PART 5 – ADVANCED CONFIGURATION

Contents

PART 5 – ADVANCED CONFIGURATION 1

CONTENTS 3

REGISTRATION INTERFACE LICENSING 5

Purpose of this Feature 5

Example 5

Procedure 5

COMMUNICATION CONFIGURATION 7

Purpose of this Feature 7

Example 7

Procedure 7

LIFT (ELEVATOR) CONTROL (BASE APPLICATION) 9

Purpose of this Feature 9

Example 9

Procedure 9

LIFT (ELEVATOR) CONTROL (IXP220 RICH CLIENT MODULE) 17

Purpose of this Feature 17

Example 17

Procedure 17

BUILDING MANAGEMENT 25

Purpose of this Feature 25

Example 25

Procedure 25

SECURE SOCKET LAYER (SSL) CONNECTION 31

Purpose of this Feature 31

Example 31

Procedure 31

LIVE VIDEO IMAGE CAPTURE 33

Purpose of this Feature 33
Procedure 33

Registration Interface Licensing

Purpose of this Feature

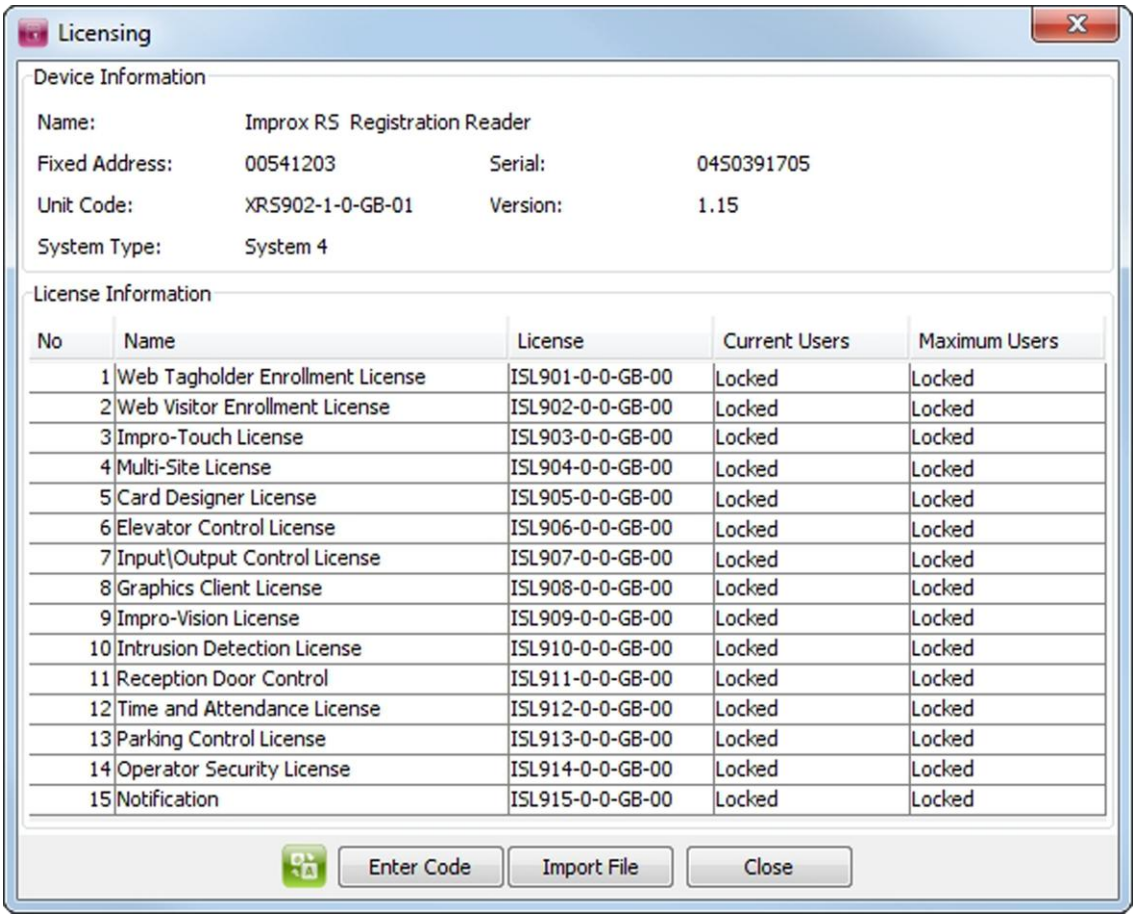
The **Registration Interface Licensing** feature enables the purchase of feature licenses (for use with System 3 and System 4 only).

Example

The following example procedure shows the use of this feature.

Procedure

Connect your ImproX RS Registration Interface before using the Registration Interface Licensing feature.



No	Name	License	Current Users	Maximum Users
1	Web Tagholder Enrollment License	ISL901-0-0-GB-00	Locked	Locked
2	Web Visitor Enrollment License	ISL902-0-0-GB-00	Locked	Locked
3	Impro-Touch License	ISL903-0-0-GB-00	Locked	Locked
4	Multi-Site License	ISL904-0-0-GB-00	Locked	Locked
5	Card Designer License	ISL905-0-0-GB-00	Locked	Locked
6	Elevator Control License	ISL906-0-0-GB-00	Locked	Locked
7	Input\Output Control License	ISL907-0-0-GB-00	Locked	Locked
8	Graphics Client License	ISL908-0-0-GB-00	Locked	Locked
9	Impro-Vision License	ISL909-0-0-GB-00	Locked	Locked
10	Intrusion Detection License	ISL910-0-0-GB-00	Locked	Locked
11	Reception Door Control	ISL911-0-0-GB-00	Locked	Locked
12	Time and Attendance License	ISL912-0-0-GB-00	Locked	Locked
13	Parking Control License	ISL913-0-0-GB-00	Locked	Locked
14	Operator Security License	ISL914-0-0-GB-00	Locked	Locked
15	Notification	ISL915-0-0-GB-00	Locked	Locked

Figure 1 – Licensing Dialog

Feature Licence Unlock Procedure

1. In the IXP220 Base Application, from the Menu Bar select **Help Topics**>**Licensing**.
2. Click the **Import File** button.
3. From the **Select Device XML File** dialog, select the downloaded XML (Web Store Unlock) File.

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

4. Click the **Open** button.
5. At the Unlock Successful dialog, click the **OK** button.
6. Click the **Close** button.

Communication Configuration

Purpose of this Feature

The **Communication Configuration** feature lets you change the Communication Port being used by your IXP220 Controller. That is, for example, moving your Controller from COM8 to COM17.

Make use of this feature when damage occurs to your IXP220 Controller along with its associated Communications Port (for example in the event of a lightning strike).

*We advise that only Network Administrators with knowledge of **Device Management** use this feature.*

Example

The following example procedure shows the use of this feature.

Procedure

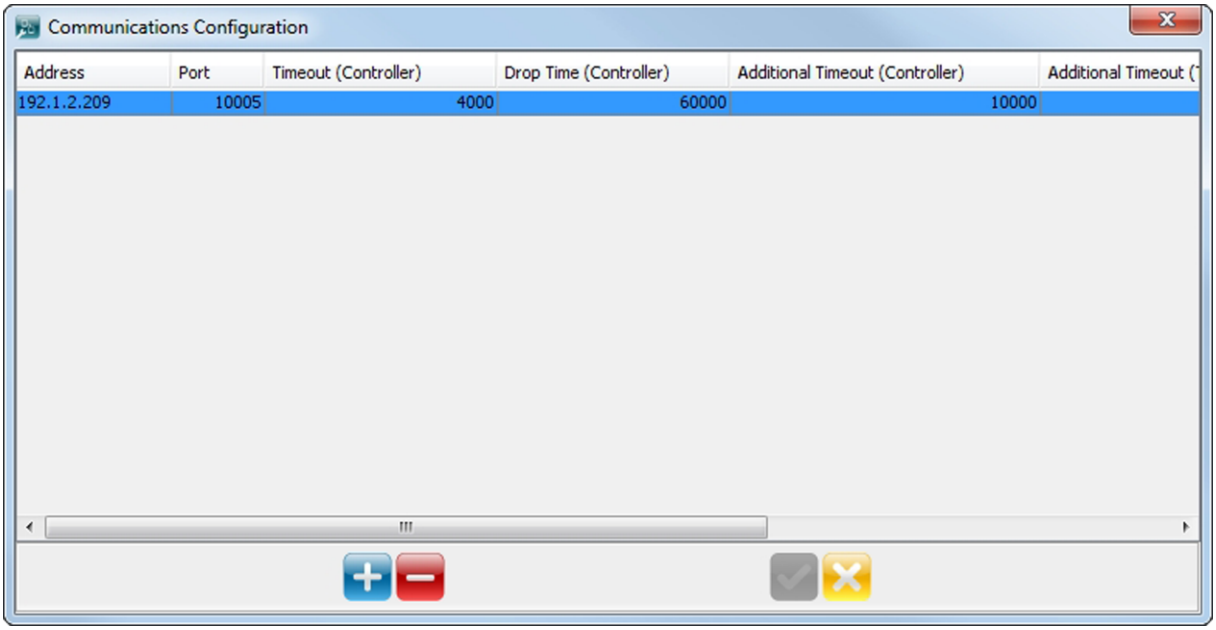


Figure 2 – Communications Configuration Dialog

1. In the IXP220 Base Application, from the Menu Bar select **Hardware**>**Communications**.
2. Double-click your mouse in the **Address** column, over the record for editing.
3. Edit the **Communication Port** number as per your requirements.

The Communications Configuration Dialog, also lets you change the following settings:

- ***Timeout (Controller)****—is the duration for which the Base Application waits for a reply from a Controller. Increase this if using a WAN, a slow connection, Radio Modems, and so on. (For example, use a setting of 5 000 for EtherPADs). Also increase this setting if you receive many 'Controller Timeout' messages.*
- ***Drop Time (Controller)****—the duration for which the Controller will be dropped if it times out. This setting rarely requires change.*
- ***Additional Timeout (Controller)****—an extra timeout value for increasing timeouts on the Controller bus. Increase this when fast polling Controllers across a WAN, a slow connection, Radio Modems, and so on. (For example, use a setting of 500). Ideally, disable fast polling for a WAN, a slow connection, Radio Modems and so on.*
- ***Additional Timeout (Terminal)****—an extra timeout value for increasing timeouts on the Communications bus. Set this when Terminals are on a different network to the Controller. For example, when a Controller connects to a Terminal across a WAN.*
- ***Inter Poll Delay****—the delay between successive polls. Use this to poll less often thus reducing network traffic over EtherPADs on a WAN (for example, use a setting of 2 000).*
- ***IC Port****—displays the inter-controller communications port number, that is the port used when controllers communicate with one another.*
- ***Respond Address****—displays the IP Address the IP Terminals use to communicate with the Controller.*

4. Click the button.

Lift (Elevator) Control (Base Application)

Purpose of this Feature

The **Lift (Elevator) Control** feature lets you setup Lift (Elevator) Control in your IXP220 System.

Using Lift (Elevator) Control, control access by a Lift (Elevator) to various floors in a building so a Tagholder can only select the floor or floors that they have access rights to.

The IXP220 Software supports configuration of up to 8 Lifts (Elevators) per Site with a maximum of 32 floors per Lift (Elevator).

Example

1. Install a Reader inside the Lift (Elevator).
2. Wire the ImproX O16 Terminals so that each Lift (Elevator) button is in series with the respective Relay on the ImproX O16 Terminal.
3. Create the required Access Groups allowing access to the necessary floors.
4. Give the respective access rights to the Tagholders that need access to these floors.

When the Tagholder presents their Tag to the Entry Reader in the Lift (Elevator), the buttons for the assigned floors light up allowing selection of the floor.

Procedure

Door Configuration

Ensure that you unlock your Registration Interface for Elevator Control before using this feature. This unlock allows for a maximum of 1 seat. See page 5 of this section for more information.

1. In the IXP220 Base Application, select the Page Tab.
2. Select the **Lift (Elevator)** Tab.
3. Click the button.

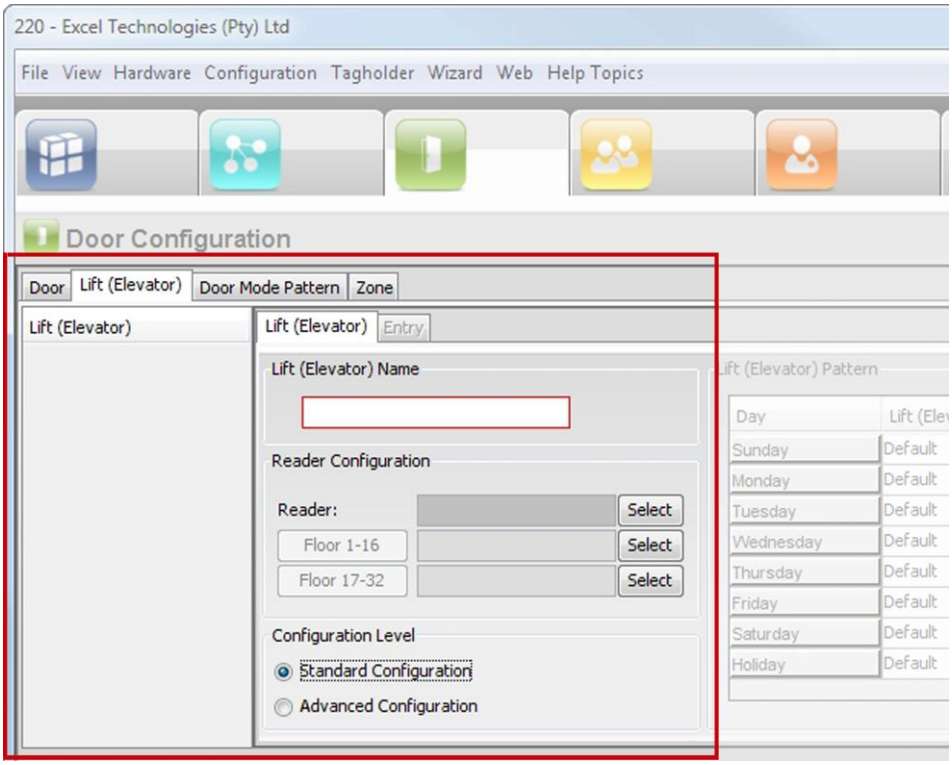


Figure 3 – Left-hand Side of the Door Configuration Pane

4. In the **Lift (Elevator) Name** textbox, assign a suitable name. This textbox has a 16 character limit.
5. Click the **Select** button alongside the **Reader** textbox.
6. In the **Unassigned Readers** dialog, from the list of displayed records, select the Lift (Elevator) Reader.
7. Click the button.
8. Click the **Select** button alongside the **Floor 1-16** textbox.
9. In the **Unassigned Readers** dialog, from the list of displayed records, select the O16 Terminal that corresponds to the Lift (Elevator).
10. Click the button.
11. Click the **Floor 1-16** button.
12. In the Floor Name Configuration dialog, in the **Name** textbox, assign a suitable name.
13. Assign **Floor Names** to the Relays.

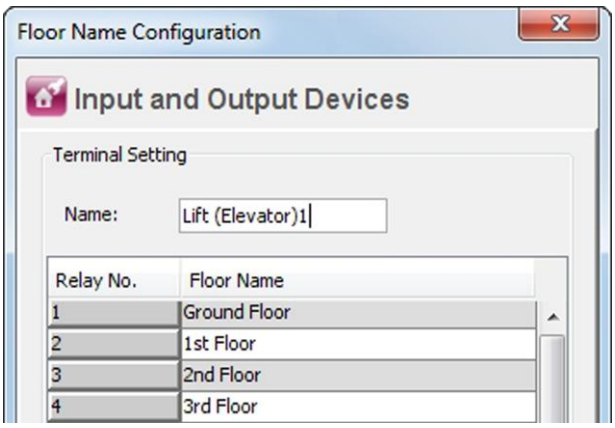


Figure 4 – Floor Name Configuration Dialog Showing Relay Assigned to Floor

Rather than entering the floor number, you may assign your floors names.

14. Click the button.
15. Click the button.
16. Click the **Floors 17-32** button and repeat steps 11 to 13 for these floors if required.

When using Lift (Elevator) Control across multiple Lifts (Elevators), Lift (Elevator) buttons must connect to the ImproX 016 Terminal's output Relays in the same order for each Lift (Elevator).

17. 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.
18. Click the button.

Entry Reader Configuration

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.

1. Select the **Entry** Tab.
2. 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.
3. 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.
4. 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.
5. Edit the **Strike Duration (0.1s)** textbox, the default value is **40** (0.1s). Setting the Strike Duration to **55555** toggles the Relay.
6. Edit the **Open Duration(s)** textbox. By default, the Open Duration is set to **0**, disabling the Door Open Sensor (DOS).
7. 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.

8. From the **ON VALID Tag** group, from the LED Action drop-down list, select the required LED colour state and Duration.
9. From the **Buzzer Volume** drop-down list, select the Buzzer volume and Duration.

10. From the **ON INVALID 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. Click the button.

Configure Lift (Elevator) Mode Pattern

The IXP220 Software supports a maximum of 8 Door Mode Patterns at each Door.

This setting regulates the Lift's (Elevator's) operating mode including the start and end time. Continue as follows to add a new Lift (Elevator) 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. Your Door Entry Code may range from between **1 to 65535**. After entering the Door Entry Code at the Reader or Terminal, complete the entry by pressing the # key.*
- ***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**. After entering your Personal Access Code at the Reader or Terminal, complete the entry by pressing the # key.*

   - **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 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.
- **LED**—sets the LED's behaviour during the stipulated time slot.

7. Click the button.

Advanced Configuration

On selecting the **Advanced Configuration** radio button, the Lift (Elevator) Patterns and Zone settings activate. Configure the following settings:

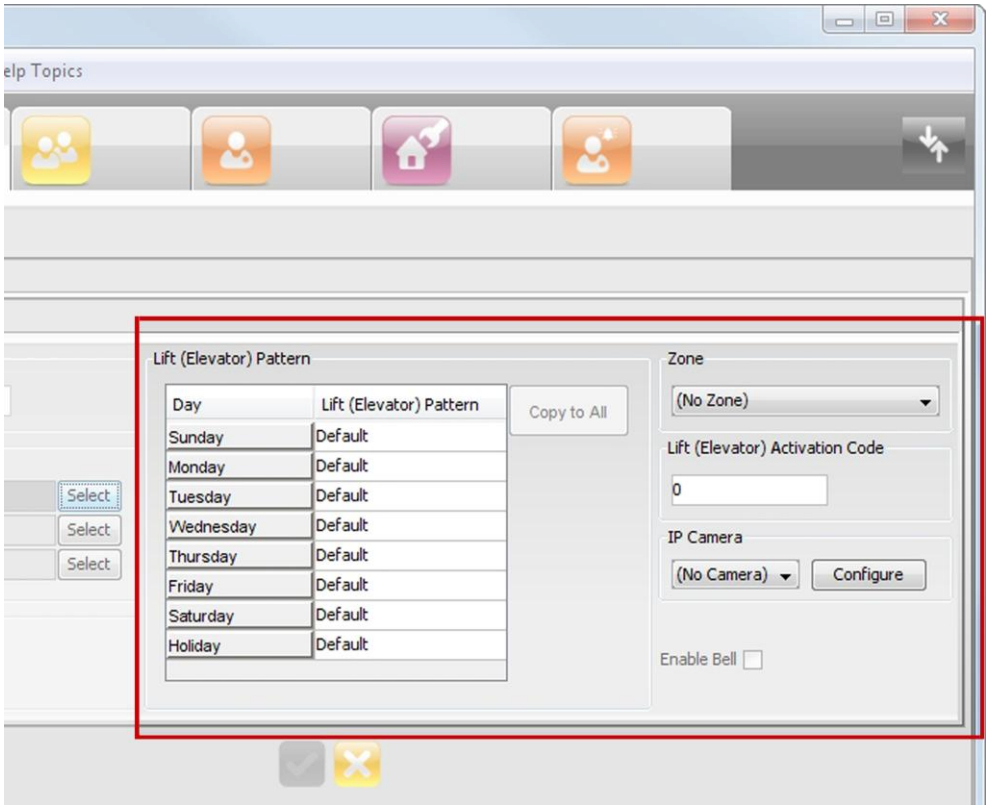


Figure 5 – Right-hand Side of the Door Configuration Pane

1. On the Configuration Pane, select the **Lift (Elevator)** Tab.
2. In the **Lift (Elevator) Pattern** group (see Figure 5), make your selections from the Day's Lift (Elevator) Mode Pattern drop-down lists.
3. In the **Zone** group, select a Zone from the drop-down list.

*Using a **Lift (Elevator) Activation Code** allows Tagholders to enter or exit a Lift (Elevator) using a numeric code. Note, however, Tags with access permissions for the Lift (Elevator) are still acknowledged by the Reader. Activate the Lift (Elevator) Activation 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 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 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 Configuration Pane, select the **Lift (Elevator)** Tab.*
9. *In the **Lift (Elevator) Activation Code** textbox, enter a 5 digit numeric code.*

CCTV integration allows for better end user site management, that is in areas with rising crime, your operator 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 **Lift (Elevator)** 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 Lift (Elevator) from the list of available Lift (Elevator) records.*
10. *From the **IP Camera** drop-down list, select a Camera record, thus associating the Lift (Elevator) and IP Camera.*
11. *Click the button.*

4. Click the button.

Access Group Configuration

Lift (Elevator) Access Tab

Ensure that all Lifts (Elevators) in a Lift (Elevator) Access Group go to the same floors. Note, you need not use all Lifts (Elevators). Selecting floors from a single Lift (Elevator), the selection works as normal.

When using distributed templates along with biometrics, after editing the Lift (Elevator) Access Group, ensure you perform a full upload. Refer to Part 3 – General Configuration for more information on performing a full upload.

1. Select the Page Tab.

2. Select the **Lift (Elevator) Access** Tab.

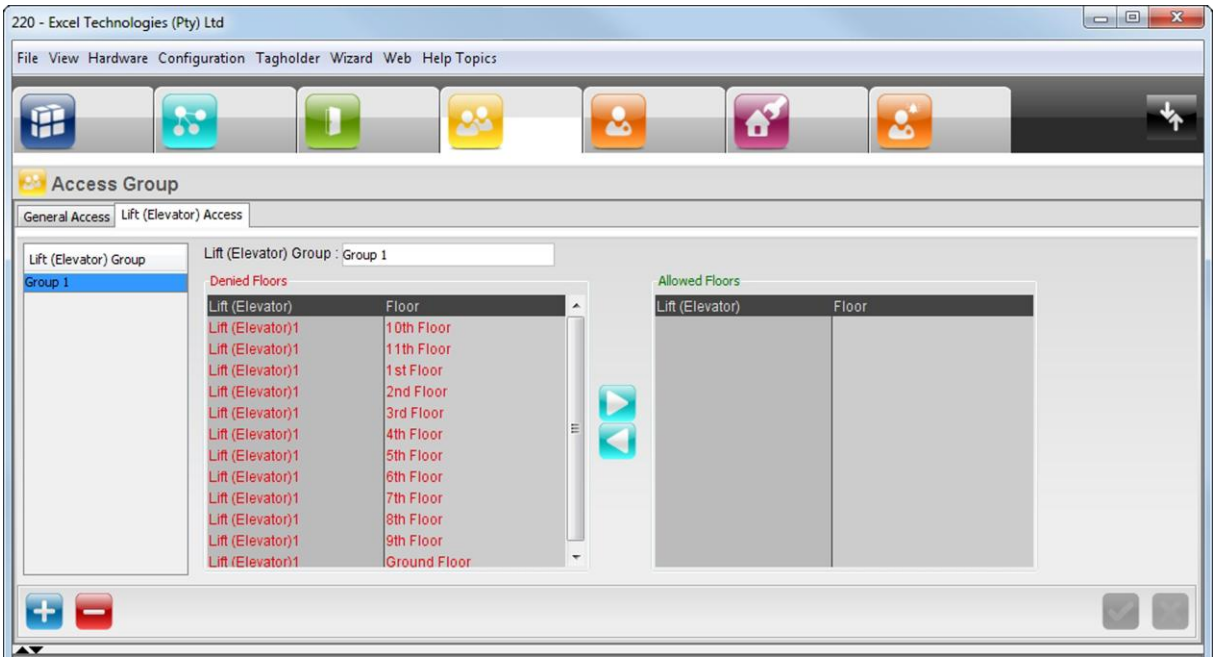


Figure 6 – Access Group Configuration Pane

3. Click the button.
4. In the **Lift (Elevator)** group textbox, assign a suitable name.
5. From the **Denied Floors** group, multi-select the Lifts (Elevators) and Floors to which you want to assign access.
6. Click the button.

Return wrongly selected Lifts (Elevators) and Floors to the Denied Floors group by clicking the button.

7. Click the button.

General Access Tab

1. Select an Access Group as created in Part 3 – General Configuration.
2. From the **Lift (Elevator)** group drop-down list, make your selection.
3. Click the button.

Lift (Elevator) Control (IXP220 Rich Client Module)

Purpose of this Feature

This procedure lists the steps involved in setting up **Lift (Elevator) Control** through the IXP220 Rich Client Module.

Using Lift (Elevator) Control, control access by a Lift (Elevator) to various floors in a building so a Tagholder can only select the floor or floors that they have access rights to.

The IXP220 Software supports configuration of up to 8 Lifts (Elevators) per Site with a maximum of 32 floors per Lift (Elevator).

Example

1. Install a Reader inside the Lift (Elevator).
2. Wire the ImproX O16 Terminals so that each Lift (Elevator) button is in series with the respective Relay on the ImproX O16 Terminal.
3. Create the required Access Groups allowing access to the necessary floors. This step is only available through the IXP220 Base Application.
4. Give the respective access rights to the Tagholders that need access to these floors.

When the Tagholder presents their Tag to the Entry Reader in the Lift (Elevator), the buttons for the assigned floors light up allowing selection of the floor.

Procedure

Door Configuration

Ensure that you unlock your Registration Interface for Elevator Control and Web Enrollment before using this feature. This unlock allows for a maximum of 1 seat. See page 5 of this section for more information.

1. In the IXP220 Rich Client Module, select the Page Tab.
2. Select the **Lift (Elevator)** Tab.
3. Click the button.

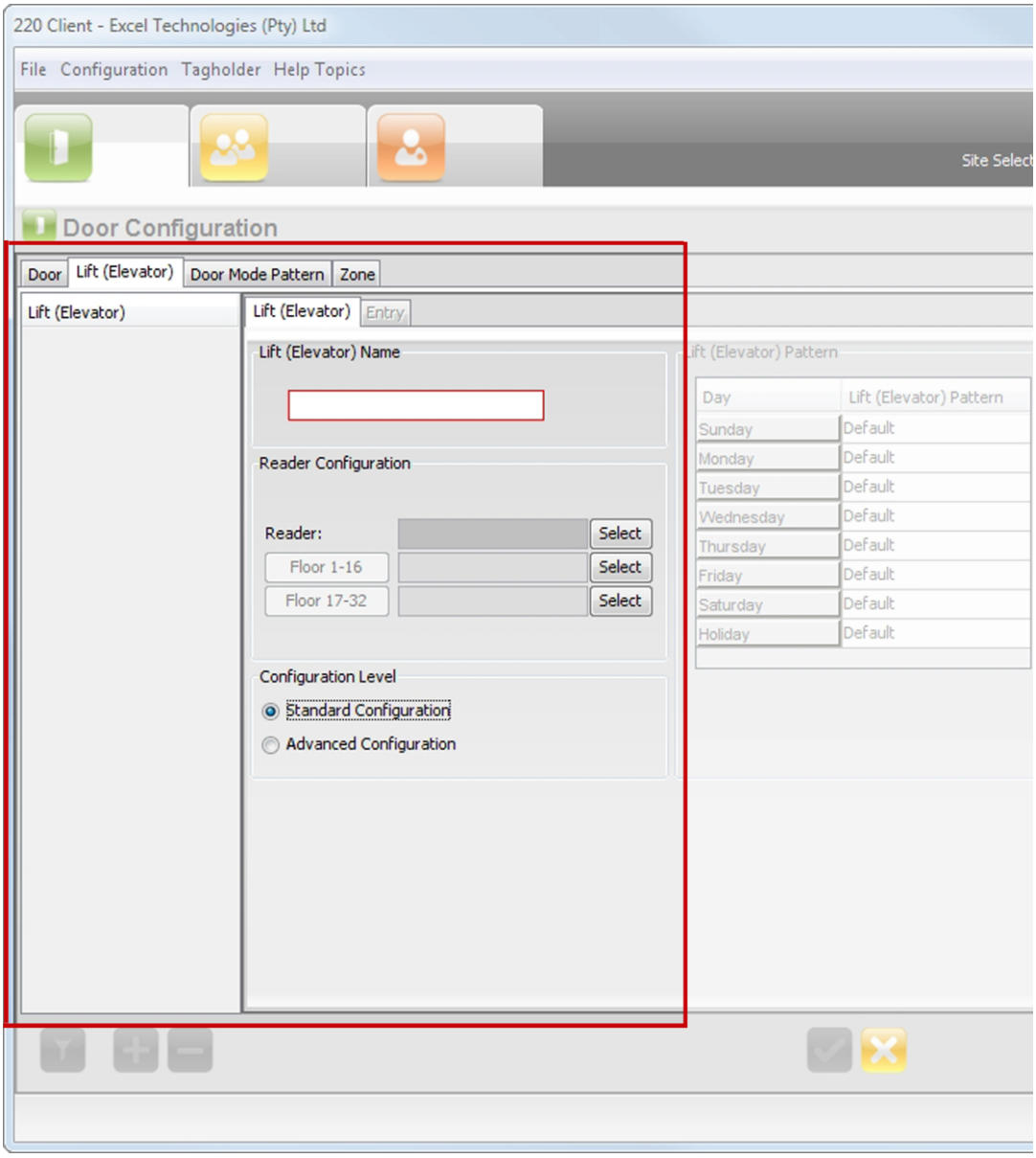


Figure 7 – Left-hand Side of the Door Configuration Pane

4. In the **Lift (Elevator) Name** textbox, assign a suitable name. This textbox has a 16 character limit.
5. Click the **Select** button alongside the **Reader** textbox.
6. In the **Unassigned Readers** dialog, from the list of displayed records, select the Lift (Elevator) Reader.
7. Click the ✅ button.
8. Click the **Select** button alongside the **Floor 1-16** textbox.
9. In the **Unassigned Readers** dialog, from the list of displayed records, select the O16 Terminal that corresponds to the Lift (Elevator).
10. Click the ✅ button.
11. Click the **Floor 1-16** button.
12. In the Floor Name Configuration dialog, in the **Name** textbox, assign a suitable name.
13. Assign **Floor Names** to the Relays.

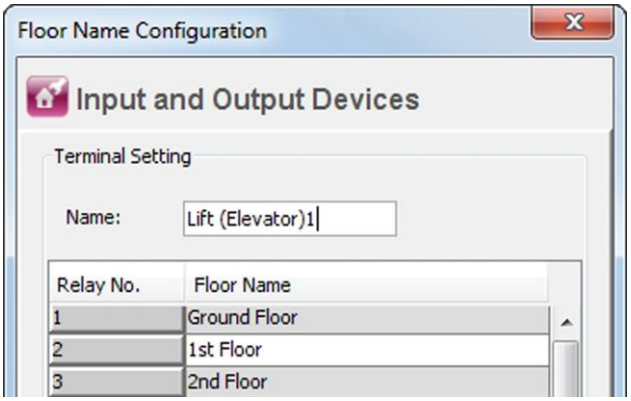


Figure 8 – Floor Name Configuration Dialog Showing Relay Assigned to Floor

Rather than entering the floor number, you may assign your floors names.

14. Click the button.
15. Click the button.
16. Click the **Floors 17-32** button and repeat steps 11 to 13 for these floors if required.

When using Lift (Elevator) Control across multiple Lifts (Elevators), Lift (Elevator) buttons must connect to the ImproX 016 Terminal's output Relays in the same order for each Lift (Elevator).

17. 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.
18. Click the button.

Entry Reader Configuration

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.

1. Select the **Entry** Tab.
2. 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.
3. 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.
4. 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.

5. Edit the **Strike Duration (0.1s)** textbox, the default value is **40** (0.1s). Setting the Strike Duration to **55555** toggles the Relay.
6. Edit the **Open Duration(s)** textbox. By default, the Open Duration is set to **0**, disabling the Door Open Sensor (DOS).
7. 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.

8. From the **ON VALID Tag** group, from the LED Action drop-down list, select the required LED colour state and Duration.
9. From the **Buzzer Volume** drop-down list, select the Buzzer volume and Duration.
10. From the **ON INVALID 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. Click the button.

Configure Lift (Elevator) Mode Pattern

The IXP220 System supports a maximum of 8 Door Mode Patterns at each Door.

This setting regulates the Lift's (Elevator's) operating mode including the start and end time. Continue as follows to add a new Lift (Elevator) 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. Your Door Entry Code may range from between **1 to 65535**. After entering the Door Entry Code at the Reader or Terminal, complete the entry by pressing the # key.*

- ***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****. After entering your Personal Access Code at the Reader or Terminal, complete the entry by pressing the # key.*

  - **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 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.
  - **LED**—sets the LED’s behaviour during the stipulated time slot.

7. Click the button.

Advanced Configuration

On selecting the **Advanced Configuration** radio button, the Lift (Elevator) Patterns and Zone settings activate. Configure the following settings:

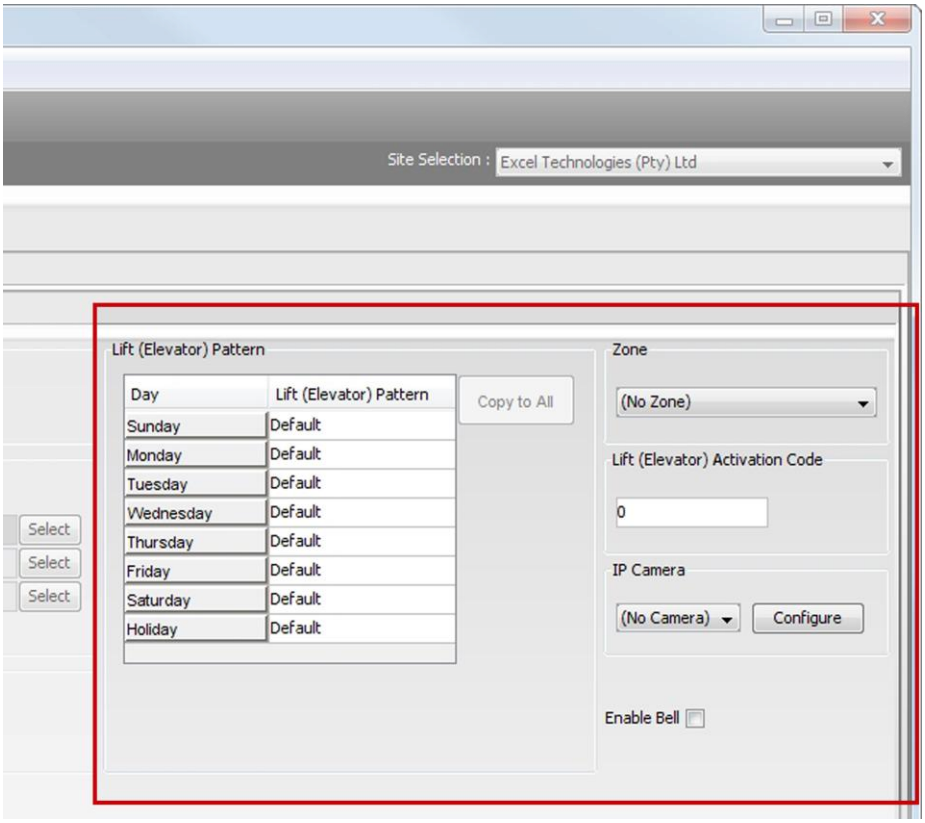


Figure 9 – Right-hand Side of the Door Configuration Pane

1. On the Configuration Pane, select the **Lift (Elevator)** Tab.
2. In the **Lift (Elevator) Pattern** group (see Figure 5), make your selections from the Day's Lift (Elevator) Mode Pattern drop-down lists.
3. In the **Zone** group, select a Zone from the drop-down list.

*Using a **Lift (Elevator) Activation Code** allows Tagholders to enter or exit a Lift (Elevator) using a numeric code. Note, however, Tags with access permissions for the Lift (Elevator) are still acknowledged by the Reader. Activate the Lift (Elevator) Activation 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 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 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 Configuration Pane, select the **Lift (Elevator)** Tab.*
9. *In the **Lift (Elevator) Activation Code** textbox, enter a 5 digit numeric code.*

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

1. *On the Door Configuration Pane, select the **Lift (Elevator)** 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 Lift (Elevator) from the list of available Lift (Elevator) records.*
10. *From the **IP Camera** drop-down list, select a Camera record, thus associating the Lift (Elevator) and IP Camera.*
11. *Click the button.*

4. Click the button.

Access Group Configuration

Ensure that all Lifts (Elevators) in a Lift (Elevator) Access Group go to the same floors. Note, you need not use all Lifts (Elevators). Selecting floors from a single Lift (Elevator), the selection works as normal.

When using distributed templates along with biometrics, after editing the Lift (Elevator) Access Group, ensure you perform a full upload. Refer to Part 3 – General Configuration for more information on performing a full upload.

Configuration of Access Groups may only be carried out by operators with the correct operator permissions. Setup is carried out through the Base Application, therefore go to Page 14 for details of the setup required.

Building Management

Purpose of this Feature

The Building Management feature lets you manage various hardware devices in and around the office, such as irrigation, lighting or airconditioning with the use of event driven or time triggered actions. The IXP220 System supports up to 18 input or output devices (that is up to 16 ImproX O16 Terminals and 2 ImproX I16 Terminals) per Site, configured as required.

- As the name suggests, set up a time triggered action by selecting a time and day and assigning a relay drive time to the Action.
- Event driven actions use the Inputs from the ImproX I16 to trigger a relay to drive and stop.

Example

The following example procedure shows the use of this feature.

Procedure

Ensure that you unlock your Registration Interface for Input/Output Control before using this feature. This unlock allows for a maximum of 1 seat. See page 5 of this section for more information.

Controller Configuration

1. In the IXP220 Base Application, select the Page Tab.
2. From the **Mode Configuration** drop-down list, select **Action**.
3. Click the button.

Terminal Configuration

From the Menu Bar select **Configuration**>**Building Management**>**Input/Output Devices**.

ImproX I16 Terminal – Input Setup

1. From the left-hand side table, select your ImproX I16 Input Terminal.
2. In the **Name** textbox, assign your Terminal a meaningful name.
3. **Disable** or **Enable End-of-Line Sensing** by selecting the appropriate radio button.
4. In the right-hand side Terminal Setting table, assign each Input in use an **Input Name**.
5. Check the corresponding **Alarm** checkbox if required.
6. Click the button.

ImproX O16 Terminal – Output Setup

1. From the left-hand side table, select your ImproX O16 Output Terminal.
2. In the **Name** textbox, assign your Terminal a meaningful name.
3. In the right-hand side Terminal Setting table, assign each Relay in use an **Output Name**.

4. Click the button.

Action Configuration

1. Select the Page Tab.
2. Click the button.
3. Give your Action a **Name**.
4. From the **Trigger Type** drop-down, make your selection:

Input Triggered Action Setup

1. From the **Trigger Type** drop-down, select **Input**.

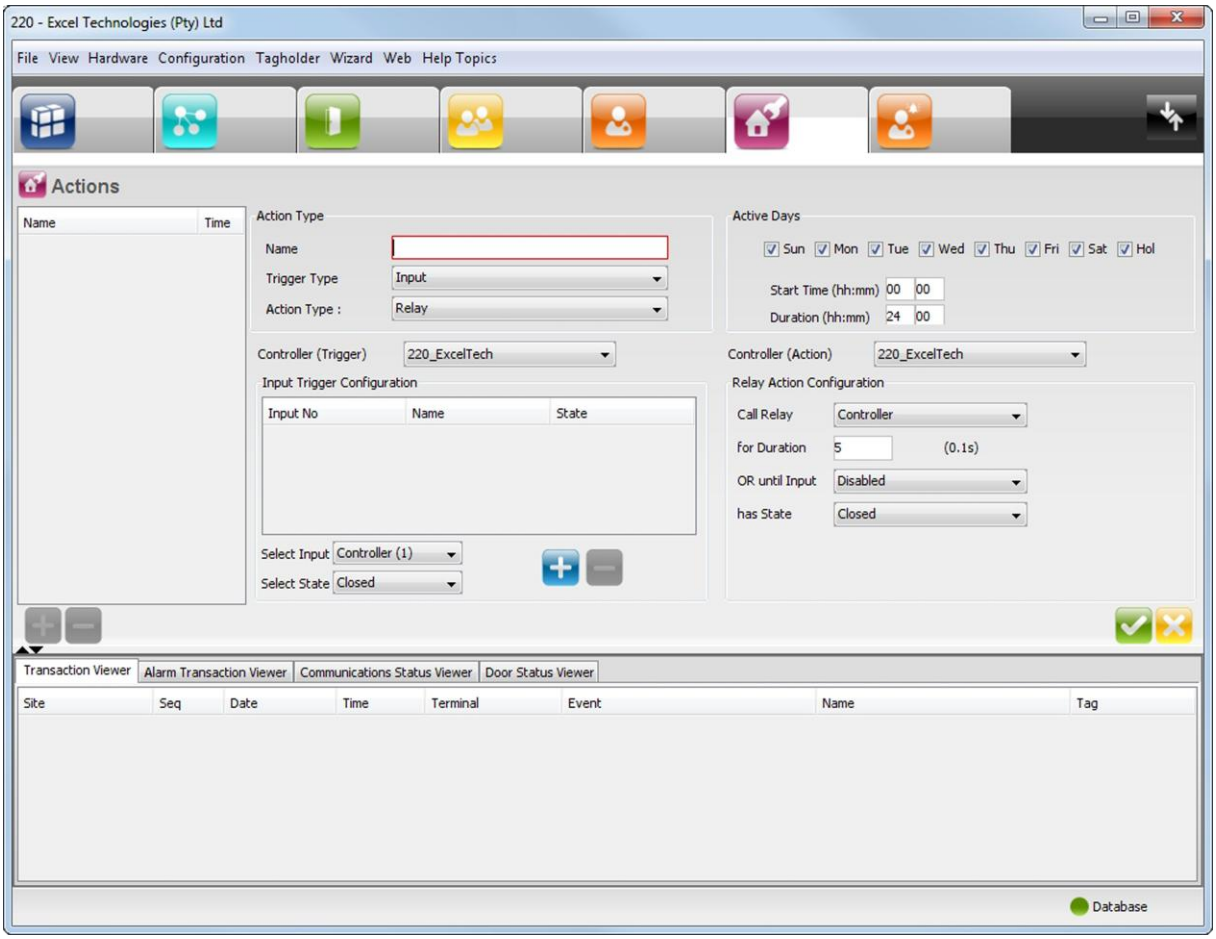


Figure 10 – Action Configuration Pane

2. From the **Action Type** drop-down list, make your selection:
   - **Relay**—configure the **Relay Action Configuration** group by making your selections from the available fields.
   - **LED and Buzzer**—configure the **LED and Buzzer Action Configuration** group by making your selections from the available fields.
   - **SMS Message**—configure the **SMS Action Configuration** group by completing the available fields. See page 29 for building management message configuration details.
   - **SMS Service Message**—configure the **SMS Network Service** group by completing the available fields.

3. From the **Controller (Trigger)** drop-down list, select the Controller that will trigger the Action.
4. From the **Select Input** drop-down list, select one of the Input names.
5. From the **Select State** drop-down list, select from the following choices:
   - **Closed**—input state closed.
   - **Open**—input state open.
   - **Toggled**—input state alternates between open and closed.
6. From within the **Input Trigger Configuration** group, click the button.
7. From the **Active Days** group, make your selection from the **Sun** to **Hol** checkboxes.
8. Select the **Start Time**.
9. Select the **Duration** (**65535** or **1 000 000** holds the Relay indefinitely).
10. From the **Controller (Action)** drop-down list, make your selection.
11. Depending on your selection in point 2, complete the activated fields as required.
12. Click the button.

Time Triggered Action Setup

1. From the **Trigger Type** drop-down, select **Time**.

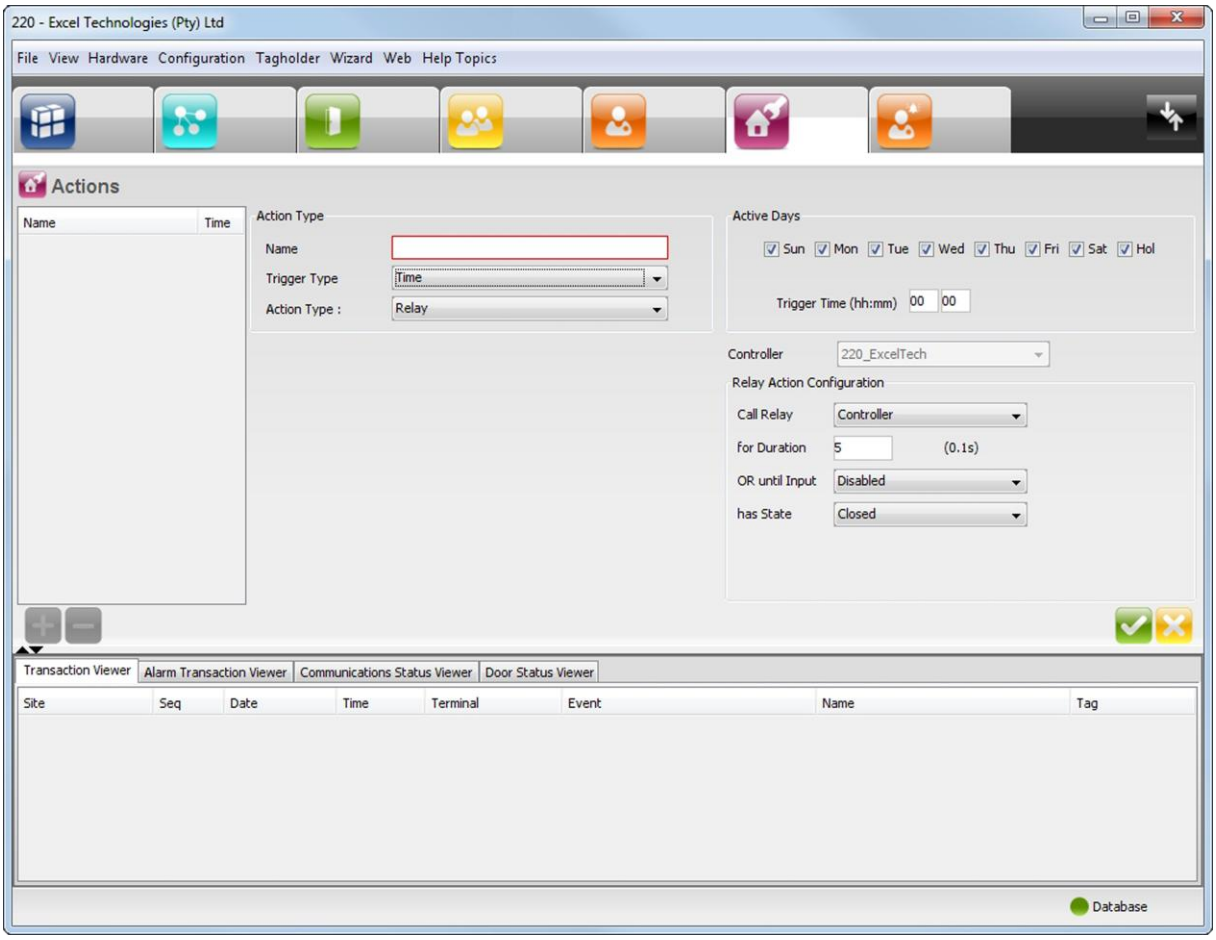


Figure 11 – Action Configuration Pane

2. From the **Action Type** drop-down list, make your selection:
   - **Relay**—configure the **Relay Action Configuration** group by making your selections from the available fields.

- **LED and Buzzer**—configure the **LED and Buzzer Action Configuration** group by making your selections from the available fields.
- **SMS Message**—configure the **SMS Action Configuration** group by completing the available fields. See page 29 for building management message configuration details.
- **SMS Service Message**—configure the **SMS Network Service** group by completing the available fields.

3. From the **Controller (Trigger)** drop-down list, select the Controller that will trigger the Action.
4. From the **Active Days** group, make your selection from the **Sun** to **Hol** checkboxes.
5. Select the **Trigger Time**.
6. From the **Controller (Action)** drop-down list, make your selection.
7. Depending on your selection in point 2, complete the activated fields as required.
8. Click the button.

Event Triggered Action Setup

1. From the **Trigger Type** drop-down, select **Event**.

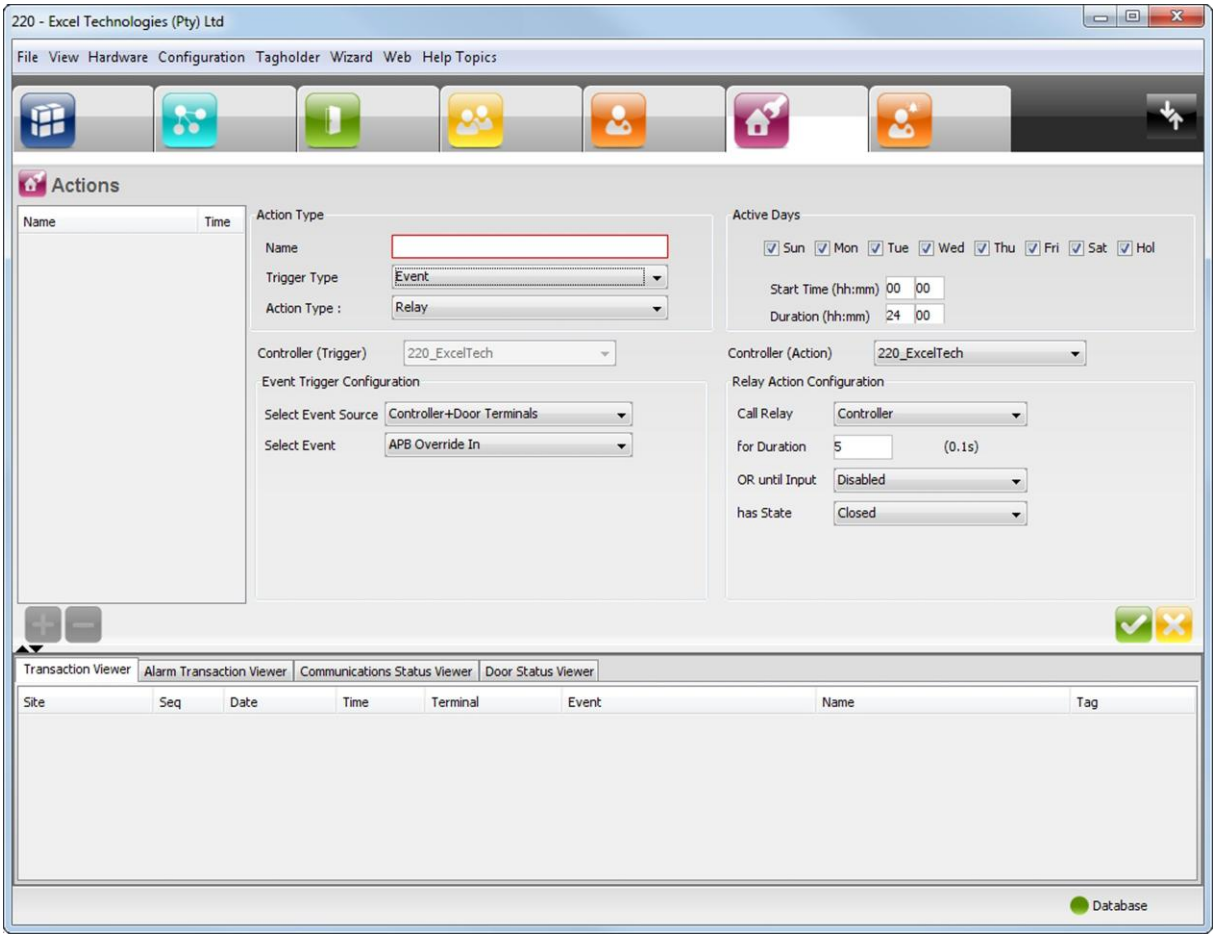


Figure 12 – Action Configuration Pane

2. From the **Action Type** drop-down list, make your selection:
   - **Relay**—configure the **Relay Action Configuration** group by making your selections from the available fields.
   - **LED and Buzzer**—configure the **LED and Buzzer Action Configuration** group by making your selections from the available fields.

- **SMS Message**—configure the **SMS Action Configuration** group by completing the available fields. See page 29 for building management message configuration details.
- **SMS Service Message**—configure the **SMS Network Service** group by completing the available fields.

3. From the **Controller (Trigger)** drop-down list, select the Controller that will trigger the Action.
4. From the **Select Event Source** drop-down list, make a selection.
5. From the **Select Event** drop-down list, make a selection from the list of Events supplied.
6. From the **Active Days** group, make your selection from the **Sun** to **Hol** checkboxes.
7. Select the **Start Time**.
8. Select the **Duration** (**65535** holds the Relay indefinitely).
9. From the **Controller (Action)** drop-down list, make your selection.
10. Depending on your selection in point 2, complete the activated fields as required.
11. Click the button.

Building Management Message Configuration

For Building Management Messages to work successfully, you need to have an IXP220 Controller and a GSM module.

Configure Building Management Messages as follows:

Adding Building Management Messages

1. From the Menu Bar select **Configuration**>**Building Management**>**Building Management Messages**.
2. Click the button.
3. In the **Message** textbox, enter your message (not exceeding 70 characters including spaces).
4. Click the button.
5. Click the button.

Deleting Building Management Messages

1. From the Menu Bar select **Configuration**>**Building Management**>**Building Management Messages**.
2. Select the Message record for deletion.
3. Click the button.
4. Click the button.

Secure Socket Layer (SSL) Connection

Purpose of this Feature

Using the IXP220 Software V1.82 onwards, you may connect to the various Web Modules using a **secure (1 024 Bit encrypted) connection**.

Example

The following example procedures show the use of this feature.

Procedure

Configuration for Windows® Internet Explorer 8

Carry out the following procedure at the Host PC with the IXP220 Base Application running.

1. In the Address textbox enter the **https://localhost/220Web/homepage.html** URL. The “s” ensures communication to the server takes place on a secure, encrypted connection.
2. Select the **Continue to this Website (Not Recommended)** option.

We supply a generic Security Certificate with the distributed IXP220 Software. Purchase Security Certificates from signing authorities such as VeriSign, Thawte or any other major signing authority.

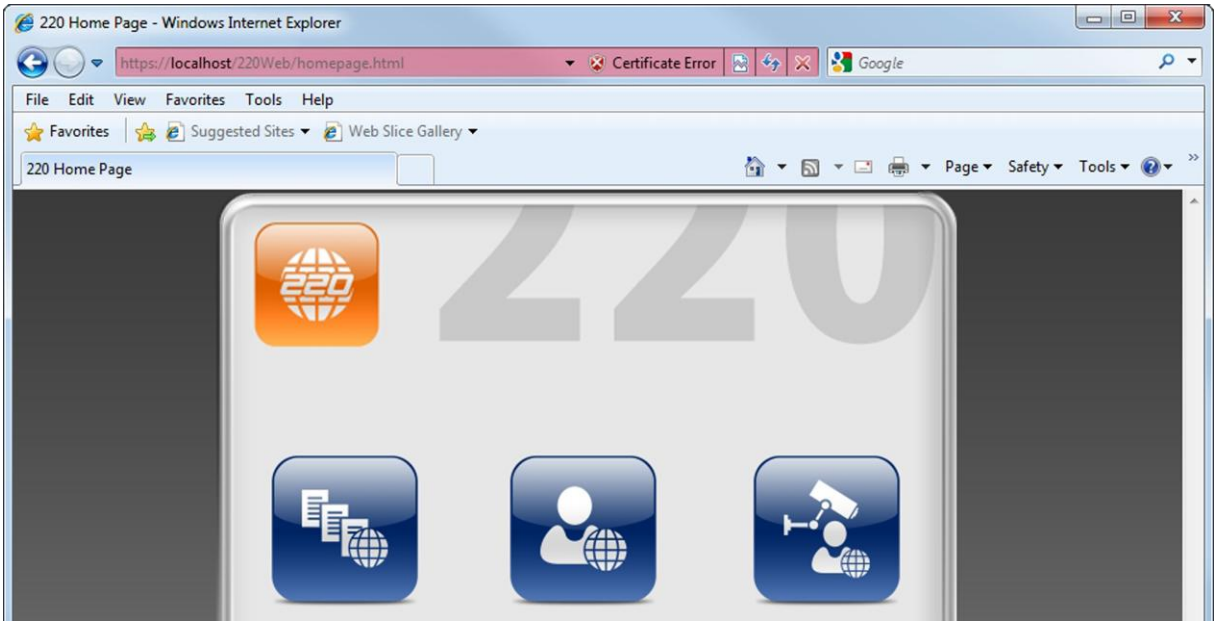


Figure 13 – Windows® Internet Explorer 8 with Secure Socket Layer (SSL) Used

Configuration for Mozilla Firefox 3.5

Carry out the following procedure at the Host PC with the IXP220 Base Application running.

1. In the Address textbox enter the **https://localhost/220Web/homepage.html** URL. The “s” ensures communication to the server takes place on a secure, encrypted connection.
2. Select the **I Understand the Risks** option.

We supply a generic Security Certificate with the distributed IXP220 Software. Purchase Security Certificates from signing authorities such as VeriSign, Thawte or any other major signing authority.

3. Click the **Add Exception** button.
4. Click the **Confirm Security Exception** button.

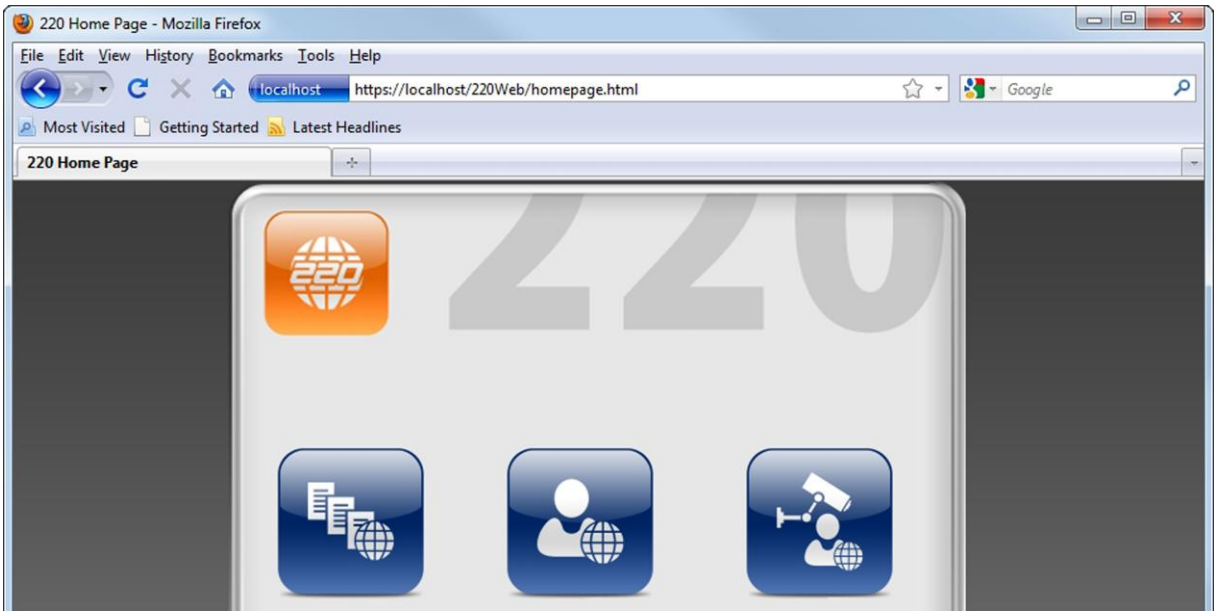


Figure 14 – Mozilla Firefox 3.5 with Secure Socket Layer (SSL) Used

Live Video Image Capture

Purpose of this Feature

The **Live Video Image Capture** feature allows you to use a web camera to capture and save Tagholder images. By connecting a web camera to a PC running either the Base Application or the Web Enrollment Module, users can capture an image from live video and save it directly to the Tagholder data. You can use this feature when loading new Tagholders or when editing existing Tagholders.

Procedure

This feature supports the following cameras:

- *Logitech® Webcam Pro 9000*
- *Logitech® 1.3 MP Webcam C500*
- *Logitech® Webcam C120*

Ensure that you load your chosen camera's drivers before using the Live Video Image Capture feature.

To use this feature in the Web Enrollment Module, install Java Runtime Environment V1.60 Update 20 or above.

*Windows® Vista users must disable the **User Account Control** before using the Live Image Capture feature in the Web Enrollment Module. Disable the control as follows:*

1. *Select **Start**>**Control Panel**.*
2. *Select the **User Accounts** icon.*
3. *Select the **Turn User Account Control On or Off** option.*
4. *Deselect the **Use User Account Control (UAC) to Help Protect Your Computer** option.*
5. *Click the **OK** button.*
6. *Click the button.*

To capture an image from video:

1. Open either the **Add Tagholde**r or **Edit Tagholder** in the Base Application or Web Enrollment Module.
2. Click the button.

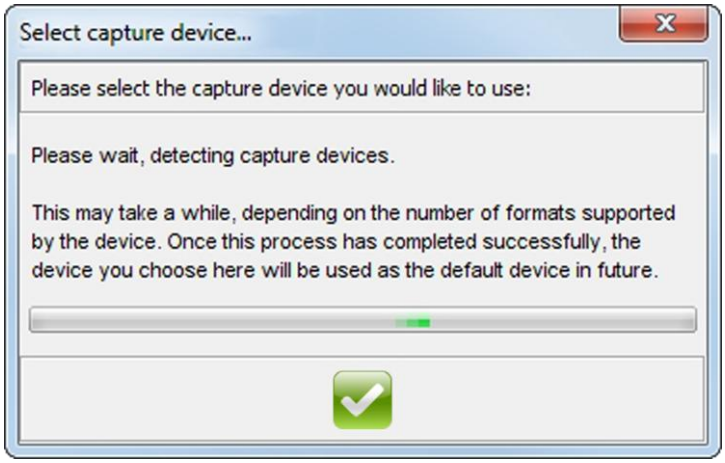


Figure 15 – Select Capture Device Dialog

3. From the next Select Capture Device dialog, from the **Available Devices** drop-down list, select the required camera device.
4. Click the button.
5. From the **Select Format** drop-down list, select the snapshot format and resolution. The recommended resolution is 640 x 480 pixels.

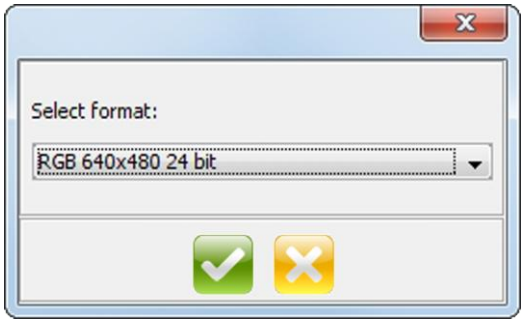


Figure 16 – Select Format Dialog

6. Click the button.

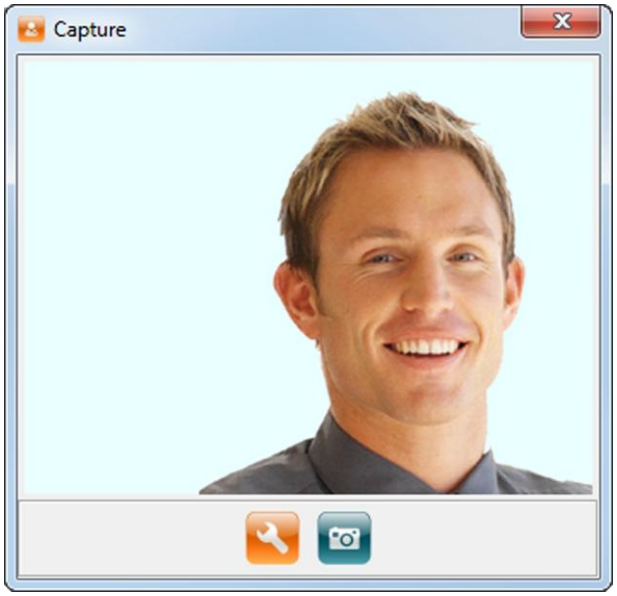


Figure 17 – Capture Dialog

*If you click the button, the **Select Format** dialog appears. This allows you to edit the snapshot format and resolution.*

7. In the Capture dialog, click the button to capture the image.

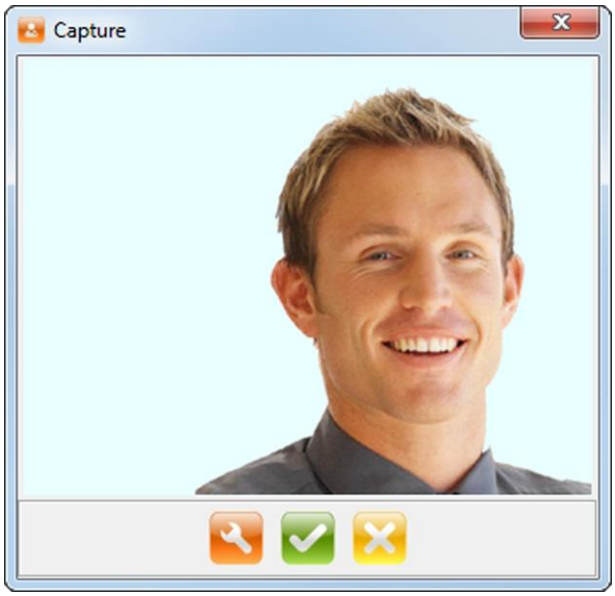


Figure 18 – Capture Dialog

*If you click the button after capturing the image, the **Edit** dialog appears. This dialog allows you to rotate, resize, mirror or crop your image. Once you crop an image this measurement becomes the default setting.*

*To reset the automatic image cropping default, in the **Add** or **Edit Tagholder** dialog, right-click over the Image Frame. From the shortcut menu select the **Reset** option.*

You may also disable the automatic image cropping feature as follows:

1. *From the **C:\:IXP220**:*
   - *Open the **IXP220.properties** file when using the Base Application.*
   - *Open the **Quicktag**>**Quicktag.properties** file when using the Web Enrollment Module.*
2. *Set the **access.image.autocrop=true** to **access.image.autocrop=false**.*
3. *From the Main Menu, select **File**>**Save**.*
4. *From the Main Menu, select **File**>**Exit**.*

*After editing the image in the **Edit** dialog, click the **OK** button to save changes and return to the Tagholder dialog.*

8. Click the button.
9. Click the button to save the Tagholder's information.

USER NOTES

USER NOTES