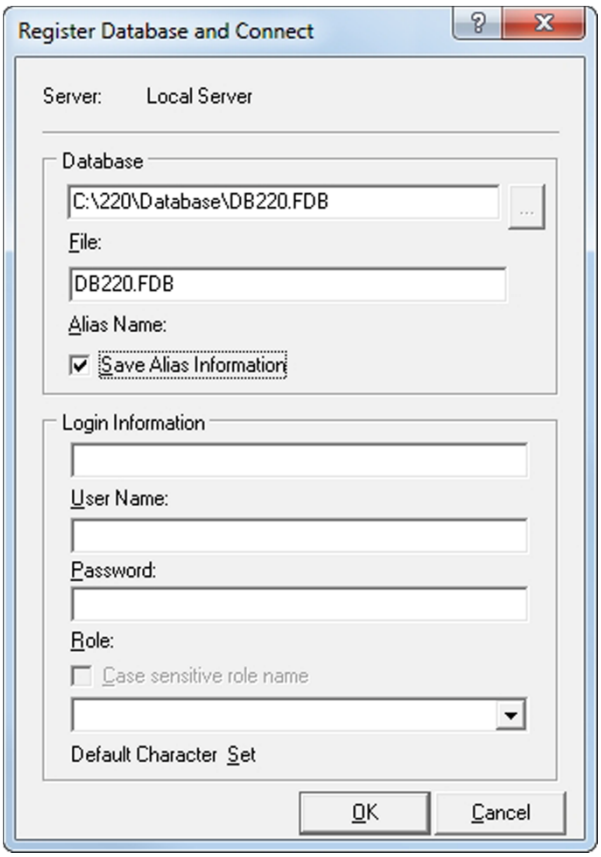


Figure 34 – Register Database and Connect Dialog

1. From the Database drop-down menu, select **Register**.
2. In the Register Database and Connect dialog, In the **Database** textbox, enter the full file path to your Database (see Figure 34).
3. Click your mouse pointer in the **File** textbox, the Database's file name automatically appears.
4. Leave the remaining fields unchanged.
5. Click the **OK** button.

The default Database path for the IXP220 Software is: ***C:\IXP220\Database\DB220.FDB***

6. In the Hierarchical Tree, double-click on the **DB220.FDB** file, starting the Database.

Database Backups

Administrators of Impro Access Control Systems have various choices for making a backup of their Access Control Database. The simplest alternative employed, is copying the Database.

Copying the Database simply copies the Database irrespective of whether there is corruption of the Database or not.

Before making a copy of the Database ensure that you shut down the IXP220 Software.

The preferred method of making a backup, however, is to use the built in backup feature included in the IXP220 Software.

During the backup procedure, the Base Application takes a snapshot of the working Database, the snapshots compacted and a new file created. The resulting backup file has an fbk file extension.

Note, a backup does not guarantee that your IXP220 Database is free from corruption. Ensure that you carry out regular database maintenance, thus ensuring that your IXP220 Database is not corrupt.

Backup of the IXP220 Database Using the IXP220 Software

1. In Windows®, click **Start**>**All Programs**>**IXP220**>**IXP220**.
2. From the Main Menu, select **File**>**Manage Backups**.

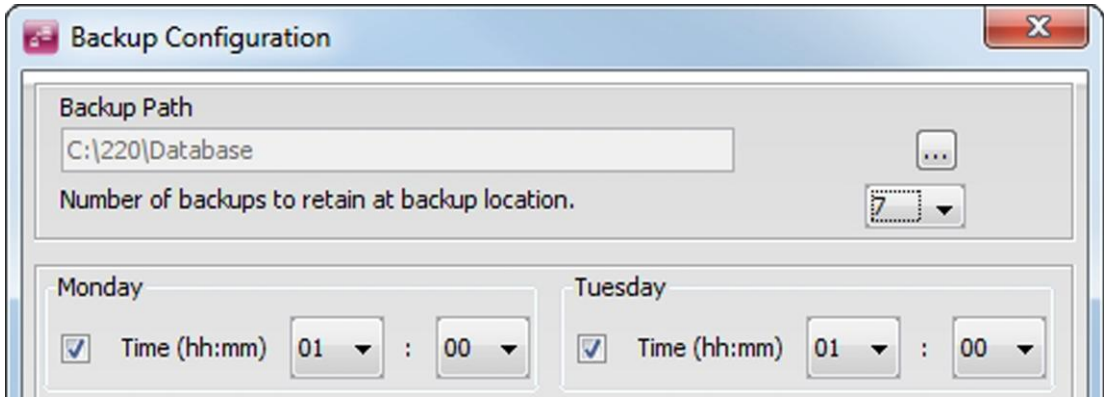


Figure 35 – Backup Configuration Dialog

3. In the **Backup Path** textbox, provide the directory path for the backup Database.

If you change the backup directory path, ensure that you enter ***text only, NO spaces****.*

*The default to backup the Database is **ON**. The default settings are:*

- *Retain 7 backups.*
- *Perform a backup every day at 01:00am.*

4. From the **Number of Backups to Retain at Backup Location** drop-down list, select a suitable number.
5. In the Groups labelled **Monday** through **Sunday**, carry out the following:
   – Select the relevant day by selecting the checkbox.
   – From the Time (hh:mm) drop-down lists, select a suitable time.

*Perform an immediate backup, by clicking the **Backup Now** button.*

6. Click the button.
7. Click the button.

Backup the IXP220 Database using IBConsole

1. In Windows®, go to **Start**>**All Programs**>**IXP220**>**Utils**>**IBConsole**.
2. From the Database drop-down menu, select **Maintenance**>**Backup / Restore**>**Backup**.

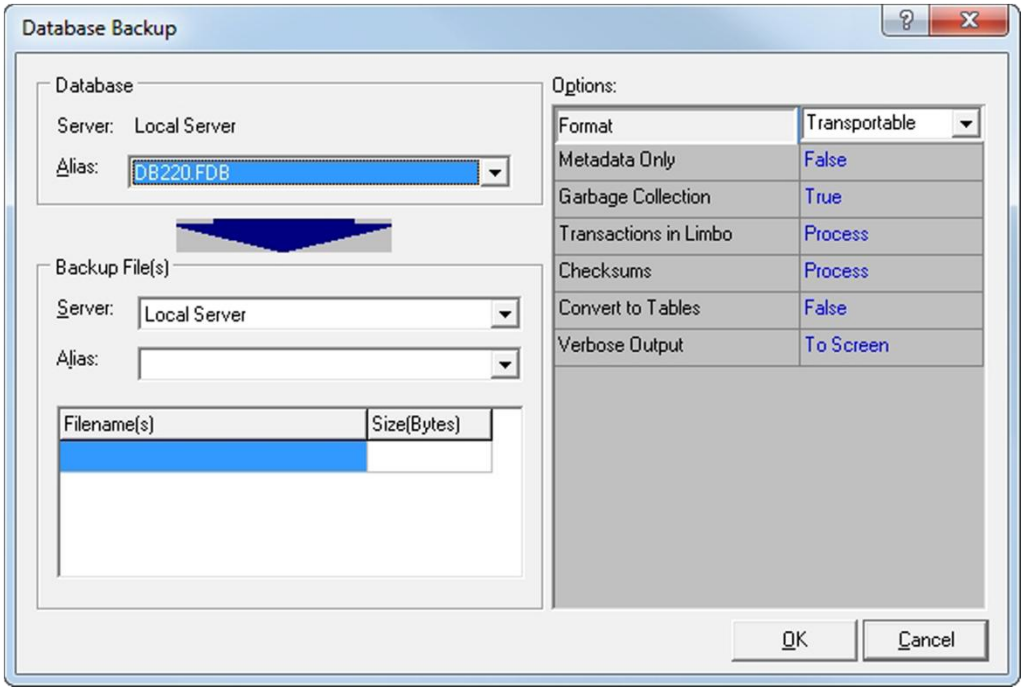


Figure 36 – Database Backup Dialog

3. In the **Database** group, from the **Alias** drop-down list, select the Database for backup.
4. In the **Backup File(s)** group, in the **Alias** textbox, provide a name for the backed up Database.

Ensure that your backed up file has an FBK file extension.

5. In the **Backup File(s)** group, in the **Filename(s)** textbox, provide the directory path and file name for the backup Database. We suggest **C:\IXP220\Database\DB220.FBK**.
6. Leave the remaining values as they are.
7. Click on the **OK** button.
8. In the Information dialog, click on the **OK** button.
9. Close the Database Backup dialog.

Backup the IXP220 Database Using a Batch File

Create the ".bat" File

1. Capture the following text into a text file (for example Notepad).

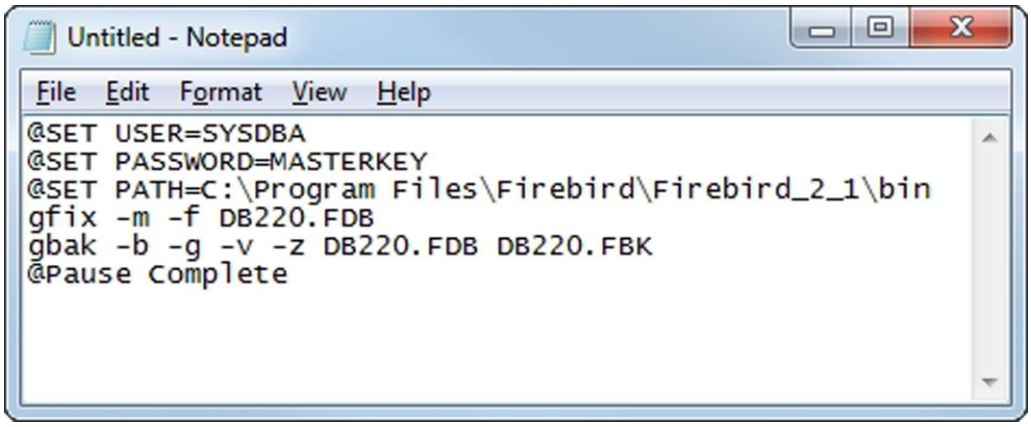


Figure 37 – Backup Using a Batch File

Settings explained:

- ***@SET USER=SYSDBA**—this sets the user name as SYSDBA, thus ensuring the backup utility connects to the Database.*
- ***@SET PASSWORD=MASTERKEY**—this sets the password. If you changed the default password, ensure that you use the new password.*
- ***@SET PATH=C:\Program Files\Firebird\Firebird_2_1\bin**—indicates the path to the GBAK backup utility. If the GBAK backup utility does not appear in this directory, set the path accordingly.*
- ***gfix -m -f DB220.FDB**—repairs minor database corruption.*
- ***gbak -b -g -v -z DB220.FDB DB220.FBK**—creates the backup file DB220.FBK. To change the name of the target database, simply change the DB220.FBK file to another name, keeping the FBK file extension.*

2. Save the text file as a **".bat"** file.

Run the ".bat" Batch File

1. In Windows®, click **Start**>**All Programs**>**Accessories**>**Run**.
2. In the **Run** dialog, click on the **Browse** button.
3. In the **Browse** dialog, select the **".bat"** file you created.
4. Click on the **Open** button.
5. In the **Run** dialog, click on the **OK** button.
6. Follow the on-screen prompts.

This backup process may take some time on large Databases. Once the backups complete, ensure that you copy the resulting backup file to a different PC or on to removable media for storage.

Database Restore

Perform a Database restoration for the following reasons:

- Your original IXP220 Database becomes corrupt.
- Your PC's hard drive is damaged for any reason.
- To ensure that Database backups are not corrupt, a successful restoration suggests a sound Database.

Restoring the IXP220 Database Using IBConsole

Disconnect from the Database

1. In Windows®, go to **Start**>**All Programs**>**IXP220**>**Utils**>**IBConsole**.
2. From the Hierarchical Tree, click on the **DB220.FDB** file.
3. From the Database drop-down menu, select **Maintenance**>**Shutdown**.
4. Click the **OK** button.
5. At the Information dialog, click the **OK** button.

Restore the Backup

1. In IBConsole, from the Database drop-down menu, select **Maintenance**>**Backup / Restore**>**Restore**.

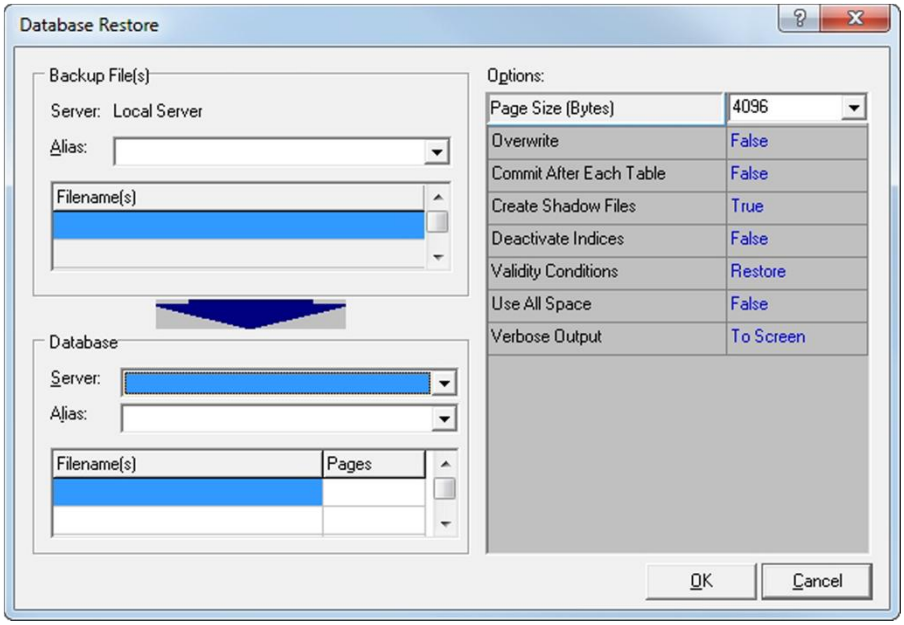


Figure 38 – Database Restore Dialog

2. In the **Backup File(s)** group, in the **Alias** textbox, select the name of the backed up Database.

If IBConsole does not auto complete the remaining fields continue as follows, otherwise continue with point 4:

- In the **Backup File(s)** group, in the **Filename(s)** textbox, provide the directory path and file name for the backup database. We suggest **C:\IXP220\Database\DB220.FBK**.
- In the **Database** group, from the **Server** drop-down list, select the server in which the Database will remain.
- In the **Database** group, from the **Alias** drop-down list, select the Database to restore to.
- In the **Database** group, in the **Filename(s)** textbox, provide the directory path and file name for the restored Database. We suggest **C:\IXP220\Database\DB220.FDB**.

3. From the **Options** group, select the **Overwrite** record.
4. From the **Overwrite** drop-down list, select **True**.
5. Click on the **OK** button.
6. Close the **Database Restore** dialog when you see the comment **"Service Ended"**.

Reconnect to the Database

1. In IBConsole, from the Hierarchical Tree, click on the **DB220.FDB** file.
2. From the Database drop-down menu, select **Maintenance**>**Database Restart**.

Restoring the IXP220 Database Using a Batch File

Create the ".bat" File

1. Capture the following text into a text file (for example Notepad).

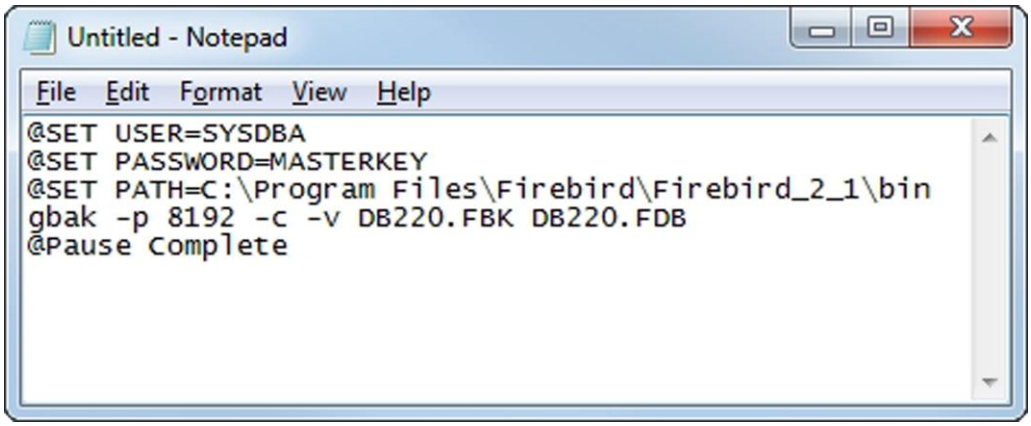


Figure 39 – Restore Using a Batch File

Settings explained:

- ***@SET USER=SYSDBA**—this sets the username as SYSDBA, thus ensuring the backup utility connects to the Database.*
- ***@SET PASSWORD=MASTERKEY**—this sets the password, if you changed the default password, ensure that you use the new password.*
- ***@SET PATH=C:\Program Files\Firebird\Firebird_2_1\bin**—points out the path to the GBAK backup utility. If the GBAK backup utility does not appear in this directory, set the path accordingly.*
- ***gbak -p 8192 –c -v DB220.FBK DB220.FDB**—restores the DB220.FBK file to the name of DB220NEW.FDB.*

2. Save the text file as **"restore.bat"**.

Run the "restore.bat" File

1. In Windows®, click **Start**>**All Programs**>**Accessories**>**Run**.
2. In the **Run** dialog, click on the **Browse** button.
3. In the **Browse** dialog, select the **".bat"** file you created.
4. Click on the **Open** button.
5. In the **Run** dialog, click on the **OK** button.
6. Follow the on-screen prompts.

This restore process may take some time on large Databases. This process restores the new Database to the same directory as where the batch file ran from. Once the restore process is complete, close all applications connected to the original Database. Rename the existing Database as DB220OLD.FDB and rename the DB220NEW.FDB Database to DB220.FDB.

Database Corruption

Lessen data loss if Database corruption occurs, by making regular Database back-ups. It is essential that these regular backups are made and kept on removable media, or on a networked drive. Storing backups on the local disk will not prevent data loss if the hard drive fails.

A Corrupt Database does not always mean a loss of data. Usually, you can recover the Database using a combination of the tools described earlier. There are various indicators of a corrupt Database:

- The Software may not start up
- The Software may hang or not upload transactions

Causes of Database Corruption

Database corruption can result from various causes beyond the scope of this document, the list below outlines the common causes of database corruption:

1. **Abnormal or incorrect shutdown of the server**, especially during power failures. Ensure the server has a working uninterrupted power supply.
2. **Server defects and hardware faults**, especially with hard disk drives, disk controllers, main memory of the PC and cache memory of raid controllers.
3. **Copying the Database while the servers running**.
4. **Hard disk drive or Operating System corruption**.
5. **Poor Database design by third-party integrators**.
6. **Sharing the Database folder** (allowing access over the network) is a security risk, and increases the chance of database corruption. Firebird cannot tolerate other applications locking sectors of the Database file.
   - DO NOT use Windows Explorer (or command line 'Copy' or 'Xcopy') when copying the Database file on a live Database. In practice, these utilities may lock the sector they're copying. So merely copying the **DB220.FDB** file with Windows Explorer is enough to corrupt the Database.
   - DO NOT use any arbitrary backup tool or archiving tool to make a backup copy of the Database. The only safe way to make a backup copy of the Database is to use the backup facility we provide as part of the IXP220 Software, or use Firebird's GBAK tool.

This creates a '.gbk' or '.fbk' backup file, suitable for safe copying after finishing the backup process. Alternatively, stop Firebird Server on the server to copy the '.fdb' file, restart the Server again afterwards.

7. **Check for other processes trying to read the Database file**. These are typically Virus and Spy-ware scanners, common on corporate PC's.
8. **The bigger the size of the Database file**, the more likely is it to become corrupt because of one of the above mentioned reasons.

If you suspect your IXP220 Database is corrupt, carry out an immediate backup and restore on the Database.

Checking, Repairing and Recovering from Minor Database Corruption

*Carry out these steps regularly for checking, repairing and recovering from **Minor Database Corruption**, for example every 2 or 3 months.*

1. Close all applications connected to the Database.
2. Copy the Database to a separate directory.
3. In the same directory, capture the following text into a text file (for example Notepad).

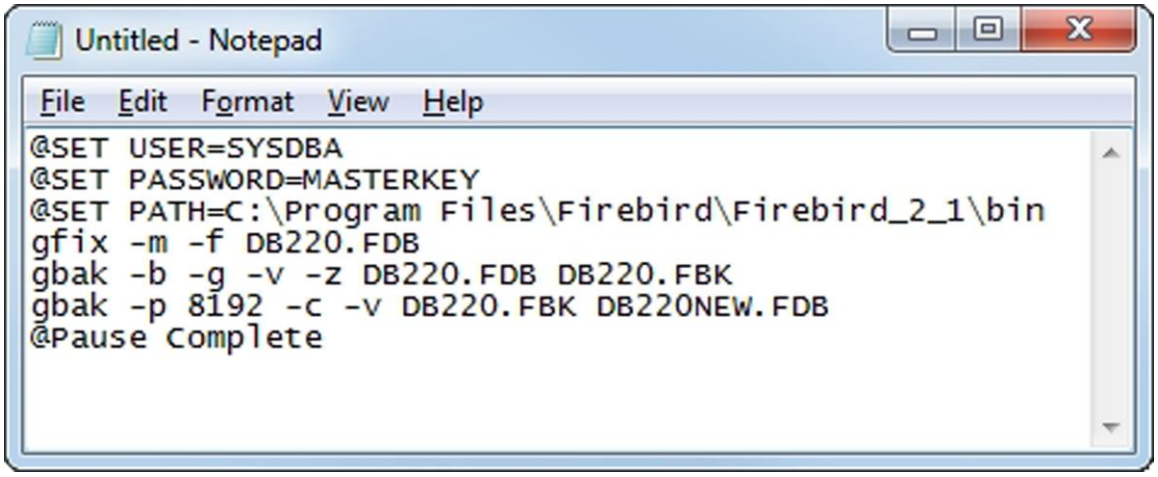


Figure 40 – "repair.bat" Batch File

4. Save the file as **"repair.bat"**.

Run the "repair.bat" Batch File

1. In Windows®, click **Start**>**All Programs**>**Accessories**>**Run**.
2. In the **Run** dialog, click on the **Browse** button.
3. In the **Browse** dialog, select the **".bat"** file you created.
4. Click on the **Open** button.
5. In the **Run** dialog, click on the **OK** button.
6. Follow the on-screen prompts.

This process mends and backs-up the Database to the same directory as where the batch file ran from. Once complete, the restore process runs resulting in the DB220NEW.FDB Database file. If successful, you may use the restored Database as a direct replacement for the existing Database.

An Introduction to IBFirstAID

For Firebird Database corruption that you cannot correct with GFIX, you may buy advanced Firebird database recovery tools from the IB Surgeon web site.

Accessing the IB Surgeon Web Site

1. In Windows®, click **Start**>**Internet Explorer**.
2. In the **Address** bar, type in the URL: **http://www.ib-aid.com/**. From here you may read up on the Software, or buy a copy for use.

USER NOTES