PART III – GENERAL CONFIGURATION

Contents

PART III – GENERAL CONFIGURATION 1

CONTENTS 2

CONFIGURATION OVERVIEW 5

Using the Nexus220 Base Application 5

Common Interface Controls 7

SYSTEM CONFIGURATION PARAMETERS 9

SITE CONFIGURATION 11

Opening the Software 11

Running Auto-ID 13

Configuring the Site 14

CONTROLLER CONFIGURATION 16

General Configuration 16

Full Upload 17

Upgrade 17

DOOR CONFIGURATION 18

Add a Door 18

Add a Zone 20

Add Door Mode Patterns 21

Advanced Door Configuration 22

Delete a Door 23

Delete a Zone 23

Delete a Door Mode Pattern 24

ACCESS GROUP CONFIGURATION 25

Configure Tagholder Access Groups 25

TAGHOLDERS – ASSIGN ACCESS TO TAGS 29

Add a Tagholder 29

Assign Tags to Tagholders 31

Delete an Assigned Tag 33

Delete a Tagholder 33

Set the Default Card Template 33

Batch Enrollment of Tags 34

Advanced Search 35

HOLIDAYS 36

MESSAGES 37

REASON CODES 38

MODES OF OPERATION 39

Power Control Mode 39

Alarm Mode 40

Intrusion Mode 40

Bell Button Mode 41

Action Mode 41

PREFERENCE CONFIGURATION 42

Setting Your Preferences 42

FULL UPLOAD 44

Full Upload Procedure 44

OPERATOR MANAGEMENT 45

SCHEDULE CREATOR 47

Communication Schedule Setup 47

Edit a Communication Schedule 49

Delete a Communication Schedule 49

WEB SERVER PORT SELECTION 50

HARDWARE REPLACEMENT 51

LOCALISATION AND TRANSLATION 53

Choose Locale 53

Translating the Software Interface 53

CLEARING THE TRANSACTION BUFFER 55

DATABASE MAINTENANCE 56

Firebird General 56

Firebird Utilities 58

Database Backups 60

Database Restore 63

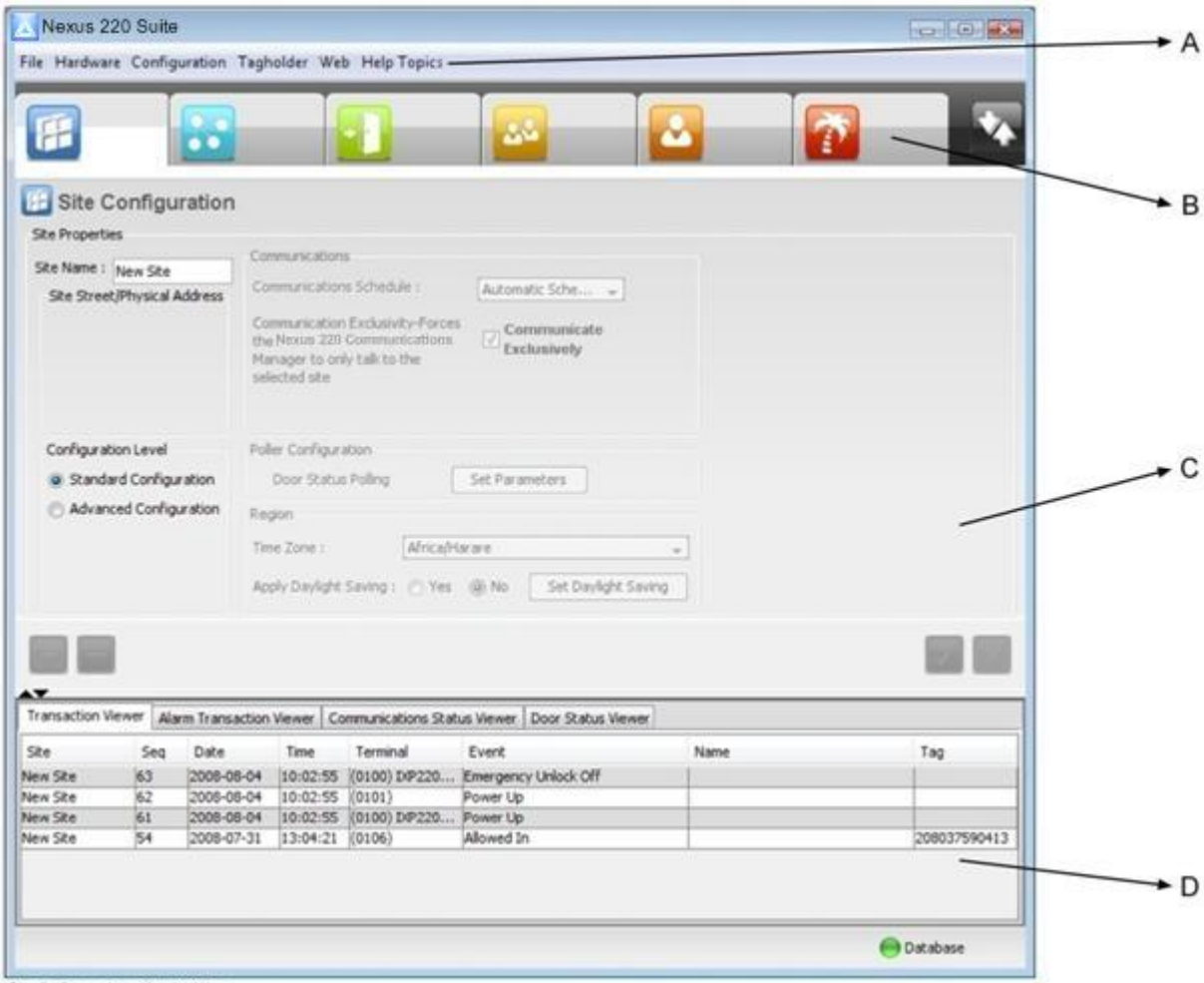
Database Corruption 65

Configuration Overview

Using the Nexus 220 Base Application

The following parts comprise the Nexus 220 Base Application's interface:

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



ConfigOverview_01-300.jpg

Figure 1 – Nexus 220 Base Application User Interface

The Nexus 220 Base Application only displays as shown in Figure 1 where you select the standard Windows® Vista (Business or Ultimate) and XP Professional themes. Using other non-standard themes results in Nexus 220 displaying incorrectly.

Menu Bar

The Menu Bar contains drop-down menus that let you navigate between different operations in the Nexus 220 Base Application. These menus include: File, Hardware, Configuration, Tagholder, 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
- Holiday Configuration

Configuration Pane

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

Viewer Pane

*The **Context Sensitive WebHelp provided with the Nexus 220 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 button on your mouse, thus ensuring the Pane has focus.*
3. *Press the **F1** key on your keyboard.*

Click the button (placed alongside the Page Tabs) to adjust the Base Applications 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.*

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 Nexus 220 Controllers communicating with the Nexus 220 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 Nexus 220 Software.

Common Interface Controls

The following types of controls let you interact with the Nexus 220 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 **e**xamples include:

Icons

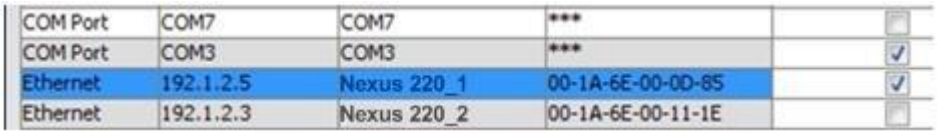
Icons are similar in function to buttons except that Icons are located in the Page Tabs. Icon examples include:

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	Nexus 220_1	00-1A-6E-00-0D-85	☑
Ethernet	192.1.2.3	Nexus 220_2	00-1A-6E-00-11-1E	☐

Textboxes

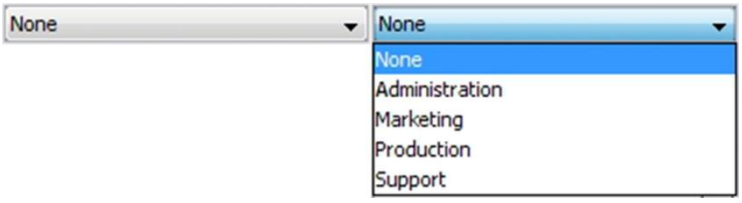
Textboxes let you enter text such as a name. Click the checkbox and type some text.

Text Areas

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

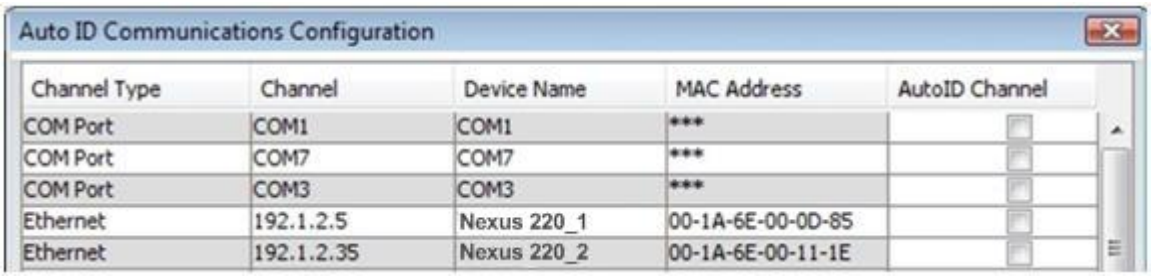
Drop-down Lists

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.



This Manual displays screenshots of various screens in the Nexus 220 Base Application Software. Some of the details displayed in a screenshot may not be available in your copy of the Nexus 220 Software. This is because some details are dependent on the hardware installed and licenses activated.

System Configuration Parameters

System Parameters

Description	Nexus220-1 Single APB Door or 2 non-APB Door System	Nexus220-2 4 APB Door System	Nexus220-3 64 APB Door System	Additional functionality available through upgrade modules:
Total Number of Tags	1 000	2 000	10 000	
Total Buffered Transactions	100 000	100 000	100 000	
Sites per System	1	1	1	1 000
Controllers per System	1	4	64	
Terminal Fixed Addresses per Controller	2	2	2	
Terminal Fixed Addresses per Door (Location)	2	2	2	
Doors (Locations) per Zone	32	32	32	
Zones per Controller	32	32	32	
Actions Supported	256	256	256	
Doors (Locations) per Controller	2	4	32	
Tags per Tagholder	4	4	4	
Tagholder Access Groups	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	
Controller Communications Baud Rate	100 Mbps when using TCP/IP	100 Mbps when using TCP/IP	100 Mbps when using TCP/IP	
Terminal Communications Baud Rate	38 400	38 400	38 400	
Digital Inputs – Per Controller (not used for Access Control)	3	3	3	
Onboard Relays – Per Controller	3	3	3	
Lift (Elevator) Control	NA	NA	NA	8
Maximum Fixed Addresses Supported	2 (Per Site)	8 (Per Site)	512 (Per Site)	
Maximum Fixed Addresses Supported - APB Doors	2 (Per Site)	4 (Per Site)	256 (Per Site)	
Maximum Fixed Addresses Supported - Single Reader Doors	2 (Per Site)	4 (Per Site)	256 (Per Site)	
Host PC Communications	RS232, USB or TCP/IP	RS232, USB or TCP/IP	RS232, USB or TCP/IP	
Controller Bus Communications	No	RS485	RS485	
Terminal Bus Communications	No	RS485	RS485	

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)
Maximum number of Controllers per Site	1	4	32	32
Tag Registration	Reader 1	Reader 1	USB Registration Reader or Reader 1	USB Registration Reader or Reader 1
Database	Firebird 2.1	Firebird 2.1	Firebird 2.1	Firebird 2.1

Table 1 – System Configuration Parameters

Nexus220-3 System is restricted to10 000 Tags per System regardless of the number of Sites. In addition this System 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.

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 Nexus220-3 for up to 1 000 Sites per System and 8 Lifts (Elevators) using the Multi-site and Elevator Control Licences.

1 Site Configuration

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

- Host PC
- Nexus 220 Controllers
- Terminals
- Zones and Doors (Locations)

Opening the Software

To open the Nexus 220 Base Application, proceed as follows:

1. In Windows®, click **Start**>**All Programs**>**Nexus220**>**Nexus220**.
2. Enter your **Username** and **Password**.

Figure 2 – Logon Dialog (Enter Username and Password)

*The default administrator username is **SYSDBA**, and the default password is **masterkey**.*

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

*On first time installation of the Nexus 220 Software, the **I do not have one** choice is by default selected. In this case, if the site has an Amano RS connected that's unlocked for a System 3 then the Nexus 220 Software starts up as a **System 1**. This means, no search is performed for the Amano RS.*

- **Automatically Search**—for Nexus220-*3* installations where an Amano RS is connected but you are unsure of the COM Port number in use by the Amano RS.
- **Enter the COM Port Name**—for Nexus220-*3* installations where an Amano RS is connected and you know the COM Port number in use by the Amano RS. *Recommended when you have an enabled Bluetooth or Infrared Port*. Automatically

searching on a computer that has an enabled Bluetooth or Infrared Port may result in the Nexus 220 application freezing. If you select this choice, enter the COM Port number in the supplied textbox.

– **I do not have one**—for *Nexus220-1* and *Nexus220-2* installations with no Amano RS.

4. Click the button.

*When using **separate PC's for the Base Application (Host PC) and Database (Server PC)** installation, start the Nexus 220 Base Application as follows:*

1. *On the Host PC, start the Nexus 220 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 Nexus 220 Software closes.

Running Auto-ID

After physically connecting and powering up the Amano Hardware, perform the following steps to confirm the hardware is communicating correctly:

*Ensure the Base Application has a working connection to the Database. Configure this connection using the Communications Configuration dialog. For more information, refer to **Part II – Software**.*

During an Auto-ID, the Base Application polls attached Controllers and Terminals, identifying their **type**, and their **Logical Address**.

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

To carry out the Auto-ID process, continue as follows:

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 you connected your Controller to the Host PC via an **Amano RS**, from the Auto ID Communications Configuration dialog, select the appropriate Com Port record.
4. If you connected your Controller to the Host PC via **TCP/IP**, click the button.
5. In the Channel column, replace the default IP Address details with the IP Address of your Controller.
6. Press **Enter**.

*Alternatively If your Controller does not appear in the **Auto ID Communications Configuration** dialog continue as follows:*

1. *Click the button.*
2. *In the Input dialog, enter the **Subnet Mask details for your Network**.*
3. *Click the **OK** button.*

7. From the list of devices displayed, in the **AutoID Channel** column, make your selection.
8. 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.

*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 Amano 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 VII – Utilities** for more information on the **Firmware Upgrade Utility**.*

Configuring the Site

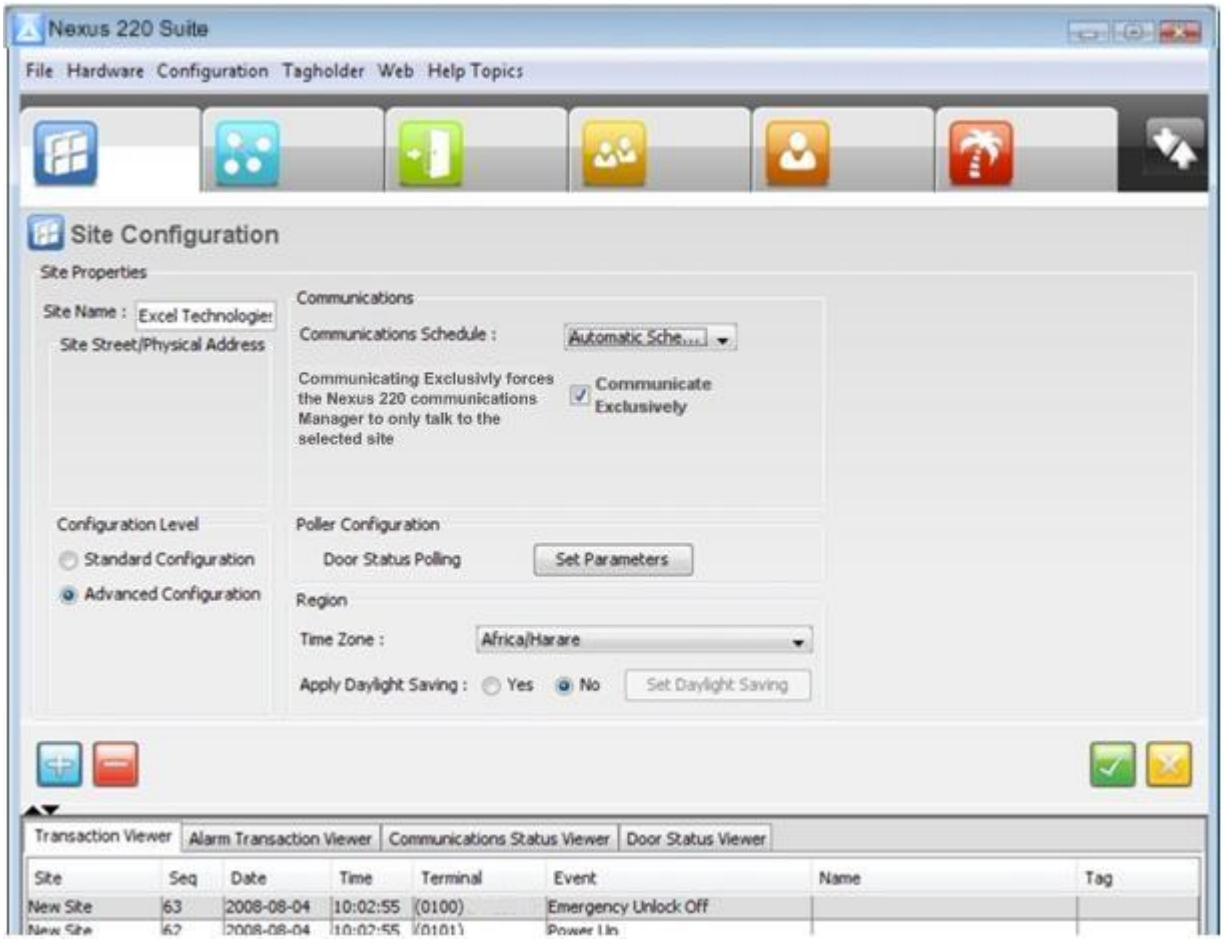


Figure 3 – Site Configuration Pane

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.
4. Select either the **Standard Configuration** or the **Advanced Configuration** radio button.

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

5. In the **Communications** group, from the **Communication Schedule** drop-down list select a Communication Schedule (see page 47 for information on setting up a Communication Schedule).
6. If you wish to communicate only with the selected site, select the **Communicate Exclusively** checkbox.

7. From the **Poller Configuration** group, 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.
8. From the **Time Zone** drop-down list, make your selection.

*Set the **Apply Daylight Saving** option as follows:*

1. *Alongside Apply Daylight Saving, click the **Yes** radio button.*
2. *Click on the **Set Daylight Saving** button.*
3. *In the Set Daylight Saving dialog, set the following:*
   - *Time Offset*
   - *Start Date*
   - *Start Time*
   - *End Date*
   - *End Time*
4. *Click the button.*

9. 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, click on the button.
3. In the Nexus 220 Site Creator dialog, complete the **Site Name** textbox.
4. Complete the **Site Street/Physical Address** textbox.
5. Click the button.

Refer to the section **Running Auto-ID** on page 12 for further information.

Delete a Site

To delete a Site, proceed as follows:

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

Do NOT disconnect the Amano RS while still connected to the Nexus 220 Software.
Should you unintentionally disconnect the Amano RS while the Software's running, close the Nexus 220 Software, reconnect the Amano RS and then restart the Software.

2 Controller Configuration

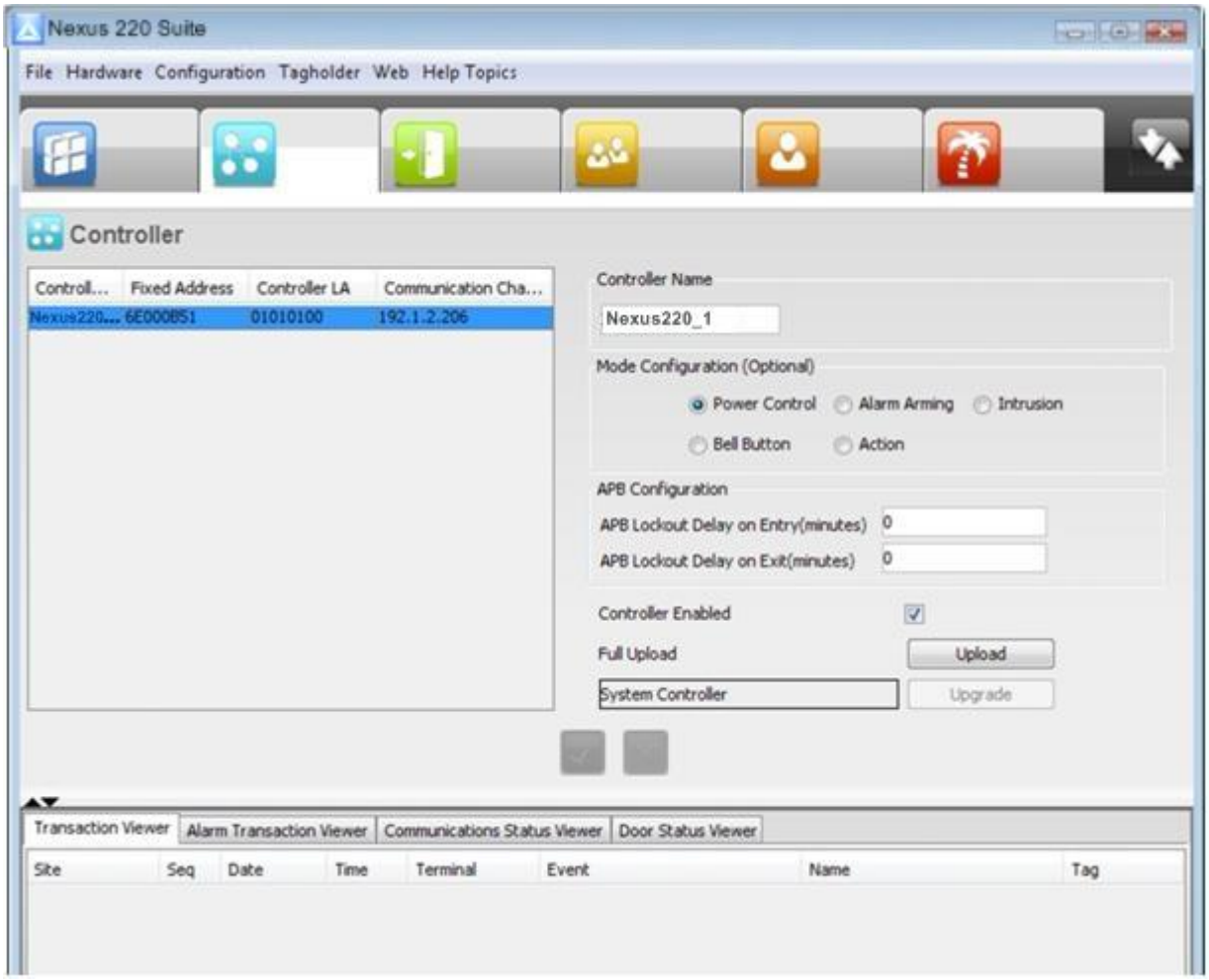


Figure 4 – Controller Configuration Pane

*The information displayed in the **Communications Channel** column varies according to your Nexus 220 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.*

General Configuration

Configure your Controller as follows:

1. Select the Page Tab.
2. In the **Controller Name** textbox, assign your Controller a suitable name.

*Refer to page 40 for details on **Alarm Arming**.*

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

Full Upload

Clicking the **Upload** button uploads the selected Controllers configuration information to the physical unit. Refer to page 44 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 Network Controller as follows:

1. Select the Page Tab.
2. Click the **Upgrade** button.
3. 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.*

4. Click the **Open** button.
5. At the Unlock Successful dialog, click the **OK** button.
6. Click the **Upload** button.
7. Select the Page Tab.
8. From the Communication group, deselect the **Communicate Exclusively** checkbox.

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 the Site's Doors (Locations) including Terminals, Readers, Zones and Door Mode Patterns.

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

Add a Door

To create a Door (Location) continue as follows:

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

*Within the previously selected Door Tab, you will notice a new set of Tabs activate. These newly activated Tabs include a new **Door** Tab, an **Entry** Tab and an **Exit** Tab.*

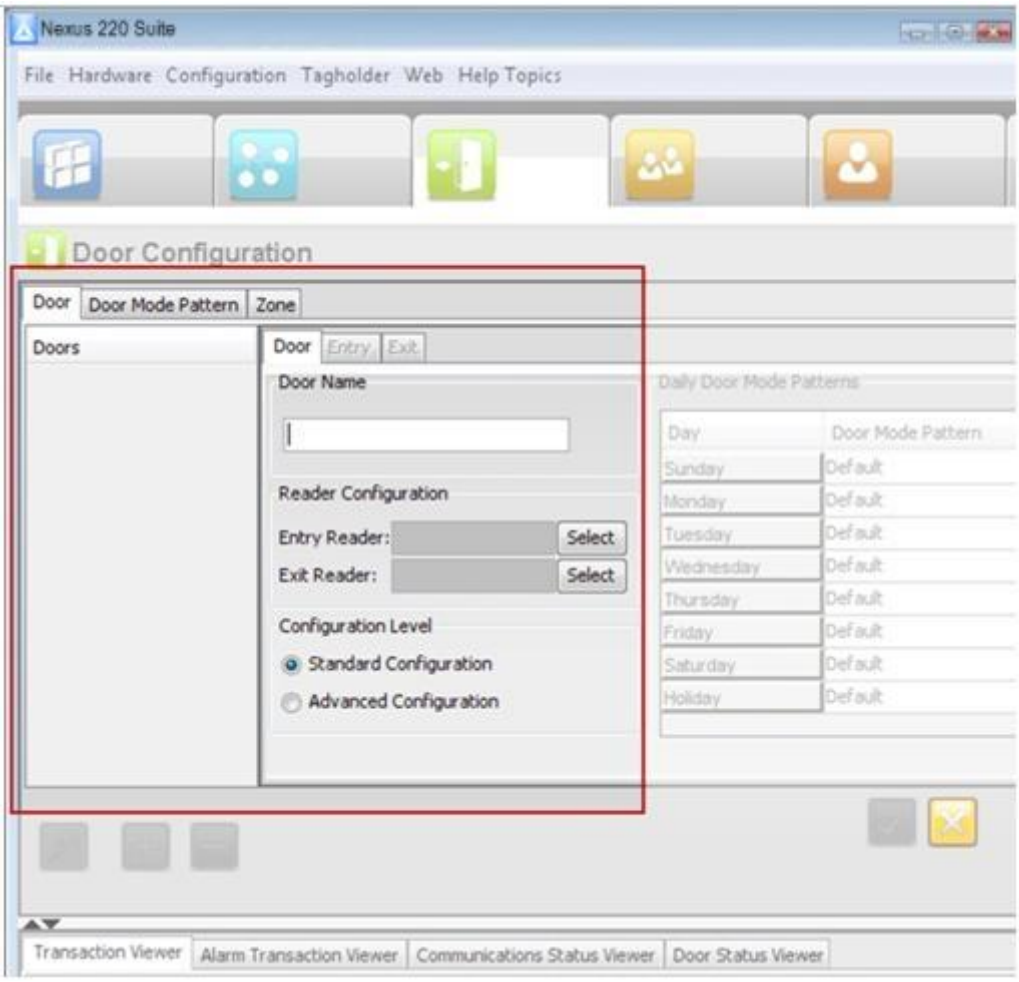


Figure 5 – Left-hand Side of the Door Configuration Pane

3. In the **Door Name** textbox, assign the Door a suitable name.

This Door Name textbox has a 16 character limit.

4. 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 Amano (KMA) Keypad Mullion Antenna Readers. Selecting this checkbox activates the Bell button (situated at the bottom of the Antenna Reader's Keypad).*

Add Readers

To add and configure Readers, continue as follows:

Reader Selection

1. In the **Reader Configuration** group (see Figure 5), 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.

*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 Nexus 220 Software automatically assigns the **top selected Reader as the Entry Reader** and the **bottom selected Reader as the Exit Reader**.*

Entry or Exit Reader Configuration

1. Select the **Entry** or **Exit** Tab.
2. Complete fields on this Tab based on your sites specific needs.
3. Click the button.

7. Click the button.

Add a Zone

To create and configure Zones, continue as follows:

1. On the Configuration Pane, select the **Zone** Tab.
2. Click the button.

Figure 6 – Create Zone Dialog

3. In the Create Zone dialog, select a Controller from the **Select Controller** drop-down list.
4. In the **Zone Name** textbox, assign the Zone a suitable name.
5. Select one of the **APB Mode** (Anti-passback Mode) radio buttons:
   - **Off**—Anti-passback 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 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**, 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 on an individual Tagholder, refer to page 33, Miscellaneous Configuration for more information.

6. 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.

Add Door Mode Patterns

The Nexus 220 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. On the 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** 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 Mode****—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****—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.*

   - **Finger (BSHO)**—no hardware support at this time.
   - **+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 38 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.
   - **Denied Alarm**—by selecting Yes, you instruct the System to treat denied events as alarms.
   - **LED**—Sets the LED's behaviour during the stipulated time slot.
7. Click the button.

Advanced Door Configuration

On selecting the **Advanced Configuration** radio button, the Daily Door Mode Patterns, Zone, Door Entry Code and Alarm Arm settings activate.

Continue as follows to configure these settings:

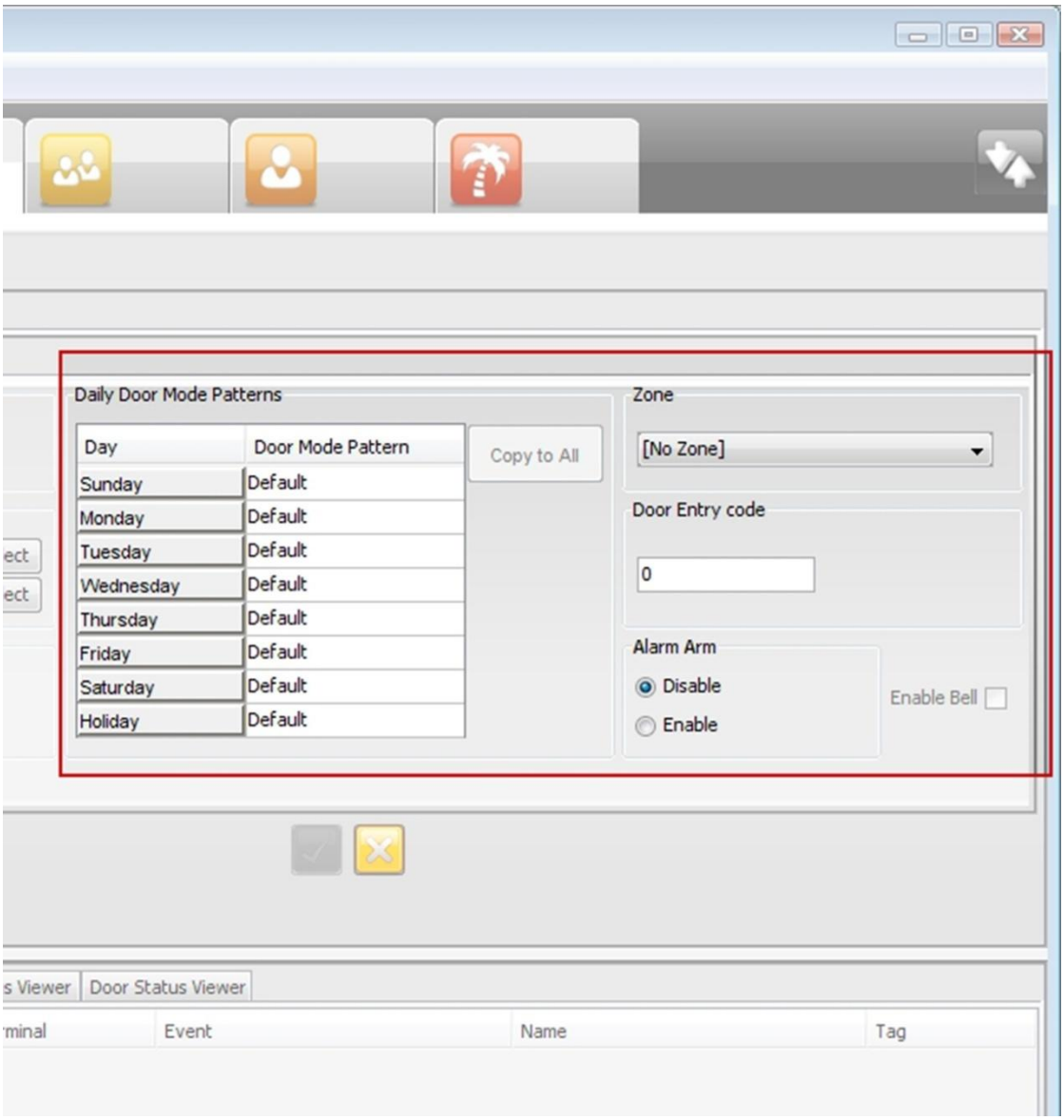


Figure 7 – Right-hand Side of the Door Configuration Pane

1. On the Configuration Pane, select the **Door** Tab.
2. In the **Daily Door Mode Patterns Group (see** Figure 7**)**, 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 4 digit numeric PIN-code instead of a Tag.*

Activate the Door Entry Code feature, as follows:

1. *On the 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 9999**).*
7. *Click the button.*
8. *On the Configuration Pane, select the **Door** Tab.*
9. *In the **Door Entry Code** textbox, enter a 4 digit numerical PIN-code.*

*Refer page 40 for details on **Alarm Arming**.*

Configuration of multiple Doors (Locations) is allowed. Configure multiple Doors (Locations), by holding down the Ctrl key and selecting multiple records. Alternately 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.

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.

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 V – Advanced Configuration.

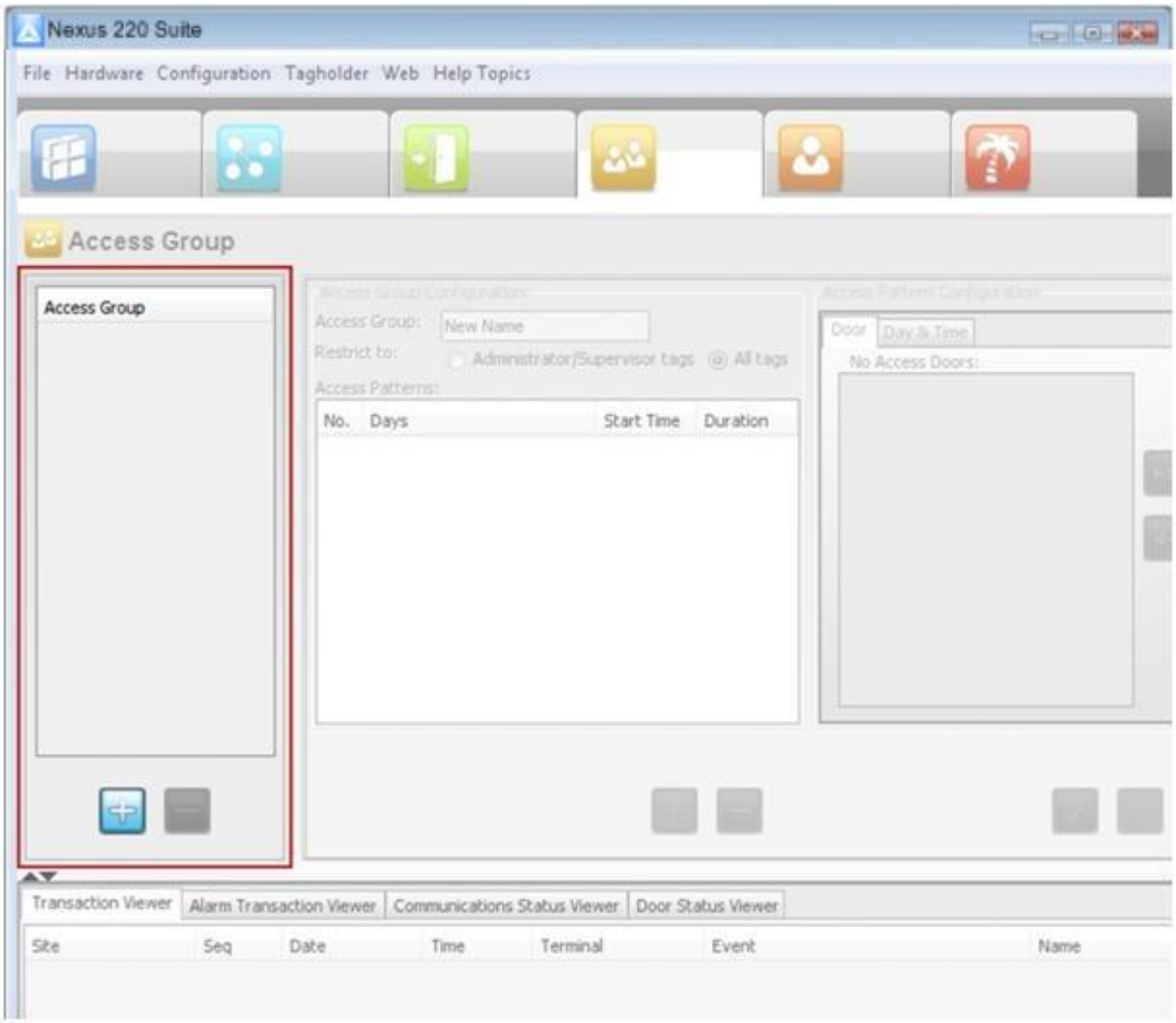


Figure 8 – Left-hand Side of the Access Group Pane (General Access Tab Selected)

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 8, click the button.
4. In the **Access Group** textbox, assign your Access Group a suitable name.
5. From the **Select To** 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 at each Door.*

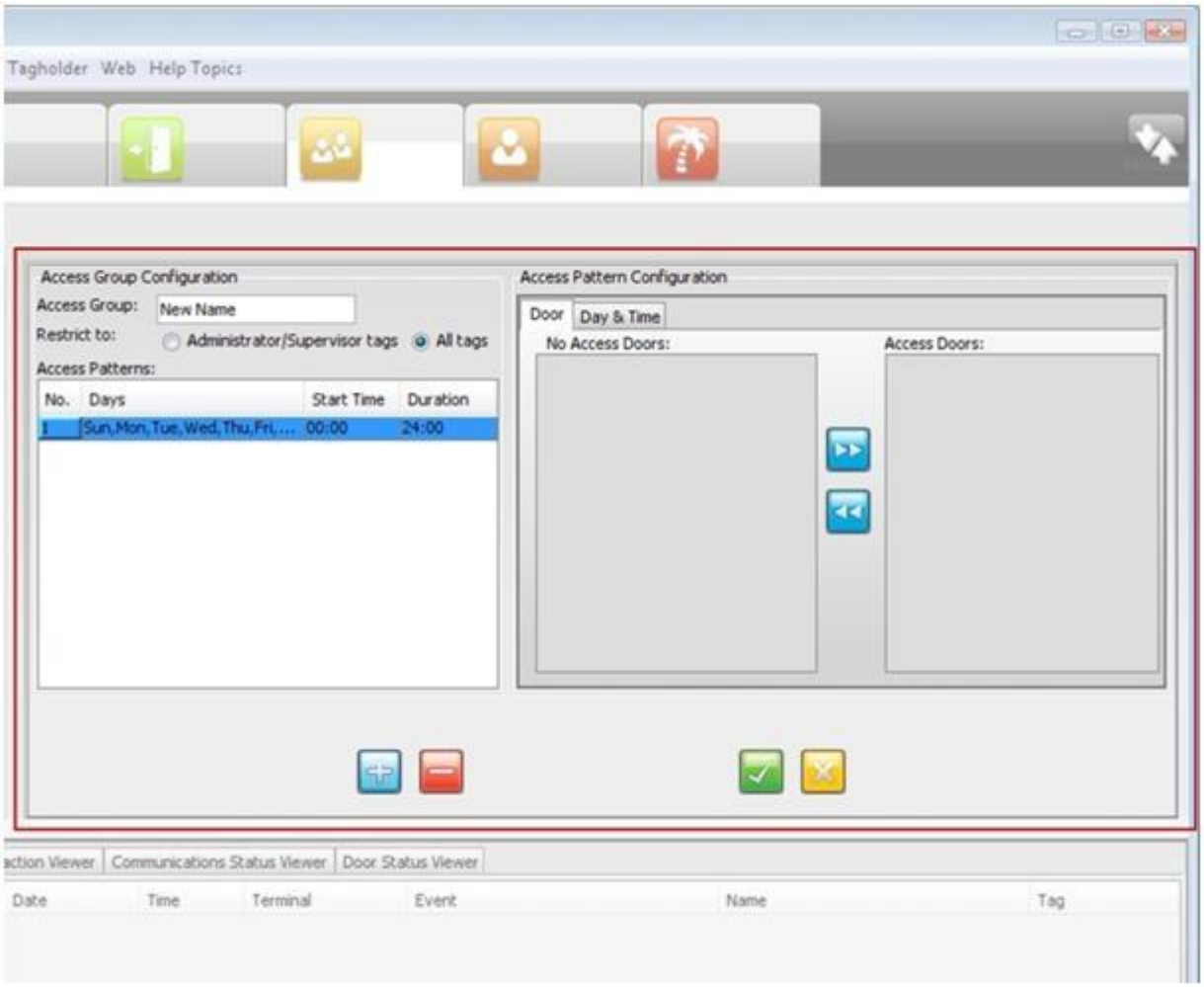


Figure 9 – Right-hand Side of the Access Group Pane (General Access Tab Selected)

To create an Access Time Pattern, proceed as follows:

1. As highlighted in Figure 9, 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 8 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 9 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 8 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 8 for more information) select a record.
4. Edit the Access Time Pattern details as required.
5. Click the button.

5 Tagholders – Assign Access to Tags

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.

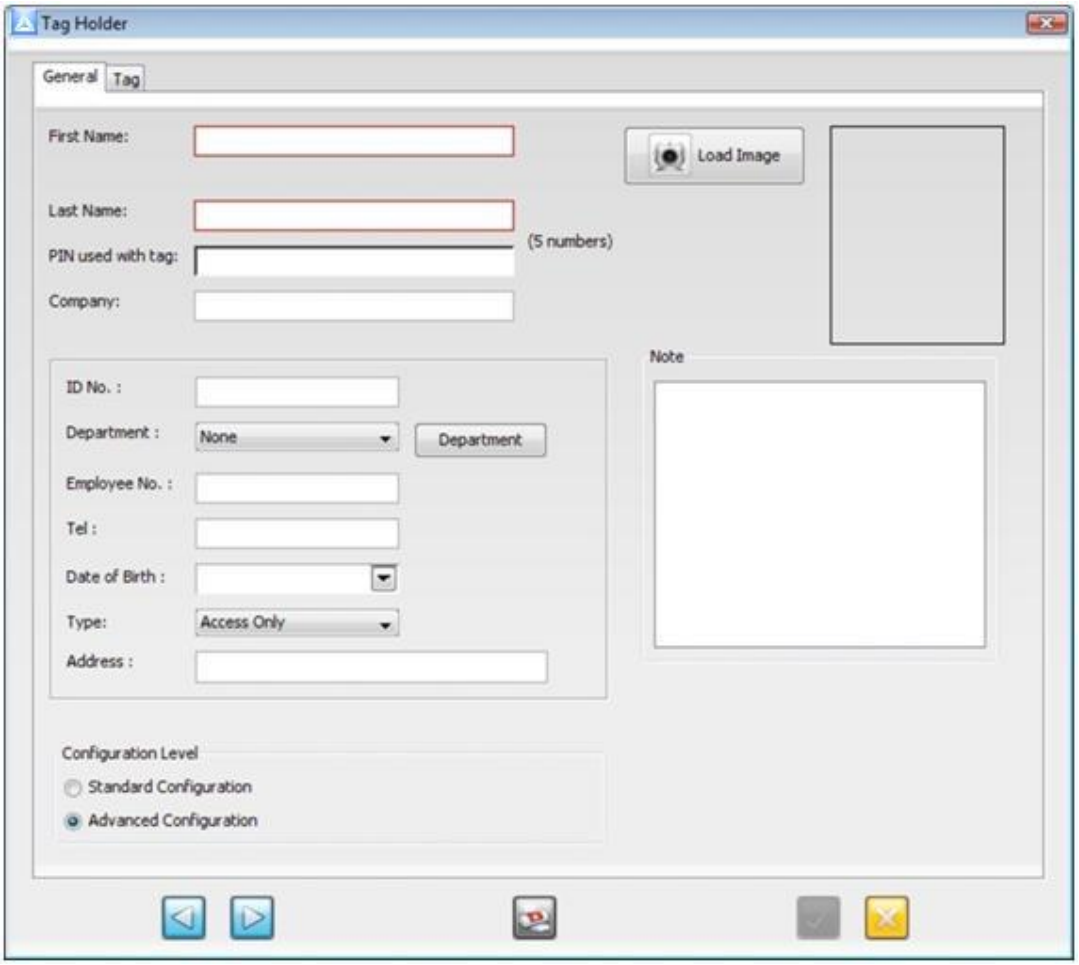


Figure 10 – Tagholder Dialog (Showing the General Tab)

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 4 digits. (PIN-codes range from **2 to 65534**).
8. 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.

9. 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 that you select the **Access and Time** option, for all other installations select the **Access Only** option.*

10. Complete other personal information as necessary.
11. Click the **Load Image** button. From the shortcut menu that appears, select one of the following choices:
    - **Load From File**—opens up the Open dialog, allowing selection of the image file. Image formats supported include: jpg, jpeg, gif, tif and tiff.
    - **Edit**—opens the Edit dialog, allowing image cropping, rotation, resizing and use of an image mirror effect.
    - **Reset**—resets the image file to its default settings.
12. Use the **Note** text area when entering further information about the Tagholder.
13. Click the button.

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.

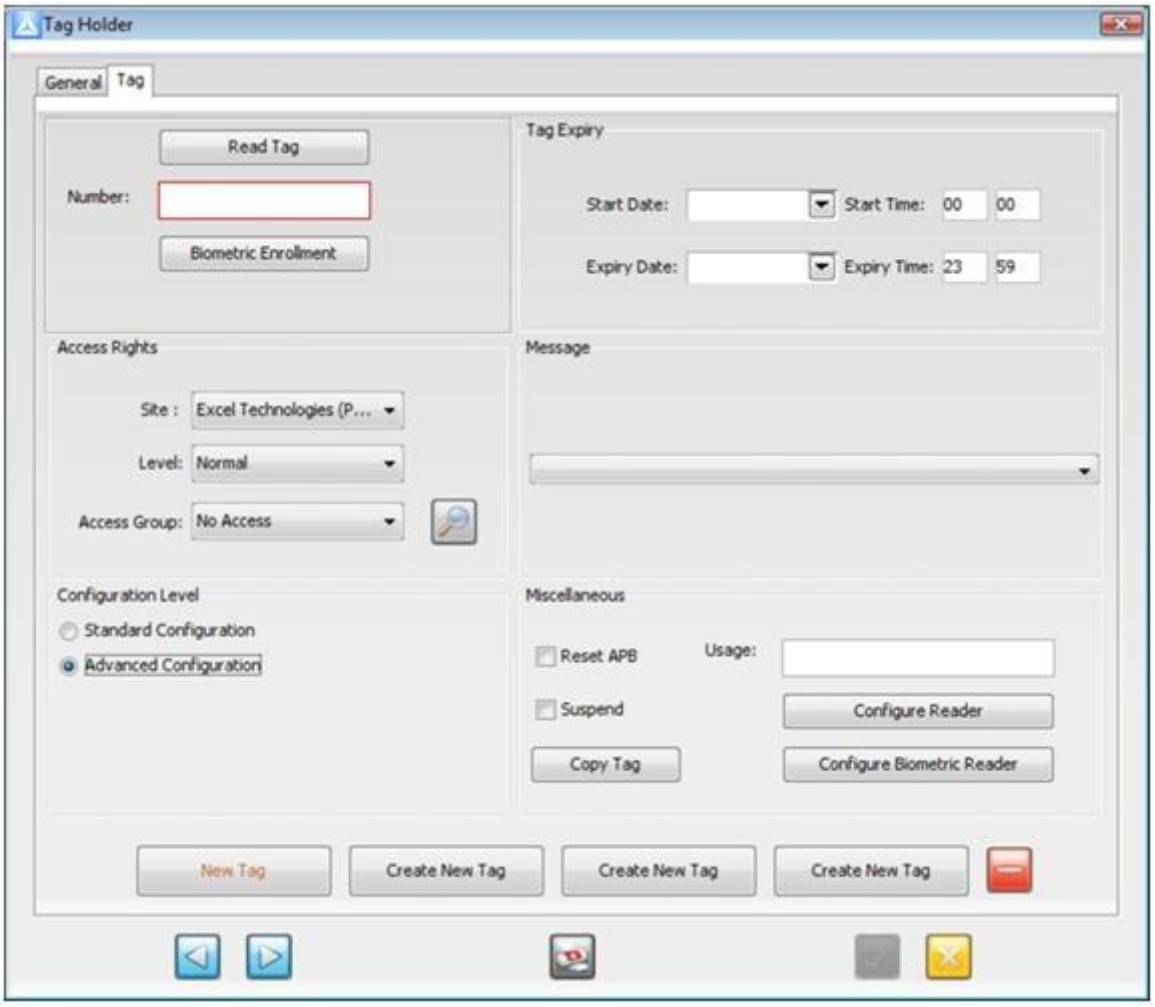


Figure 11 – Tagholder Dialog (Showing the Tag Tab)

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 Nexus 220 Software detects the Tag, the Tag number displays in the **Number** textbox.*

Access Rights Configuration

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

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 37.*

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

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.
- **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 VIII – 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 Nexus 220 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 VI – Nexus 220 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 T**agholder**>**Batch Tagholders**.

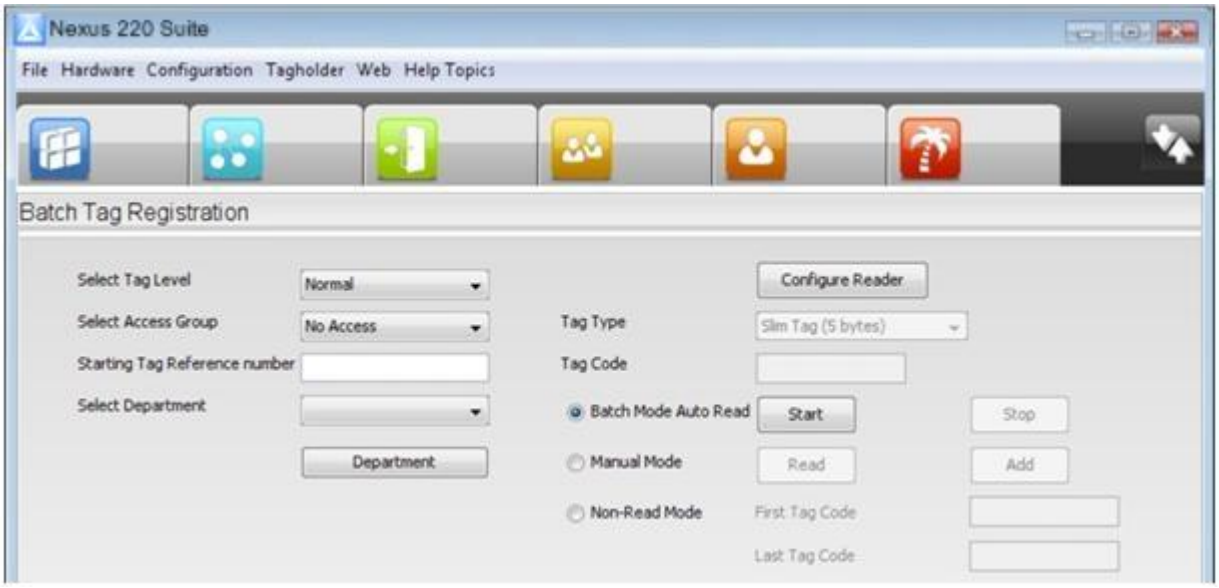


Figure 12 – Batch Tag Registration Configuration Pane

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** if needed.

The Start 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 number displays in the **Tag Code** textbox.
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.

Advanced Search

To search for a Tagholder, continue as follows:

1. Select the Page Tab.
2. From the **Search By** drop-down list, select a search field, for example:
   - **First Name**—searches the First Name column for a matching record.
   - **Last Name**—searches the Last Name column for a matching record.
   - **Address**—searches the Address column for a matching record.
   - **Company**—searches the Company column for matching records.
   - **Department**—searches the Department column for matching records.
   - **Tag**—searches the Tag column for the matching Tag code.
3. Enter a suitable keyword in the **Value** textbox.

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

6 Holidays

Holidays are days or periods when access to a Site is restricted to Administrators. 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.

Add, Edit, or Delete a Holiday

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

1. Select the Page Tab.
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

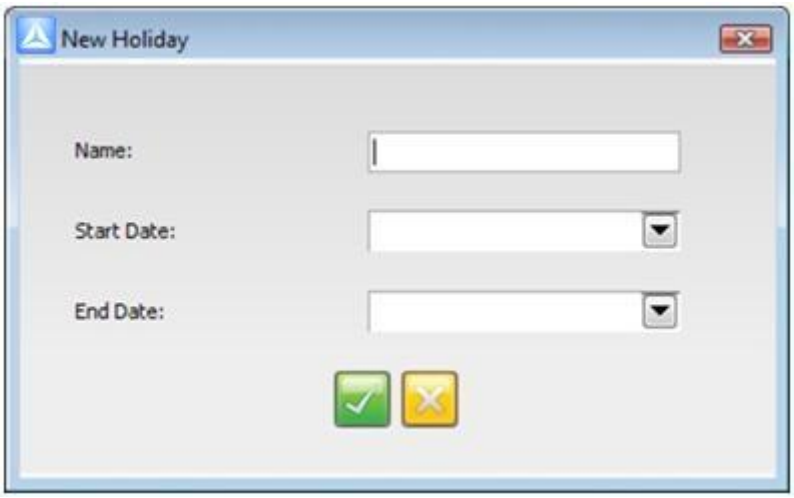


Figure 13 – New Holiday Dialog

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 Nexus 220 Controller when used with a Liquid Crystal Display (LCD). After adding a Message record, this Message appears on the Messages drop-down list (displayed on the Tagholders dialog). For more information, see page 32.

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

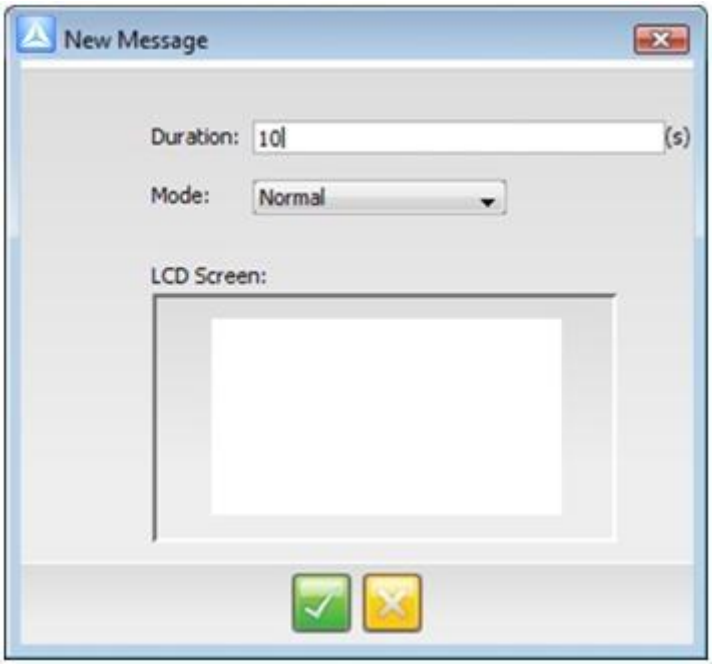


Figure 14 – New Message Dialog

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.
2. In the **LCD Screen** text area, enter the Message text.
3. 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.

Add, Edit, or Delete a Reason Code

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

4. From the Main Menu, select **Configuration**>**Reason Codes**.
5. 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.
6. In the Reason Codes Configuration Pane, click the button.

Configure Reason Codes

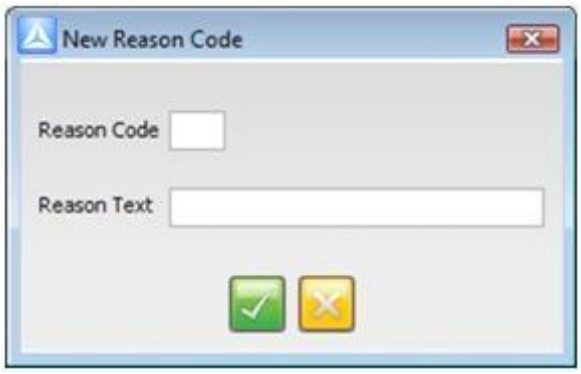


Figure 15 – New Reason Code Dialog

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.
2. In the **Reason Text** textbox, enter the Reason Code's text.
3. Click the button.

Modes of Operation

The Nexus 220 System provides five “Modes of Operation”. These Modes are selected via the PC Software.

Power Control Mode

Refer to the Alarm Relay’s maximum current and voltage ratings listed in the Nexus 220 Controller’s Hardware Installation Manual and Product Specification Catalogue.

In this Mode, the Alarm Relay (on the Nexus 220 Controller) switches on or off various building devices, such as lights or air conditioners. Use an external switching device to remove the dangers of high voltage from the terminal connector, and also to handle the high current associated with these devices.

The “Emergency Open” input unlocks all doors in the System.

Activating Power Control Mode

After setting up your Site, Controllers and Doors continue as follows to activate Power Control Mode:

Refer to the Nexus 220 Controller’s Hardware Installation Manual for connection details relating to this Mode.

To activate Power Control Mode, there must be at least one Anti-passback (APB) Zone. The Controller will count the number of Tags inside the Zone(s) and switch off the Alarm Relay when the count is zero.

1. Select the Page Tab.
2. From the Mode Configuration (Optional) group, ensure that the **Power Control** radio button is selected (default).
3. Click the button.
4. Select the Page Tab.
5. If not already selected, select the **Advanced Configuration** radio button.
6. From the Alarm Arm group, select **Enable**.
7. Click the button.

Alarm Mode

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

Activating Alarm Arm Mode

After setting up your Site, Controllers and Doors continue as follows to activate Alarm Arm Mode:

Refer to the Nexus 220 Controller's Hardware Installation Manual for connection details relating to this Mode.

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

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 intrusion alarm is required.

Activating Intrusion Mode

After setting up your Site, Controllers and Doors continue as follows to activate Intrusion Mode:

Refer to the Nexus 220 Controller's Hardware Installation Manual for connection details relating to this Mode.

3. Select the Page Tab.
4. From the Mode Configuration (Optional) group, select the **Intrusion** radio button.
5. Click the button.

Bell Button Mode

In this Mode, the Bell Button on the Amano (KMA) Mullion Keypad Antenna Reader, when pushed, drives Relay 3 on the Nexus 220 Controller.

Activating Bell Button Mode

Continue as follows to activate Bell Button Mode:

Refer to the Nexus 220 Controller's Hardware Installation Manual for connection details relating to this Mode.

1. Select the Page Tab.
2. From the Mode Configuration (Optional) group, select the **Bell Button** radio button.
3. Click the button.
4. Select the Page Tab.
5. From the Doors column, select the **Door** using the Amano KMA Antenna Reader.
6. If not already selected, select the **Advanced Configuration** radio button.
7. Select the **Enable Bell** checkbox.
8. Click the button.

Action Mode

Use this Mode to drive Relay 3 when using the Building Management feature.

Activating Action Mode

Continue as follows to activate the Action Mode:

Refer to the Nexus 220 Controller's Hardware Installation Manual for connection details relating to this Mode.

1. Select the Page Tab.
2. From the Mode Configuration (Optional) group, select the **Action** radio button.
3. Click the button.

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

Preference Configuration

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

- **General Tab**—lets you select the Nexus 220 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 Nexus 220 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 Nexus 220 Software stores the Tag Code and not the Tag Type. Pre Nexus 220 V1.80 you enrolled each Amano (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**.

Setting Your Preferences

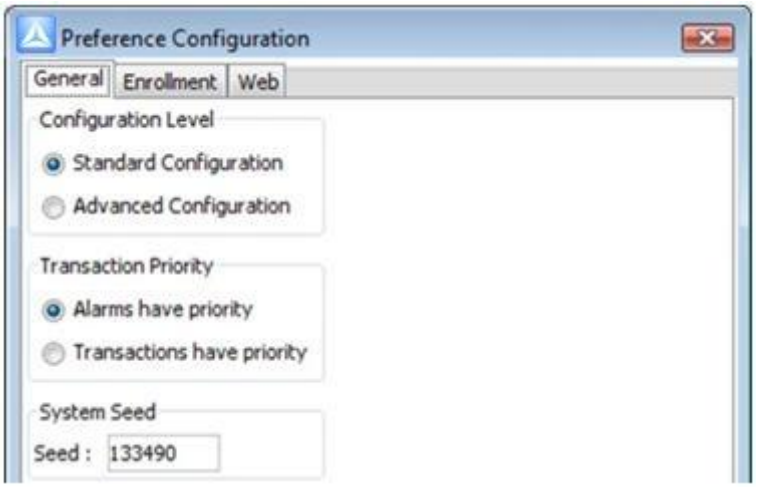


Figure 16 – Preference Configuration Dialog

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

General Tab

1. Select the **General** Tab.
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 Nexus 220 Software display all advanced settings. By selecting the **Standard Configuration** radio button, you elect that the Nexus 220 Software display only standard settings, greying out the 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 Nexus 220 Software give Alarms the highest priority. By selecting the **Transactions have Priority** radio button, you elect that the Nexus 220 Software give Transactions the highest priority.*

Enrollment Tab

1. Select the **Enrollment** Tab.
2. Select either the **Tag Type is Ignored when Validating a Tag** or **Tag Type is Taken into Consideration when Validating a Tag** radio button.

*By selecting the **Tag Type is Ignored when Validating a Tag** radio button, you elect that the Nexus 220 Software activate the AnyTag Mode. In this Mode, the Nexus 220 Software stores the Tag Code and not the Tag Type. Pre Nexus 220 V1.80 you enrolled each Amano (QT) Quad Transmitter Tag twice (once for RF and once for the Passive Tag), using AnyTag Mode, you only enroll the Tag once.*

3. After changing from **Tag Type is Ignored when Validating a Tag** to **Tag Type is Taken into Consideration when Validating a Tag** ensure that you perform a Full Upload. (See Page 44 for more information).
4. Make your selection from the **3rd Party Tag and Any Tag, Tag Code Truncation** group. (See **Part VIII – Integration Modules** for more information on using this Preference).

Web Tab

1. Select the **Web** Tab.
2. Select either the **Anyone can View Web Reports** 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.*

2. Click the button.

7 Full Upload

A Full Upload writes data from the Site Database to the Nexus 220 Controller.

Full Upload Procedure

After configuring your Nexus 220 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 SYSDBA user's roles include Site definition and configuration, while Operators carry out the day to day "operations" of the Nexus 220 System. The Manage Operator feature therefore lets you add extra operators thereby restricting access to features that may affect Sites or Operator Groups.

Note, an Operator does 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. Click the button.
3. In the **Tagholders without Login Privileges** dialog, select a Tagholder.
4. Click the button.

Figure 17 – User Configuration Dialog

5. In the User Configuration dialog, enter a **User Name** and **Password**.
6. Click the button.
7. 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 **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.

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 Nexus 220 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**.

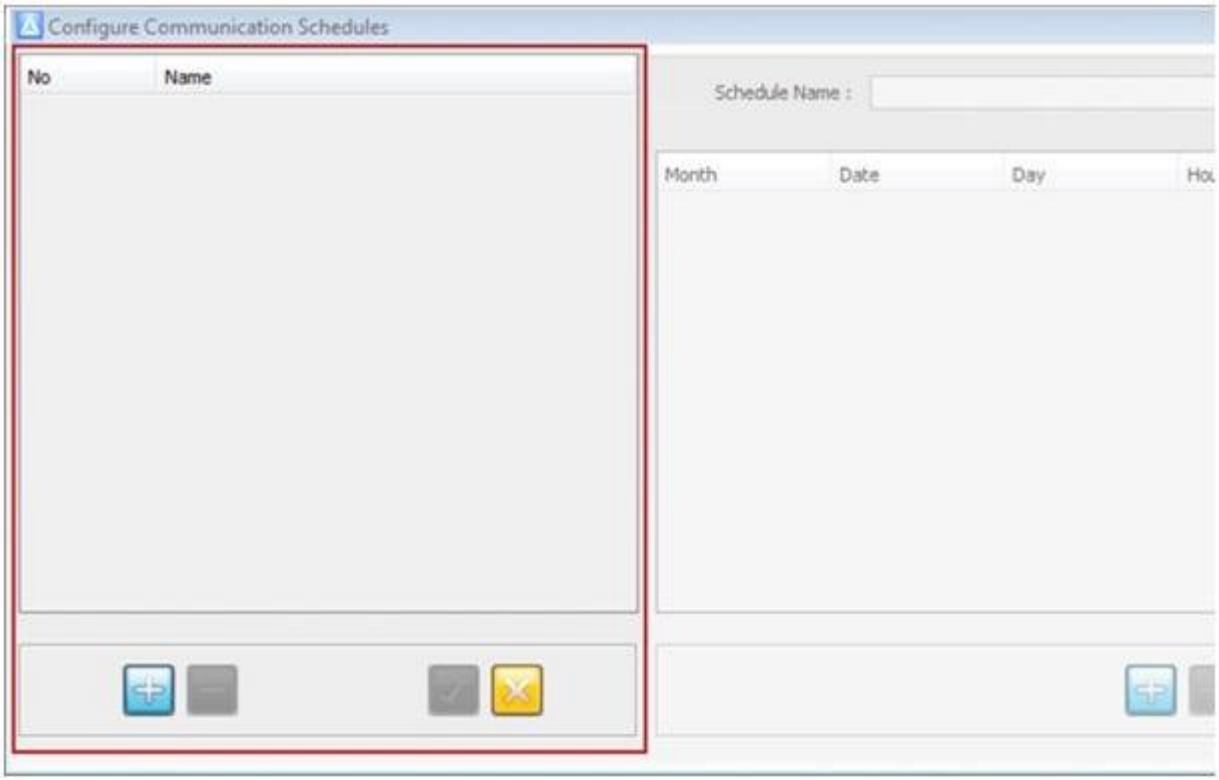


Figure 18 – Left-hand Side of the Configure Communication Schedules Dialog

2. Click the button (as highlighted in Figure 18).
3. In the **Schedule Name** textbox, assign your new Schedule a name.

4. Click the button (as highlighted in Figure 19).

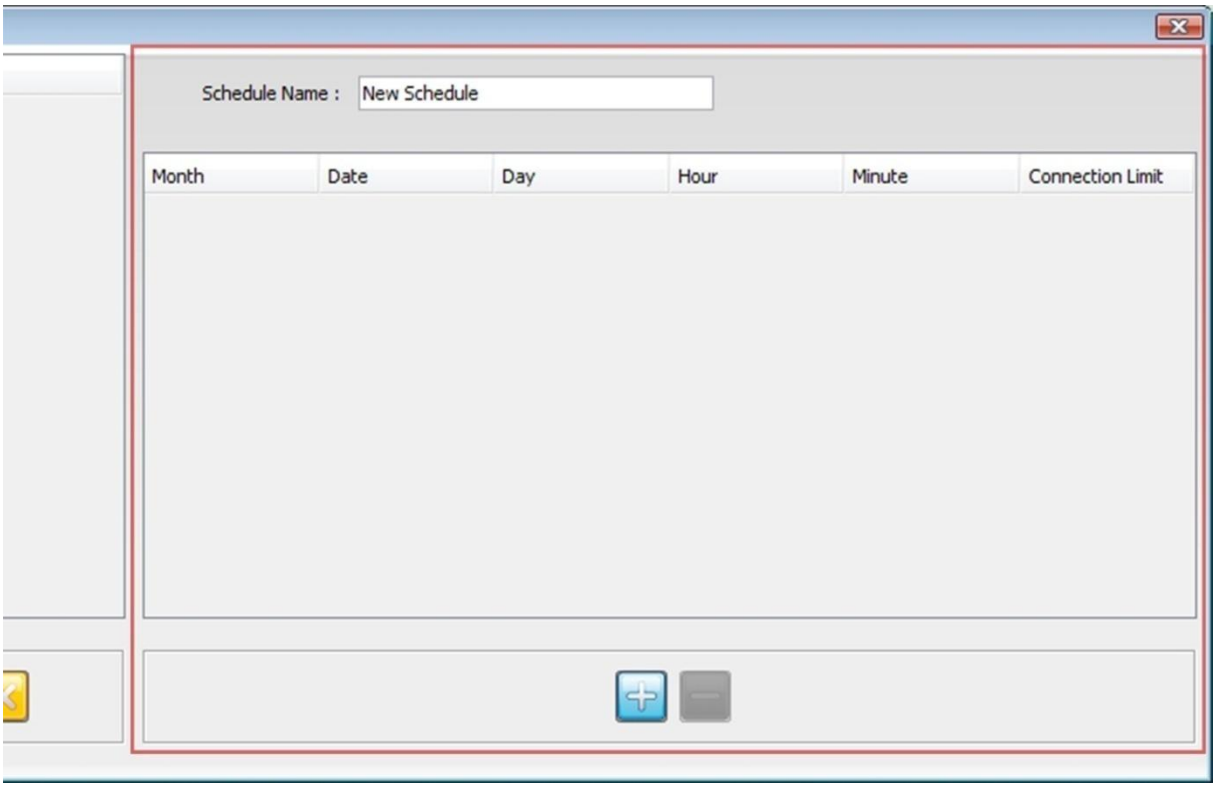


Figure 19 – Right-hand Side of the Configure Communication Schedules Dialog

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 Nexus 220 Software is running for the scheduled Site communication to take place.

Edit a Communication Schedule

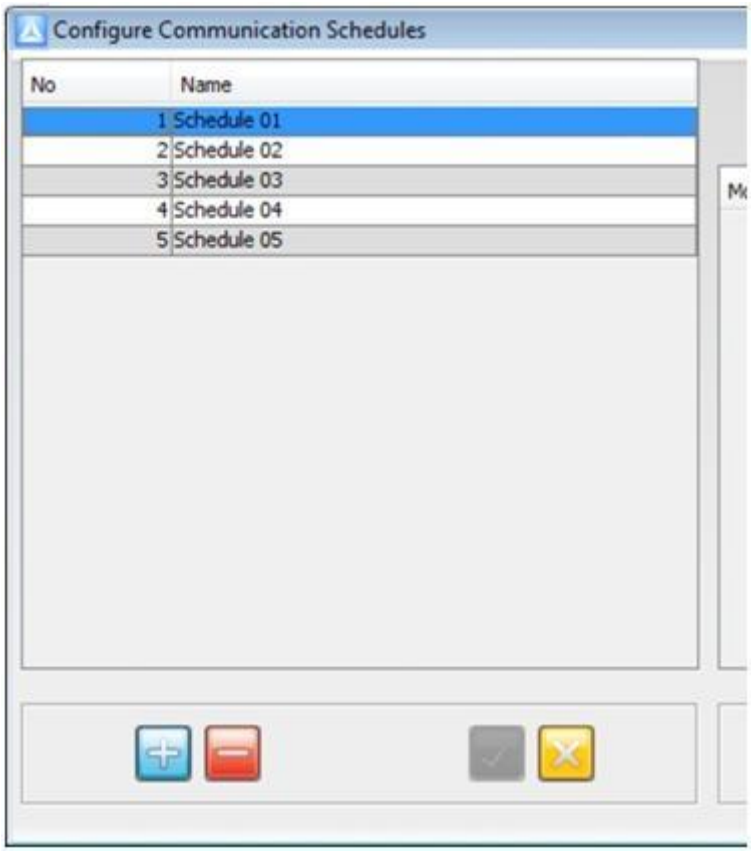


Figure 20 – Left-hand Side of the Configure Communication Schedules Dialog

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 20 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 20 for clarification).
3. Click the button.
4. Click the button.

Web Server Port Selection

By default the Web Server uses **Port 80**. In the event that Port 80 is already in use, change the port number as follows:

1. From the Main Menu, select **Web**>**Webserver Port**.

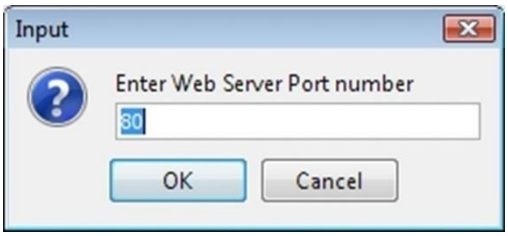


Figure 21 – Input Dialog

2. In the **Enter Web Server Port Number** textbox, enter a new port number.
3. Click the **OK** button.

Hardware Replacement

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

Using the Nexus 220 Software, continue as follows:

Uninstall OLD Hardware

1. From the Main Menu, select **Hardware**>**Replace Unit**.

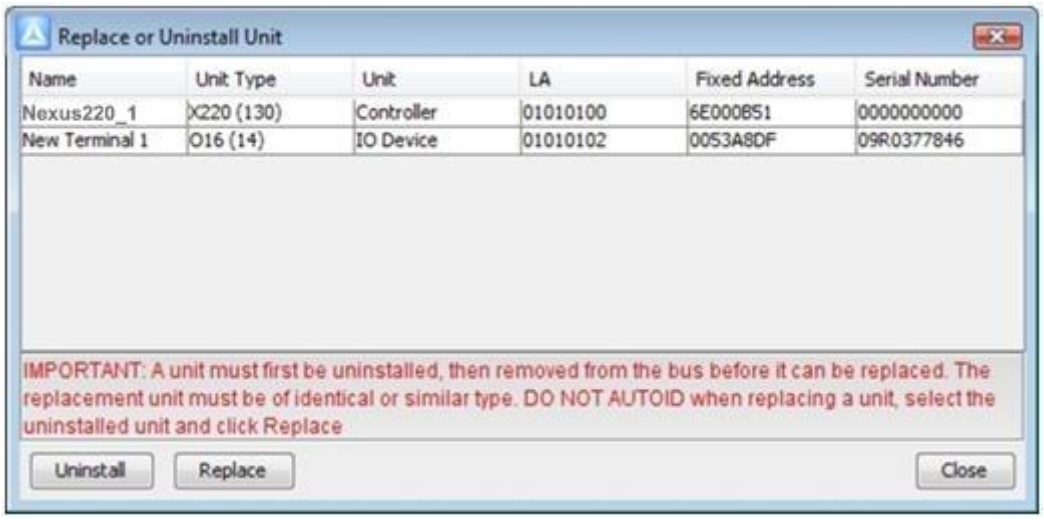


Figure 22 – Replace or Uninstall Unit Dialog

2. In the **Replace or Uninstall Unit** dialog, select the unit for replacement.
3. Click the **Uninstall** button.
4. At the Uninstall Unit dialog, click the **Yes** button.
5. Disconnect the ***OLD* Hardware**.
6. At the Uninstall Unit 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. Replacing any one of these results in the Fixed Address of the other devices also being uninstalled.

Install Replacement (NEW) Hardware

When replacing a Controller (connected direct to the PC), ensure the new Controller uses the same COM Port number as the old Controller.

1. Click the **Replace** button.

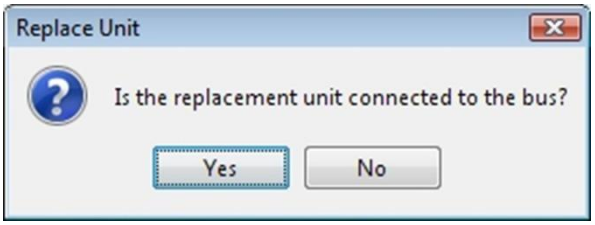


Figure 23 – Replace Unit Dialog

2. At the Replace Unit dialog, connect the ***NEW* Hardware**.
3. Click the **Yes** button.

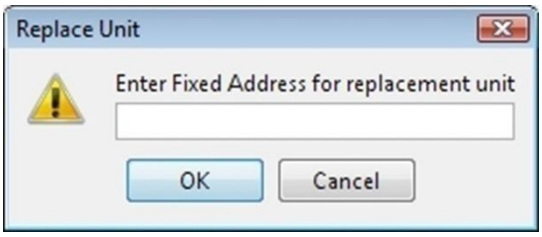


Figure 24 – Replace Unit Dialog

4. At the Replace Unit dialog, enter the new Hardware's **Fixed Address** into the textbox.
5. Click the **OK** button.
6. At the Replace or Uninstall Unit dialog, click the **Close** button.

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 Nexus 220 Software in their own language. The Nexus 220 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 25 – 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.

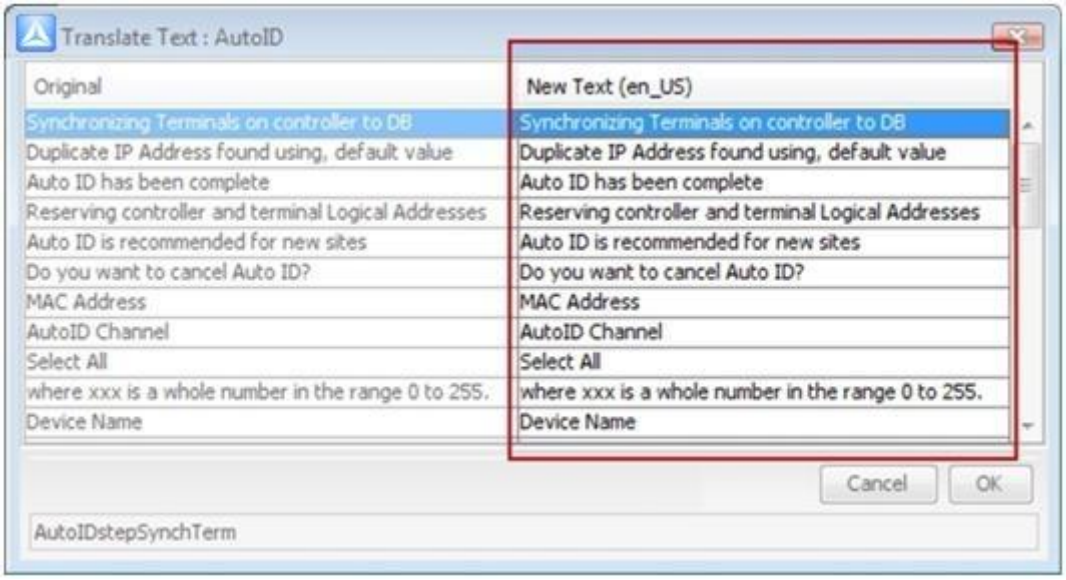


Figure 26 – Translate Text : Dialog

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 Nexus 220 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 27 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 27 – 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 Amano 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 Amano Database is registering the Database Server. The following examples refer to the default Database **DB220.FDB** used by the Nexus 220 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**>**Nexus220**>**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.

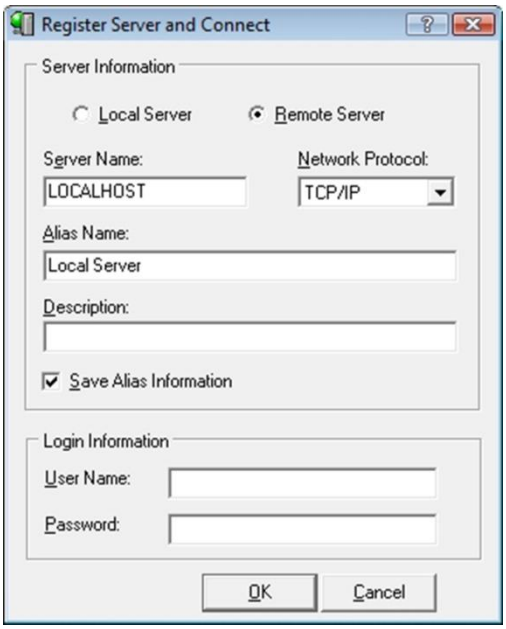


Figure 28 – Register Server and Connect Dialog

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 28 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

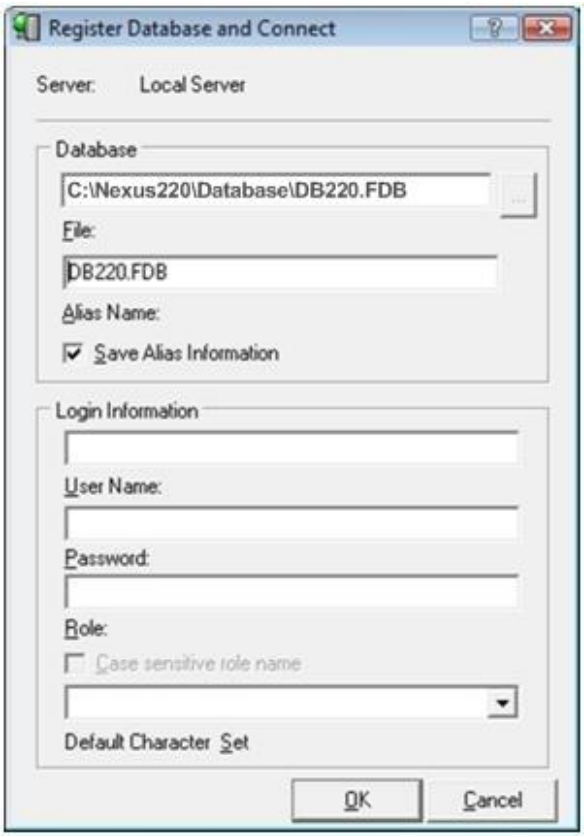


Figure 29 – Register Database and Connect Dialog

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 29).
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 Nexus 220 Software is: ***C:\Nexus220\Database\DB220.FDB***

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

Database Backups

Administrators of Amano 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 Nexus 220 Software.

The preferred method of making a backup, however, is to use the built in backup feature included in the Nexus 220 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 Nexus 220 Database is free from corruption. Ensure that you carry out regular database maintenance, thus ensuring that your Nexus 220 Database is not corrupt.

Backup of the Nexus 220 Database Using the Nexus 220 Software

1. In Windows®, click **Start**>**All Programs**>**Nexus220**>**Nexus220**.
2. From the Main Menu, select **File**>**Manage Backups**.

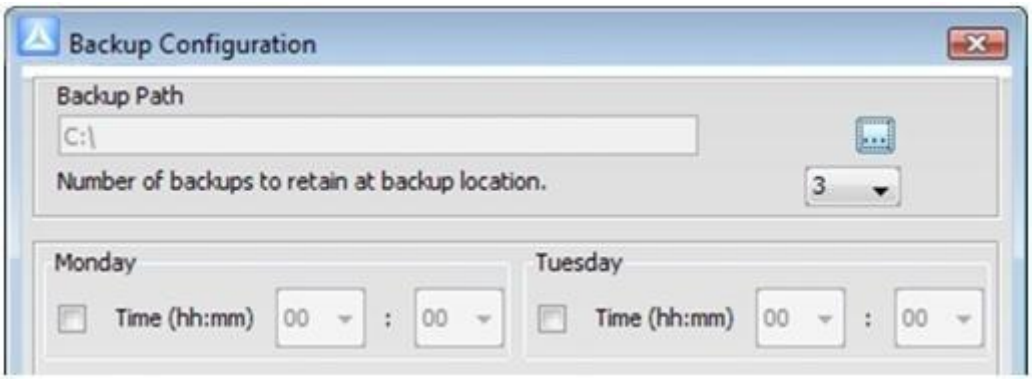


Figure 30 – Backup Configuration Dialog

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**.*

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 Nexus 220 Database using IBConsole

1. In Windows®, go to **Start**>**All Programs**>**Nexus220**>**Utils**>**IBConsole**.
2. From the Database drop-down menu, select **Maintenance**>**Backup / Restore**>**Backup**.

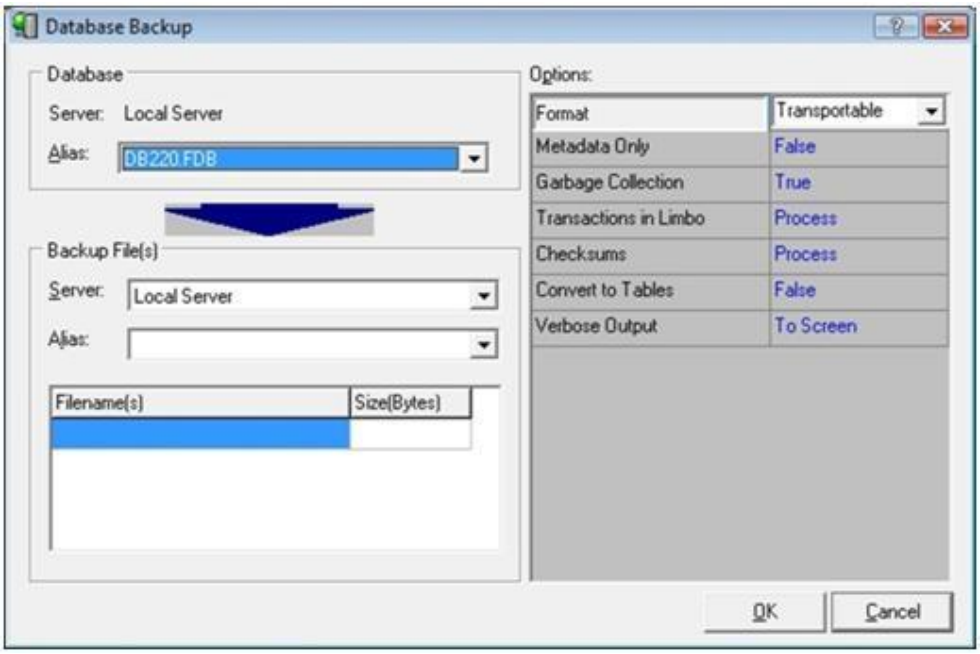


Figure 31 – Database Backup Dialog

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:\Nexus220\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 Nexus 220 Database Using a Batch File

Create the ".bat" File

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

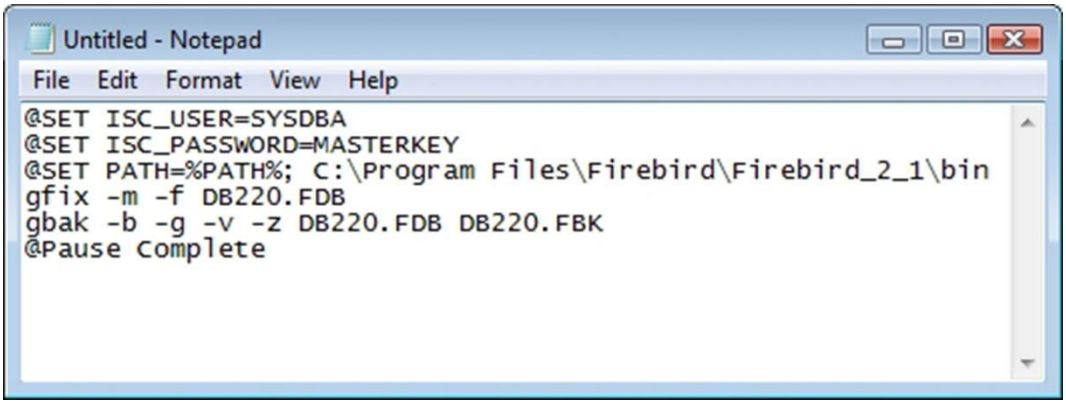


Figure 32 – Backup Using a Batch File

Settings explained:

- ***@SET ISC_USER=SYSDBA**—this sets the user name as SYSDBA, thus ensuring the backup utility connects to the Database.*
- ***@SET ISC_PASSWORD=MASTERKEY**—this sets the password. If you changed the default password, ensure that you use the new password.*
- ***@SET PATH=%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 Nexus 220 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 Nexus 220 Database Using IBConsole

Disconnect from the Database

1. In Windows®, go to **Start**>**All Programs**>**Nexus220**>**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**.

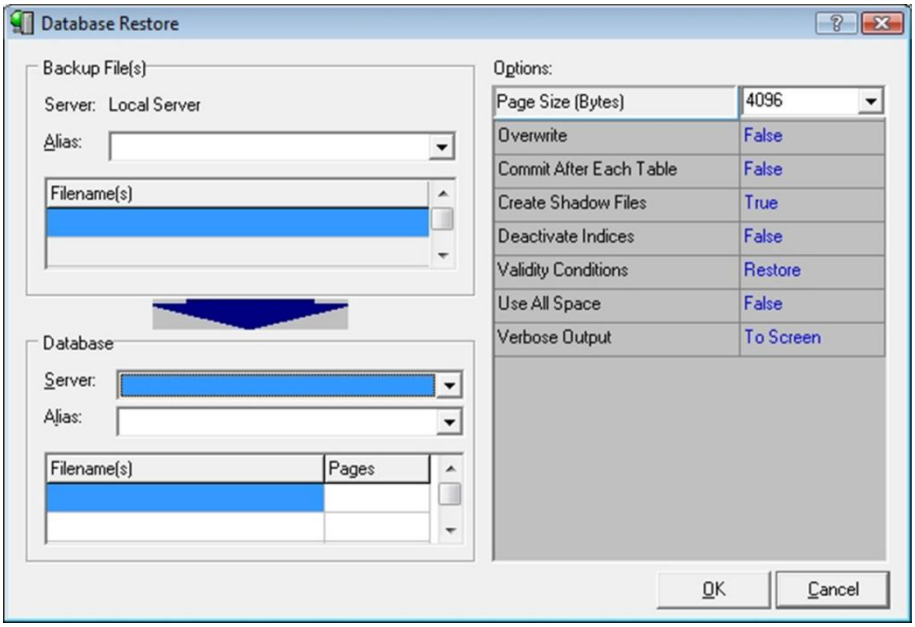


Figure 33 – Database Restore Dialog

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:\Nexus220\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:\Nexus220\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 Nexus 220 Database Using a Batch File

Create the ".bat" File

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

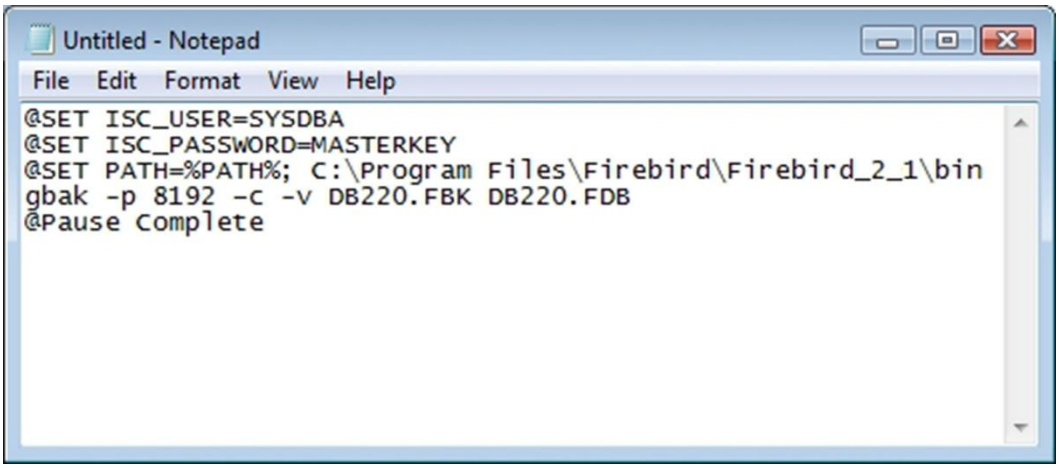


Figure 34 – Restore Using a Batch File

Settings explained:

- ***@SET ISC_USER=SYSDBA**—this sets the username as SYSDBA, thus ensuring the backup utility connects to the Database.*
- ***@SET ISC_PASSWORD=MASTERKEY**—this sets the password, if you changed the default password, ensure that you use the new password.*
- ***@SET PATH=%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 a **"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**.
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 Nexus 220 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.
   - Check for other processes trying to read the Database file. These are typically Virus and Spy-ware scanners, common on corporate PC's.
7. **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 Nexus 220 Database is corrupt, carry out an immediate backup and restore on the Database.

Checking and Repairing Minor Database Corruption

Follow these steps when checking and repairing minor corruption:

Carry out these steps regularly, 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).

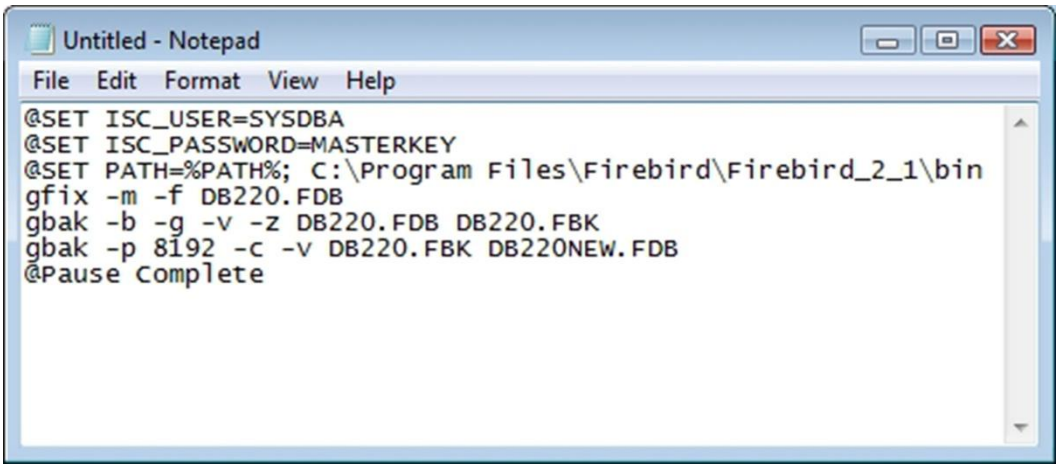


Figure 35 – "repair.bat" Batch File

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

Run the "repair.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 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. If the restore fails for any reason, perform the steps described in the section Recovering a Corrupt Database on page 67.

Recovering a Corrupt Database

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).

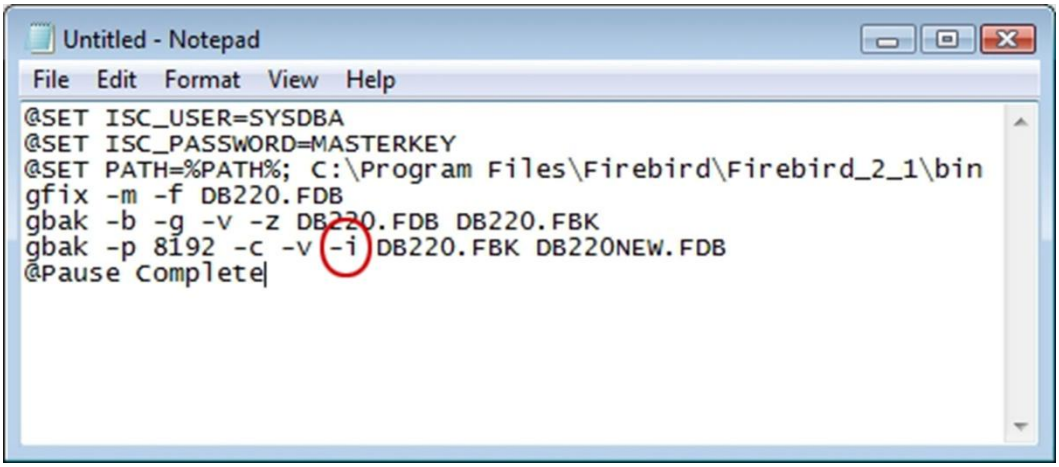


Figure 36 – Batch File

*The **-i** option highlighted in **gbak -p 8192 -c -v -i DB220.FBK DB220NEW.FDB**—restores the Database without indexes.*

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

Run the 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. If the restore fails for any reason, contact your nearest Amano support representative.

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.