PART 5 – ADVANCED CONFIGURATION

Contents

PART 5 – ADVANCED CONFIGURATION 1

CONTENTS 3

UNLOCK ON FIRST TAG 5

Purpose of this Feature 5

Example 5

Procedure 5

LIFT (ELEVATOR) CONTROL 13

Purpose of this Feature 13

Example 13

Procedure 13

INTERLEADING ZONE ROUTING 17

Purpose of this Feature 17

Example 17

Procedure 18

Troubleshooting 21

RANDOM SEARCH 23

Purpose of this Feature 23

Example 23

Procedure 24

MESSAGES 31

Purpose of this Feature 31

Procedure 31

EMERGENCY DOOR OPEN 33

Purpose of this Feature 33

Example 33

Procedure 33

LOCKDOWN TERMINAL MODE 37

Purpose of this Feature 37

Example 37

Procedure 37

FORCE UPLOAD OF HARDWARE OR TAGHOLDER DATA 41

Purpose of this Feature 41

Example 41

Procedure 41

DEVICE TIME PATTERNS (DTP'S) SUPPORTED IN ACTIONS 43

Purpose of this Feature 43

Example 43

Procedure 43

ANTI-PASSBACK (APB) LOCKOUT ENTRY AND EXIT DELAYS 45

Purpose of this Feature 45

Procedure 45

OPERATOR SECURITY 47

Purpose of this Feature 47

Procedure 47

SMS SUPPORT ON EVENTS AND ACTIONS 55

Purpose of this Feature 55

Example 55

Procedure 55

ALARM ARMING 61

Purpose of this Feature 61

Example 61

Procedure 63

SUPERVISOR UNLOCK 75

Purpose of this Feature 75

Procedure 75

DOOR STRIKE LOCK SETUP 79

Purpose of this Feature 79

Procedure 79

Unlock on First Tag

Purpose of this Feature

Unlock on First Tag feature provides the facility of unlocking selected door(s) when the first valid Tag is presented during a specified time period. The door remains unlocked for that time period, but is locked outside that time period, opening only on presentation of a valid Tag.

Example

In the following example procedure, activate the **Unlock on First Tag** feature only on weekdays from 7 am to 5 pm. This means that you must create the following Device Time Patterns (in Access) for the Terminal(s) concerned:

- A Device Time Pattern from 7 am until 5 pm on weekdays (Monday to Friday). This is the period for which the **Unlock on First Tag** feature **must be enabled**.
- A Device Time Pattern from Sunday until Friday, 5 pm until 12 am. This is the remaining time on each of the above days during which the **Unlock** feature **must be disabled**.
- A Device Time Pattern from Sunday until Friday, 12 am until 7 am. The Sunday period covers the time from midnight to 7 am on Monday.
- A Device Time Pattern called **Deactivate Relay at 17:00**. Set the start time to 5 pm and select Monday to Friday.
- A Device Time Pattern for Saturday, Sunday and public holidays for the full 24 hours. These are the days on which the feature must be disabled.

Procedure

Device Time Pattern Setup

1. In Access, in the Navigate Pane (from the Hierarchical Tree) select the icon.
2. In the Main Pane, click the button.

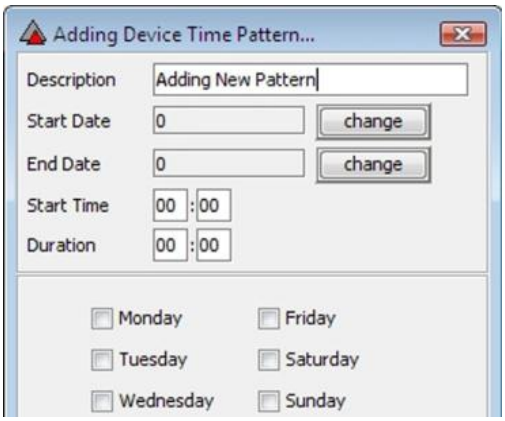

Figure 1 – Adding Device Time Pattern Dialog

3. In the **Description** textbox, enter a name for the Device Time Pattern.
4. If required, complete the **Start Date** and **Stop Date** textboxes.
5. In the **Start Time** field, enter **0700**.
6. In the **Duration** field, enter **1000**.
7. Select the **Monday** through **Friday** checkboxes.
8. Repeat the processes mentioned in steps 2 to 7 for the remaining Device Time Patterns.

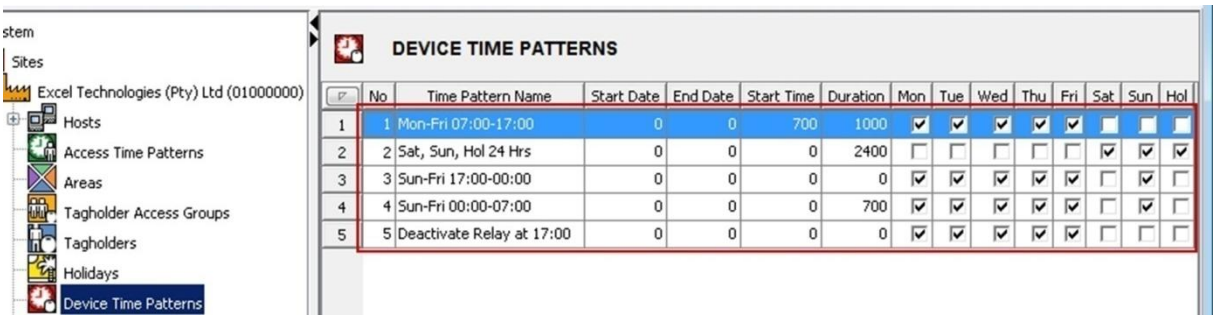

Figure 2 – Completed Device Time Patterns

Relay Action Setup

New Action - Mon-Fri 07:00-17:00 Device Time Pattern

1. Select the **Actions** tab, for the output relay on the Terminal controlling the door strike.
2. In the Main Pane, click the button.
3. In the **Action Name** textbox, assign your action the name **Enable Relay Indefinitely**.
4. Alongside the **Time Pattern** textbox, click the button.
5. From the list of displayed Device Time Patterns, select the **Mon-Fri 07:00-17:00** record.
6. Click the button.

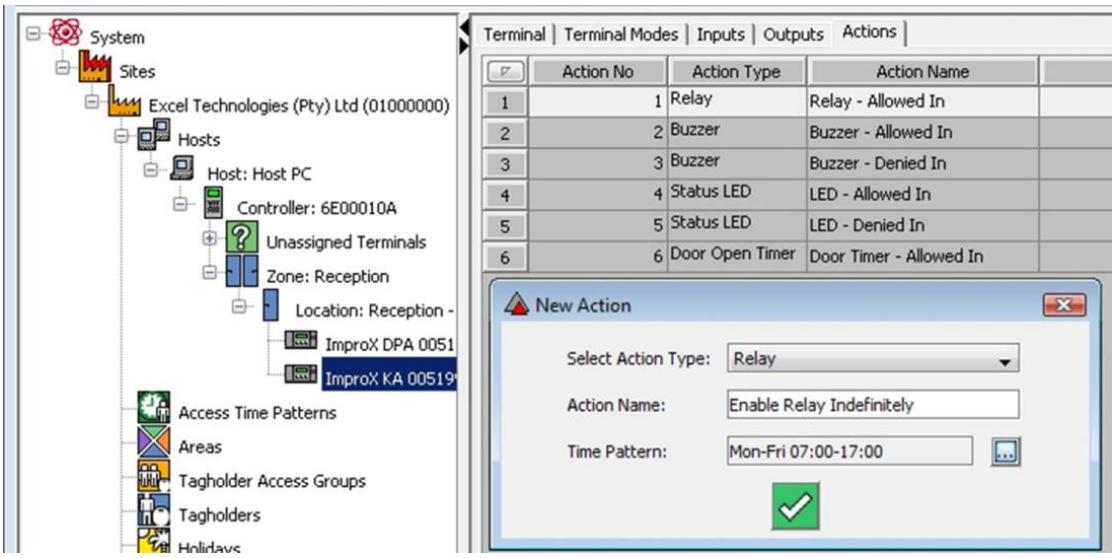

Figure 3 – New Relay Action – Enable Relay Indefinitely

7. At the New Action dialog, click the button.
8. In the Action Parameters dialog, set the **Duration (0.1s)** to **65535**.

This Action enables the relay for an indefinite period.

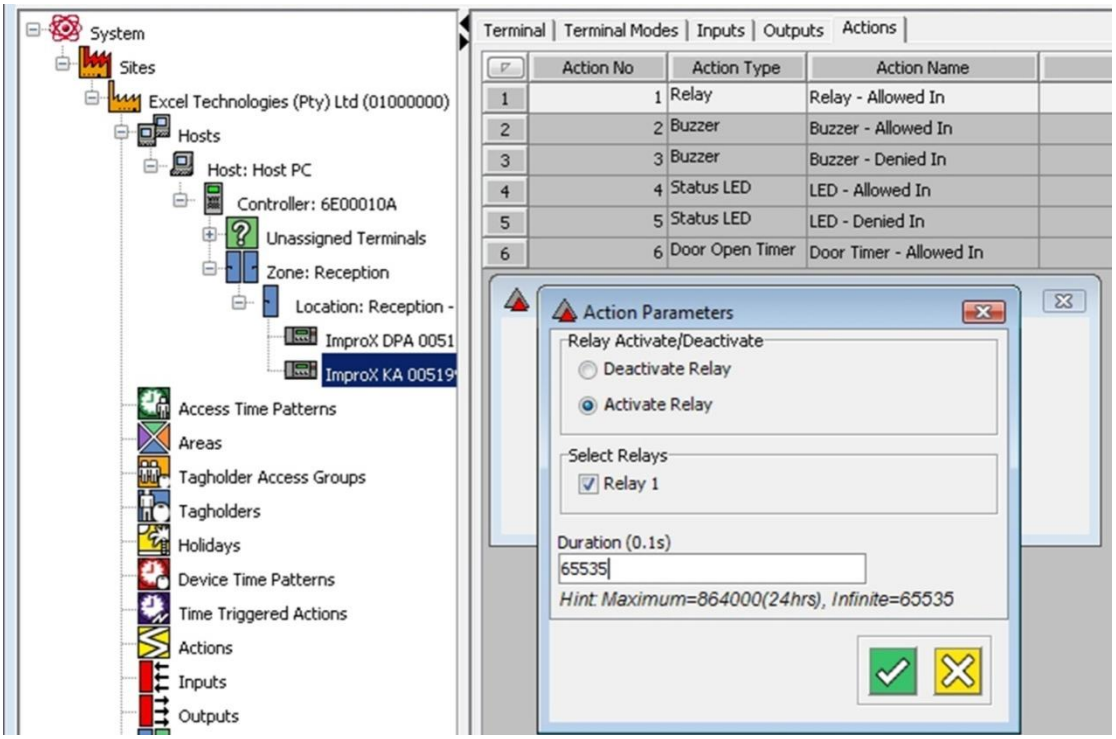

Figure 4 – Set Relay Action Duration to "Infinite"

9. Click the button.

New Action - Sat, Sun, Hol 24hrs Device Time Pattern

1. In the Main Pane, click the button.
2. In the **Action Name** textbox, assign the action a name (for example **Drive Relay 4 Seconds**).
3. Alongside the **Time Pattern** textbox, click the button.
4. From the list of displayed Device Time Patterns, select the **Sat, Sun, Hol 24 Hrs** record.

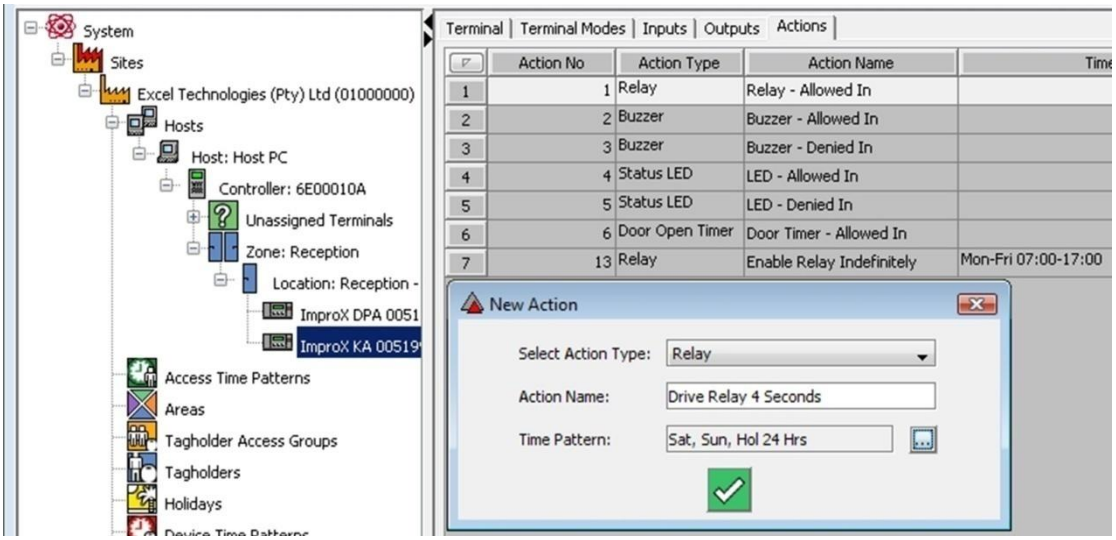

Figure 5 – New Relay Action – Drive Relay 4 Seconds

5. Click the button.
6. At the New Action dialog, click the button.

7. In the Action Parameters dialog, set the **Duration (0.1s)** to **40** (4 seconds).
8. At the Action Parameters dialog, click the button.

Edit Action - Sun-Fri 17:00-00:00 Device Time Pattern

1. In the Main Pane select the existing **Relay – Allowed In** Action.
2. Click the button.
3. In the **Action Name** textbox, assign the action a new name (for example **Sun-Fri 1700-0000**).
4. Alongside the **Time Pattern** textbox, click the button.
5. From the list of displayed Device Time Patterns, select the **Sun-Fri 17:00-00:00** record.
6. Click the button.

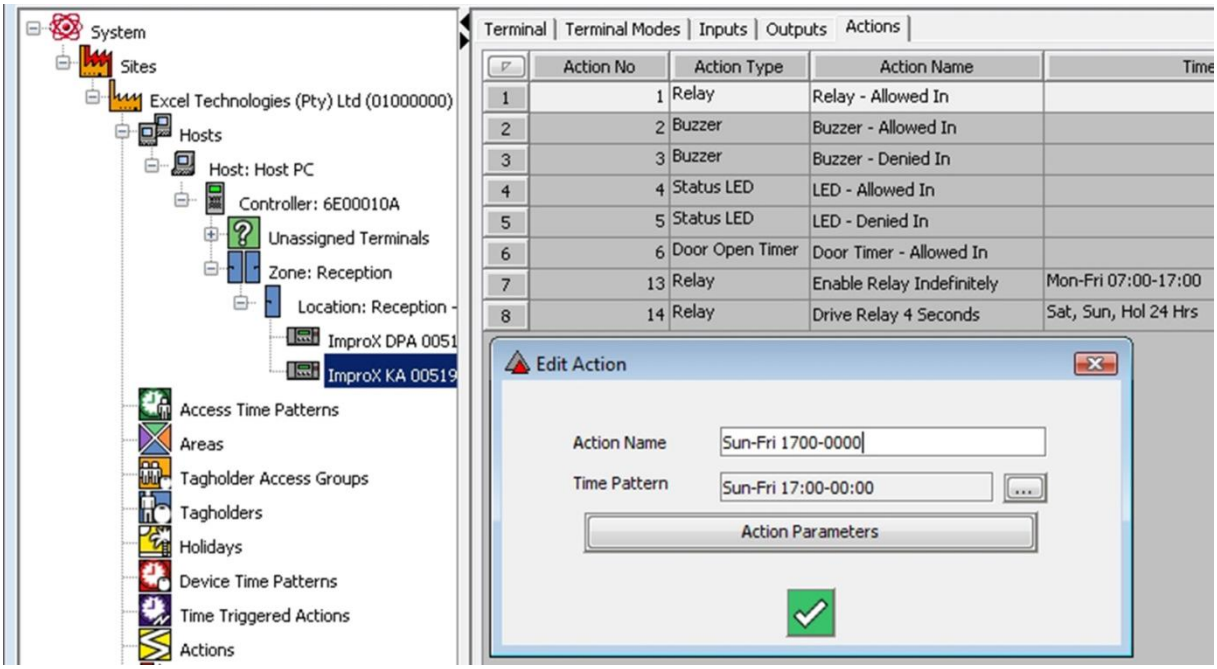

Figure 6 – Edit Relay – Allowed In Action

7. At the Edit Action dialog, click the button.

New Action - Sun-Fri 00:00-07:00 Device Time Pattern

1. In the Main Pane, click the button.
2. In the **Action Name** textbox, assign your action a name (for example **Sun-Fri 0000-0700**).
3. Alongside the **Time Pattern** textbox, click the button.
4. From the list of displayed Device Time Patterns, select the **Sun-Fri 00:00-07:00** record.

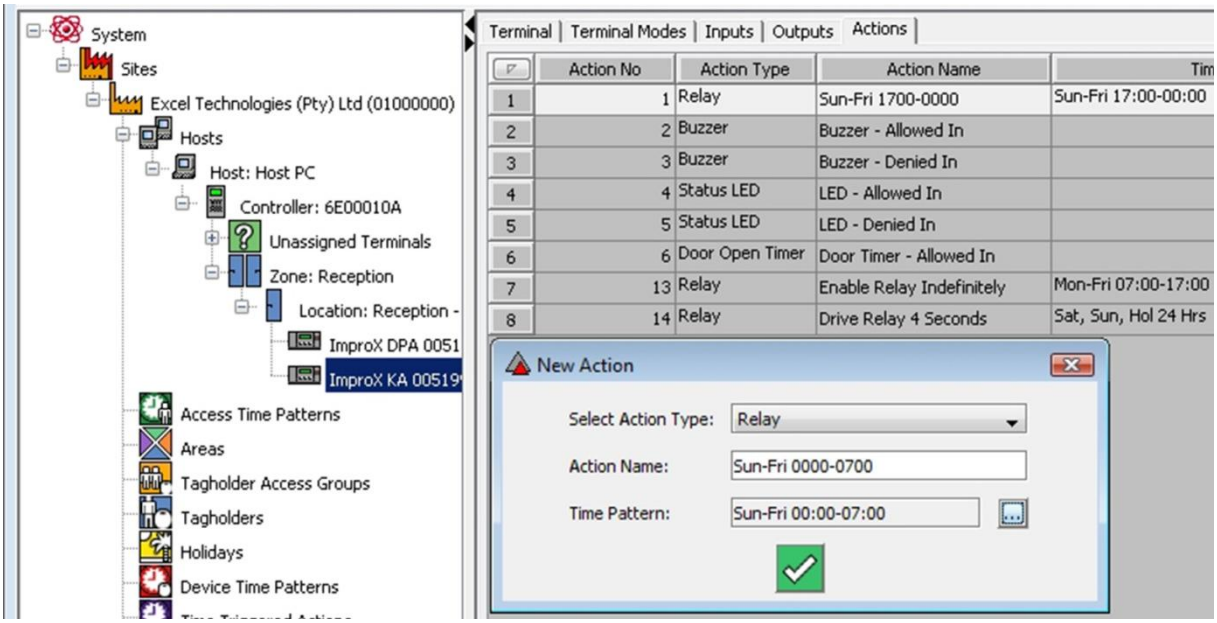

Figure 7 – New Relay Action – Sun-Fri 00:00-07:00

5. Click the button.
6. At the New Action dialog, click the button.
7. At the Action Parameters dialog, click the button.

New Action - Deactivate Relay at 17:00 Device Time Pattern

1. In the Main Pane, click the button.
2. In the **Action Name** textbox, assign your action a name (for example **Deactivate Relay**).
3. Alongside the **Time Pattern** textbox, click the button.
4. From the list of displayed Device Time Patterns, select the **Deactivate Relay at 17:00** record.

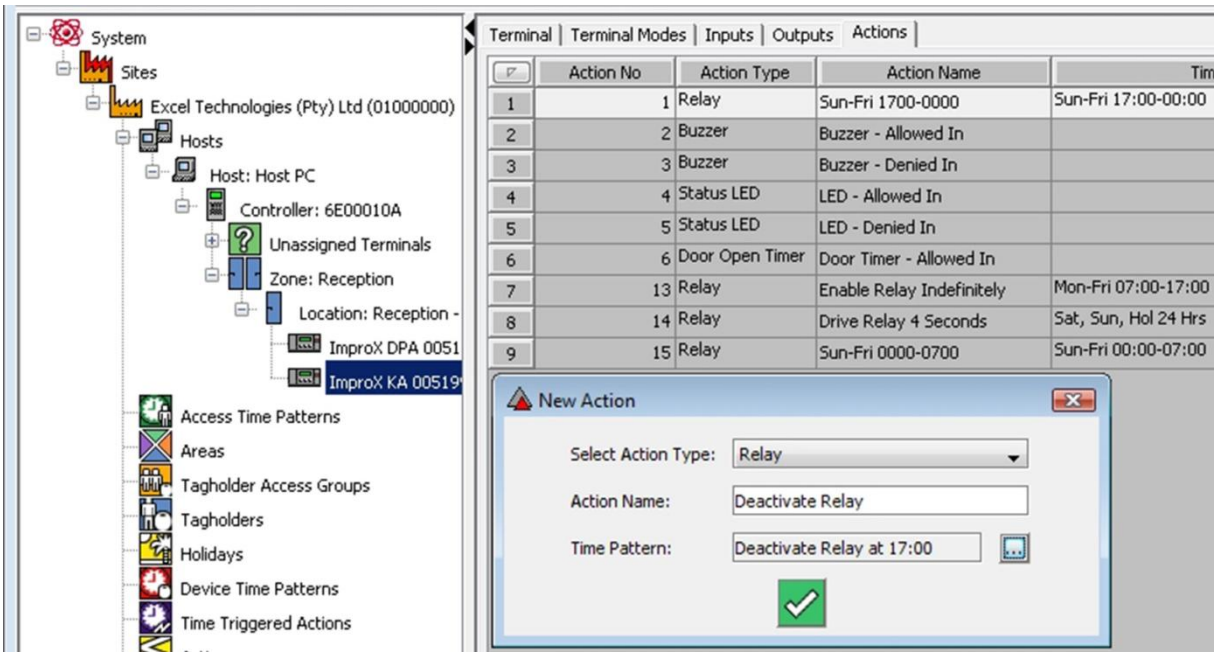

Figure 8 – New Relay Action – Deactivate Relay at 17:00

5. Click the button.
6. At the New Action dialog, click the button.
7. In the Action Parameters dialog, set the Duration (0.1s) to **65535**.
8. At the Action Parameters dialog, click the button.

New Action - All Relays

1. In the Main Pane, click the button.
2. From the Select Action Type drop-down list, select the **Multiple Actions** option.
3. In the **Action Name** textbox, assign your action a name (for example **All Relays**).

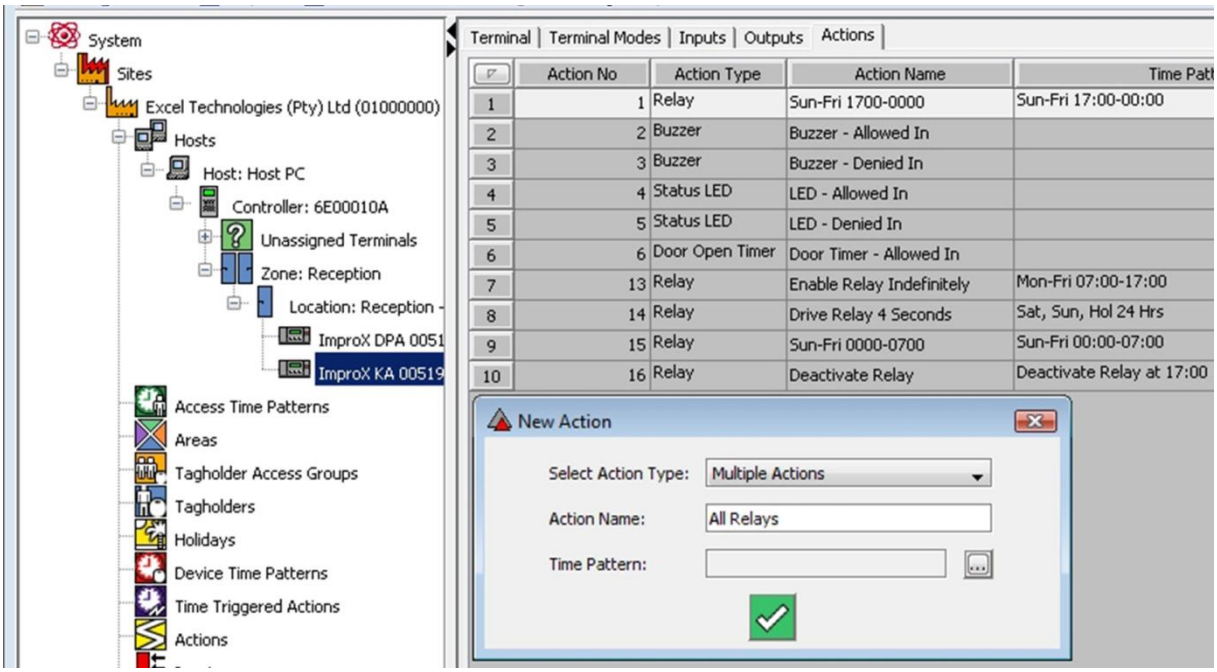

Figure 9 – New Relay Action – Deactivate Relay at 17:00

4. In the Action Parameter dialog, for the **First Action**, click the **1** button.
5. From the list of displayed actions, select the **Sun-Fri 1700-0000** action created earlier.
6. For the **Second Action**, click the **2** button.
7. From the list of displayed actions, select the **Sun-Fri 0000-0700** action created earlier.
8. For the **Third Action**, click the **3** button.
9. From the list of displayed actions, select the **Enable Relay Indefinitely** action created earlier.
10. For the **Fourth Action**, click the **4** button.
11. From the list of displayed actions, select the **Drive Relay 4 Seconds** action created earlier.
12. Click the button.
13. At the Action Parameters dialog, click the button.

Active System Events Editor

1. In the Main Pane, click the **Active System Events** button.

On opening, under **Actions for Allowed Events**, the **First Action** appears as **Sun-Fri 1700-0000**, add the remaining actions as follows:

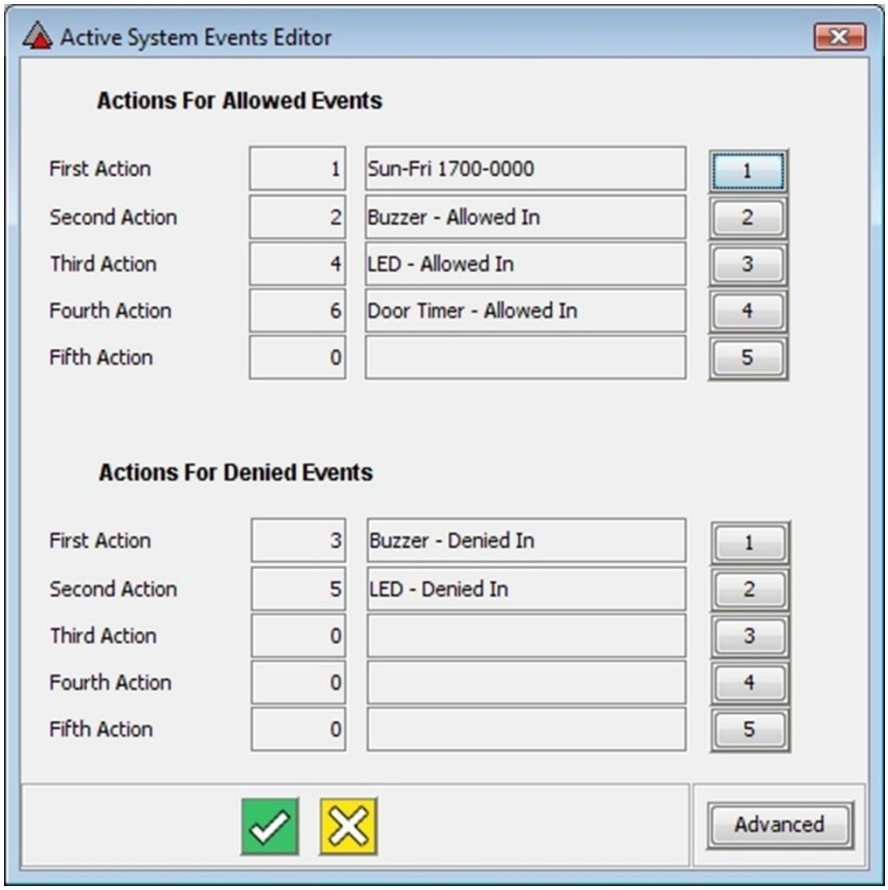

Figure 10 – Active System Events Editor Dialog

2. Under **Actions For Allowed Events**, replace the **First Action**, by clicking the **1** button.
3. From the list of actions displayed, select the **All Relays** action you created earlier.
4. Click the button.
5. At the Active System Events Editor dialog, click the button.
6. At the Confirm Save dialog, click the **Yes** button.

Time Triggered Action Setup

1. In Access, in the Navigate Pane (from the Hierarchical Tree), select the icon.
2. In the Main Pane, click the button.
3. In the **Action Name** textbox, give your Time Triggered Action a meaningful name (for example **Deactivate Relay 1**).
4. Click the **Trigger Time's** associated button.
5. From the list of displayed Device Time Patterns, select the **Deactivate Relay at 17:00** record.
6. Click the button.
7. Click the **Execute Action's** associated button.
8. From the list of displayed actions, select the **Deactivate Relay** action created earlier.
9. Click the button.
10. At the Create Time Triggered Action dialog, click the button.

Lift (Elevator) Control

Purpose of this Feature

Lift (Elevator) Control feature provides the facility of setting up Lift (Elevator) Control in your Access Control System.

Example

The following example procedure shows the use of this feature.

Procedure

Relay Setup

1. In Access, in the Navigator Pane (from the Hierarchical Tree), select the icon selecting the ImproX O16 Terminal's Zone.
2. In the Main Pane, from the **Anti-passback** group, select the **Strict** radio button.
3. In the Navigator Pane, from the Hierarchical Tree, select the **ImproX O16 Terminal**.
4. In the Main Pane, on the Terminal tab, from the **Position** group, select the **Exit** radio button.
5. Select the **Actions** tab.
6. On the Main Pane, click the button.
7. In the New Action dialog, from the **Select Action Type** drop-down list select the **Relay** option.
8. In the **Action Name** textbox, assign your action a name (for example **Elevator Access**).
9. Click on the button.
10. In the Action Parameters dialog, from the select **Relay Activate/Deactivate** group, select the **Activate Relay** radio button.
11. From the Select Relays group, select the required Relay.

You may select more than 1 Relay.

To change the Duration value, click in the field and type in the required time duration (10 = 1 second). If, for example, wheelchair access is required, it may be necessary to extend this time.

12. Click on the button.

Configure the Area

Remember, a Lift (Elevator) Area CANNOT co-exist in another physical Area as well as its own Area.

An Area is a user-defined grouping of Locations to assist with access allocation. Configure the Area as follows:

1. In the Navigator Pane (from the Hierarchical Tree) select the icon.
2. In the Main Pane, click the button.

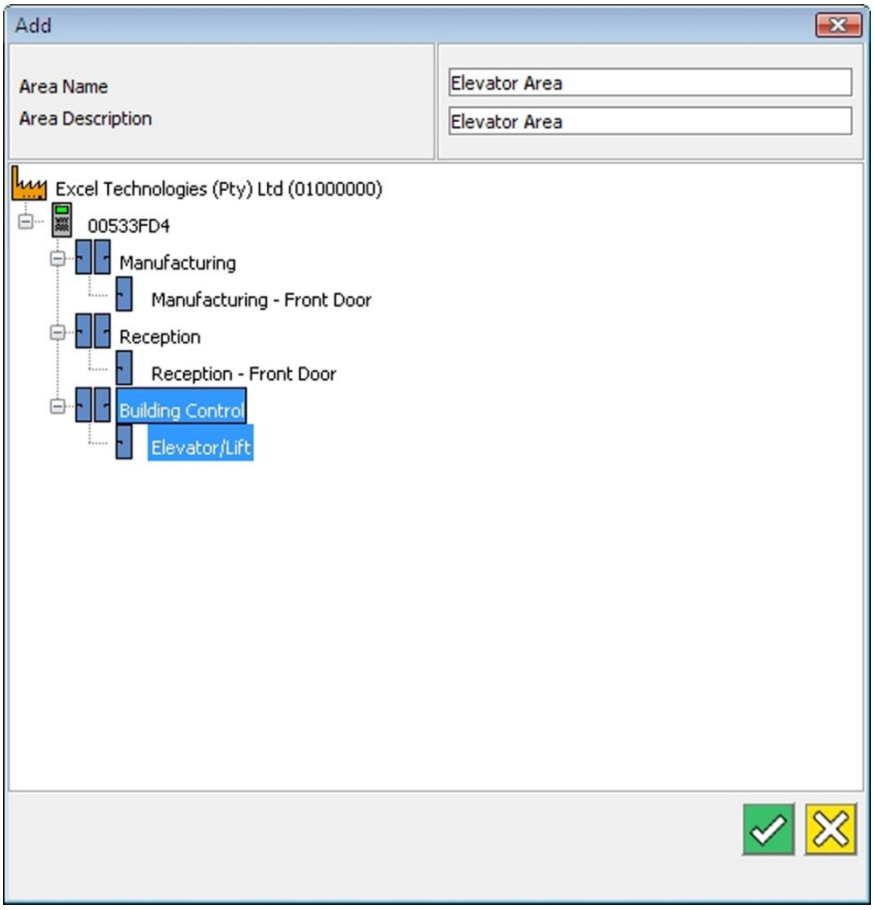

Figure 11 – Add Dialog

3. In the **Area Name** field, enter a name for the new Area.
4. In the **Area Description** field, enter a unique description of the new Area.
5. On the Location tree, click on the specific Location where you set up the Lift (Elevator).
6. Click on the button.

The newly defined Area displays, showing details of the included Zones and their Locations.

Select the button to display the full tree in order to select or deselect Locations, thus forming an amended Area.

Configure the Tagholder Access Groups

1. In the Navigator Pane (from the Hierarchical Tree) select the icon.

*The Main Pane defaults to the **General** (Employees/Staff) tab, if **Visitors** is required; select that tab before proceeding further.*

2. In the Main Pane, click the button.

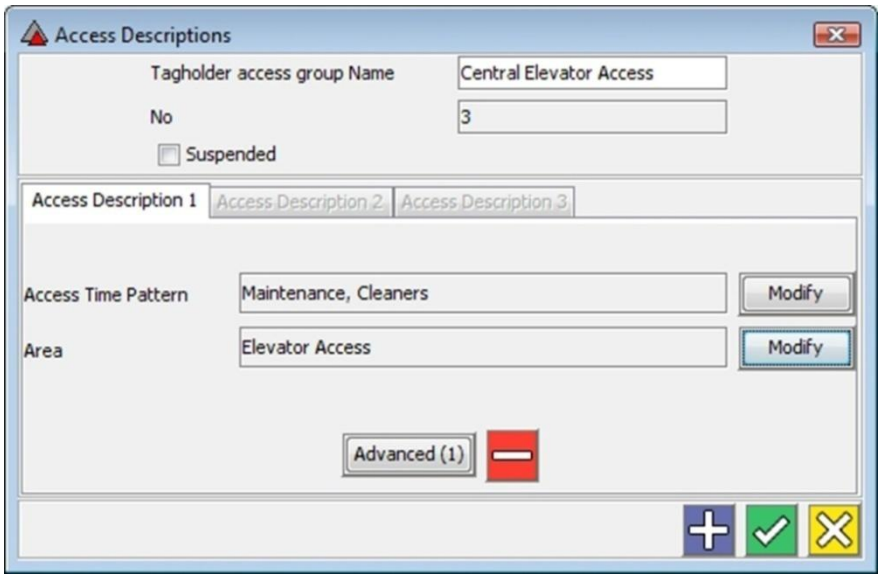

Figure 12 – Access Descriptions Dialog

3. In the **Tagholder Access Group Name** field, assign a meaningful name (for example **Central Elevator Access**).
4. Click the button, activating the Access Description.
5. Alongside the **Access Time Pattern** field, click the **Select** Button.
6. From the displayed records, choose the required Time Pattern.
7. Alongside the **Area** field, click the **Select** button.
8. From the displayed records, choose the required Area.
9. Click the **Advanced (1)** button.

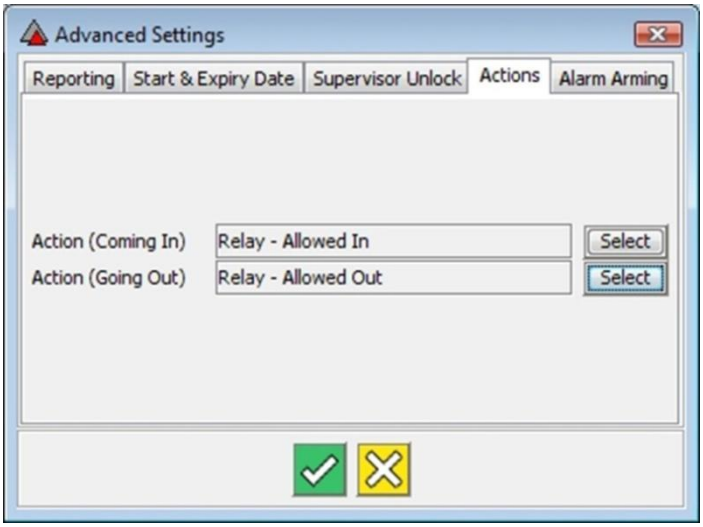

Figure 13 – Advanced Settings Dialog

10. Select the **Actions** tab.

The Select buttons shown in Figure 13 only activates if you set the Zone Anti-passback setting as Strict. Refer to the Relay Setup procedure on page 13.

11. Alongside the **Action (Coming In)** field, click the **Select** button.
12. From the **Actions at Locations** drop-down list, select the required **Location**.
13. Following with the example we used in the section Relay Setup (on page 13), select the ImproX O16 Terminal's **Elevator Access** action.
14. Click the button.
15. In the Advanced Settings dialog, select the **Start & Expiry Date** tab.
16. Edit the dates as necessary.
17. Click the button.
18. Close the Access Descriptions dialog by clicking on the button.

Assign Access to Tagholders

1. In the Navigator Pane (from the Hierarchical Tree) select the icon.
2. From the records displayed in the Main Pane select a Tagholder who requires access to the Lift (Elevator).
3. With the Tagholder's record selected, click the button.
4. In the Edit Tagholder dialog, click the **Tag** (1-8) button associated to the Tag for editing.
5. From the **Tagholder Access Groups Available for Site** group, from the next available **Group** (1-10) drop-down list, select the **Central Elevator Access** group that you created earlier.

Interleading Zone Routing

Purpose of this Feature

Select the Strict Anti-passback (APB) Zone setting, when enforcing Interleading Zone Routing.

The purpose of **Interleading Zone Routing** is to force people to follow a logical path of tagging IN and OUT. Interleading Zone Routing is used mostly with Time and Attendance Software where it's necessary for Tagholders to clock in and out of their work area for payment purposes. For example the Work Area Zone lies within a larger access controlled Perimeter Zone. A Tagholder's normal tagging route for a work-day is:

1. IN at the Perimeter Zone.
2. IN at the Work Area Zone.
3. OUT of the Work Area Zone.
4. OUT of the Perimeter Zone.

Once inside the Perimeter Zone, the Tagholder is allowed to freely tag-in and tag-out of the Work Area Zone. However, the Tagholder is prevented from tagging-out of the Perimeter Zone if currently tagged into the Work Area Zone. This means the following sequence is NOT allowed:

1. IN at the Perimeter Zone.
2. IN at the Work Area Zone.
3. OUT of the Perimeter Zone (Denied Interleading Zone Routing).

A Tagholder must also have tagged into the Perimeter Zone otherwise access to the Work Area Zone is denied. There may be several perimeter access points on different Controllers but all the Perimeter Zones MUST belong to a Common Zone. There may be several work area access points on different Controllers but, again, all the Work Area Zones MUST belong to a Common Zone. You MUST set the entry and exit locations for the Work Area Zones to interlead to one of the Perimeter Zones.

Example

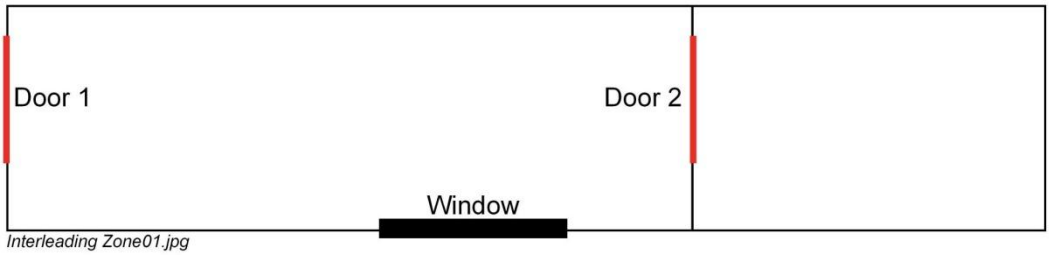

Figure 14 – Interleading Zone Routing

We want Tagholders to tag-in at Door 1 and THEN tag-in at Door 2, and not to tag-in at Door 2 if they have not tagged-in at Door 1. In reality somebody may climb through the window, and try tagging-in through door 2 without tagging-in at door 1.

Procedure

Let's look at it from an ImproNet point of view:

Interleading Zones

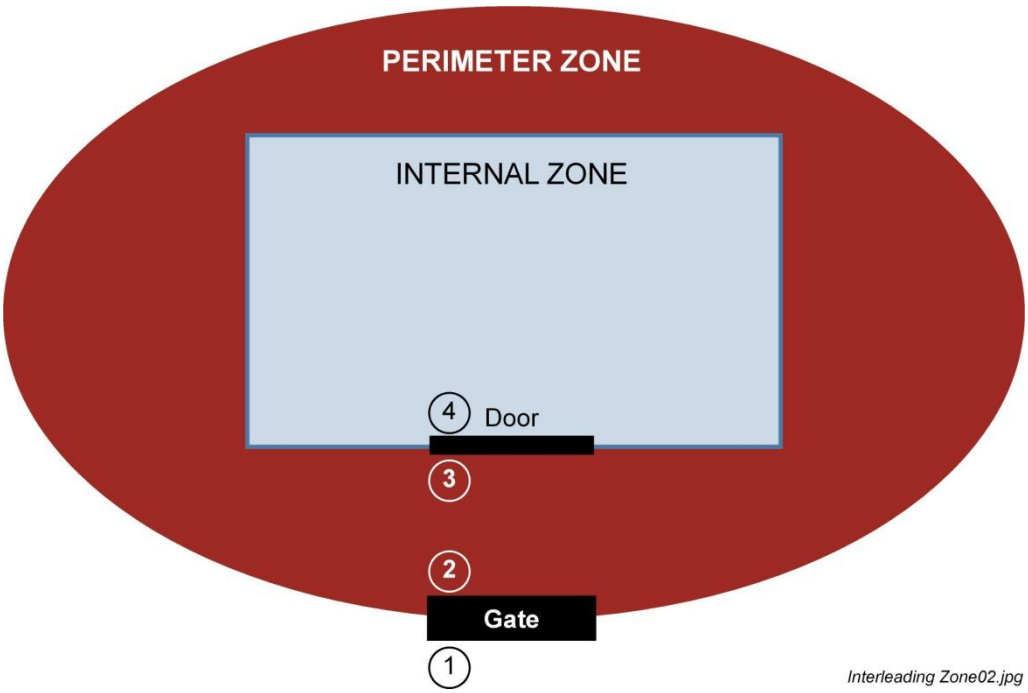

Figure 15 – Interleading Zone Routing

We configured the System using 2 zones, and a minimum of 4 Readers. Two Readers for each access point, 1 IN and 1 OUT for Anti-passback (APB). So when Tagholder A presents their Tag at Reader 1, Tagholder A's considered to be inside the Perimeter Zone. At this point Tagholder A has two available transactions: OUT at Reader 2 or IN at Reader 3.

This routing thus prevents Tagholder A from passing their Tag back through the gate for use by another person trying to enter at Reader 1. Tagholder A's also prevented from passing their Tag through a window to the Internal Zone for a person trying to exit at Reader 4.

In summary, the Gate (Perimeter Zone) is in one zone, and the Office Door (Internal Zone) is another zone. To get into the internal office area, you need to go through the gate and through the door.

To set up this scenario:

1. In Access, select the **Site** in the Navigator Pane.
2. Select the **Enforce Zone Routing** checkbox.

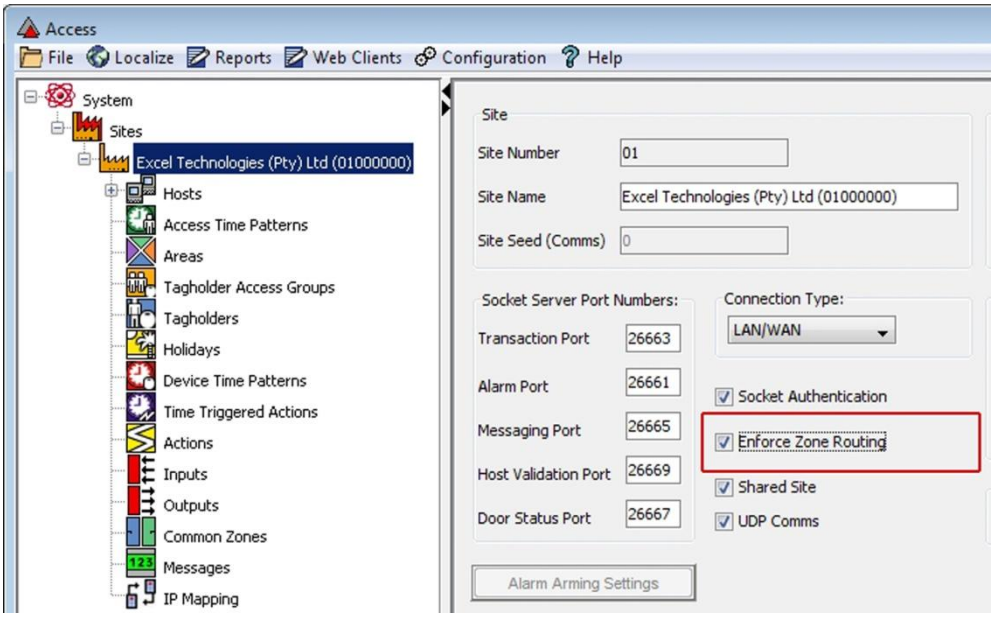

Figure 16 – Enforce Zone Routing Checkbox

3. Click on **Location: Office Door**.
4. And in the **Interleading to Zone** drop-down list, select the **Perimeter Zone**.
5. Select the **Enforce Interleading Zone Routing** checkbox.

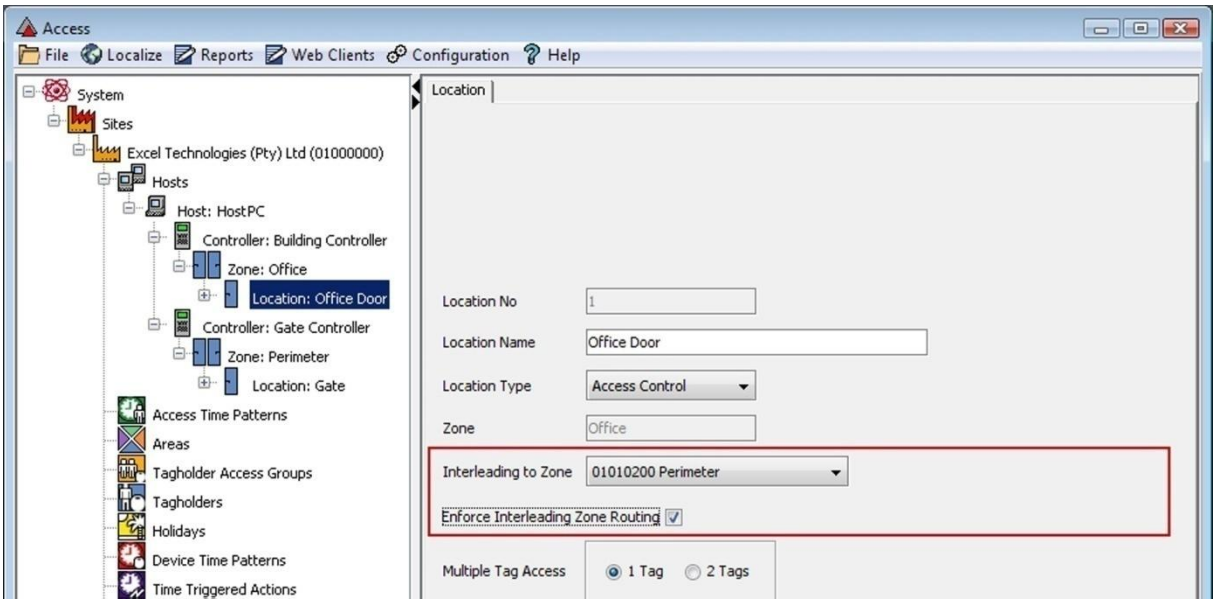

Figure 17 – Interleading to Zone and Enforce Interleading Zone Routing Options

Always interlead your INTERNAL ZONE to your EXTERNAL ZONE.

Common Zones for Anti-passback (APB)

Needed when zones belonging to different Controllers must have Anti-passback (APB) controls applied as these zones form a single physical work area. If Anti-passback is set, then tagging-in to any of the zones belonging to a common zone prevents entry to any of the zones until tagging-out of the common zone has taken place. In this scenario, the Controllers must

communicate with one another, and update each other on presentation of the Tag. Zones can only be specified as common if they exist on different Controllers.

Each Controller can have only ONE configured Common Zone.

Common Zones for Interleading Routing

You may also apply Interleading Zone Routing to Common Zones. Consider the following:

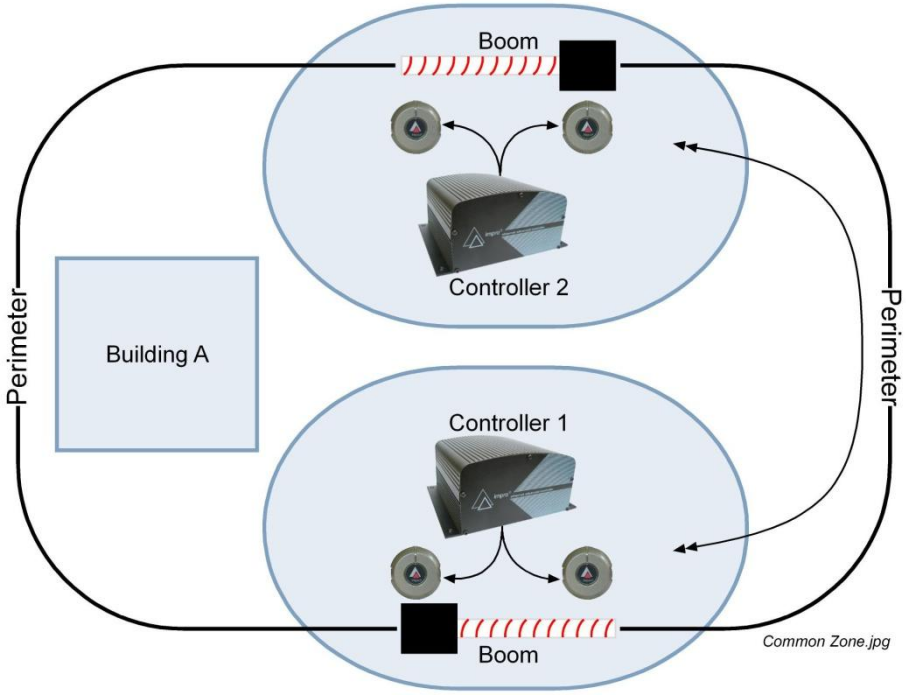

Figure 18 – Interleading Zone Routing

Consider 2 internal zones (Office 1 and Office 2) on different Controllers belonging to a common zone. Each zone must be separately configured to interlead to the same Perimeter Zone. If there are several Perimeter Zones all belonging to a common zone then choose any one of those zones to interlead all the internal zones to.

If interleading to a zone on a different Controller then ensure that that zone is a member of a Common Zone even if it is the only member.

Location for Office Door 1

1. In Access, click on **Location: Office Door 1**.
2. In the Main Pane, in the **Interleading to Zone** drop-down list, select the **Perimeter Zone**.
3. Select the **Enforce Interleading Zone Routing** checkbox.

Location for Office Door 2

1. Click on **Location: Office Door 2**.
2. In the Main Pane, in the **Interleading to Zone** drop-down list, select the **Perimeter Zone**.
3. Select the **Enforce Interleading Zone Routing** checkbox.

Troubleshooting

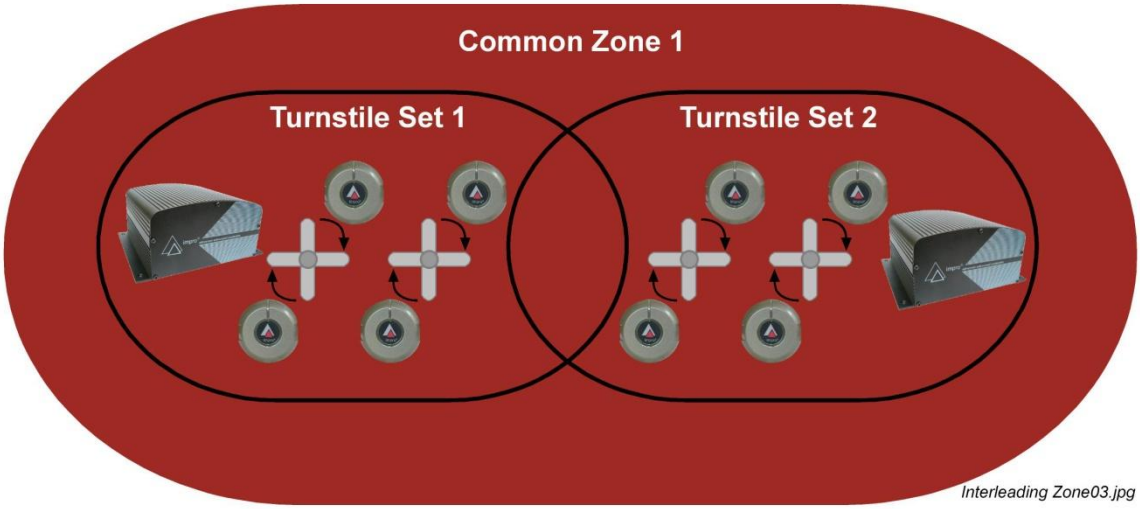

Figure 19 – Interleading Zone Routing

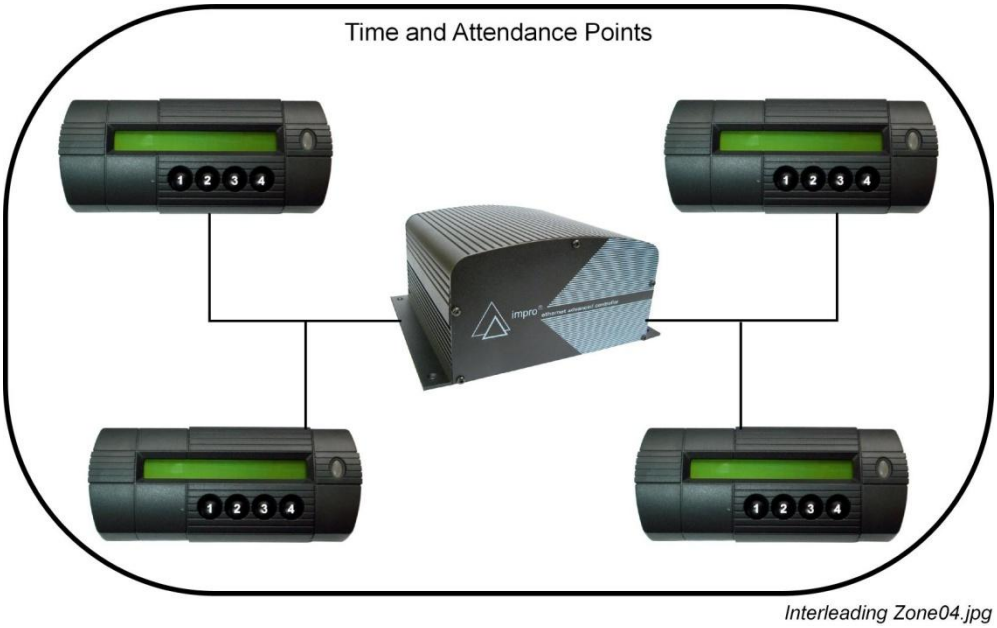

Figure 20 – Interleading Zone Routing

In the scenario outlined in Figure 19 and Figure 20:

- The Red area represents a Common Zone.
- This Common Zone includes 2 double sets of Turnstiles, each controlled by their own Controller.
- The Time and Attendance points also have their own Controller.
- Zone Broadcast is enabled on each of the Zones.
- Interleading Zone Routing is set up and the Time and Attendance points interlead to the Turnstiles.

In this scenario, create another Common Zone for the Time and Attendance points, ensuring that the 2 Common Zones communicate with one another.

Random Search

Purpose of this Feature

When Random Search is active, the System randomly selects a Tagholder for searching. The System can select ANY Tagholder. When the System selects the Tagholder for searching, a red light shines, an external buzzer sounds and the IN and OUT Antenna Readers prevent other Tagholders gaining access. Security officials must then take the selected Tagholder aside, and then present their "security" Tag to the Override Antenna Reader on the turnstile. This Tag presentation unlocks the inhibited IN and OUT Antenna Readers allowing normal traffic flow.

There is a chance the searched Tagholder may be selected again when they re-present their Tag at the IN or OUT Antenna Reader. This is possible and some inconvenience may arise.

Example

This example procedure and Figure 21 refer to connections using the ImproX iTT. You may however use other Terminals from the ImproX family, including the ImproX MfT, ImproX iTRT or ImproX I16.

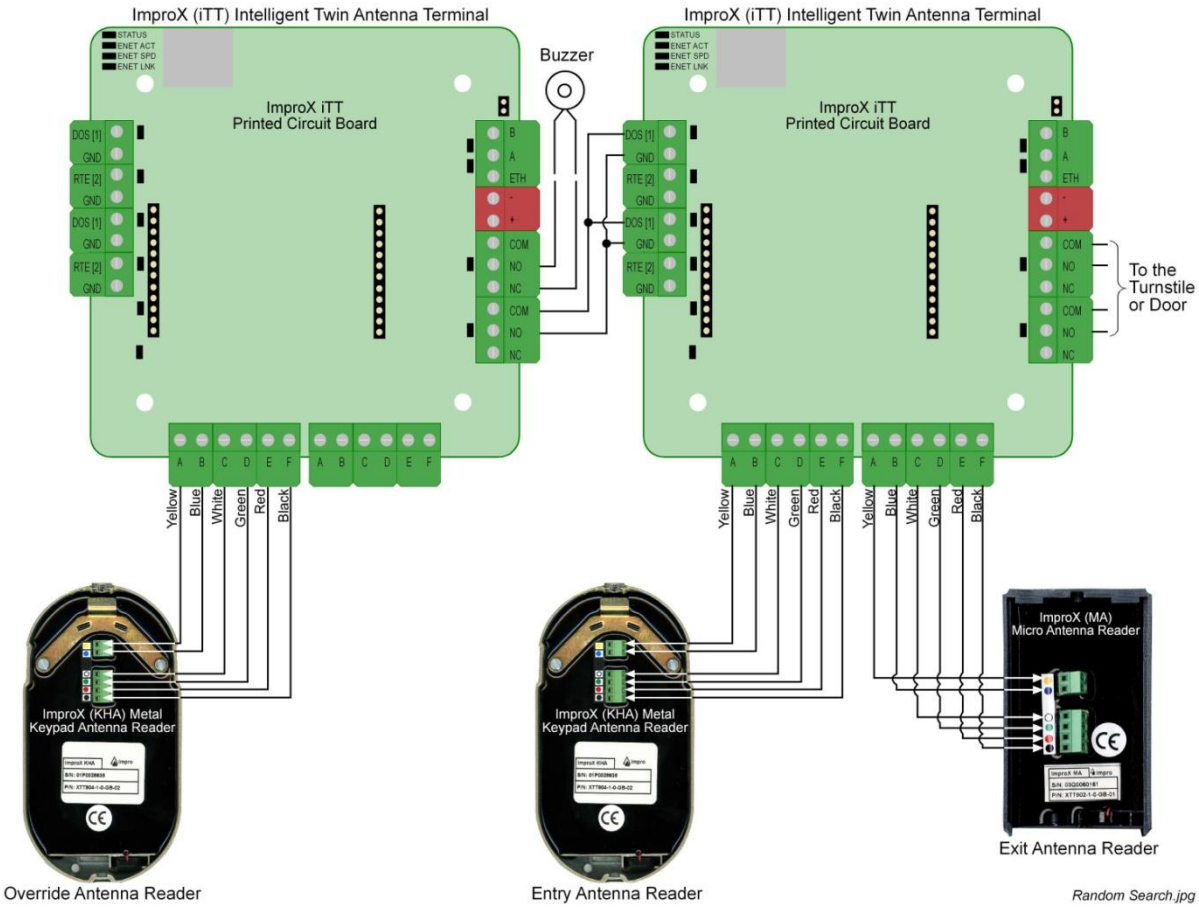

Figure 21 – Random Search Connection Details

Procedure

Initial Setup

Set up and name the Terminals and Readers as shown in Figure 21 and Figure 22.

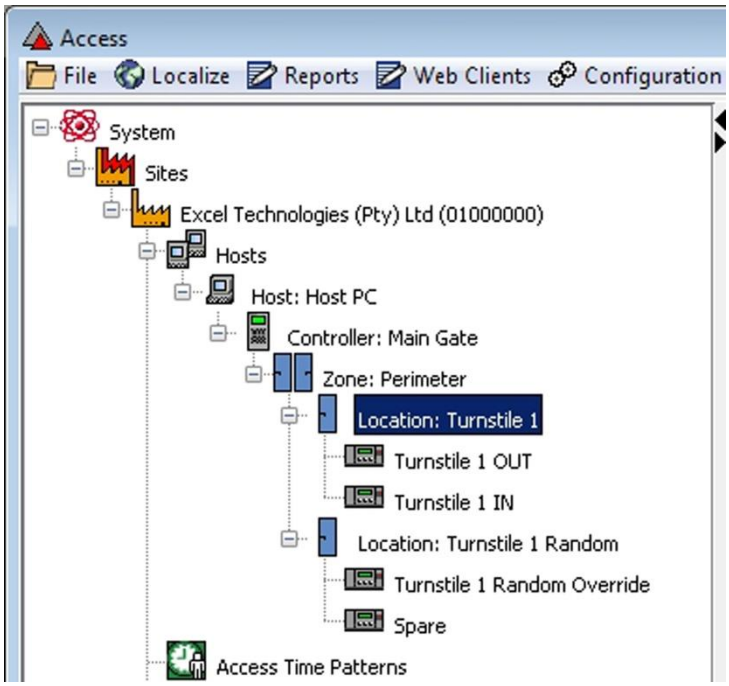

Figure 22 – Random Search Setup

1. In Access, select the **Site** in the Navigator Pane.
2. Select the Location, **Turnstile 1**.
3. Select the Terminal, **Turnstile 1 In**.
4. Select the **Edit Terminal Parameters** button.
5. In the **Random Search** textbox, enter a suitable value.

A low value here selects more often, a high value selects less frequently.

6. Click the button.
7. Select the Terminal, **Turnstile 1 Out**.
8. On the Main Pane, click the **Edit Terminal Parameters** button.
9. In the **Random Search** textbox, enter a suitable value.
10. Click the button.

Input Setup

Next setup the Door Inhibiting Inputs on the **ACCESS iTT**, do this for both Antenna Readers:

Turnstile 1 In

This step is important, if not carried out correctly; you could inhibit the wrong Antenna Reader.

1. In the Navigator Pane, select the Terminal, **Turnstile 1 In**.
2. In the Main Pane, select the **Inputs** tab.
3. On the Main pane, select the **General Input 1** record.
4. Click the button.

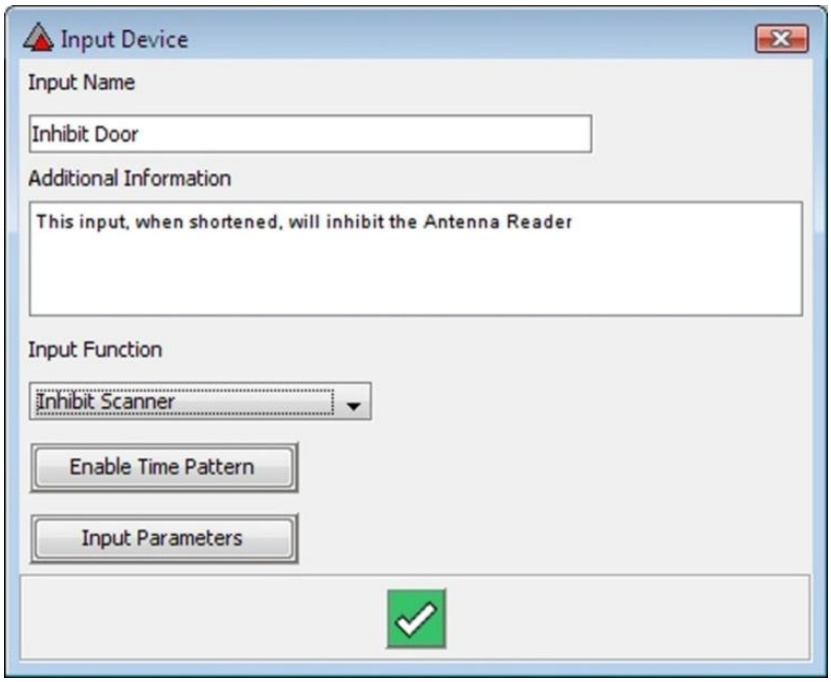

Figure 23 – Input Device Dialog

5. In the **Input Name** field, assign the Input a name.
6. From the **Input Function** drop-down list, select **Inhibit Scanner**.
7. Click the **Input Parameter** button.

The ability to inhibit multiple units, as shown in Figure 24, is only available on sites using EC^{II} Controllers (IXP400i Sites). In configurations using IC's or EC's (IXP300 and IXP400 Sites) the dialog only lets you inhibit a single unit.

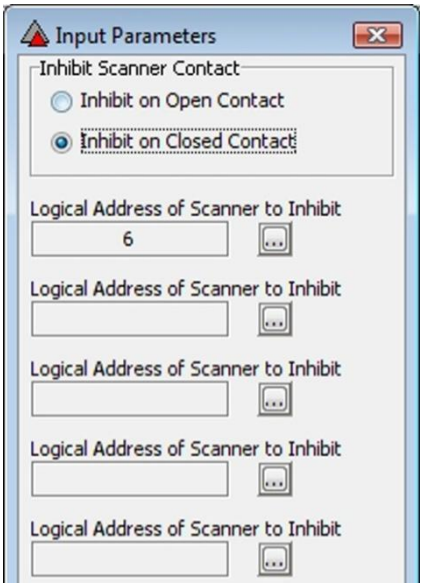

Figure 24 – Input Parameters Dialog

8. Based on the connections shown in Figure 21, in the Input Parameters dialog, select the **Inhibit on Closed Contact** radio button.
9. Ensure the **Logical Address of Scanner to Inhibit** textbox displays the correct scanner to inhibit, if incorrect, click the button alongside the textbox and make your selection accordingly.
10. Close the Input Parameters dialog by clicking the button.
11. Close the Input Device dialog by clicking the button.

Turnstile 1 Out

1. In the Navigator Pane, select the Terminal, **Turnstile 1 Out**.
2. In the Main Pane, select the **Inputs** tab.
3. On the Main pane, select the **General Input 1** record.
4. Click the button.
5. In the **Input Name** field, assign the Input a name.
6. From the **Input Function** drop-down list, select **Inhibit Scanner**.
7. Click the **Input Parameter** button.
8. Based on the connections shown in Figure 21, in the Input Parameters dialog, select the **Inhibit on Closed Contact** radio button.
9. In the Input Parameters dialog, alongside the first available **Logical Address of Scanner to Inhibit** textbox, click the button.
10. From the dialog, select the record associated to **Turnstile 1 Out**.
11. Click the button.
12. Close the Input Parameters dialog by clicking the button.
13. Close the Input Device dialog by clicking the button.

Setting up Actions

Next set up an action on the **Random iTT**, for driving a relay when the Tagholders selected:

Scanners Disabled Action

1. In the Navigator Pane, select the Terminal, **Turnstile 1 Random Override**.
2. In the Main Pane, select the **Actions** tab.
3. Click on the button.

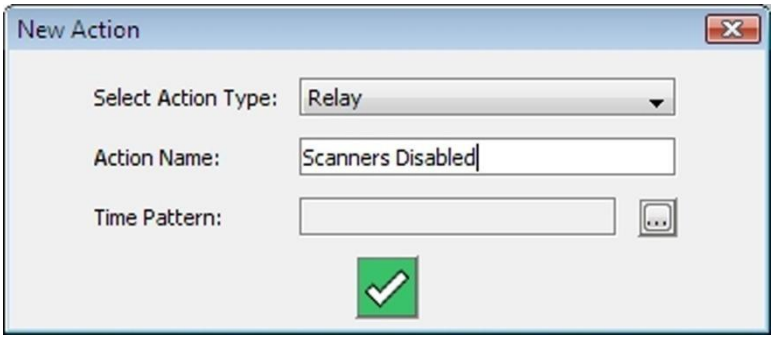

Figure 25 – New Action Dialog

4. From the **Select Action Type** drop-down list, select **Relay**.
5. Assign the Action a name, such as **Scanners Disabled**.
6. Click the button.

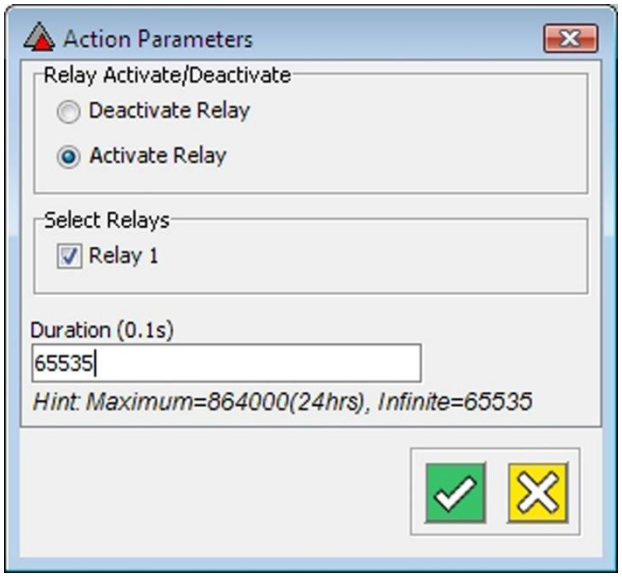

Figure 26 – Action Parameters Dialog

7. In the **Action Parameters** dialog, set the **Duration** to **65535,** to drive the relay indefinitely.
8. Click the button.

Relay Allowed In Action

1. In the Main Pane, on the Actions tab, select the action **Relay Allowed In**.
2. Click the button.

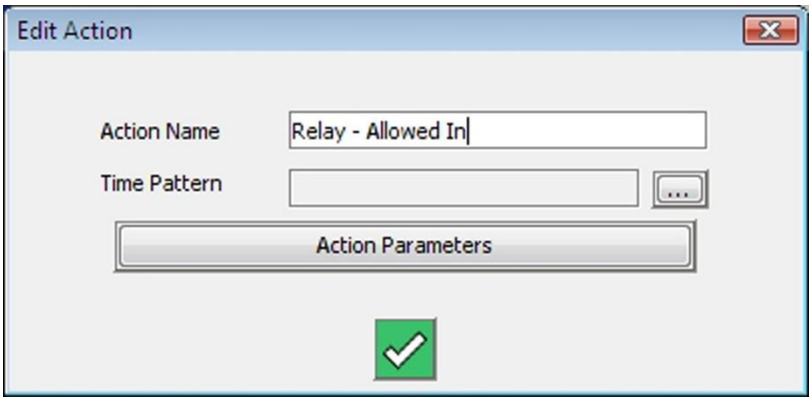

Figure 27 – Edit Action Dialog

3. In the Edit Actions dialog, click on the **Action Parameters** button.
4. From the Relay Activate/Deactivate group, select the **Deactivate Relay** radio button.
5. Set the **Duration (0.1s)** to **65535,** to drive the relay indefinitely.
6. Close the Action Parameters dialog by clicking the button.
7. Click the button.

Buzzer Action

1. In the Navigator Pane, select the Terminal, **Spare**.
2. In the Main Pane, on the Actions tab, click the button.
3. From the **Select Action Type** drop-down list, select the **Relay** option.
4. Assign your action a suitable **Action Name** (for example **Buzzer**).
5. Click the button.

6. From the Relay Activate/Deactivate group, select the **Activate Relay** radio button.
7. Click the button.

Now, tell the Antenna Readers, that if a Tagholder's denied by Random Search, the **Random Turnstile iTT** must drive it's relay Inhibiting the Scanners.

Turnstile 1 In

1. In the Navigator Pane, select the Terminal, **Turnstile 1 In**.
2. In the Main Pane, select the **Actions** tab.
3. At the bottom left-hand side of the Main Pane, click the **Active System Events** button.

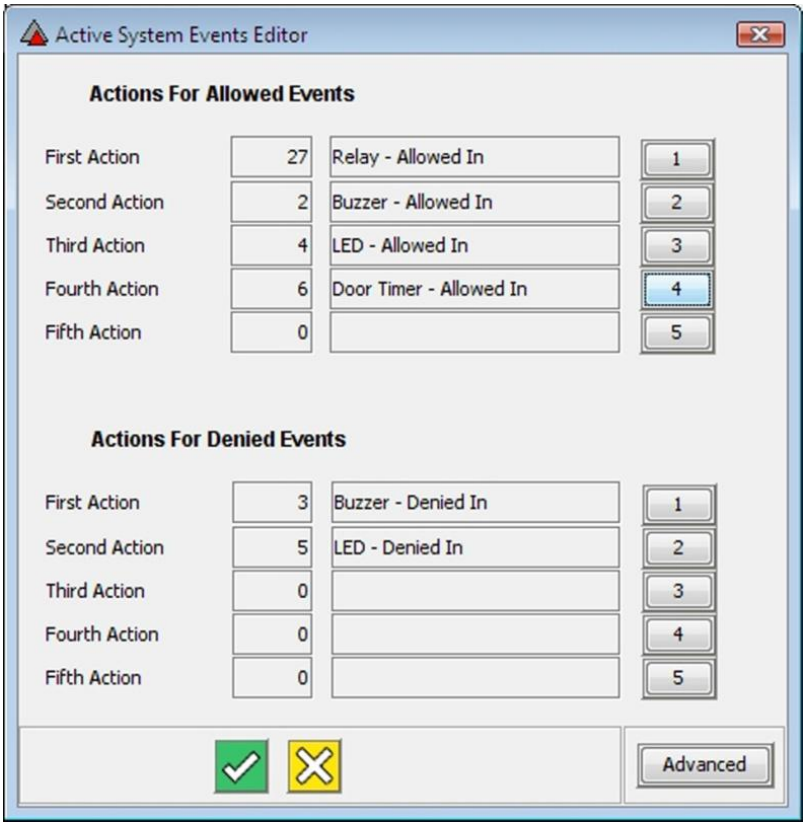

Figure 28 – Active System Events Editor Dialog

4. At the bottom right-hand side of the Active System Events Editor dialog, click the **Advanced** button.

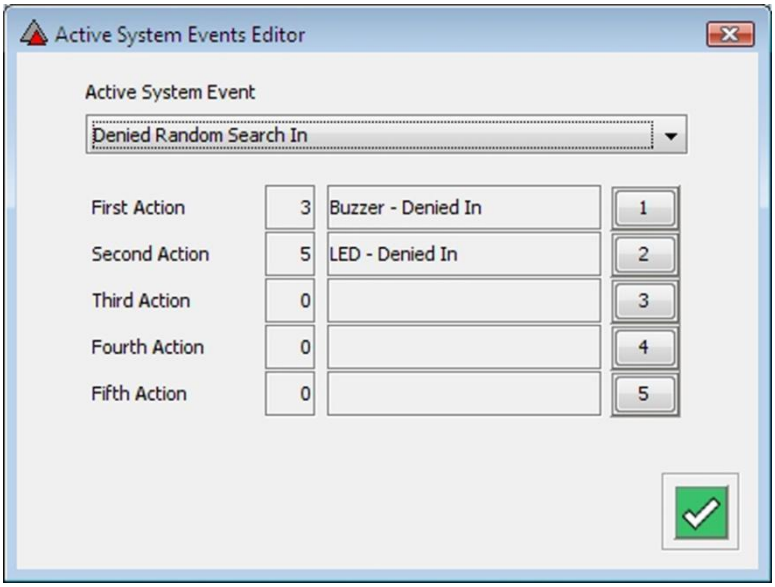

Figure 29 – Active System Events Editor (Advanced) Dialog

5. From the **Active System Event** drop-down list, select **Denied Random Search In**.
6. Select the next unassigned action.
7. Click the action's associated numeric button.
8. In the **Action Selector** dialog, select the **Scanners Disabled** action created earlier.
9. Click the button.
10. Select the next unassigned action.
11. Click the Actions numeric button.
12. In the **Action Selector** dialog, select the **Buzzer** action created earlier.
13. Click the button.
14. Close the Active System Events Editor dialog by clicking on the button.

Turnstile 1 Out

1. In the Navigator Pane, select the Terminal, **Turnstile 1 Out**.
2. In the Main Pane, select the **Actions** tab.
3. At the bottom right-hand side of the Main Pane, click the **Active System Events** button.
4. At the bottom right-hand side of the Active System Events Editor dialog, click the **Advanced** button.
5. From the **Active System Events** drop-down list, select **Denied Random Search Out**.
6. Select the next unassigned action.
7. Click the action's associated numeric button.
8. In the **Action Selector** dialog, select the **Scanners Disabled** action created earlier.
9. Click the button.
10. Select the next unassigned action.
11. Click the action's associated numeric button.
12. In the **Action Selector** dialog, select the **Buzzer** action created earlier.
13. Click the button.
14. Close the Active System Events Editor dialog by clicking on the button.

Messages

Purpose of this Feature

Devices fitted with an LCD, such as a Time and Attendance Reader, can display a **Message**. Messages can be activated by Events and Time Triggered Events. The Message screen in ImproNet Access enables you to create up to **63** Messages for assignment to suitable hardware.

Procedure

Create a Message

To create a new Message, proceed as follows:

1. In the Navigator pane, click the icon.
2. In the Main pane, select a **Message** number from the No drop-down list. The default value is 1.
3. Enter the Message content in the **Message** textbox.
4. Click the button to save.
5. Repeat steps 1 to 4 to create additional messages.

Remember to select an unused Message Number each time; otherwise the original Message will be overwritten.

Using Messages

To use the Messages you created, proceed as follows:

Create the Action

1. In the Navigator pane, select the Terminal or Remote you want to display the Message.
2. In the Main pane, select the **Actions** tab.
3. Click the button.
4. In the New Action dialog, from the **Select Action Type** drop-down list, select **LCD**.
5. In the **Action Name** textbox, give the Action a suitable name.
6. Click the button.
7. In the Action Parameters dialog, in the **Text Message Number** textbox enter the appropriate message number. For example based on the Figure 30, enter 2 to display “Welcome”.

Only complete the Line and Column textboxes when using an ImproX DL.

8. In the **Duration** field, enter the duration for displaying the Message. The default duration is **40**.
9. In the LCD Mode group, select the **Clear Display** checkbox.

10. Click the button.

Assign the Action

1. On the Actions tab, click the **Active System Events** button.
2. In the Active System Events Editor dialog, from the Actions for Allowed Events group, click the numeric button alongside the next available **unused Action**.
3. In the Action Selector dialog, select the appropriate **LCD Action** type.
4. Click the button.
5. Click the button.
6. In the Confirm Save dialog, click the **Yes** button.

The ImproX TA, iTA, TAR and iTAR range of Terminals and Readers only display 16 characters. Messages longer than 16 characters will NOT display in their entirety.

Delete a Message

To Delete a Message, proceed as follows:

1. In the Navigator pane, click the icon.
2. In the Main pane, click a **Message** to select it.

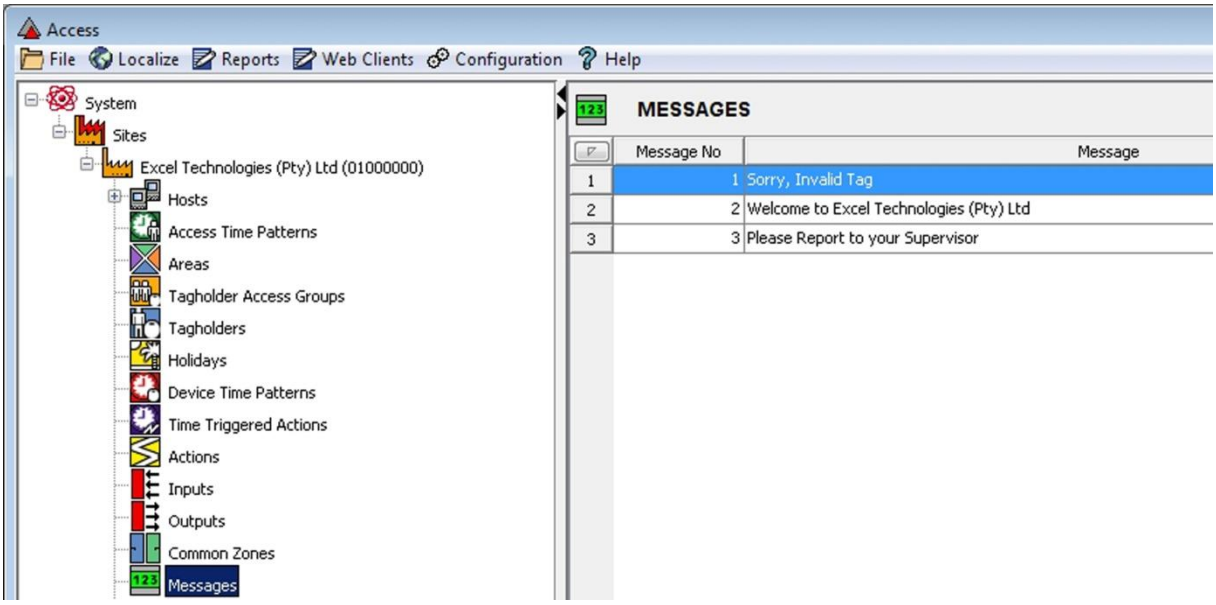

Figure 30 – Messages Screen

3. Click the button.

Emergency Door Open

Purpose of this Feature

The **Emergency Door Open** feature provides an exit route in the unlikely event of an emergency.

Example

The fire panel provides an output linked up to an input on the Access Control System.

Procedure

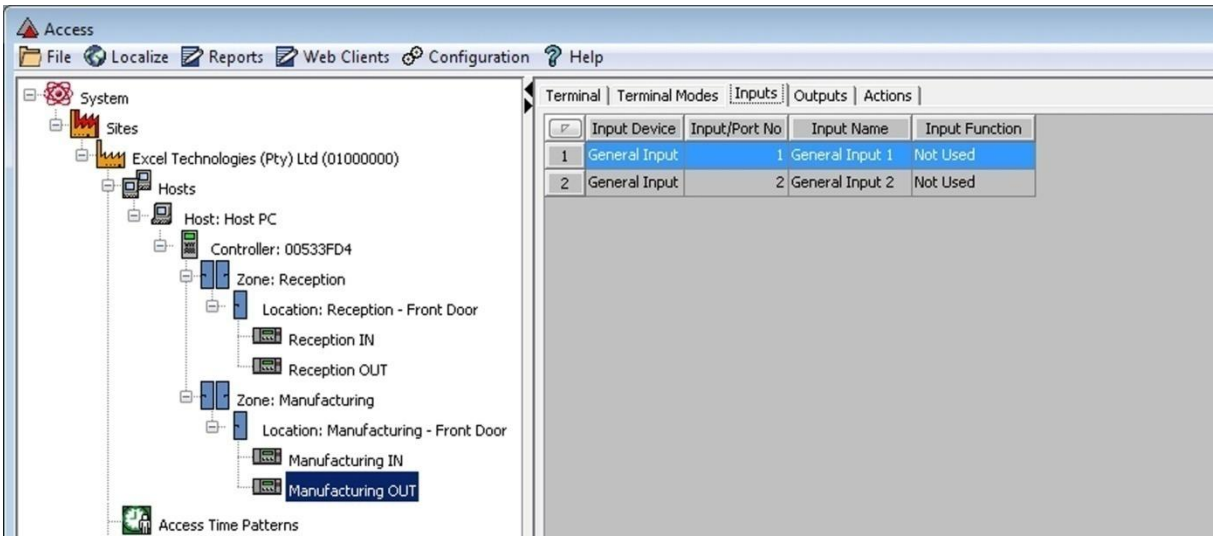

Figure 31 – Main Pane Showing the Inputs Tab Selected

Configure the Inputs

1. Select the specific Terminal that must receive the output from the Fire Panel.
2. Click on the **Inputs** tab.
3. Select either **Input 1** or **Input 2**.
4. Click the button.

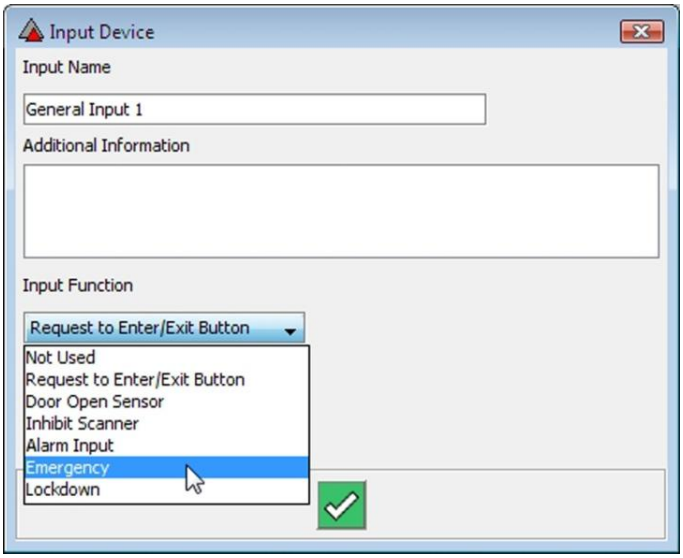

Figure 32 – Input Device Dialog

5. In the **Input Name** field, type in a name for the Input.
6. From the **Input Function** drop-down list, select **Emergency**.

Ensure that your input parameters are correct. Either open or closed state.

7. Click the button.

Configure the Outputs

1. Click on the **Outputs** tab.
2. Click the button.

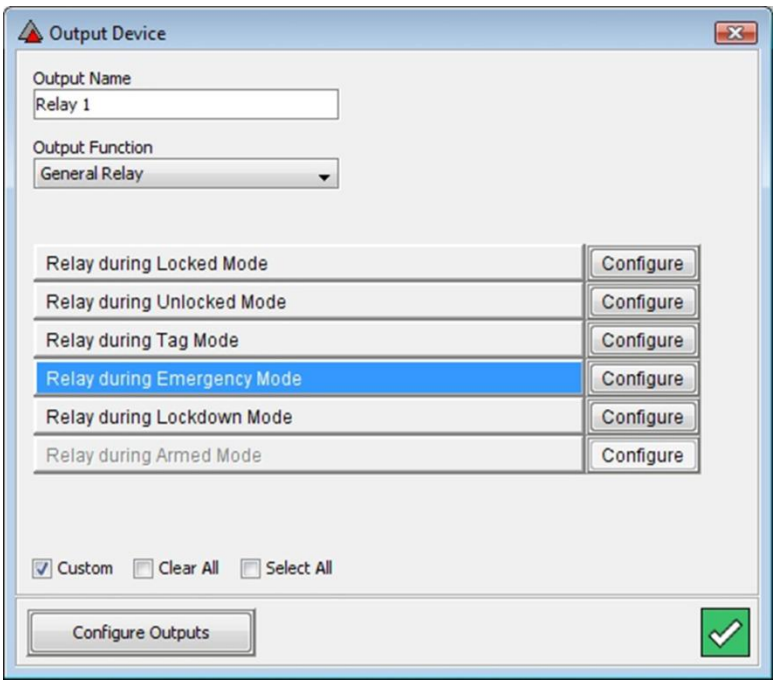

Figure 33 – Output Device Dialog

3. In the **Output Name** field, type in a name for the Output.
4. Alongside **Relay During Emergency Mode** click the **Configure** button.

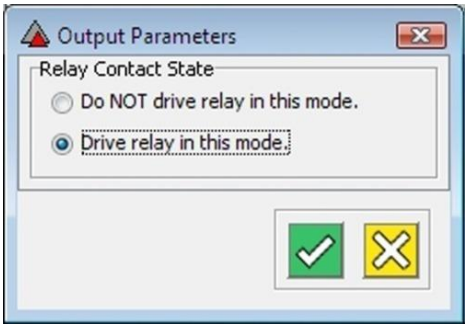

Figure 34 – Output Parameters Dialog

5. Select the **Drive Relay in this Mode** radio button.
6. Click the button, to return to the Output Device Dialog.
7. Click the button.

Repeat the output procedure on all doors that must open in case of emergency.

Lockdown Terminal Mode

Purpose of this Feature

Lockdown Terminal Mode locks selected doors in such a way that no Tagholder can gain access through those doors. This Mode can be used, for example, when intruders are in the area concerned, and they are to be denied exit through a selected Door or group of Doors. You may select this Mode at Controller or Terminal level.

Example

An intruder is detected in the company Strong Room. The Operator decides to place the Strong Room door in Lockdown Terminal Mode.

Procedure

Lock-down On Mode

Start the Engine thereby ensuring that the Site is on-line before continuing further.

1. In Access, Navigator Pane:
   - select the appropriate **Site** icon.
   - under the **Host** icon, select the **Strong Room Exit Terminal**.
2. With the Terminal (Reader) selected Right-click your mouse, opening the menu below.

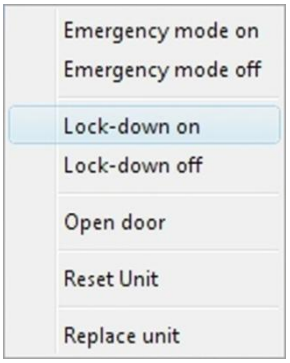

Figure 35 – Lock-down Menu

3. Select **Lock-down On**.
4. In Windows®, select **Start**>**Programs**>**ImproNet**>**Graphics Runtime**.
5. Enter your **Username** and **Password**.

*The default username is **SYSDBA**. The default password is **masterkey**. The Password is case-sensitive.*

6. Select the **Door Status** tab.

The Strong Room Door displays in Lock-down Mode see Figure 36.

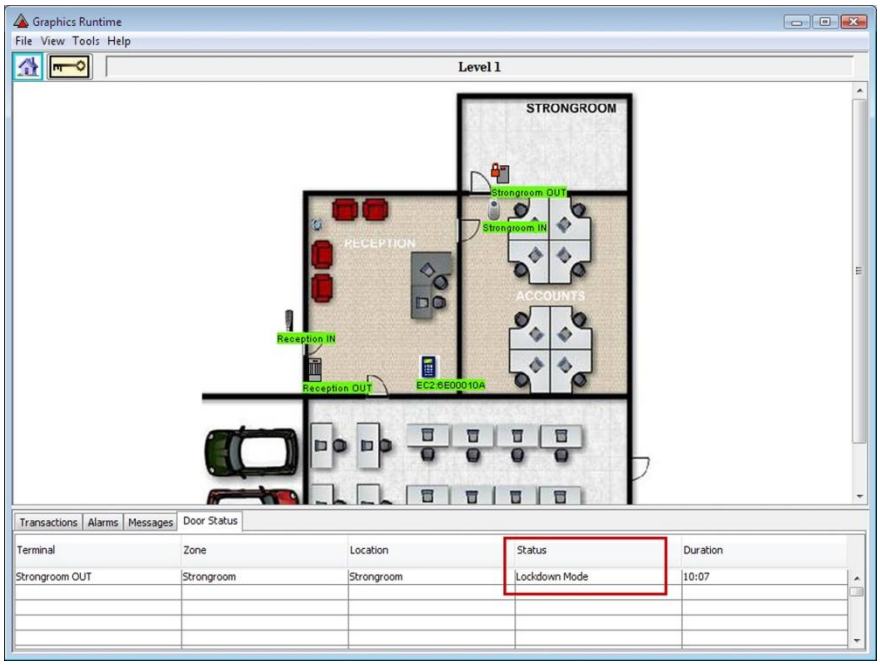

Figure 36 – Lockdown Mode at Terminal Level

You may apply the same procedure at Controller level, in which case all Terminals connected to that Controller are placed in Lock-down Mode. Figure 37 shows the Door Status display in Graphics Runtime when Lock-down Mode is applied at **<u>Controller 1</u>** (Controller 00533FD4).

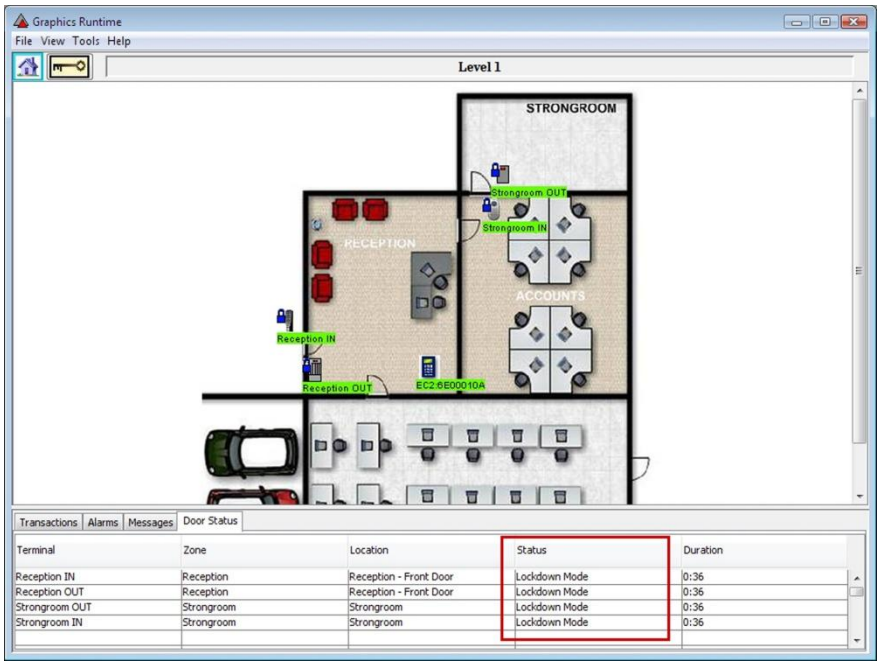

Figure 37 – Lockdown Mode Applied at Controller Level

Lock-down Off Mode

Start the Engine thereby ensuring that the Site is on-line before continuing further.

1. In **Access**, **Navigator Pane**:
   - select the appropriate **Site** icon.
   - under the **Host** icon, select the **Strong Room Exit Terminal**.
2. With the Terminal selected Right-click your mouse, opening the menu below.

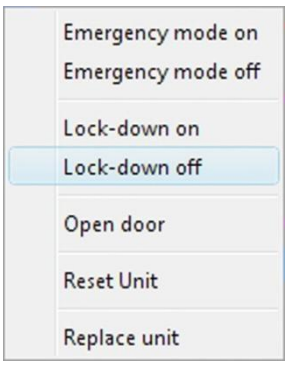

Figure 38 – Lock-down Menu

3. Select **Lock-down Off**.
4. In Windows®, select **Start**>**Programs**>**ImproNet**>**Graphics Runtime**.
5. Select the **Door Status** tab.

*In **Graphics Runtime**, view the **Door Status** by selecting **View**>**Door Status**>**Show Lockdown Mode**.*

If you apply Lock-down Mode to a Terminal, you can switch the Mode off either at Terminal level or at Controller level. However, when you apply Lock-down Mode to a Controller, you can only switch off the Mode at Controller level.

Force Upload of Hardware or Tagholder Data

Purpose of this Feature

The **Force Upload of Hardware or Tag Data** feature is used to force the upload of data from the Engine to the Controllers, without disrupting normal access control operation. The Feature operates at Host level. The Feature could be used, for example, where you have edited a large number of Tags, or you have made other configuration changes.

Example

Changes have been made to Tagholders Groups for a large building with several Controllers, and it is necessary to make this data available to the Controllers.

Procedure

1. In **Access**, select **Configuration**>**Force Upload** from the Menu Bar.

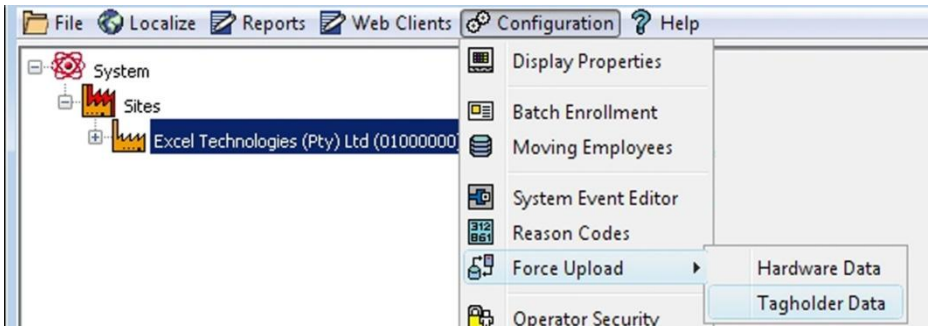

Figure 39 – Tagholder Data Selection

2. Select either **Hardware Data** or **Tagholder Data**. (For this example, we selected the **Tagholder Data** option).

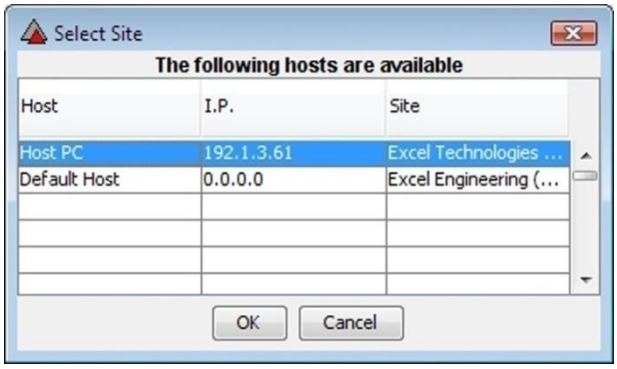

Figure 40 – Site Selection Dialog

3. In the **Select Site** dialog select the required Site.
4. Click the **OK** button.
5. The selected data uploads (if Engine is running).

Device Time Patterns (DTP's) supported in Actions

Purpose of this Feature

The **Device Time Patterns (DTP's) Supported in Actions** Feature allows Device Time Patterns to be associated with system Actions. When a Device Time Pattern is attached to an Action, this makes the Action active only during the period specified by the Device Time Pattern.

Example

For example, adding a Device Time Pattern to a Relay Action. In this case, the Action is to be enabled between the hours of 7 am to 5 pm, Sunday to Friday, and during those hours the Relay duration is required to be 2 minutes to permit handling of goods at that Location.

Procedure

1. In Access, select **Device Time Patterns** from the Navigator Pane.
2. In the Main Pane click the button.

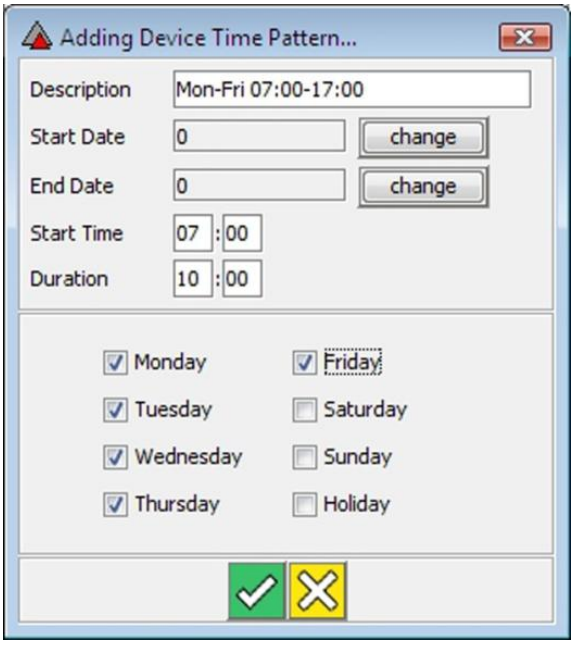

Figure 41 – Adding Device Time Pattern Dialog

3. In the **Description** textbox, enter a name for the Device Time Pattern.
4. In the **Start Time** field, enter **0700**.
5. In the **Duration** field, enter **1000**.
6. Select the **Monday** through **Friday** checkboxes.

7. Click the button.
8. Select the required **Terminal** in the Navigator Pane.
9. Select the **Actions** tab for the Terminal.
10. Select the **Relay – Allowed In** action.
11. Click the button.
12. In the **Edit Action** dialog, add the **Mon-Fri 0700-1700** device time pattern to the action.

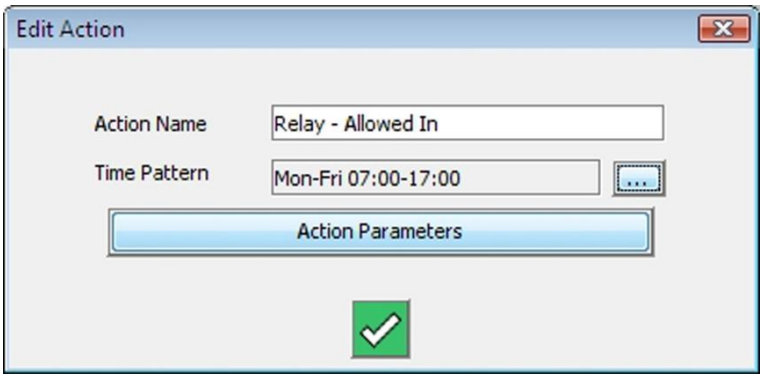

Figure 42 – Modify Relay – Allowed In Action

13. Click on the **Action Parameters** button.

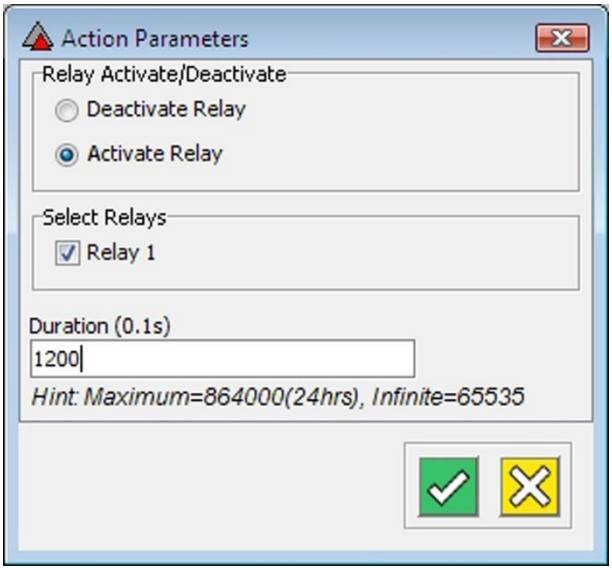

Figure 43 – Modify Relay – Allowed In Action Parameters

14. Set the **Relay Duration** to **120** seconds (10 = 1 second).
15. Close the **Action Parameters** dialog by clicking on the button.
16. Close the **Edit Action** dialog by clicking on the button.

Anti-passback (APB) Lockout Entry and Exit Delays

Purpose of this Feature

The **Anti-passback Lockout Entry and Exit Delays** feature lets you set delay periods enforcing Anti-passback (APB) Entry and/or Exit Lockout restrictions after the presentation of a Tag. This prevents multiple presentations of a Tag to the same Terminal during the delay period. And so provides extra protection against a Tag being passed back to another person for unauthorized access.

Procedure

1. Select the **Zone** required. A screen similar to Figure 44 displays in the Main Pane.

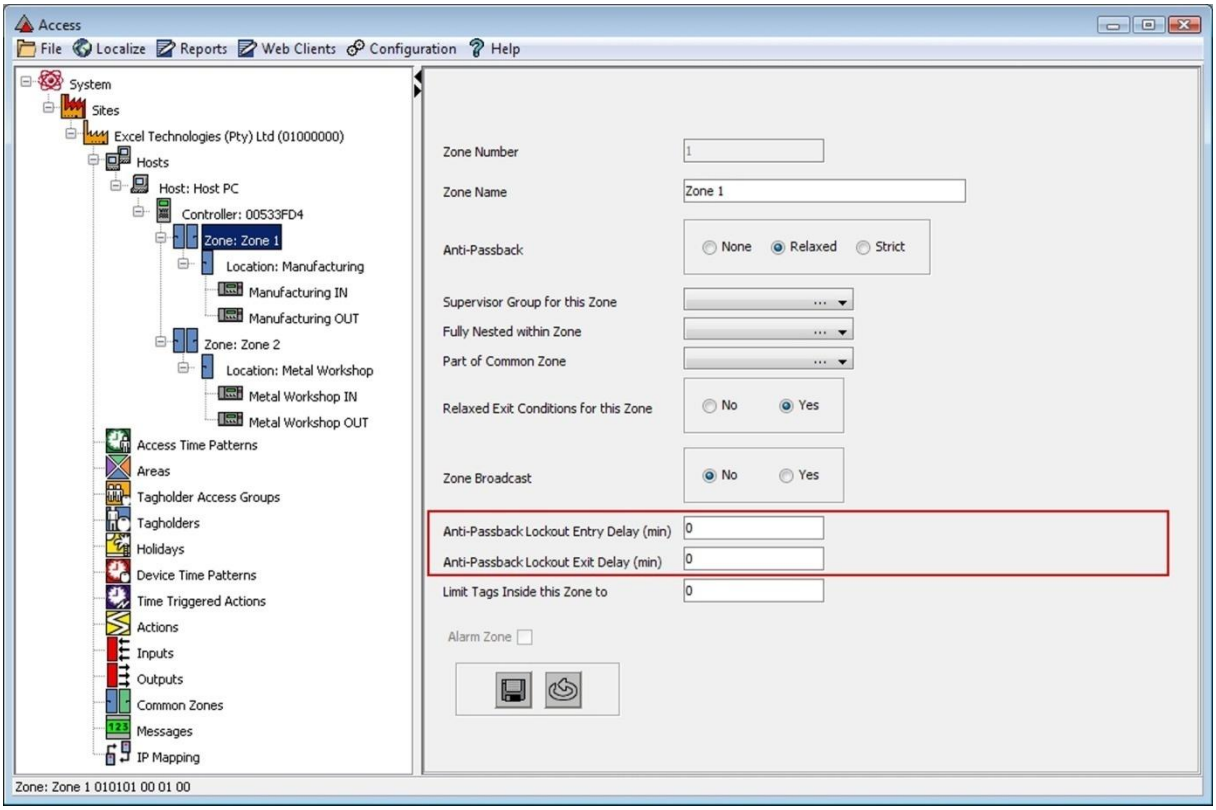

Figure 44 – Zone Selected

2. When either Relaxed APB or Strict APB is selected, the Anti-Passback Lockout fields enable.
3. In the **Anti-passback Locked Entry Delay** and/or **Anti-passback Locked Exit Delay fields**, enter the required time in minutes.
4. Click the button to accept these changes.

Operator Security

Purpose of this Feature

The ImproNet Software Suite offers full User and Operator Security. Previously, the third-party database utility, **IBConsole**, was required to administer usernames and passwords. Now, ImproNet facilitates administration of usernames and passwords.

Any User or Operator can be configured to have access to any part of the ImproNet Software. It is possible to restrict Operator access to specific Tagholders and ImproNet Applications.

Procedure

To open the Operator Security screen, proceed as follows:

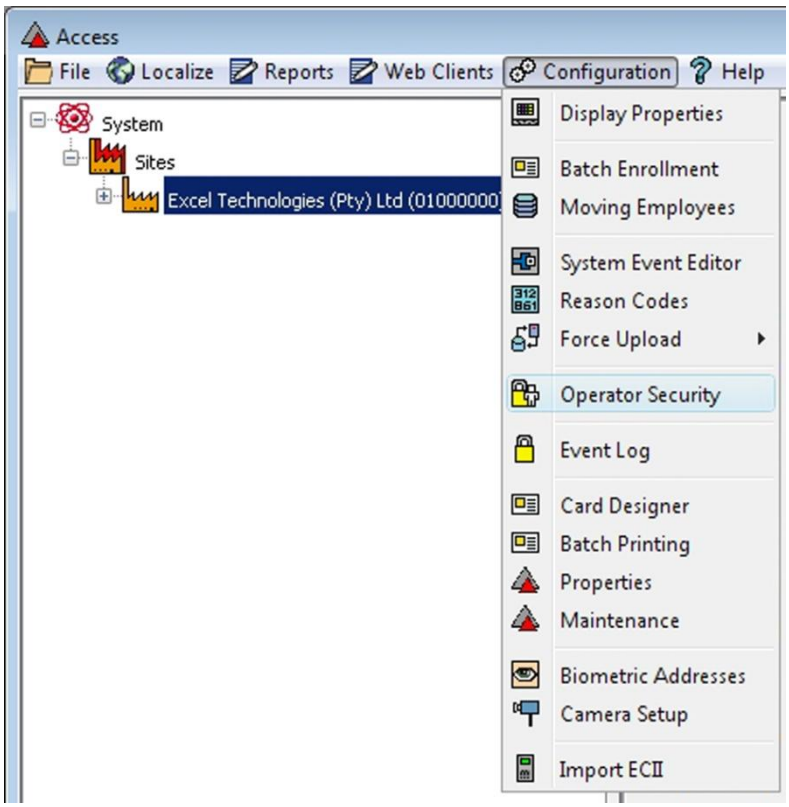

Figure 45 – Operator Security Selection

In Access, select **Configuration**>**Operator Security**.

System Administrator Group

By default, the Operator Security screen displays the System Administrator group. This group has *full access* to all ImproNet Software applications and all Tagholders.

The System Administrator group *cannot be edited or deleted*. **SYSDBA** is the *only* user that is a member of the System Administrator operator group.

Create Group

To create a new Operator Group, proceed as follows:

1. In Access, select **Configuration**>**Operator Security**.
2. Click the button.
3. Enter an **Operator Group Name**.
4. Click **OK**.

Operator Security Sections

The Operator Security screen consists of the following sections; configure each section for each Operator Group that you create.

- **Security Access**—the Security Access section defines the Software interfaces that different Users have access to. The Full Security access template is enabled by default. To change this, choose from a list of preset access template, or click the Advanced button to configure a new access template in the Security Control Panel.
- **Users**—add Users to the database BEFORE assigning them to an Operator Group.
- **Tagholder Access Groups**—the Tagholder Access Groups section specifies the Access Groups that the selected Operator has access to.
- **User Profiles**—when adding Tagholders to the database, you may assign them to a User Profile. However, you must create User Profiles in the Operator Group screen BEFORE you can assign Tagholders to them.

Security Access Section

Change Template

1. To change to a different template, click the button.
2. Select another template from the drop-down list.
3. Click the button.

Templates

You can select default, pre-configured templates from the **Security template name** drop-down-list. These templates are not editable but are useful for standard Users. Alternatively, create a new template as follows:

1. Click the **Advanced** button.
2. Click the button.

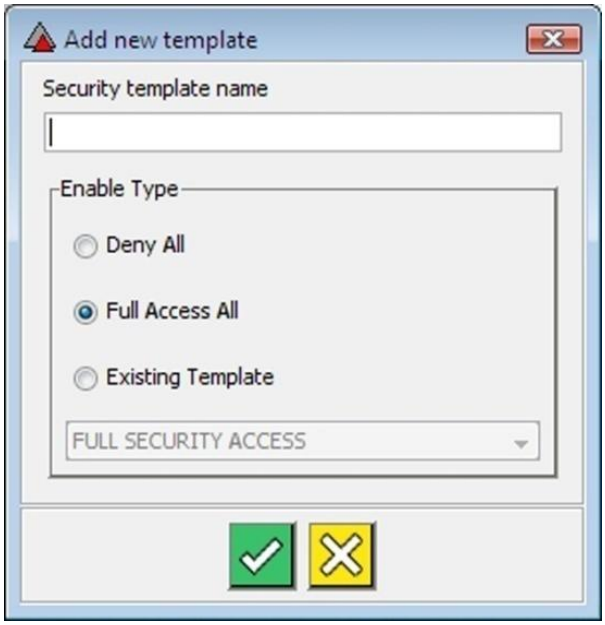

Figure 46 – Add New Template Dialog

3. In the **Add New Template** dialog, enter a **Security template name**.
4. Select one of the following options as a starting point:
   - **Deny All**—all parts of ImproNet Access are restricted. Use this option if you are only enabling a few items.
   - **Full Access All**—all parts of ImproNet Access are accessible. Use this option if you are only restricting a few items.
   - **Existing Template**—the new template settings are the same as an existing template. Use this option if you are designing a template that is similar to an existing template and has only a few differences.
5. Click the button.

Using the Security Control Panel

The Security Control Panel lets you restrict access to almost every screen, section, or object in ImproNet Access. Figure 47 shows the **Security Control Panel**. ImproNet applications list in the left-hand pane. When you select an application, its features display on tabs in the main Security Control Panel pane.

To customize a template proceed as follows:

1. Select each application one at a time.
2. In the Main Pane, carry out one of the following:
   - Click the **Full Access** option to enable access to *all* items.
   - Click the **Denied Access** option to deny access to *all* items.
   - Click an item to toggle its accessibility—the **Customised Access** option is selected
3. Click the button to save.

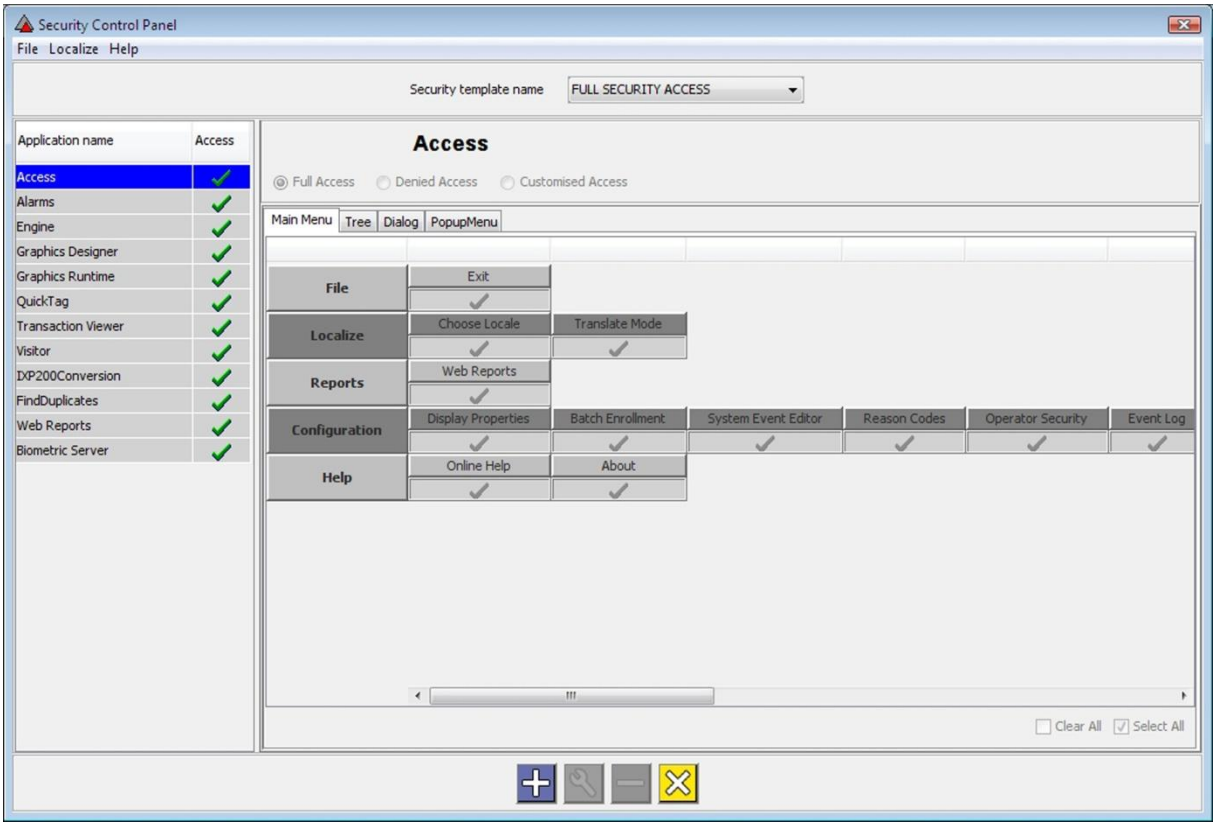

Figure 47 – Security Control Panel

Users Section

Add Users to the database BEFORE assigning them to an Operator Group.

To add users to the database, proceed as follows:

1. In the **Users** panel, click the **Advanced** button. The first time the **Advanced** button is clicked, the following dialog box displays.

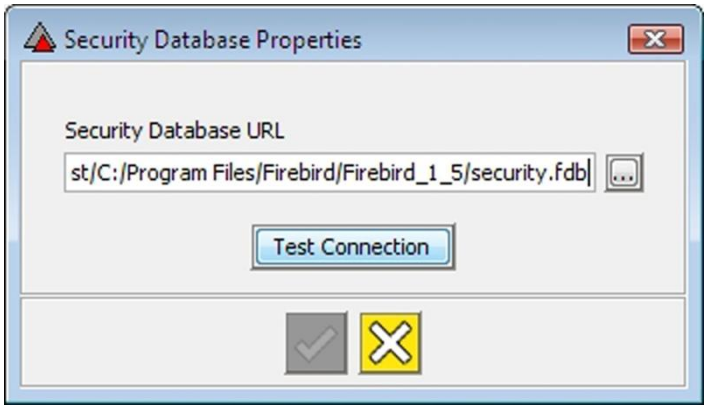

Figure 48 – Security Database Properties Dialog

Use this window to specify or confirm the location of the Security Database that you are connecting to. A default path is shown if a Database exists.

2. If no Database file path displays in the textbox, click the button.
3. Browse to the location of the Security Database (**C:\Program Files\Firebird\Firebird_1_5**).
4. Select the **security.fdb** file.
5. Click **Open**.

*The Security Database is installed to **c:\program files\firebird\firebird_1_5** by default. However, if the default directory does not exist, consult the person who installed the Firebird Database Server.*

6. Click the **Test Connection** button.
7. If Access connects to the Security Database successfully, the button turns green to let you save the setting.

The location of the Security Database is saved in the Access.properties file. Therefore, if the location of the Security Database changes, you must edit the last line of the Access.properties file to reflect the change.

Add and Delete Users

In the Users Panel, click the **Advanced** button.

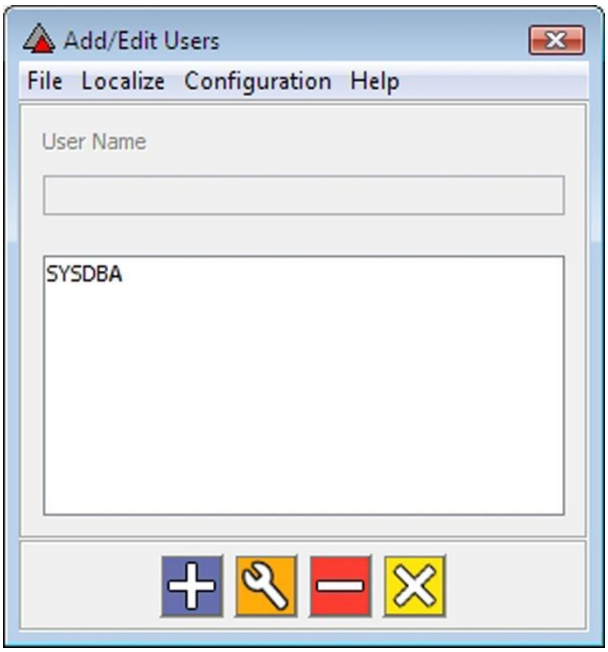

Figure 49 – Add/Edit Users Dialog

In the **Add/Edit Users** dialog, do one of the following:

- Click the button to add a User.
- Select a User and click the button to delete them.

Change Password

In the **Add/Edit Users** dialog, proceed as follows to change a User's password:

1. Select a User.
2. Click the button.
3. In the **Old Password** textbox, enter the **OLD Password**.
4. Click the button.
5. In the **New Password** textbox, enter a **NEW Password**.
6. In the **Re-enter Password** textbox, re-enter the **NEW Password** in confirmation.
7. Click the button.

Assign Users

1. Click the button. The **Select Group's Users** dialog displays.
2. Select users in the **Available Users** section.
3. Click the > button to move them to the **Assigned Users** section.
4. Click the button.

Use the >> button to move all users at once.

Tagholder Access Groups Section

To edit the available **Tagholder Access Groups**, proceed as follows:

1. Click the button.

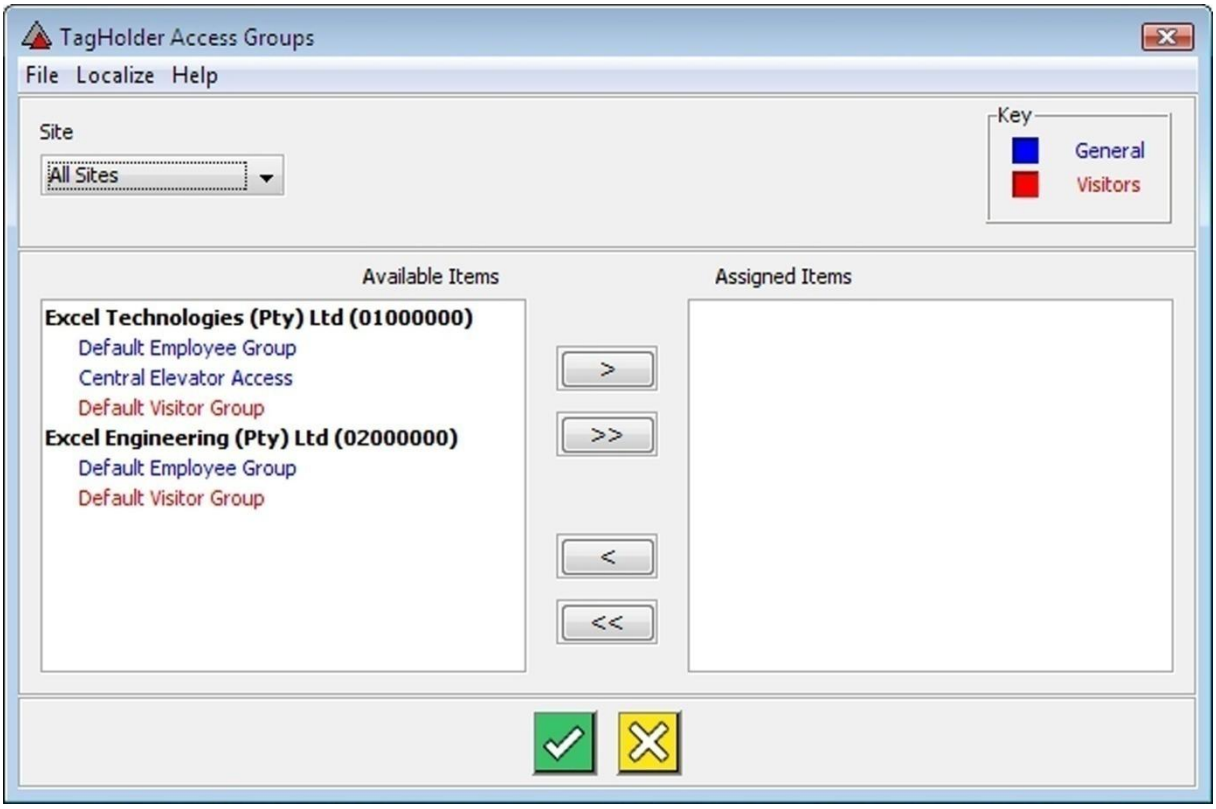

Figure 50 – Tagholder Access Groups Dialog

2. In the Tagholder Access Groups dialog, select Access Groups in the **Available Items** section.
3. Click the > button to move them to the **Assigned Items** section.
4. Click the ✓ button.

Use the >> button to move all Access Groups at once.

User Profiles Section

A Tagholder assigned to a User Profile is visible and editable only to Security Users who are configured for the particular User Profile.

For example, Andrew Young is an Operator Security User. He belongs to an Operator Group called **Operator Group 2**—refer to Figure 51. Andrew is assigned the **Contract Staff** and **Casuals** User Profiles. This means that when Andrew uses Access, he can only see and edit Tagholders who are assigned to one of these groups. Andrew will not see Tagholders belonging to other User Profiles.

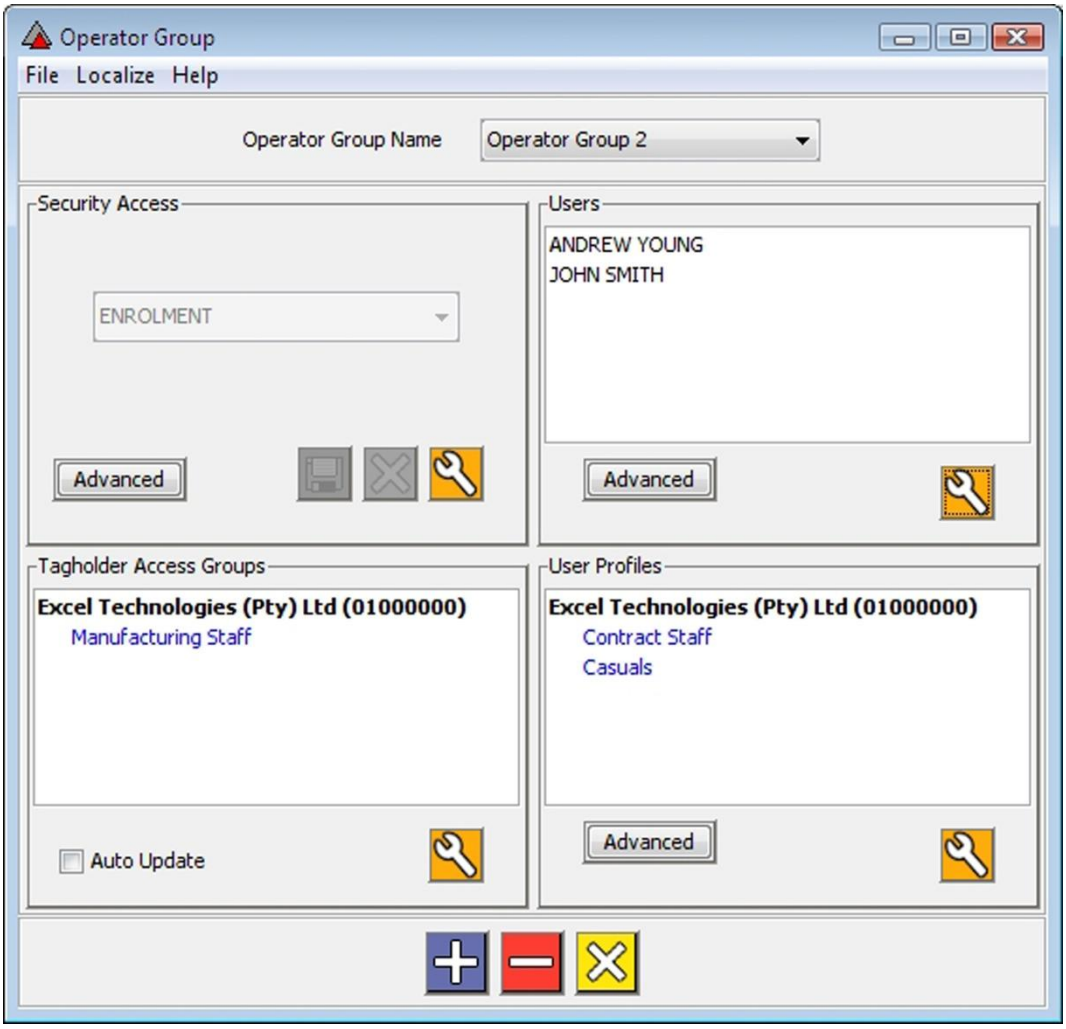

Figure 51 – User Profile Example

Create User Profile

To create a User Profile, proceed as follows:

1. In the **User Profile** section, click the **Advanced** button.
2. From the **Select Site** drop-down menu, select a site.
3. Click the button.
4. In the User Profile dialog, click the button.
5. Enter a **User Profile Name**.
6. Click the button.
7. At the Confirm Insert dialog, click the **No** button. (Clicking the Yes button adds the user profile to all operator groups).
8. Click the button.

Assign User Profiles to Users

Ensure that you select the correct **Operator Group Name**, then proceed as follows:

1. In the **User Profiles** section, click the button.
2. Select User profiles in the **Available Items** section.
3. Click the button to move them to the **Assigned Items** section.
4. Click the button.

Use the button to move all User Profiles at once.

Assign Tagholders

Assign User Profiles to Tagholders in the **Edit Tagholder** screen.

To do this, proceed as follows:

1. In the Access, Navigator pane, click the button.
2. In the Main pane, select a Tagholder.
3. Click the button. The **Edit Tagholder** screen displays.
4. From the **User Profile** drop-down list, select a User Profile.
5. Click the button to save.

If the All value is selected, the Tagholder is visible to Operator Security Users who are assigned any User Profile.

SMS Support on Events and Actions

Purpose of this Feature

The **SMS Support on Events and Actions** Feature allows an ImproX EC^{II} Controller to send and respond to received SMS messages when certain trigger events occur.

Example

OUTGOING SMS from Your ImproNet System

You may only create this SMS action on the Controller; however, you may link the SMS action to *ANY* event on the Controller or any of its Terminals.
An outgoing SMS sent by your ImproNet System could alert you of an alarm being triggered, such as a door forced, Anti-tamper, power failure, Emergency Mode on or Lock-down Mode on.

INCOMING SMS to Your ImproNet System

Alternately an incoming SMS sent to your ImproNet System's Controller, could activate or remove certain modes before you arrive at your site. These SMS instructions could include, removing Lock-down Mode or Emergency Mode, or driving a relay thereby opening a door.

Procedure

Ensure that you unlock your ImproX RH for SMS support before continuing.

Connect the USB GSM Modem to the ImproX EC^{II} Controller.

Set GSM Modem Configuration

1. Open the **Ethernet Discovery Utility**.
2. On the menu bar, go to **Action**>**Search Local Subnet**.
3. Wait for the Controllers to display.

On display of the Controllers and Terminals, the following icons appear: the icon represents unlinked Controllers. The icon represents Terminals and the icon represents Controllers with linked Terminals. On expanding the Controller tree, the icon displays, with the linked Terminals displaying below.

4. Select the Controller for configuration.
5. On the menu bar, go to **Action**>**Set GSM Modem Configuration**.
6. In the **Device Password** dialog, enter your password.

*The default password is **impro**.*

7. Click on the button.

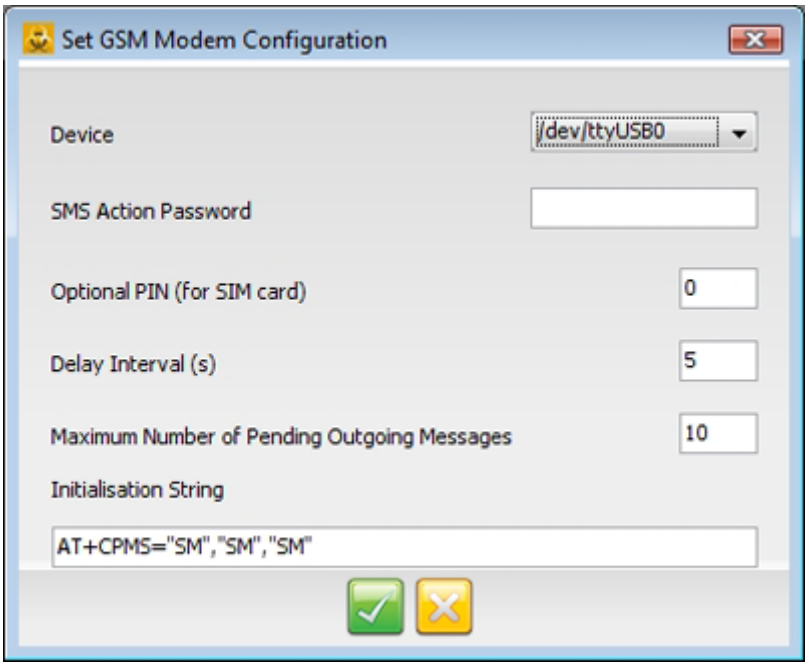

Figure 52: Set GSM Modem Configuration Dialog

In the **Set GSM Modem Configuration** dialog, configure the following:

1. **Device**—depends on the Modem used. The default suggested (*/dev/ttyACM0*) is for the *Falcom Samba 75 Modem*.
2. **SMS Action Password**—set this password for use when sending SMS messages. This password prevents unauthorized applications from using the GSM service.
3. **Optional PIN (for SIM card)**—enter your SIM card's PIN if using one.
4. **Delay Interval**—the interval in seconds between checking for SMS messages. Change this setting only to ensure the best possible operation.
5. **Maximum Number of Pending Outgoing Messages**—this setting limits the buffer in case an event repeatedly creates false messages. Change this setting only to ensure the best possible operation.
6. **Initialisation String**—depends on the Modem used. The default suggested *AT+CPMS="SM","SM","SM"* is for the *Falcom Samba 75 Modem* pre-approved for use with this System.
7. Click the button to confirm.
8. Close the Ethernet Discovery Utility.

Outgoing Message Setup

Create a Message

To create a new Message in Access, proceed as follows:

1. In the Navigator Pane, click the icon.

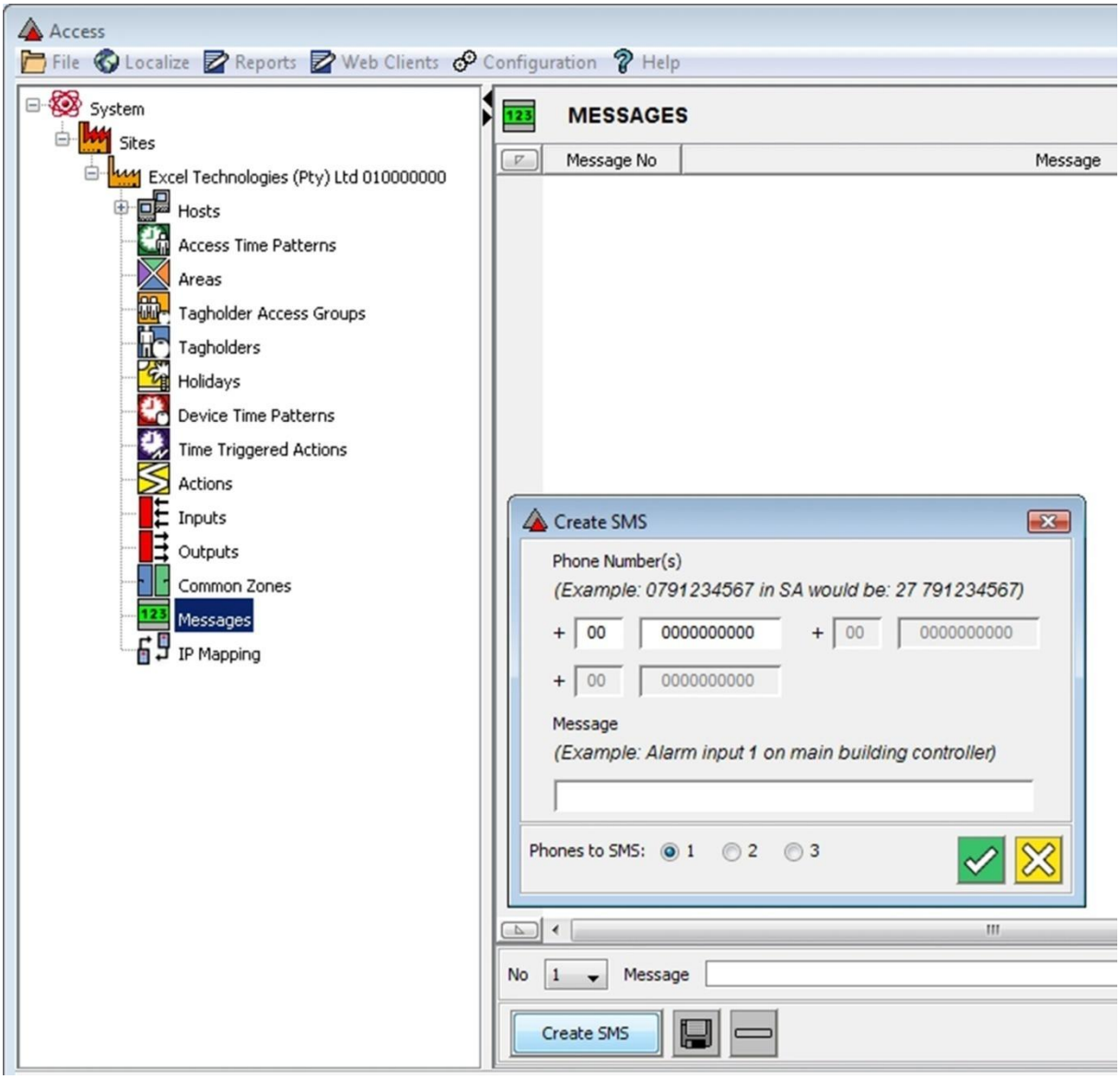

Figure 53: Set GSM Modem Configuration Dialog

2. In the Main Pane, click the **Create SMS** button.
3. Select the required **Phones to SMS** radio button. That is:
   - **1**—sends the message to a single cellular telephone.
   - **2**—sends the message to two cellular telephones.
   - **3**—sends the message to three cellular telephones.
4. Based on the selection you made above, complete the highlighted Phone Number(s) text boxes.

Specify the 2-digit country code (in the textbox directly after the "+" symbol) even when the cellular telephone operates within the same region.

5. Enter the Message content in the **Message** textbox.

Ensure that your Message is NOT preceded by a numeric digit. Numeric digits may however appear in the middle and at the end of your Message.

6. Click the button.
7. In the **Message Exists** dialog, make your selection:
   - **Yes**—overwrites the message selected when you pressed the Create SMS button. The Message No confirmation dialog informs you of the message number used.
   - **No**—selects the next un-used message number and stores the message. The Message No confirmation dialog informs you of the message number used.
   - **Cancel**—cancels the create sms process.

Create an Action

1. In the Navigator Pane, select an EC^{II} Controller by clicking the icon.
2. In the Main Pane, select the **Actions** tab.
3. Click the button.
4. From the Select Action Type drop-down list, select the **SEND SMS** option.
5. In the Action Name textbox, assign your action a suitable name.
6. Select the Time Pattern by clicking on the button.
7. Click the button.
8. In the New Action dialog, click the button.
9. In the Action Parameters dialog, select the Message number by clicking on the button.
10. Select a Message from the records displayed.
11. Click the button.
12. In the Action Parameters dialog, click the button.

Link Action *to* an Event

You may link the SMS action to any event on the Controller (or any of its Terminals). When the event triggers (for example door forced) the SMS action takes place and an SMS sends to the cellular telephone numbers listed in the Message.

1. In the Navigator Pane, select an EC^{II} Controller by clicking the icon.
2. In the Main Pane, select the **Actions** tab.
3. Click on the **Active System Events** button.
4. From the **Active System Event** drop-down list, select an event.
5. Alongside your first available action, (for example First Action, Second Action and so on), click the numeric Select Action button.

In the Action Selector dialog, click on the Global button for a larger search result.

6. From the Action Selector dialog, select the SMS action (created on the Controller).
7. Click the button.
8. At the Active System Events Editor dialog, click the button.

When the event occurs, the SMS transmits (according to your action and Time Pattern settings) to your cellular telephone.

Incoming Message Setup

To set up incoming Messages for direction to your GSM Modem, continue as follows:

1. From your cellular telephone, type your SMS.

Ensure that your Message structure is as follows:
<Action Number>,<Password>,<Confirm>,<Description>
For example: ***10,1234,c,Open Reception IN****.*
Broken down, the Message structure is explained as follows:

- ***Action Number****—the number of the Action you want performed by the Controller.*
- ***Password****—this is the SMS Action Password set up in the Ethernet Discovery Utility (refer to the section Set GSM Modem Configuration on page 55).*
- ***Confirm****—enter the character "c" if you want a confirmation SMS returned, or leave the field blank if you don't want confirmation (for example:* ***10,1234,,Open Reception IN)****.*
- ***Description****—this field is optional and is ignored by the ImproNet Software. Use the Description field as a reminder as to what the Action does.*

2. Send the SMS to your GSM Modem (SIM Card).

Alarm Arming

Purpose of this Feature

The **Alarm Arming** feature, incorporated in ImproNet V7.60 upwards, monitors relays and drives digital inputs of third-party alarm panels.

This feature therefore lets you arm and disarm your third-party alarm system direct from your ImproX Keypad Antenna Reader or Keypad Remote Reader.

While your alarm panel is in an armed state, ImproNet denies access by Tagholders into or out of the armed Zone.

Alarm Arming offers the following setup options:

- Single Controller Configuration
- Multiple Controller Configuration

While using the Alarm Arming feature, you may still arm or disarm your alarm from your third-party alarm panel.

Example

Ensure that you unlock your ImproX Registration Reader for Alarm Arming support before continuing.

The Alarm Arming feature only works on sites using ImproX EC^{II} Controllers. On mixed sites using ImproX IC's and EC's, the feature is disabled.

Figure 54 and Figure 55 show sample connections using the ImproX iTT. You may however use other Terminals from the ImproX family, including the ImproX MfT (Firmware V7.18 and upwards only), ImproX iTRT, ImproX I16 or ImproX O16.

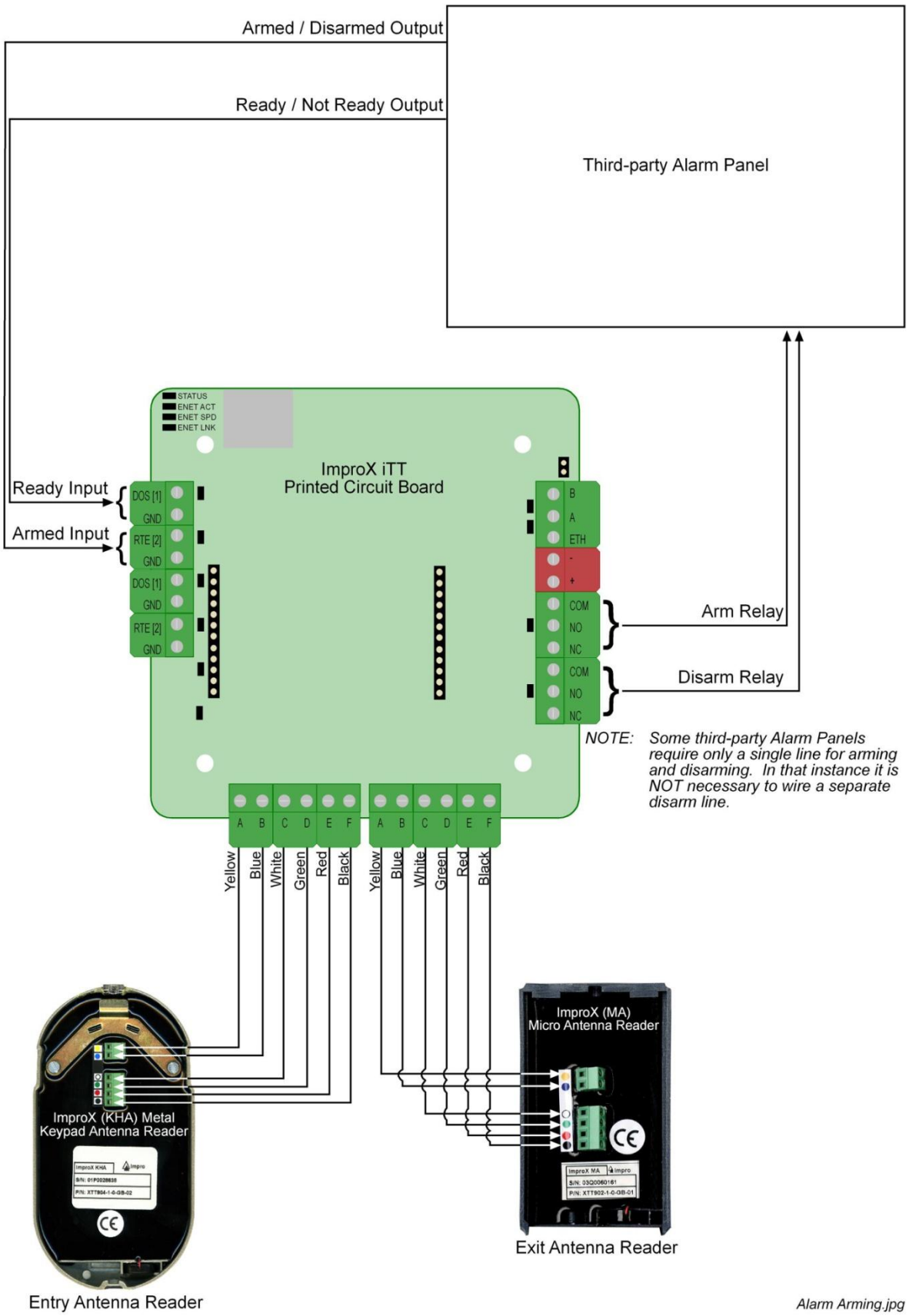

Figure 54: Alarm Arming - Single Controller Configuration

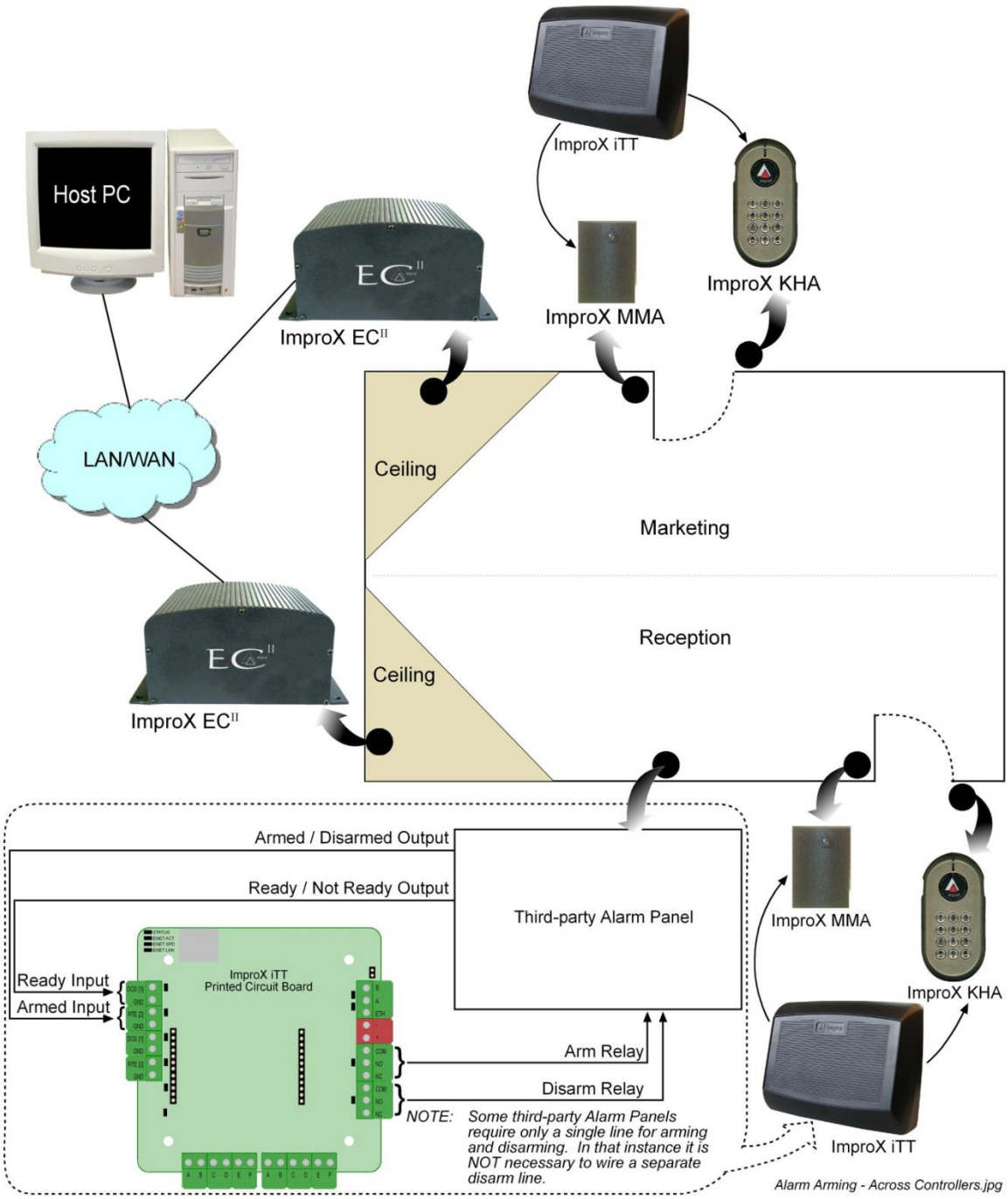

Figure 55: Alarm Arming - Multiple Controller Configuration

Procedure

The following procedure is for Alarm Arming setup using SINGLE CONTROLLER configuration. For extra instructions relating to Alarm Arming across MULTIPLE CONTROLLERS, refer to the sections marked as being specific to Alarm Arming using Multiple Controllers.

1. In Access, select the **Zone** in the Navigator Pane.
2. Select the **Alarm Zone** checkbox.
3. Click the button.

When you select the Alarm Zone checkbox, Access creates several extra default Actions needed by the Alarm Arming feature.

If you remove Alarm Arming from a zone or common zone, deselecting the Alarm Zone checkbox only removes the extra Alarm Arming actions. Therefore, manually delete the Arm and Disarm relays and inputs making the Allowed Normal Relays available.

Removing the Alarm Zone setting from a zone in a Common Zone, all zones in the common zone lose their Alarm Zone setting and their extra Alarm Arming actions.

Action Setup

*You may only set up one **Arm Alarm System** and one **Disarm Alarm System** Relay per Zone.*

*Remember, all Zones under a Common Zone are treated as one Zone. Therefore, you may only create one **Arm Alarm System** and one **Disarm Alarm System** Relay per Common Zone.*

Once a Relay is set up for Alarm Arming, you cannot use it for anything else. Note also that you cannot edit the outputs for that Relay.

Action 1 – Arm Alarm System Relay

1. Select the Terminal that will control the Alarm Panel.
2. In the Main Pain, select the **Actions** tab.
3. Click the button.
4. From the Select Action Type drop-down list, select **Arm Alarm System Relay**.
5. Give your action a suitable name.
6. Click the button.

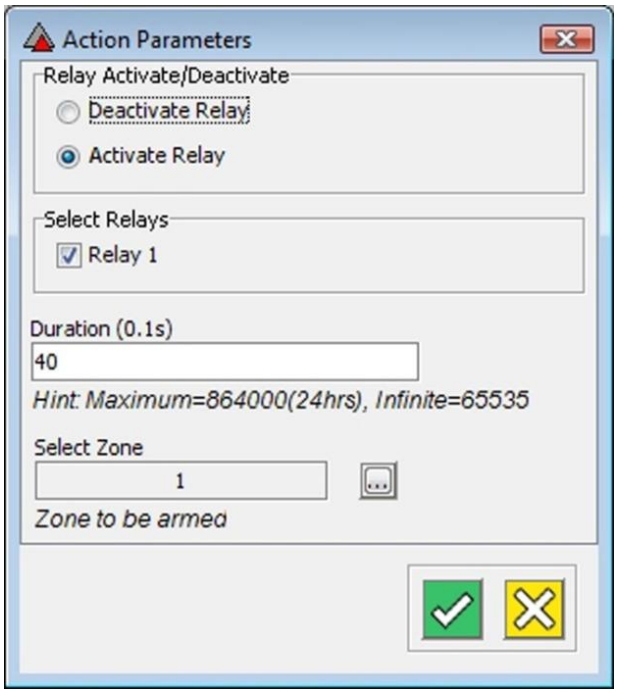

Figure 56: Action Parameters Dialog

7. The Action Parameter settings vary according to the brand of third-party alarm panel in use. Please consult your alarm panel's user manual for settings specific to your installation.
8. Click the button.

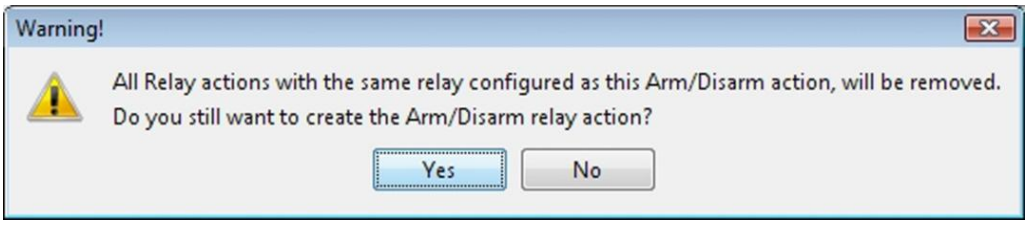

Figure 57: Warning Dialog

9. At the Warning dialog, click the **Yes** button.

Action 2 – Disarm Alarm System Relay

1. In the Main Pain, select the **Actions** tab.
2. Click the button.
3. From the Select Action Type drop-down list, select **Disarm Alarm System Relay**.
4. Give your action a suitable name.
5. Click the button.

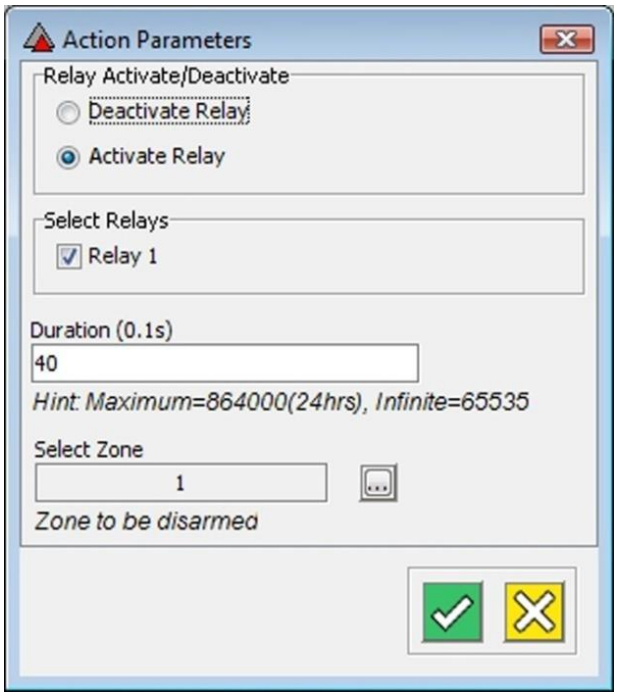

Figure 58: Action Parameters Dialog

6. The Action Parameter settings vary according to the brand of third-party alarm panel in use. Please consult your alarm panel's user manual for settings specific to your installation.
7. Click the button.

*Before deleting an Arm or Disarm Relay from a Zone or Common Zone that has Alarm Armed or Alarm System Ready inputs, ensure that you delete the **Alarm Arming Inputs** and or **Time Triggered Actions** first. Failure to delete the Alarm Arming Inputs and or Time Triggered Actions results in the appearance of an Error dialog.*

Input Setup

*You may only set up one **Alarm Armed** and one **Alarm System Ready** input per Zone.*

*Remember, all Zones under a Common Zone are treated as one Zone. Therefore, you may only create one **Alarm Armed** and one **Alarm System Ready** input per Common Zone.*

General Input 1

1. From the Main Pane, select the **Input** tab.
2. From the displayed records, select **General Input 1**.
3. Click the button.
4. At the Input Device dialog, in the **Input Name** textbox, assign your input a suitable name, for example **Alarm Ready**.
5. From the **Input Function** drop-down list, select **Alarm System Ready**.
6. Click the **Input Parameters** button.

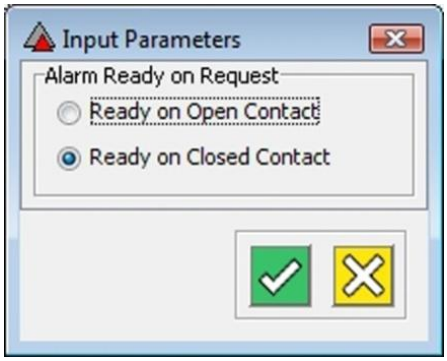

Figure 59: Input Parameters Dialog

7. The Input Parameter settings vary according to the brand of third-party alarm panel in use. Please consult your alarm panel's user manual for settings specific to your installation.
8. Click the button.
9. At the Input Device Dialog, click the button.

General Input 2

1. From the displayed records, select **General Input 2**.
2. Click the button.
3. At the Input Device dialog, in the **Input Name** textbox, assign your input a suitable name, for example **Alarm Armed**.
4. From the **Input Function** drop-down list, select **Alarm Armed**.
5. Click the **Input Parameters** button.
6. The Input Parameter settings vary according to the brand of third-party alarm panel in use. Please consult your alarm panel's user manual for settings specific to your installation.
7. Click the button.
8. At the Input Device Dialog, click the button.

Failure to assign the Location or Zone an Alarm Arm or Disarm Alarm System Relay Action results in display of the Actions Required warning dialog.

Site Setup

1. From the Navigator Pane, select the icon.
2. In the Main pane, click on the **Alarm Arming Settings** button.

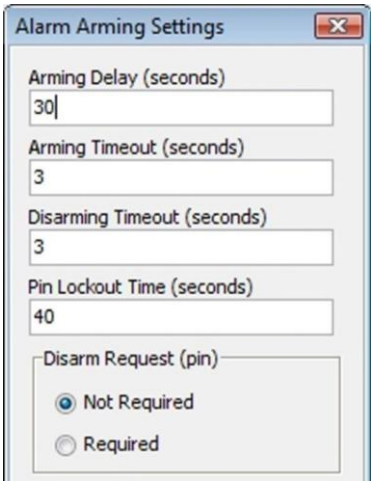

Figure 60: Alarm Arming Settings Dialog

3. In the Alarm Arming Settings dialog, adjust the following settings:
   - **Arming Delay (seconds)**—the amount of time between issuing the arming request and ImproNet arming the alarm panel.
   - **Arming Timeout (seconds)**—if the alarm panel is not armed within the time period specified, the arming instruction fails.
   - **Disarming Timeout (seconds)**—if the alarm panel is not disarmed within the time period specified, the disarming instruction fails.
   - **Pin Lockout Time (seconds)**—the Terminal "locks" for the specified time period, on successive entry of 3 incorrect PIN-codes.
   - **Disarm Request (pin)**—Select either *Required* or *Not Required*, thus indicating whether PIN-code entry is required or not required when disarming the alarm panel.
4. Click the button.

You may NOT move a Terminal or Location with Alarm Armed or Alarm System Ready Inputs to another Zone with the same Inputs. Attempting this move, results in the appearance of an Arming Conflict warning dialog.

Specific to Alarm Arming across MULTIPLE CONTROLLERS

Create the Common Zone

1. From the Hierarchical Tree, select the icon.
2. From the **No** drop-down menu select an unused number.
3. In the **Name** textbox, enter in a name for the Common Zone. *Alarm Common Zone* is the preferred name.
4. Complete the **Description** textbox.
5. Click the button.

Create a New Alarm Zone

1. On a separate Controller, create a ***new* Alarm Zone**.
2. On the Main Pane, select the **Alarm Zone** checkbox.

Making this new Alarm Zone common with an existing Zone (that already has the Arm and Disarm Alarm System Relay Actions) means you cannot add these Actions to the new Alarm Zone.

A common Alarm Zone performs in the same way as a stand-alone Alarm Zone; therefore, you can only control a single alarm panel within the common Zone.

Setup the Common Zone

1. From the Hierarchical Tree, select the **Zone** for which you created the relays *Arm Alarm System Relay* and *Disarm Alarm System Relay*, see Action Setup on page 64.
2. In the Main Pane, from the **Part of Common Zone** drop-down menu, select the Common Zone you created earlier (that is Alarm Common Zone).
3. Click the button.

Access Time Pattern Setup

Setup your required Access Time Patterns, as follows:

1. In Access in the Navigator Pane, click the icon.
2. Do one of the following:
   – Select an Access Time Pattern, and click the button
   – Click the button to create a new Access Time Pattern
3. Enter a **Description** for the Access Time Pattern.
4. Enter a **Start Time**.
5. Enter the **Duration** in hours and minutes.
6. Select the days of the week when the Access Time Pattern is enabled.

Area Setup

1. In the Navigator Pane, click the icon.
2. In the Main Pane, click the button.
3. Enter an Area Name and Area Description.
4. From the Hierarchical Tree select locations by clicking on them.
5. Click the button.

Tagholder Access Group Setup

The following settings do NOT apply to Visitor Tagholder Access Groups, therefore visitors do NOT have arming or disarming rights.

1. In the Navigator Pane, click the icon.
2. In the Main Pane, click the button.
3. Enter a name in the **Tagholder Access Group Name** textbox.

*If you call your Tagholder Access Group **"Reception"** for example, we suggest you add the phrase **With Arming** to the name. This will assist you when you assign the Tagholder Access Group later.*

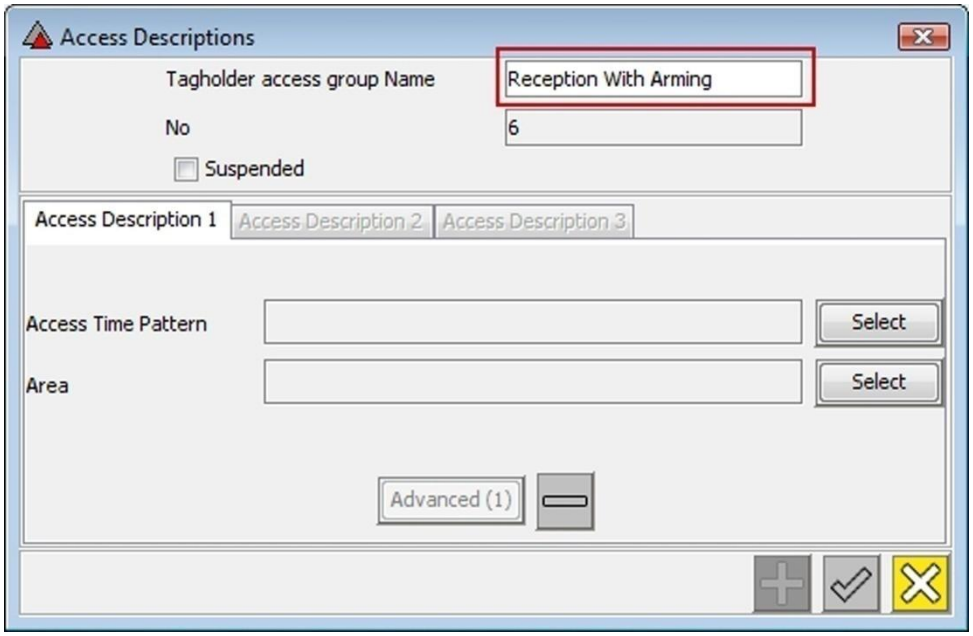

Figure 61: Access Descriptions Dialog

4. Alongside the **Access Time Pattern** textbox, click the **Select** button.
5. From the list of records select an Access Time Pattern.
6. Click the button.
7. Alongside the **Area** textbox, click the **Select** button.
8. Select the Area you created earlier under Area Setup.

The Area selection includes access and arming rights.

9. Click the button.
10. Click the **Advanced (1)** button.
11. In the Advanced Settings dialog, select the **Alarm Arming** tab.

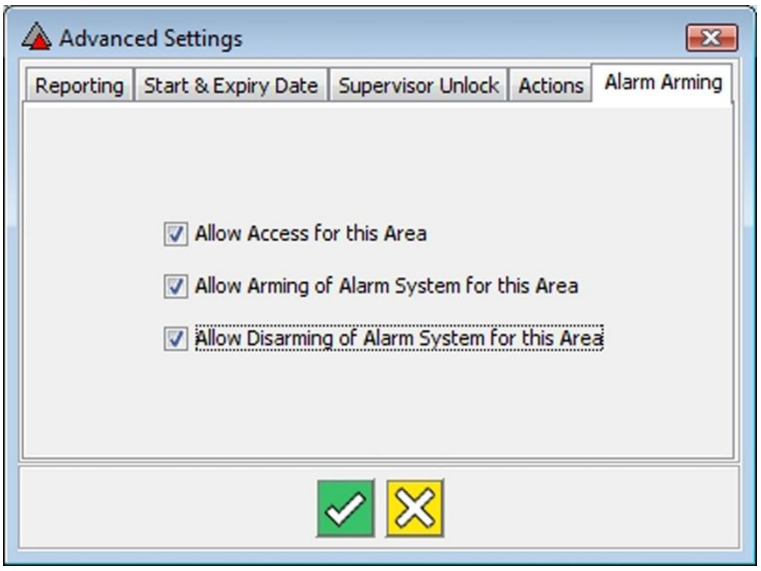

Figure 62: Advanced Settings Dialog

12. On the Alarm Arming tab, select from the following options:
    - **Allow Access for this Area**—allows the user access to the area.

> *If **Allow Access for this Area** is deselected, and the Allow Arming and Allow Disarming option is selected, the user could for example arm and disarm the System, but not physically enter the Zone.*

    - **Allow Arming of Alarm System for this Area**—selecting this option gives the user permission to arm the Zone.
    - **Allow Disarming of alarm System for this Area**—selecting this option gives the user permission to disarm the Zone.
13. Click the button.
14. At the **Access Descriptions** dialog, click the button.

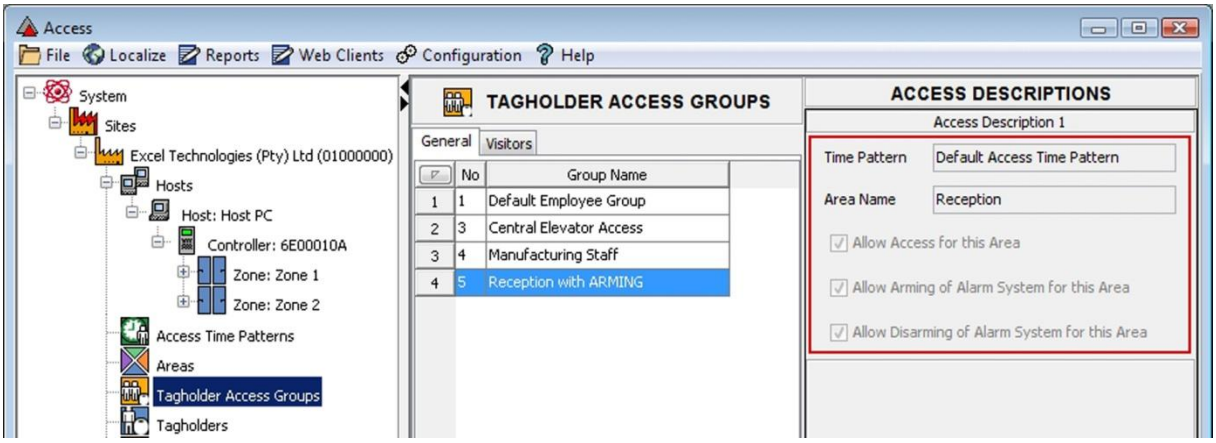

Figure 63: Access Window Showing Access Descriptions Summary

The Access Descriptions pane highlighted in Figure 63 shows a summary of the settings you've applied earlier. This Access Description information is **read only**.

Edit your Tagholder Access Group by selecting the **Tagholder Access Group record** and clicking the button. Figure 63 shows record number 4 selected.

Tagholder Setup

1. In the Navigator Pane, click the icon.
2. In the Main Pane, do one of the following:
    - Click the button to add a Tagholder.
    - Click the button to edit a Tagholder.
3. Enter the Tagholder's **First Name** and **Last Name**.
4. Complete other personal information as necessary.
5. Select the **Current** checkbox to enable the Tagholder (selected by default).
6. Use the **Notes** text area to enter other information about the Tagholder.
7. In the PIN textbox, enter a PIN-code of up to 5 digits (required for disarming the alarm panel).
8. Select the Tagholder's Department from the **Department** drop-down list.
9. On the Edit Tagholder dialog, click any of the **New Tag** buttons.
10. On the Tag Details dialog, select one of the following Tag Options:
    - **Normal**—normal employee.
    - **Suspend**—Tag is suspended from all access on the Site.

- **Blacklist**—Tagholder is blacklisted and denied access to the Site.
- **Special Event 1**—Tag raises an Event when presented to the Reader – in this case Special Event 1. The Event can be linked to a specific Action.
- **Special Event 2**—Tag raises an Event when presented to the Reader – in this case Special Event 2. The Event can be linked to a specific Action.

11. Configure the following:
    - **APB Override**—Tags are not subject to APB rules.
    - **Report Always**—all transactions for the Tag are written to the Database.
12. Assign the Tagholder to a Site by selecting a value from the Site Assigned drop-down list.
13. Assign the Tagholder to one or more **Tagholder Access Group**. From the next available Group (1-10) drop-down list, select the Tagholder Access Group you created under the heading Tagholder Access Group Setup on page 68. (For example **Reception With Arming**).

At least one Tagholder Access Group must be assigned for the Tag to have any access rights.

14. Present a Tag to an Enrollment Reader and click the **Read Tag** button.
15. If the Tag Type is not displayed when the card is read, or if you are entering a Tag code manually, select the **Tag Type** from the drop-down list.
16. Click the button.
17. Click the button.
18. At the Add or Edit Tagholder dialog, click the button.
19. Click the button.

Full Upload

Upload all data in the ImproNet Database to the Controllers:

1. In Engine, click the Stop button.
2. Click the Full Upload button.
3. At the Confirm Upload dialog, click the **Yes** button.
4. Click the Start button.

Arming and Disarming

Only arm or disarm the alarm from locations that you have rights to arm or disarm from.

You may arm or disarm the Alarm using a Time Triggered Action. See Part 3 – General Configuration for details on adding a Time Triggered Action.

Zone Arming

*The * used below, represents the * button on either your Keypad Antenna Reader or Keypad Remote Reader. Where the instructions state ** or *** this indicates that you must press the * button the respective number of times.*

- **Arm Zone**—* + present Tag.
- **Arm ALL Zones on the Controller**—** + present Tag.
- **Arm ALL Zones on the Site**—*** + present Tag.

Zone Disarming

The # used below, represents the # button on either your Keypad Antenna Reader or Keypad Remote Reader. Where the instructions state ## or ### this indicates that you must press the # button the respective number of times.

- **Disarm Zone**—# + present Tag + enter PIN-code + #.
- **Disarm ALL Zones on the Controller**—## + present Tag + enter PIN-code + #.
- **Disarm ALL Zones on the Site**—### + present Tag + enter PIN-code + #.

*If during Site Setup (see page 67) you selected **Not Required** for the **Disarm Request (pin)** setting, you are NOT required to enter a PIN-code when disarming the alarm. Please note however you are still required to press the # key after presenting your Tag.*

Zone Arming Status

The Zone Arming Status dialog that indicates the Zones status:

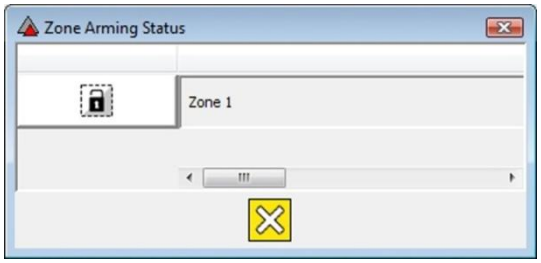

Figure 64: Zone Arming Status Dialog

Access the dialog, by right-clicking your mouse over the icon and selecting **Zone Arming Status** from the shortcut menu.

- When the lock icon is **BLACK**, this indicates the Zone is **NOT READY**.
- When the lock icon is **GREEN**, this indicates the Zone is **READY**.
- When the lock icon is **RED**, this indicates the Zone is **ARMED**.

Action Buzzer and LED States

Table 1 below shows the buzzer and LED states for the following actions:

Action	State
Buzzer—Armed Out of Sequence	Medium (60 seconds)
Buzzer—Failed to Arm	High (20 seconds)
Buzzer—Failed to Arm All Zones	High (20 seconds)
Buzzer—No Arm Authority	High (20 seconds)
Buzzer—Zone Already Armed	Medium (20 seconds)
Buzzer—Zone Armed	Medium (40 seconds)
Buzzer—Zone Not Ready	High (20 seconds)
LED—Armed Out of Sequence	Green Strobe Red (60 seconds)

Action	State
LED—Failed to Arm	Red (20 seconds)
LED—Failed to Arm All Zones	Red (20 seconds)
LED—No Arm Authority	Red (20 seconds)
LED—Zone Already Armed	Green Strobe Red (20 seconds)
LED—Zone Armed	Green (40 seconds)
LED—Zone Not Ready	Red (20 seconds)
Buzzer—Already Disarmed	Medium (20 seconds)
Buzzer—Disarm Failed	High (20 seconds)
Buzzer—Disarmed Emergency Unlock	Medium (60 seconds)
Buzzer—Disarmed out of Sequence	Medium (60 seconds)
Buzzer—No Disarm Authority	High (20 seconds)
Buzzer—Zone Disarmed	Medium (40 seconds)
LED—Already Disarmed	Green Strobe Red (20 seconds)
LED—Disarm Failed	Red (20 seconds)
LED—Disarmed Emergency Unlock	Green Strobe Red (60 seconds)
LED—Disarmed out of Sequence	Green Strobe Red (60 seconds)
LED—No Disarm Authority	Red (20 seconds)
LED—Zone Disarmed	Green (40 seconds)

Table 1 – Action Buzzer and LED States

Supervisor Unlock

Purpose of this Feature

The **Supervisor Unlock** feature prevents general Tagholders from entering a Zone without prior entry by the Supervisor Tagholder.

Procedure

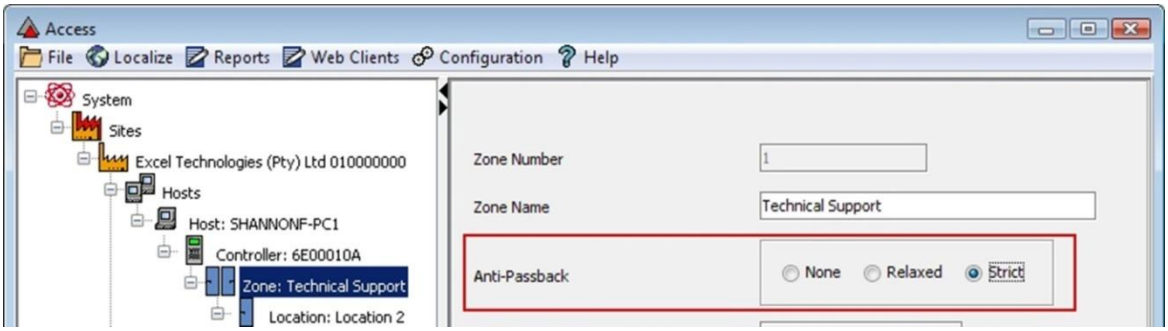

Figure 65: Zone Configuration

Zone Setup

1. In Access from the Navigator Pane, select the **Zone** for configuration.
2. From the **Anti-passback** radio buttons, select the **Strict** choice.
3. Click the button.

Area Setup

Supervisor Area

1. From the Navigator Pane, select the icon.
2. Click the button.
3. In the **Area Name** textbox assign your Area a name (for example ***Supervisor Area***).
4. Assign a suitable **Area Description**.
5. Select the zone you want to configure for Supervisor Unlock. (You may also add any other required zones at this point).
6. Click the button.

General Area

1. From the Navigator Pane, select the icon.
2. Click the button.
3. In the **Area Name** textbox assign your Area a name (for example ***General Area***).
4. Assign a suitable **Area Description**.
5. Select ONLY the zone you want to configure for Supervisor Unlock.

Ensure that this area contains only a single zone, otherwise Supervisor Unlock will NOT work.

6. Click the button.

Tagholder Access Group Setup

Supervisor Tagholder

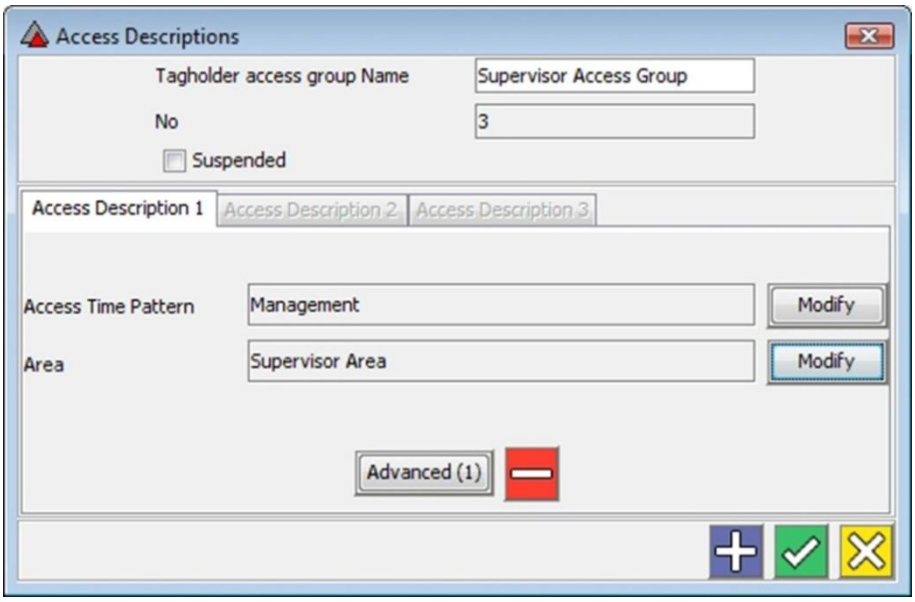

Figure 66: Access Descriptions Dialog

1. From the Navigator Pane, select the icon.
2. Click the button.
3. Enter a name in the **Tagholder Access Group Name** textbox (for example ***Supervisor Access Group***)
4. Click the button.

Assign Access Time Pattern

1. Click the top **Select** button to assign an Access Time Pattern to the Access Description.
2. Click a **Time Pattern Name** to select it.
3. Click the button.

Assign Area

1. Click the bottom **Select** button to assign an Area to the Access Description.
2. From the **Area Name** drop-down list, make your selection (for example Supervisor Area).
3. Click the button.

5. Close the Access Descriptions dialog by clicking the button.

General Tagholder

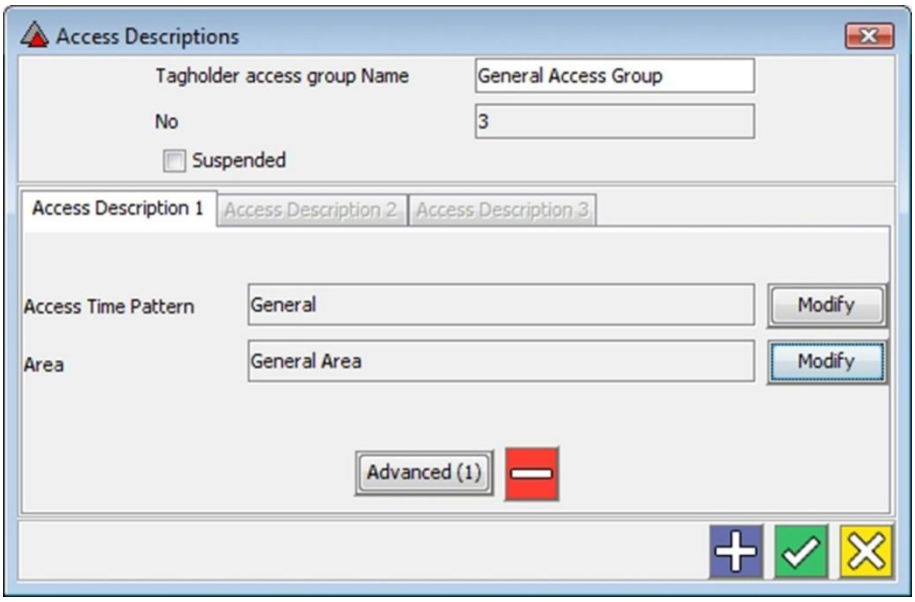

Figure 67: Access Descriptions Dialog

1. From the Tagholder Access Groups Main Pane, click the button.
2. Enter a name in the **Tagholder Access Group Name** textbox (for example ***General Access Group***).
3. Click the button.

Assign Access Time Pattern

1. Click the top **Select** button to assign an Access Time Pattern to the Access Description.
2. Click a **Time Pattern Name** to select it.
3. Click the button.

Assign Area

1. Click the bottom **Select** button to assign an Area to the Access Description.
2. From the **Area Name** drop-down list, make your selection (for example ***General Area***).
3. Click the button.

Advanced Configuration

1. Click the **Advanced (1)** button.

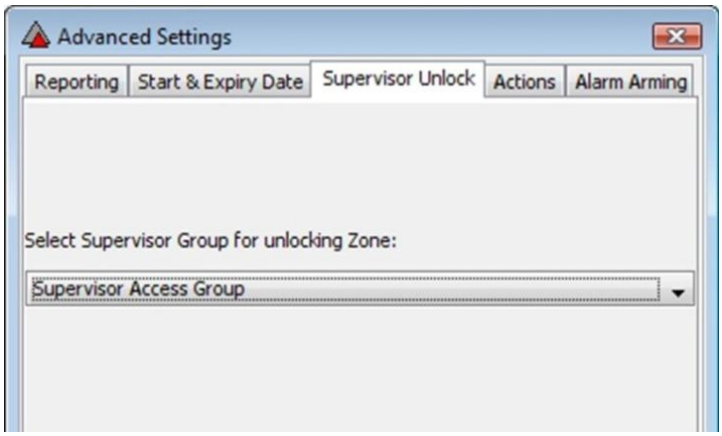

Figure 68: Advanced Settings Dialog

2. Select the **Supervisor Unlock** tab.
3. From the **Select Supervisor Group for Unlocking Zone** drop-down list, select the **Supervisor Access Group** you created earlier.
4. Click the button.
5. Close the Access Descriptions dialog by clicking the button.

Tagholder Setup

From the Navigator Pane, select the icon.

Supervisor Tagholder

1. Open the appropriate Tagholder record for editing.
2. Select the Tag for editing.
3. Assign the Tagholder to the Supervisor Tagholder Access Group by selecting **Supervisor Access Group** from the next available **Group** (Group1 to Group 10) drop-down list.
4. Click the button.
5. Click the button.
6. Close the Edit Tagholder dialog by clicking the button.

General Tagholder

1. Open the appropriate Tagholder record for editing.
2. Select the Tag for editing.
3. Assign the Tagholder to the General Tagholder Access Group by selecting **General Access Group** from the next available **Group** (Group1 to Group 10) drop-down list.
4. Click the button.
5. Click the button.
6. Close the Edit Tagholder dialog by clicking the button.

Zone Configuration

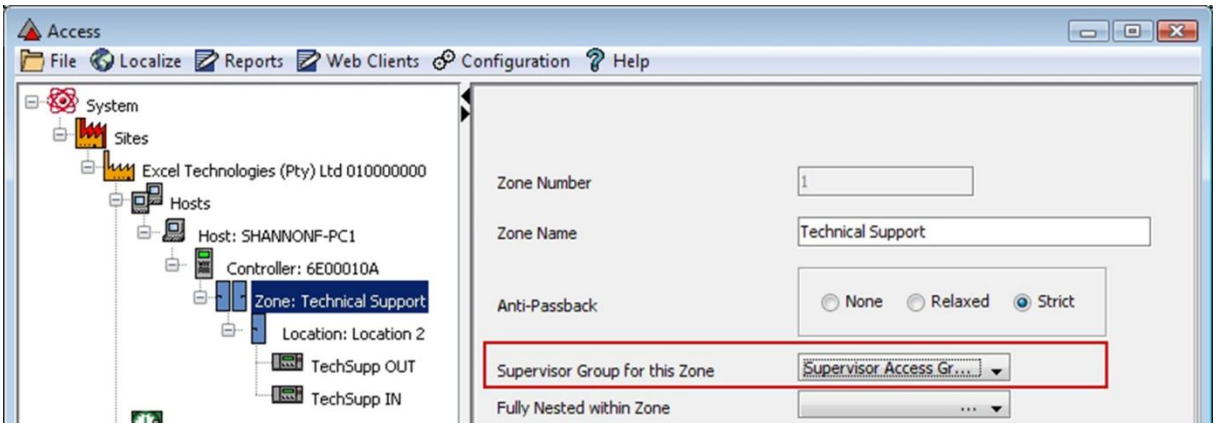

Figure 69: Zone Configuration

1. In Access from the Navigator Pane, select the **Zone** you configured earlier.
2. From the **Supervisor Group for this Zone** drop-down menu, select the **Supervisor Access Group** option you created earlier.
3. Click the button.

Door Strike Lock Setup

Purpose of this Feature

The Door Strike is the usual mechanical type of lock but with an electromechanical action enabling it to be actuated by the presence or absence of a current flowing through an internal solenoid.

Follow the procedure below in order to setup your Door Strike Lock in the ImproNet Software.

Procedure

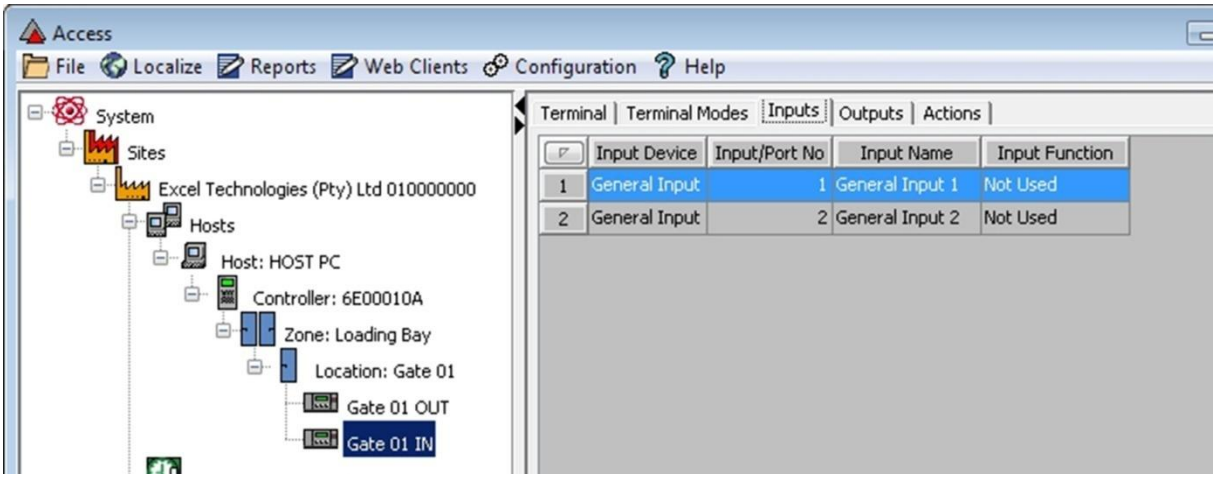

Figure 70: Access Dialog

Input Configuration

1. Select the specific Terminal that will control the Strike Lock (for example **Gate 01 IN** as highlighted in Figure 70).
2. In the Main Pane, select the **Inputs** tab.
3. Click the button.
4. In the **Input Device** dialog, assign your input a name (for example **Door Open Sensing**).
5. From the **Input Function** drop-down list, select the **Door Open Sensor** choice.
6. Click the **Input Parameters** button.
7. In the Input Parameters dialog, select the **Door Open is Open Contact** radio button.
8. Click the button.
9. At the Input Device dialog, click the button.

Action Configuration

1. In the Main Pane, select the **Actions** tab.
2. Click the button.
3. In the New Action dialog, from the **Select Action Type** drop-down list, select **Relay**.
4. Assign your action a meaningful name (for example **Stop Relay Drive Entry**).

5. Assign your action a meaningful time pattern.
6. Click the button.

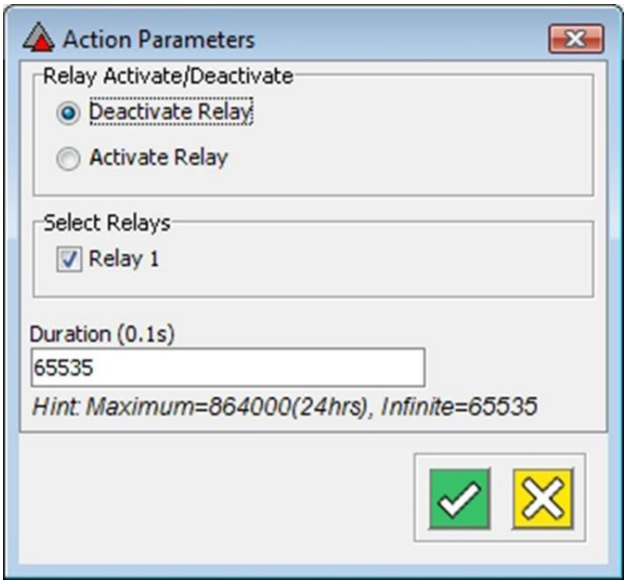

Figure 71: Action Parameters Dialog

7. From the **Relay Activate/Deactivate** group, select the **Deactivate Relay** radio button.
8. In the **Duration (0.1s)** textbox, set the duration to **65535**.
9. Click the button.
10. Click the button.
11. In the Main Pane, click the **Active System Events** button.
12. Click the **Advanced** button.

Door Open Sensing Door Open Normal 1

1. From the **Active System Event** drop-down list, select **Door Open Sensing Door Open Normal 1**.

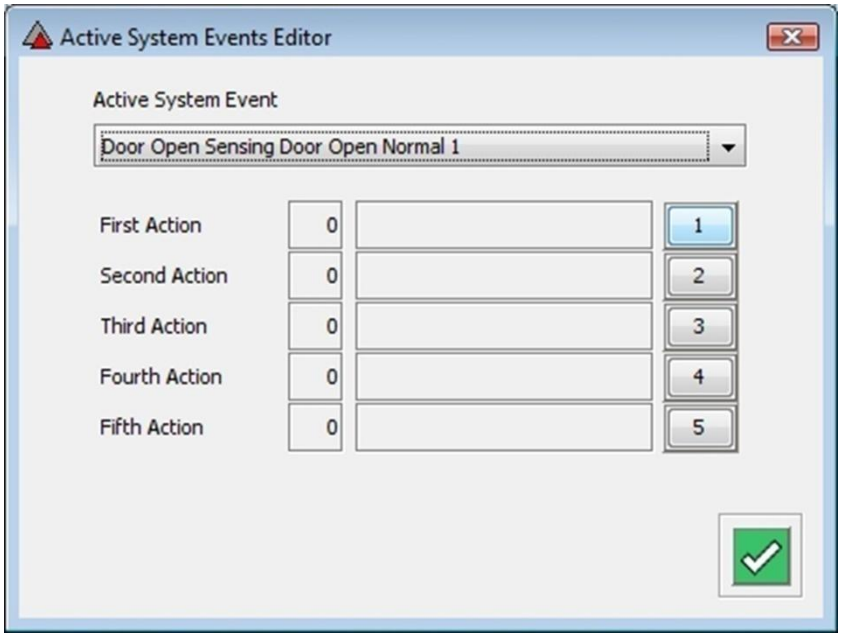

Figure 72: Active System Events Editor Dialog

2. Alongside the **First Action** textbox, click the **1** button.
3. From the list of displayed action records, select the action you created under Action Configuration in 4 (**Stop Relay Drive Entry**).
4. Click the button.

Door Open Sensing Door Open Too Long 1

1. From the **Active System Event** drop-down list, select **Door Open Sensing Door Open Too Long 1**.

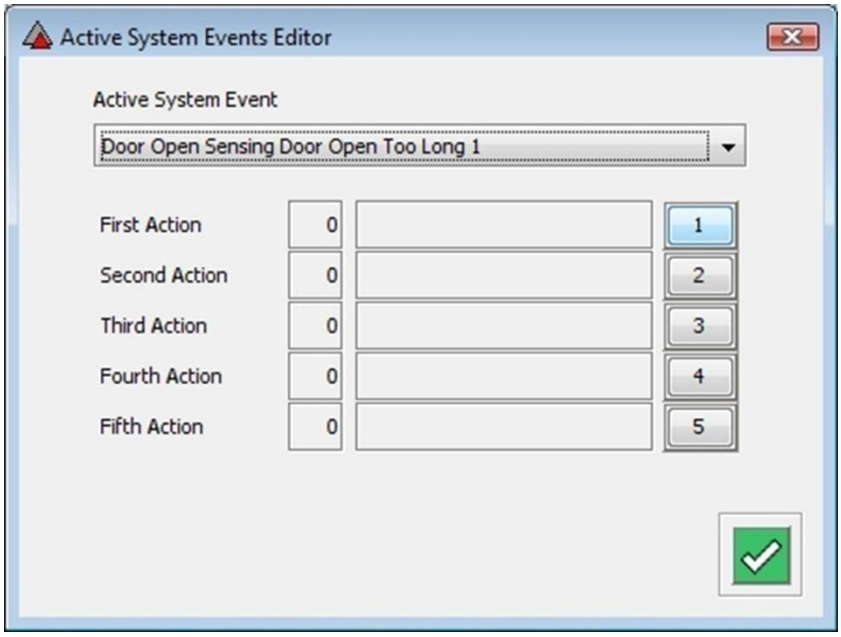

Figure 73: Active System Events Editor Dialog

2. Alongside the **First Action** textbox, click the **1** button.
3. From the list of displayed action records, select the action you created under Action Configuration in 4 (**Stop Relay Drive Entry**).
4. Click the button.
5. At the Active System Events dialog, click the button.

USER NOTES

USER NOTES