PART III – GENERAL CONFIGURATION

Contents

PART III – GENERAL CONFIGURATION 1

CONTENTS 3

CONFIGURATION OVERVIEW 7

Using ImproNet Access 7

Common Interface Controls 8

SYSTEM CONFIGURATION PARAMETERS 10

Fixed Addresses 11

ENGINE FUNCTIONS 12

Engine Menu Functions 12

Engine Properties 16

Advanced Properties 17

Import ECII 20

System Configuration Procedure 21

SITES 22

Shared Data 23

About Time Patterns 23

Configure Site 24

Set Up the Host PC 25

About Hardware Configuration 26

CONTROLLER 27

Assign Terminals 27

TERMINALS 30

Terminal Mode Configuration 32

Inputs 33

Outputs 40

Actions 41

Active System Events 42

ACCESS TIME PATTERNS **46**
Configure Access Time Patterns 46
AREAS **48**
ACCESS GROUPS **50**
Configure Tagholder Access Groups 51
Configure Access Descriptions 52
TAGHOLDERS – ASSIGN ACCESS TO TAGS **54**
Add or Edit a Tagholder 54
Quick Search for Tagholder 54
Configure Tagholder 54
Batch Enrollment of Tags 58
Advanced Search 60
DEVICE TIME PATTERNS **62**
HOLIDAYS **65**
TIME TRIGGERED ACTIONS **66**
ACTIONS **67**
Edit and Delete Actions 67
INPUTS **69**
OUTPUTS **70**
COMMON ZONES **71**
MOVING EMPLOYEES (TAGHOLDERS) **72**
REPLACING CONTROLLERS AND TERMINALS **74**
Replace Controller 74
Replace Terminal 75
DATABASE MAINTENANCE **76**
Firebird General 76
Firebird Utilities 78
Database Backups 80
Database Restore 83
Database Corruption 85
Archiving Transactions 89

Archiving Tagholders 89

EVENTS AND ACTIONS 91

Configuration Overview

ImproNet Access is the software application used to configure an ImproNet Access Control System.

*Run the **Auto-ID** process in **ImproNet Engine** to find what hardware is installed and to assign addresses to the hardware.*

*Ensure that the **Unit Location Chart** is correctly filled in when installing the Controllers.*

Using ImproNet Access

The following panels comprise the ImproNet Access interface:

- Menu Bar
- Navigator Pane
- Main Pane

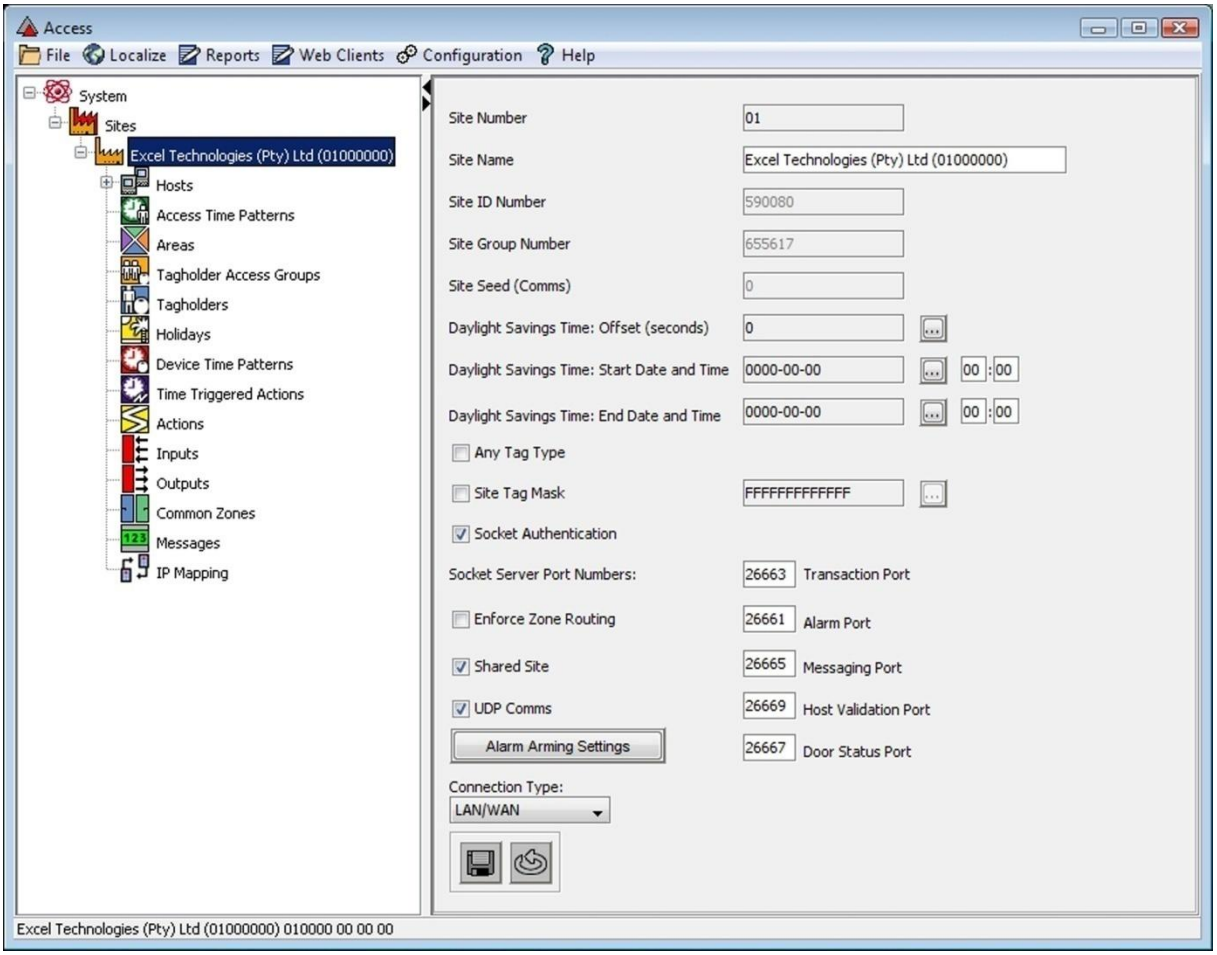


Figure 1 – ImproNet Access Interface

Menu Bar

The Menu contains drop-down lists that let you navigate to different screens in ImproNet Access

Navigator Pane

The Navigator provides an expanding *hierarchical tree* menu. It lets you view and navigate to different items. The Navigation Tree consists of *nodes* that display components by connection.

Main Pane

Items selected in the Navigation Tree display their details in the Main Pane.

Common Interface Controls

The following types of controls let you interact with the ImproNet Access interface:

Buttons

Open another screen, window or dialog when clicked on. They are usually different colours. Examples include the following:

Icons

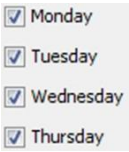
Icons are similar in function to buttons except that Icons are located in the Navigation Tree. Examples include the following:

Radio Buttons

Use Radio Buttons to select an option. Only one radio button in a group can be selected. Click to enable or disable.

Checkboxes

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

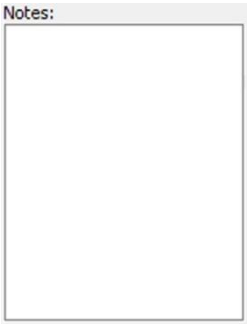


Textboxes

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

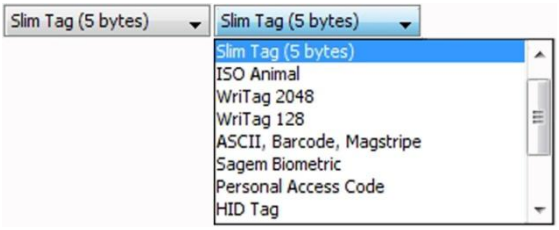
Text Areas

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



Drop-down Lists

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



Records

Records are *rows* of information displayed in a grid format. A record is a collection of fields that correspond to *column* names. In the following example, record number **1** is selected. It has the following fields: **No**, **Title**, **First Name**, **Last Name**, **Department** and **Employee No**. Click a record to select it.

	No	Title	First Name	Last Name	Department	Employee No
1	1	Mr	Paul	Smith	Default Department	1
2	2	Mr	Andrew	Young	Manufacturing	2
3	3	Miss	Sarah	Durnsfield	Manufacturing	3

This Manual displays screenshots of various screens in ImproNet Access. Some of the details displayed in a screenshot may not be available in your copy of ImproNet Access. This is because some details are dependent on the hardware installed.

System Configuration Parameters

Table 1 displays important configuration parameters for the ImproNet System. Some parameters have additional requirements—these are indicated by notes.

Item (see Note 9)	**ImproX IC Controller IXP300**	**ImproX AC Controller IXP400**	**ImproX EC Controller IXP400** (see Note 7)	**ImproX EC^{II} Controller IXP400i** (see Note 8)
Total Number of **Tags**	Up to 8 000	Up to 160 000 (see Note 1)	Up to 160 000	Up to 300 000
Total Buffered Transactions	9 000 (see Note 2)	Up to 500 000 (see Note 3)	Up to 500 000 (see Note 3)	Up to 1 000 000 (see Note 3)
Sites per System	255	255	255	255
Hosts per Site	1	1	1	1
Controllers per System	16	64	64	64
Terminal Fixed Addresses per Controller	48 (see Note 4)	64 (see Note 4)	64 (see Note 4)	64 (see Note 4)
Terminal Fixed Addresses per Location	3 (see Note 4)	3 (see Note 4)	3 (see Note 4)	3 (see Note 4)
Locations per Zone	16	64	64	64
Zones per Controller	16	64	64	64
Actions Supported	10 000	10 000	10 000	50 000
Locations per Controller	16	64 (see Note 5)	64 (see Note 5)	64 (see Note 5)
Tags per Person	4	4	4	8
Tagholder Access Groups	256	1 024	1 024	10 000
Operating Voltage	10 V DC - 30 V DC	10 V DC - 30 V DC	10 V DC - 30 V DC	10 V DC - 30 V DC
Controller Communications Baud Rate	38 400	38 400	38 400	38 400
Terminal Communications Baud Rate	38 400	38 400	38 400	38 400
Digital Inputs (not used for Access Control)	4	None	None	None
Onboard Relays	2	None	None	None
Elevator Control	6 (see Note 6)	6 (see Note 6)	6 (see Note 6)	15 (see Note 10)

SysConfigParameters.jpg

Table 1 – System Configuration Parameters

*If a Site uses a combination of Controllers, it is limited by the **lowest** Controller's parameters. Only the number of transaction types that each Controller can buffer is independent. For Systems with preinstalled ImproX EC's, AC's or IC's, on addition of the EC^{II} ensure the Systems configured for NO cross-controller communications (including Interleading Zone Routing).*

Note 1—160 000 Tags requires population of all the Memory Modules in the Controller.

Note 2—Up to 9 000 buffered transactions in the Controller Transaction Buffer at one time.

Note 3—This amount is relative to the number of Tags in the ImproNet Database, and the number of memory modules in the Controller.

Note 4—A Terminal with two Fixed Addresses, such as the ImproX TT, is treated as two separate Terminals. In the same way, a Terminal with 3 Fixed Addresses (that is the ImproX MfT), is treated as three Terminals by the Software.

*Note 5—In Anti-passback (APB) Mode, two Terminals per Location are required. Therefore, if all locations are in Anti-passback (APB) Mode, the limit is 32 Locations per **ImproX AC**—assuming all Terminals have a single Fixed Address.*

Note 6—When using IXP300 or IXP400, we recommend a maximum of 6 Elevators. This enables one Access Group per Tag for normal access control requirements. A maximum of 80 floors per Elevator is supported.

*Note 7—The **ImproX EC** Controller is functionally identical to the **ImproX AC** Controller except for the way it communicates with the Host PC.*

*Note 8—The **ImproX EC^{II} Controller** generally has the same features as the ImproX EC Controller. However, the ImproX EC^{II} does support more advanced functionality not supported in the EC.*

Note 9—All figures provided are the maximum. In some cases interdependence between parameters; that is the maximum number of Zones per Controller depends on how many Terminals are used per Location.

Note 10—When using IXP400i, we recommend a maximum of 15 Elevators. A maximum of 80 floors per Elevator is supported.

Fixed Addresses

Most Terminals (**ImproX TT**, **ImproX TRT**, **ImproX MfT** and the **ImproX PT** (with a Remote connected)) have two Fixed Addresses.

Fixed Addresses limit how many physical units a device such as a Controller can connect to.

Engine Functions

Engine Menu Functions

ImproNet Engine has the following user-controlled functions:

- Engine Start
- Engine Stop
- Full Upload
- Auto-ID
- Advanced

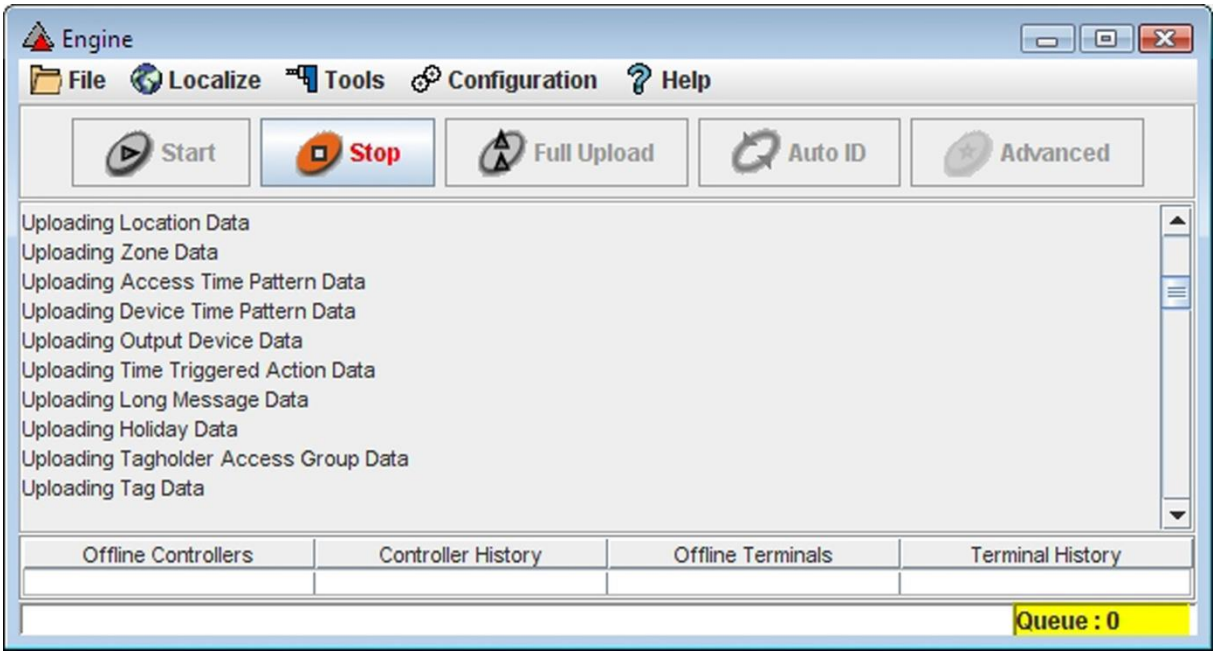


Figure 2 – ImproNet Engine Started

Engine Start

Run this only after you have performed an Auto-ID (setting up and configuring the Site using Access) and a Full Upload.

Engine Start starts the Engine. Transactions are downloaded from the Controllers and logged to the Database. In addition, changes are uploaded to the Controllers.

Engine Stop

Stops all Engine processes and procedures.

Full Upload

During a Full Upload, the selected Site is on-line until the Upload process stops.

Uploads all data in the ImproNet Database to the Controllers. The Engine polls each Controller three times to verify its presence before starting the upload. The engine stops when the upload is complete.

Perform a Full Upload when the Terminals and Controllers are initially configured, and each time that major hardware changes are made to a Site.

Auto-ID

*Stop the Engine **before** executing Auto-ID.*

*If your Site consists of EC^{II} Controllers (IXP400i), ensure that you run the Ethernet Discover Utility **before** running Auto-ID.*

*If your Site consists of EC Controllers (IXP400) connected via UDP comms, ensure that you run the Ethernet Configuration Utility **before** running Auto-ID.*

Auto-ID is a process that polls Controllers to identify their type and their Logical Address. Similarly, other units such as Terminals are also polled and identified. Newly connected units are assigned Logical Addresses.

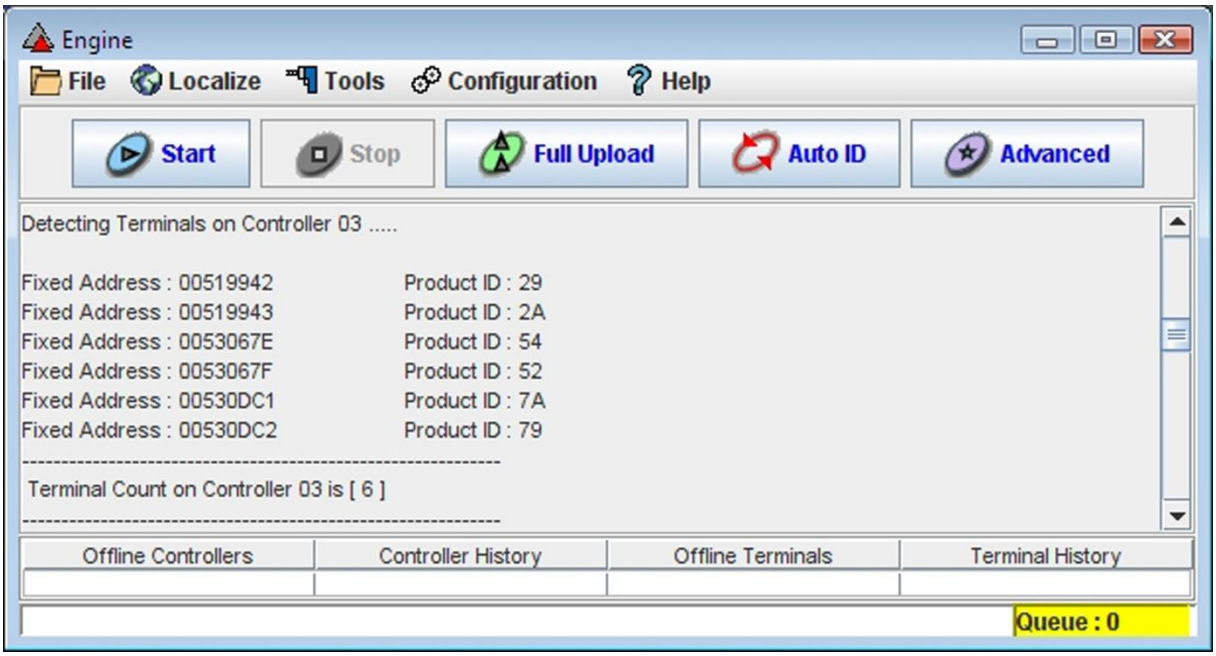


Figure 3 – Auto-ID Complete

Comms Queue

ImproNet (V7.40 and later) now uses a Comms Queue for uploading data to Controllers. The Queue allows preparation of a list of messages for each Controller that upload as each Controller becomes available. If a Controller is down, this does not affect uploading to the on-line Controllers. The Queue acts independently for each device so when an off-line Controller comes back on-line, the Controller soon synchronises with all the other Controllers already updated.

Before V7.40, a change uploaded repeatedly until all Controllers received the message. This caused problems on sites where it was difficult to keep all Controllers permanently on-line. A communications error on a single Controller affects all the other Controllers.

The Engine displays a count of pending messages in the lower right-hand corner. If this count is 0, then all uploads have been posted to all Controllers. If there are pending messages, they process as Controllers become available. You may view a **Queue List** showing the number of messages outstanding for each Controller, in Engine select **Tools**>**Queue Status**. If the Engine's running and the list is not decreasing, then the Engine is unable to communicate.

If for some reason, the messages are no longer needed to be sent to a particular Controller (perhaps before performing a full upload); you may clear the Queue for that Controller by selecting the row and selecting **Clear**.

Advanced

The Advanced function provides a Command Prompt that lets you manually enter and execute specific commands. The Command prompt is illustrated in Figure 4, and is recommended for advanced users only. Some common commands include the following:

- **Start AutoID**—starts the Auto ID process.
- **Start Download 01**—downloads data from Controller 1 to the ImproNet Database.
- **Start Upload 01 03 05**—uploads data from the ImproNet Database to Controller 1, Controller 3, and Controller 5.
- **AlarmServer**—starts the Alarms Server Software so that the Alarm Status of the System is displayed.
- **Estart**—places the Site in **Emergency Mode**.
- **Estop**—reverts the Site from Emergency Mode to **Normal Mode**.
- **APB Reset**—resets the APB status of all Tags.

Figure 4 – Advanced Screen Command Prompt

Broadcast Transactions by UDP to a Specified IP Address

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

Enable this feature as follows:

Engine.properties File

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

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

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

3. From the **File** drop-down menu select **Save**.
4. From the **File** drop-down menu select **Exit**.

Start Engine

1. In Windows®, click **Start**>**Programs**>**ImproNet**>**Engine**.
2. Click on the

button.

The format of the broadcast transactions is a list of comma separated values, in this order:

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

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

Engine Properties

Open Advanced Properties

To open ImproNet Engine, **Engine Properties**, proceed as follows:

1. In Windows®, click **Start**>**Programs**>**ImproNet**>**Engine**.
2. From the Menu Bar, select **Configuration**>**Engine Properties**.

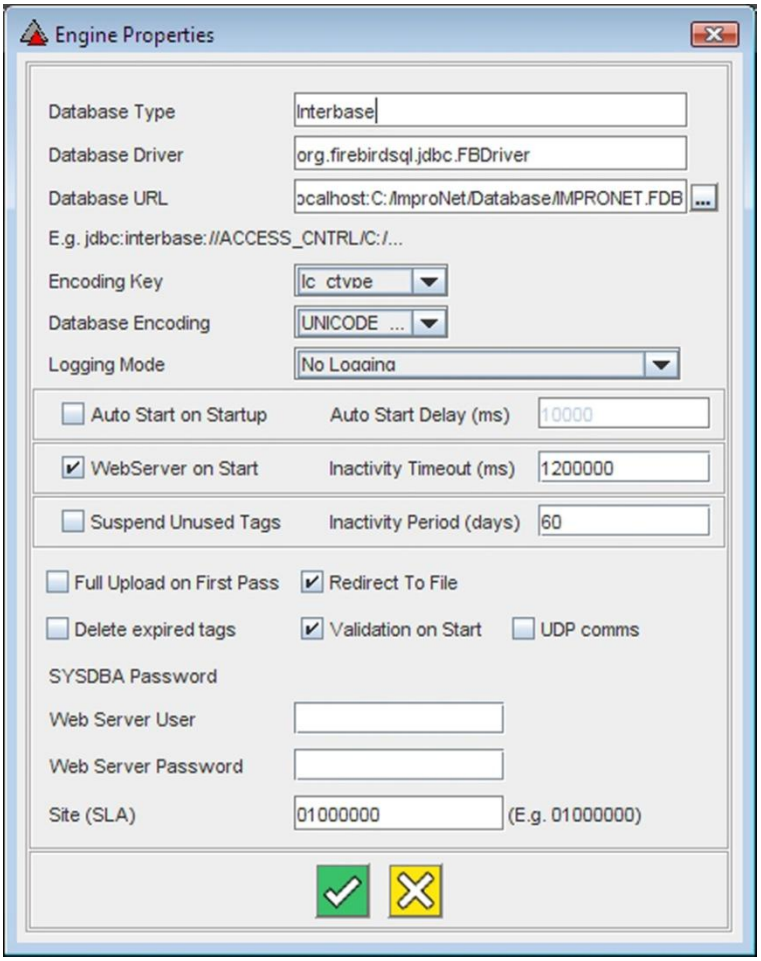


Figure 5 – Engine Properties

The **Engine Properties** dialog lets you view and change the following settings:

*Settings described in this section are stored in the **Engine.properties** file.*

- **Database Type**—the name of the ImproNet Database type. The default is **Interbase**—the name of the company that produced Firebird.
- **Database Driver**—specifies the driver file for the ImproNet Database.
- **Database URL**—specifies the location of the ImproNet Database. You can select mapped network drives from the Browse dialog, click the ... button to browse.
- **Encoding Key**—refers to the type of database driver used. Jaybird is the default database driver. In the **Engine.properties** file, the encoding key is **lc_ctype**.
- **Database Encoding**—specifies the applicable database-encoding format as displayed in **Table 2**.

Encoding format lc_ctype	Encoding format charSet
ISO8859_1	8859_1
WIN1250	Cp1250
UNICODE_FSS	UTF_8

Table 2 – Database Encoding Format

- **Logging Mode**—used for diagnostic purposes when there are communication problems between the Engine and Controllers.
- **Auto Start on Start-up**—enables the Engine to **Start** when it is opened. By default, you have to manually **Start** the Engine.
- **Auto Start Delay**—specifies the amount of time to delay starting the Engine after it is opened. For example, a setting of **5 000** ms delays the Engine starting by five seconds after it is opened.
- **Web Server on start**—sets the Web Server to start when the Engine is started.
- **Inactivity Timeout**—sets the time-out delay for a connected Web Server session.
- **Suspend Unused Tags**—suspends Tags not used for a period of time.
- **Inactivity Period (Days)**—specified number of days (where the Tag is not used) before the Tag is suspended.
- **Full Upload on First Pass**—sets the Engine to perform a full upload on start-up.
- **Redirect to File**—specifies that Error Messages are written to a Log file.
- **Delete Expired Tags**—deletes expired Tags from the Database.
- Validation on start—validate the ImproNet Database on start-up.
- **UDP Comms**—enables the Engine to communicate on UDP Unicast (Ethernet enabled Controllers only).
- **Web Server User and Web Server Password**—enforces logon (entry of a User Name and Password) when viewing Reports from a client PC.
- **Site SLA**—the Site's Logical Address.

Advanced Properties

The **Advanced Properties** window in ImproNet Engine enables you to fine-tune the timing between ImproNet Engine, the ImproNet Database, and System Hardware.

We recommend that you do not change the Engine settings for a standard configuration. You should only edit Engine settings to improve the efficiency of ImproNet across a WAN.

Open Advanced Properties

To open ImproNet Engine **Advanced Properties**, proceed as follows:

1. In Windows®, click **Start**>**Programs**>**ImproNet**>**Engine**.
2. From the Menu Bar, select **Configuration**>**Advanced Properties**.

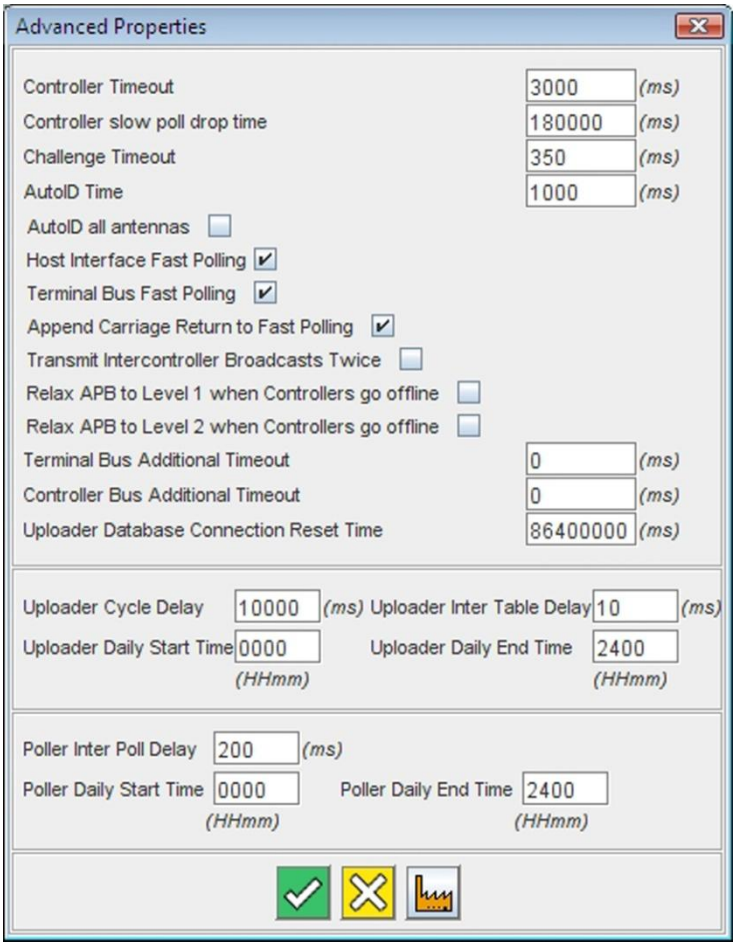


Figure 6 – Advanced Properties

The **Advanced Properties** dialog lets you view and change the following settings:

Time is measured in ms (milliseconds), unless stated otherwise. 1 000 ms = 1 second.

- **Controller Timeout**—the length of time that the Engine will wait for a reply from a Controller. The default time is **3 000**. Increase to **5 000** if Ethernet converters or radio modems are used. Increase the value if **Controller Dropped** error messages display.
- **Controller Slow Poll Drop Time**—the amount of time that a Controller is dropped from the poll sequence, if it times out. The default is **180 000** (3 minutes). After the drop time has passed, polling continues normally.
- **Challenge Timeout**—amount of time allowed for detecting a Host Interface. If a Host Interface is not detected within the **Challenge Timeout** time, the **Not Authorised to Run** error message is displayed. The Default is **350**. If a valid Host Interface is connected and all connections are correct, you can extend the time to 800.
- **AutoID Time**—amount of time a Controller allows to *Auto-ID* its Terminals. The default is **1 000**. Increase AutoID Time to 2 000 if there are Auto-ID problems over Ethernet, radio modem, or WAN.
- **AutoID All Antennas**—forces the ImproX TT to report back Fixed Addresses for both Reader 1 and 2, even if you've only connected Reader 1.

- **Host Interface Fast Polling**—enables fast polling of the Controllers by the Host Interface, and facilitates inter-Controller communication. If Ethernet converters or radio modems are used, you can disable fast polling. The default is **true**.
- **Terminal Bus Fast Polling**—enables fast polling. Default value **= true**.
- **Append Carriage Return to Fast Polling**—enables more efficient fast polling, when you use a transmission device that terminates messages on a carriage return. Enable this setting when you use serial to ethernet devices, radio modems and so on. Default value = **True**.
- **Transmit Inter-controller Broadcast Twice**—broadcasts all Inter-controller communications twice. Only enable this setting when the communications channel is less reliable, dropping inter-controller messages. Note, however, that communications are less efficient with this setting enabled.
- **Relax APB to Level 1 when Controllers go Offline**—if a Controller goes off-line, the remaining Controllers remain on-line. Only the off-line Controller disables Anti-passback (APB) for all Tags.
- **Relax APB to Level 2 when Controllers go Offline**—if a Controller goes off-line, the Host Interface informs the remaining Controllers relaxing Anti-passback (APB) until ALL the Controllers come back on-line. The original off-line Controller disables Anti-passback (APB) for all Tags.
- **Controller Bus Additional Timeout**—increases the timeout duration for the Controllers and Host Interface fast polling. The default is **0**. We recommend that you use the default value.
- **Terminal Bus Additional Timeout**—increases the timeout duration for Fast Polling Terminals. Default value is **0**. We recommend that you use the default value.
- **Uploader Cycle Delay**—sets the delay between upload cycles to the Controllers. Default is **10 000**. If operating on a Wide Area Network (WAN), increase the **Uploader Cycle Delay** to **60 000** (1 minute) to reduce network traffic.
- **Uploader Inter Table Delay**—time taken between processing Database tables in the Uploader. Default value is **10**. Increase to **1 000** to reduce bandwidth usage on a Wide Area Network (WAN).
- **Uploader Daily Start Time**—sets the start time for the upload cycle. The default is **0000**. Change this value to specify starting an upload during specific periods. For example, running an upload after-hours does not reduce network usage during office hours.
- **Uploader Daily End Time**—sets the end time for the upload cycle. The default is **2400** (midnight). If uploading is limited to after-hours, set the **Uploader Daily End Time** to **0600** – this ensures that upload cycles are stopped before the work day begins.
- **Poller Inter Poll Delay**—sets the time between successive polls. The default is **200**. Increase to **2 000** to reduce network traffic over Ethernet converters on a WAN.
- **Poller Daily Start Time**—specifies when the Engine starts polling Controllers. The default is **0000**.
- **Poller Daily End Time**—specifies when the Engine stops polling Controllers. The default is **2400**.
- **Uploader Database Connection Reset**—limits amount of PC memory used by the Software. This value is reset periodically. We recommend that you do not change it. The default is **86400000** (once a day).

Import ECII

The **Import ECII** window in ImproNet Engine enables you to import Fixed Addresses, Logical Addresses, IP Addresses, Hardware and PC Ports of ImproX EC^{II} Controllers into the ImproNet System. Import ECII writes the values into the Database and creates the IP to Logical Address mapping for the communications driver.

Open Import ECII

To open ImproNet Engine **Import ECII**, proceed as follows:

1. In Windows®, click **Start**>**Programs**>**ImproNet**>**Engine**.
2. From the Menu Bar, select **Configuration**>**Import ECII**.

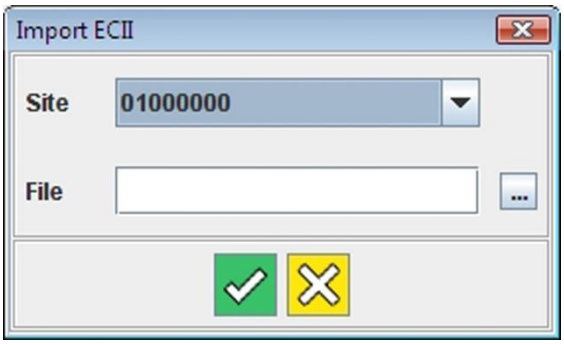


Figure 7 – Advanced Properties

The **Import ECII** option lets you view and change the following settings:

Site

Displays the Site corresponding to the Engine. This drop-down list is only active through Access.

File

Select the file you exported from the Ethernet Discovery Utility containing information on the ImproX EC^{II} Controller you want to import.

System Configuration Procedure

Perform the Configuration Procedure in the following order:

3. Sites
   - Host PC
   - Hardware auto-detection
4. Controller
   - Identify
   - Name
   - Configure
   - Assign Terminals to Zones and Locations
   - Configure Zones and Locations
5. Terminals
   - Identify
   - Name
   - Configure
   - Readers
   - Inputs
   - Outputs
   - Parameters
6. Events and Actions
7. Access Time Patterns
8. Areas
9. Access Groups
   - Time Patterns
   - Areas
10. Tagholders
    - Tags
    - Assign Tags
11. Time Triggered Actions
    - Actions
    - Inputs
    - Outputs
12. Common Zones
13. Messages

Sites

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

- Host PC
- Controllers
- Terminals
- Zones and Locations

Open ImproNet Access

To open ImproNet Access, proceed as follows:

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

Figure 8 – Enter User Name and Password

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

3. In the Navigator Pane, click the icon to create a new Site. A **New Site *node*** is added to the tree.
4. Click the icon. The new Site's details display in the **Main Pane**.
5. The **Host** node expands displaying the Host PC icon. Click the icon.
6. In the Main Pane, enter the Host PC details.

Run Auto-ID to Detect Access Hardware

Before you can use ImproNet Access to configure hardware, you must run the **Auto-ID** function in the ImproNet Engine to detect the hardware.

*If ImproNet Engine and ImproNet Access are on different Host PCs, you must change the **Engine.properties** file.*

To open ImproNet Engine and run Auto-ID, proceed as follows:

1. In Windows®, click **Start**>**Programs**>**ImproNet**>**Engine**.
2. Click the button.

When hardware units are detected, they are added to the ImproNet Database and become available in the ImproNet Access tree. Controllers are assigned default names that contain their logical addresses. Each Controller has a node displaying its unassigned Terminals.

Use your Unit Location Chart to re-name Controllers and Terminals.

Deleting Nodes

You can delete Sites, Controllers, Terminals, Zones, and Locations only, from the Navigator tree. Other node types cannot be deleted.

*When deleting a unit, you must first delete its child components. That is, to delete a Controller, you must first delete its Terminals, Zones, and Locations. Note, however, when deleting a Site the Access Module prompts you for confirmation on whether it must also delete the Sites child components. Delete a unit by simply selecting the unit and pressing **Delete** on your keyboard.*

Shared Data

Do not delete Tagholder Access Groups or Areas unless you are sure that they are not required by other Site components.

ImproNet Access includes user-configurable data that is shared by other Modules; Deleting this data can result in other Modules functioning incorrectly. The following data is shared:

- Device Time Patterns
- Access Time Patterns
- Tagholder Access Groups
- Areas

About Time Patterns

There are two types of time patterns:

- **Device Time Patterns**—determine *when* a device is physically operational.
- **Access Time Patterns**—determine *when* Zones and Locations are accessible.

Device Time Pattern

A Device Time Pattern (DTP) determines when an electrical function or mechanical state on a hardware device is active. Device Time Patterns must be active for the same duration as all Access Time Pattern, and Tagholder Time Patterns that use a relevant device.

Access Time Pattern

An Access Time Pattern (ATP) determines when a Tagholder has access to an Area. When an **Access Time Pattern** and an **Area** are linked, they form an **Access Description**.

Configure Site

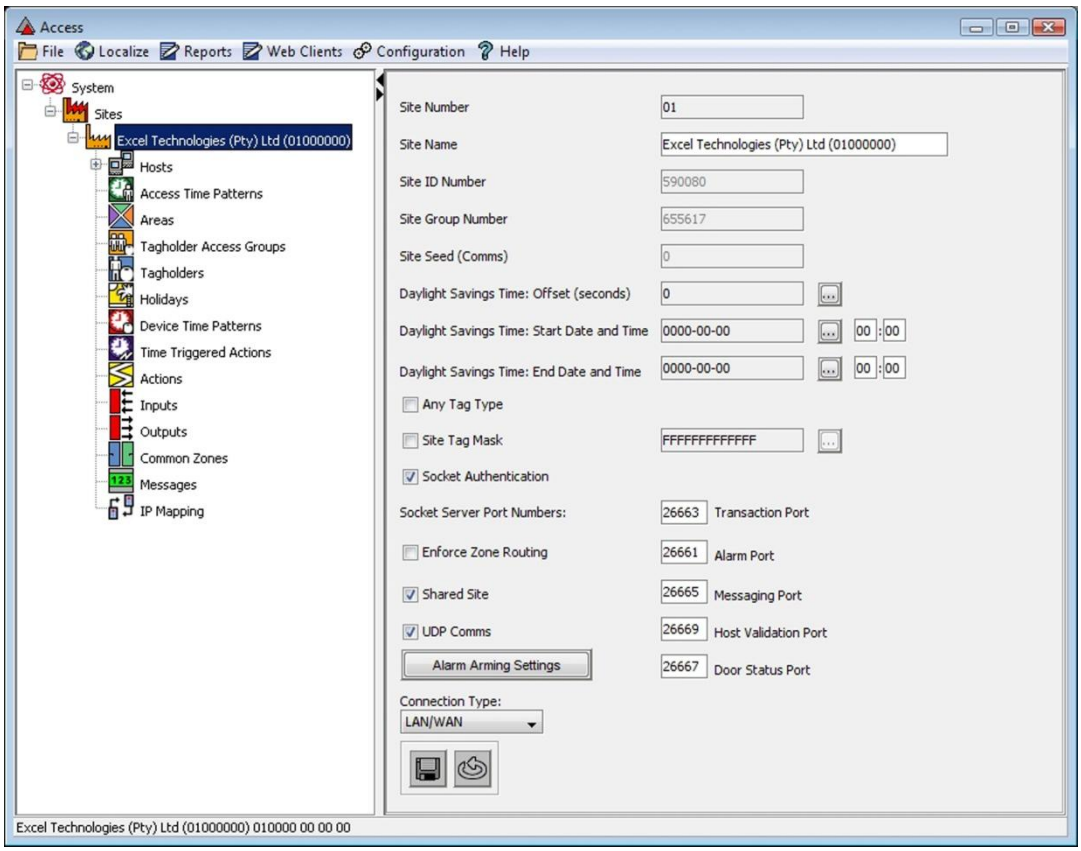


Figure 9 – Configure the Site

1. Select a Site in the Navigator Pane.
2. Complete the following fields in the Main Pane:
   - **Site Number**—automatically assigned Site number.
   - **Site Name**—enter a name for the Site.
   - **Daylight Savings Time**—if applicable, click the ... button and enter a daylight savings offset.
   - **Enforce Zone Routing**—requires Tagholders to access Zones in a specified sequence. Refer to page 29 for details.
   - **UDP Comms**—select this only if you want to map the IP Address to the Logical Address. Once selected, refresh the Site and the IP Mapping table appears.

*The **Daylight Savings Time** setting only works if the PC's Operating System has the **Daylight Savings Offset** feature enabled.*

*Activating the **Any Tag Type** checkbox lets the Controller ignore the Tag Type focusing on validating only on the Tag Code. This setting makes Anti-passback (APB) work across different Tag types, as long as the Tags have the same Tag Code.*

*Activating the **Site Tag Mask** checkbox reduces the number of bits the Controller checks when validating a Tag Code. You may configure the Controller to ignore certain bits.*

3. Leave the remaining fields with their default values.

Add Site

To add a new Site, proceed as follows:

1. In the Navigator Pane, click the icon.
2. In the Main Pane, click the button. The new Site is added to the Navigator tree.

Delete Site

To delete a Site, proceed as follows:

1. In the Navigator Pane, click the icon.
2. In the Main Pane, select the row containing the Site to delete.
3. Click the button.
4. Enter the ImproNet Access password confirming the action.

Set Up the Host PC

*ImproNet Engine enters the Host PC's **IP address** and **Computer Name** (network name) on opening.*

View the Host information, by selecting the **Host** icon.

For Sites using UDP Comms, you must enter the Port Number of the Host PC. We suggest that you use the number **10002**.

About Hardware Configuration

Types of Address

Each hardware unit is allocated a unique *Fixed Address* when it is built. ImproNet Engine allocates a *Logical Address* to the unit for communication purposes.

Recording Installation Information

Ensure the following information is recorded on the **Unit Location Chart** when a new hardware unit is received:

- Fixed Address—supplied on a label included with the unit.
- A unique description of the unit's physical Location.

A Unit Location Chart is provided with every Controller.

Address Allocation

ImproNet Engine assigns Logical Addresses to hardware units when it starts-up, or on request, depending on the system configuration.

Controller

To configure a Controller, proceed as follows:

1. In the Navigator Pane, select a Controller by clicking the icon.
2. Change the default **Controller Name** to the name specified on the Unit Location Chart.
3. Click the Edit Controller Parameters button.
4. In the **Enable Tag Types** section, select the types of Tags to be used. If **HID** Tags are used, enable them here.
5. In the **Terminal Port Baud Rate** section, leave the default setting of **38 400**.
6. Click the button to accept.

Assign Terminals

The first step in configuring a Controller is to assign its Terminals to Zones and Locations. Terminals must be manually assigned to a Controller before they can be configured for Zones and Locations. Unassigned Terminals are terminals that the Auto-ID process has identified, but not assigned to a Location. To assign Terminals to a Controller, proceed as follows:

1. In the Navigator Pane, select a Controller, an **Unassigned Terminals** node is displayed.

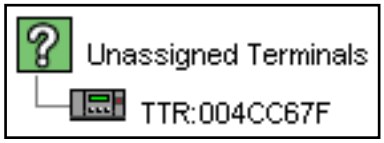


Figure 10 – Unassigned Terminals

2. Double-click the icon to expand the Unassigned Terminals node.
3. Drag-and-drop unassigned Terminals onto a **Controller**. A new **Zone** containing a **Location** is created. **Terminals** display in the Location.

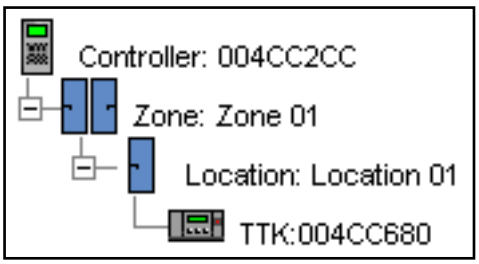


Figure 11 – Zones and Locations

Move a Terminal

If you placed a Terminal in the wrong Location, drag-and-drop it to another Location.

Create New Zones and Locations

- To add another Terminal to an existing Location, drag-and-drop an unassigned Terminal to that Location.
- To create a new Location within an existing Zone, drag-and-drop an unassigned Terminal to the existing Zone.

There is a limit of three Fixed Addresses per Location.

A Terminal can be assigned to one Controller only.

Name each Terminal and Location according to the Unit Location Chart.

Configure Zones and Locations

Locations in the same physically bounded vicinity are grouped into Zones. The total number of Zones per Controller is dependent on the number of Locations per Zone.

Configure Zones

To configure Zones, proceed as follows:

1. In the Navigator Pane, click a icon to select a Zone. The Zone's settings display in the Main Pane.
2. Enter a name for the Zone in the **Zone Name** textbox.
3. Set the **Anti-Passback** (APB) mode.
   - **None**—APB off.
   - **Relaxed**—Once a Tagholder has entered a Zone, they must exit the Zone using their Tag *before* they can re-enter. However, Tagholders can use their Tags for multiple, consecutive exits in this mode.
   - **Strict**—APB Zone rules are enforced for **in** and **out** directions. A Tagholder cannot enter or exit a Zone consecutively.
4. **Supervisor Group for this Zone**—specifies the Supervisor group that must have entered a Zone before a non-supervisor Tagholder is permitted access to that Zone. The default value for this option is none (no value).
5. **Fully Nested within Zone**—select an option from this drop-down list if the Zone is physically contained within another Zone. This option is useful for **Zone Routing**.
6. **Part of Common Zone**—select an option if the Zone is part of a Common Zone. Due to Controller restrictions, you may only assign one Zone as a Common Zone per Controller.
7. **Relaxed Exit Conditions for this Zone**—enables a Tagholder to exit a Zone even if the Access Time Pattern for the Zone has expired. The default value is **Yes**.
8. **Zone Broadcast**—used only on large Sites, where Interleading Zone Routing works ineffectively. The default is **No**.

9. **Anti-Passback Lockout Entry or Exit Delay**—enter a time in minutes to enforce APB. Only available if **Relaxed** or **Strict APB** mode is selected. Refer to point 3 above for APB details.
10. **Limit Tags Inside the Zone to**—enter the maximum number of Tags permitted in the Zone at the same time. Only available if **Strict APB** mode is selected.
11. **Alarm Zone**—sets the Zone as an alarm arming Zone. Activating the checkbox, allows arming and disarming of the Zone.

*When you select the **Alarm Zone** checkbox, Access creates a number of extra default Actions required by the Alarm Arming feature.*

Configure Locations

A Location is a physical point of access. Examples include doors, turnstiles, vehicle gates, and Time and Attendance points. A Location can have a maximum of three Terminals, but can also host a non-scanner Terminal such as the **I16** 16 Channel Input Terminal.

To configure Locations, proceed as follows:

1. In the Navigator Pane, select a Location ( ). The Location's settings display in the Main Pane.
2. Enter a descriptive **Location Name**.
3. If the Location is a Time and Attendance point, select the **Time and Attendance** option from the Location Type drop-down list.
4. If the Location accesses an Interleading Zone, select it from the **Interleading Zone** drop-down list.
5. Click **Enforce Interleading Zone Routing** if required.
6. To specify **Multiple Tag Access**, select the **2 Tags** option. This option is a security feature that requires two Tagholders to access a Zone.

Zone Routing

Zone Routing ensures that a Tagholder accesses Zones in a specified sequence.

To set up Zone Routing, proceed as follows:

1. In the Navigator Pane, select a Site.
2. In the Main Pane, select the **Enforce Zone Routing** option.
3. In the Navigator Pane, select a nested Zone.
4. In the Main Pane, select a Zone from the **Fully Nested Within Zone** drop-down list to specify the selected outer Zone.

Nested Zone must be configured on the same Controller.

Terminals

The Terminals screen enables you to configure a Terminal and set-up its Actions, Inputs, and Outputs. To configure a Terminal, proceed as follows:

1. In the Navigator Pane, click a Terminal to select it. The **Terminal** tab displays.
2. Enter a descriptive **Terminal Name**.
3. Select whether the Reader is an **Entry** or **Exit** Reader.

This step determines the default Actions assigned to the Reader.

4. Click the button to save the settings.

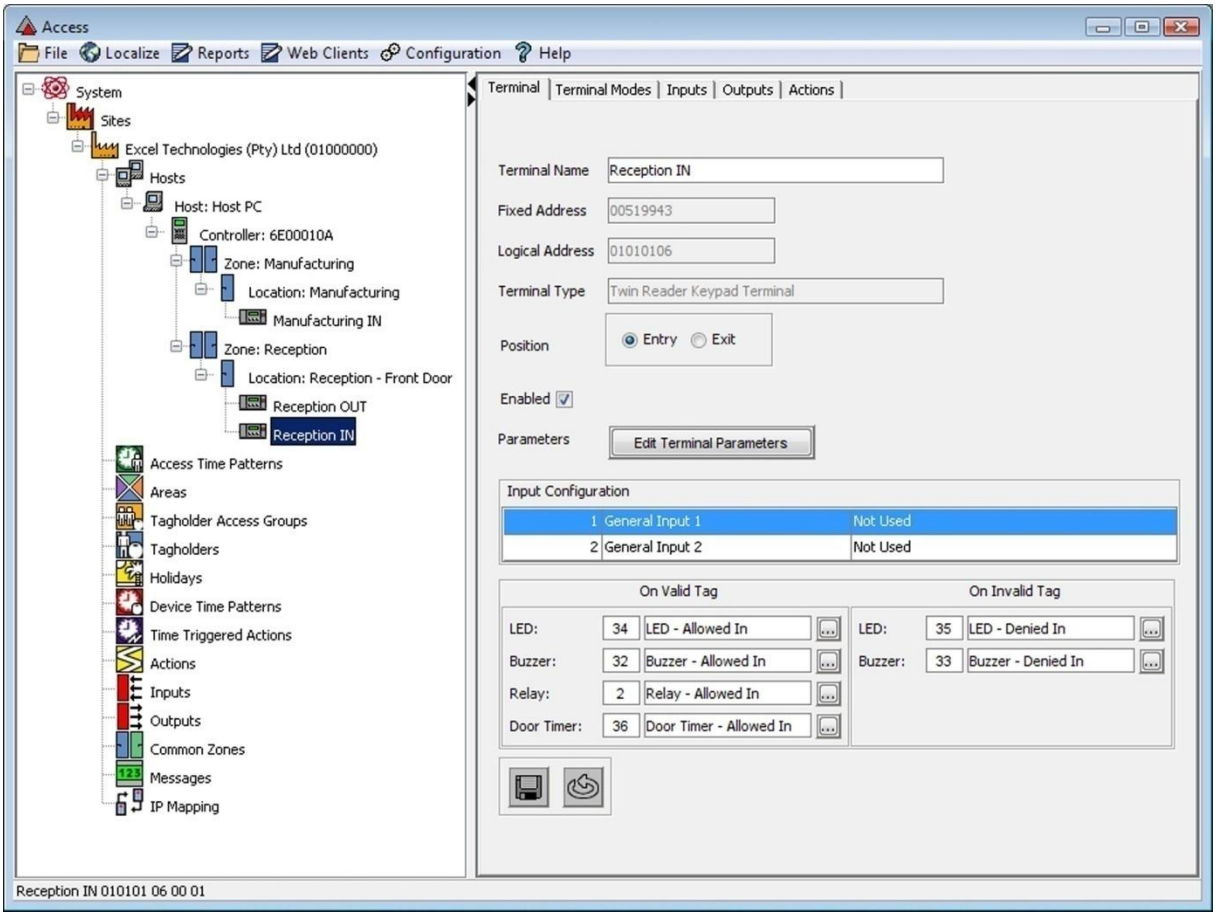


Figure 12 – Terminal Tab

Edit Terminal Parameters

Terminal Parameters are different for each Terminal type. This section provides information on the most common parameters only.

1. Click the **Edit Terminal Parameters** button.
2. Select a **Buzzer Volume**.
3. Enter the value for **Same Tag Timeout** in milliseconds—this is the minimum time that must elapse before the same Tag can be re-read at the Terminal.
4. Select a **Tag Validation** option:
   - **Controller Validation**—the Tag is authenticated by the Controller. This is the default setting.
   - **Host Validation**—the Tag is authenticated by the Host PC. With this option, the Reader does not respond if the Host PC is off-line.
   - **Terminal Validation when Controller Offline**—option enabled by default. This feature is specific to the ImproX MfT Terminal. The Tag is authenticated by the ImproX MfT Terminal when the Controller is off-line.
5. Enter **Random Search** values if required.
6. Click the button to save the settings.

*The **Host Validation** option should only be enabled if third-party software is being used and requires validation.*

Special Codes

You can use Special Codes to manually activate specific Actions, such as opening a door or sounding a siren.

Special Codes are only available on Terminals with a Keypad. However, they are not available if the Terminal is configured for Personal Access Code (PAC) Mode.

Restrict Special Codes to specific Tagholders.

In the **Edit Terminal Parameters** dialog, under **Keypad Transaction Reporting** select **Activate Special Key Codes** thus enabling this feature.

The Special Code format has a maximum of five digits in the following configurations:

- Three digits and a hash. For example, 123#.
- Four digits and a hash. For example, 1234#.
- Five digits up to the number 65535.

Duress Codes

Duress Codes generate an Alarm action when entered on a Keypad Terminal. You can allocate them to Tagholders who have a PIN-code. The Duress Code format is one digit higher or lower than the Tagholder's PIN-code. For example, if the PIN-code is 1234**5**, the Duress Code is 1234**4** or 1234**6**.

Terminal Mode Configuration

*Device Time Patterns must be set-up **before** Terminal Modes can be configured.*

Terminal Mode specifies the state of a Terminal during a selected Time Pattern. The following Terminal Modes and access conditions are available:

- **Tag Mode**—the Terminal requires a valid Tag to be accessible. This is the default mode.
- **Locked Mode**—the Terminal is Locked and access is denied, even to valid Tags.
- **Unlocked Mode**—the Terminal is Unlocked.
- **Tag + PIN**—the Terminal requires a Valid Tag *and* a PIN-code to be accessible.
- **Tag + Reason Code—**the Terminal requires a Valid Tag *and* a Reason Code to be accessible.
- **Tag + PIN + Reason Code—**the Terminal requires a Valid Tag *and* a PIN-code *and* a Reason Code to be accessible.
- **PAC—**the Terminal requires a valid Personal Access Code (PAC) *or* Tag to be accessible.

To configure Terminal Modes, proceed as follows:

1. In the Main Pane, select the **Terminal Mode** tab.
2. Select the **Default Terminal Mode** from the drop-down list.
3. Click the button to create a new Terminal Mode.
4. Click the button alongside the **Select Device Time Pattern** field.
5. Select an existing **Device Time Pattern** record.
6. Click the button.
7. Select a corresponding Terminal Mode from the **Select Terminal Mode** drop-down list.
8. Select the **Report** checkbox to enable reporting of all access actions.
9. Click the button.

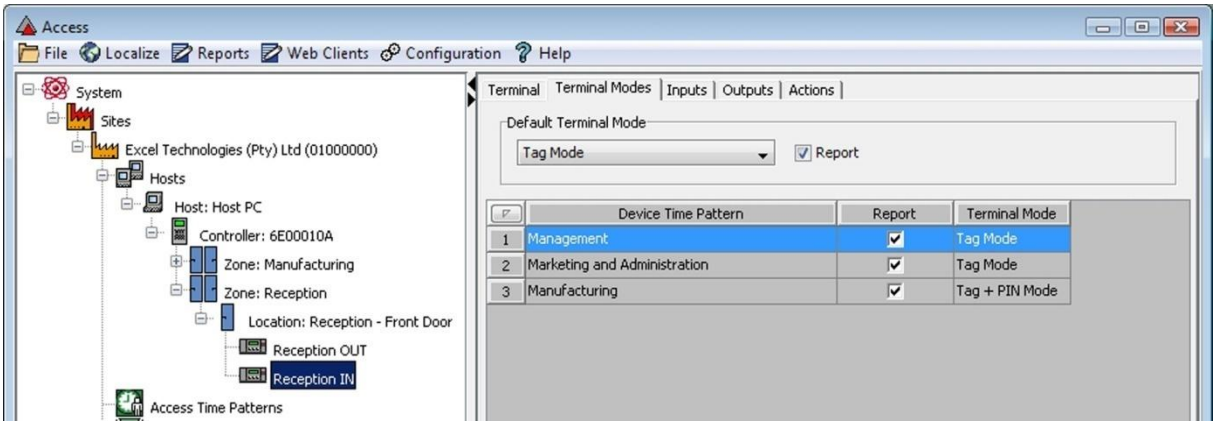


Figure 13 – Terminal Mode Configuration

ImproNet supports up to 128 Device Time Patterns. Each Terminal can have up to eight Device Time Patterns.

Inputs

The **Inputs** tab lets you configure the inputs on the **ImproX I16**, **ImproX DR**, **ImproX DL**, **ImproX PT**, **ImproX TT**, **ImproX TRT** and **ImproX MfT** Terminals. However, Inputs can also be edited and assigned, directly from the Terminals tab. Figure 14 shows the area of the **Terminal** tab where you can edit Inputs and assign Actions.
Configure Inputs for the following:

- Request to Enter / Exit buttons
- Door Open / Door Forced sensing
- Inhibit Scanner function
- Alarm monitoring

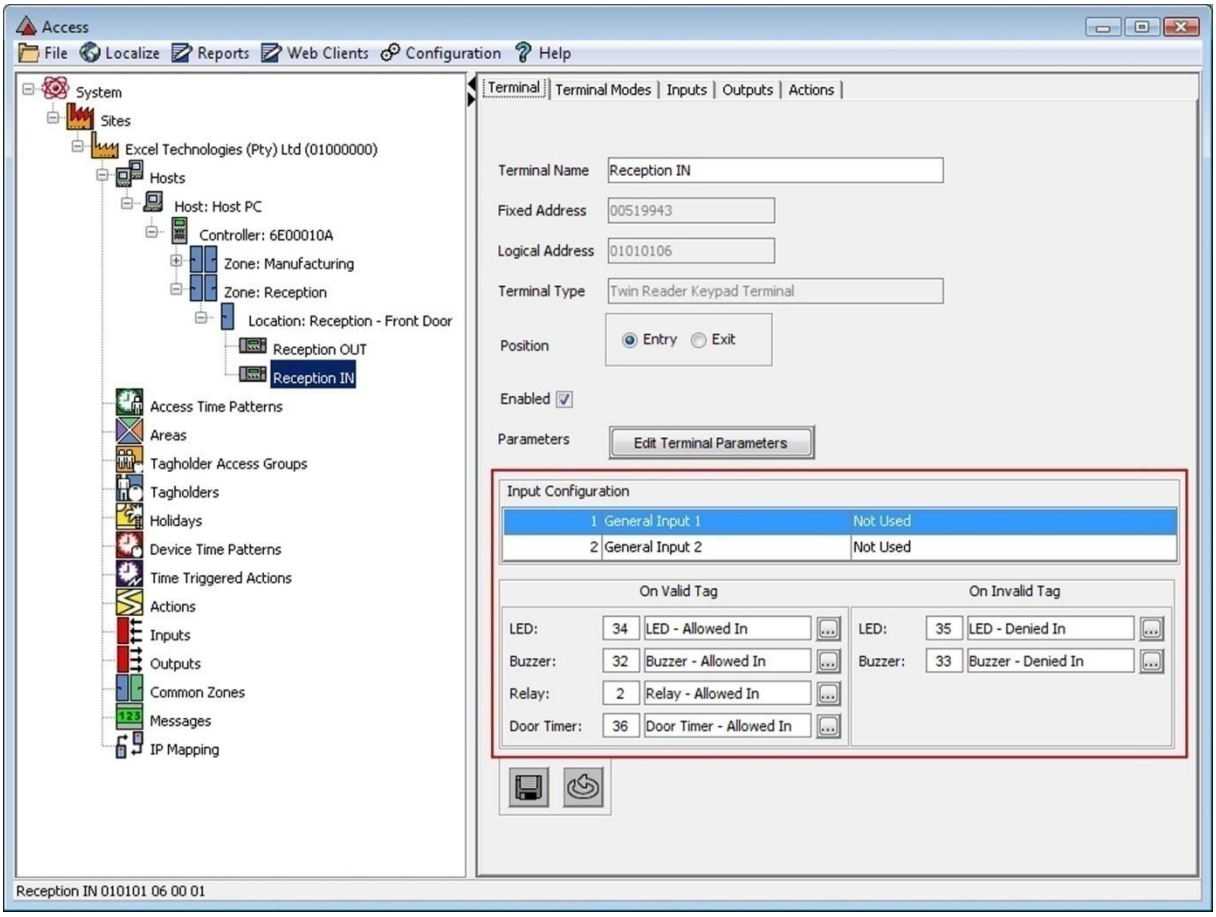


Figure 14 – Terminal Input Configuration

Example of Input Configuration

The following example demonstrates how to create an RTE configuration from the **Terminal** tab:

Figure 15 – Input Configuration Field

1. In the **Input Configuration** field, double-click a General Input that is **Not Used**.

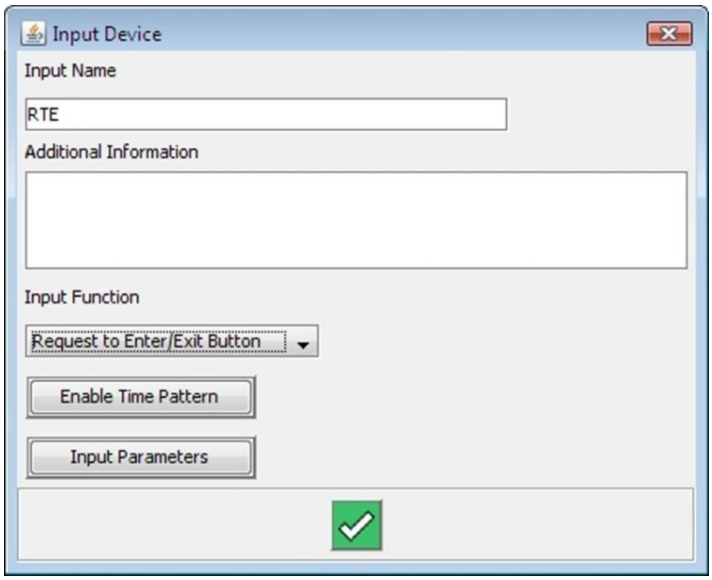


Figure 16 – Input Device Dialog

2. In the Input Device dialog, in the **Input Name** textbox, enter **RTE**.
3. From the **Input Function** drop-down list, select the **Request to Enter/Exit Button** option.
4. Click the button to save.

Input Configuration

To configure Terminal Inputs, proceed as follows:

1. In the Main Pane, select the **Input** tab.
2. Select an Input row.
3. Click the button.

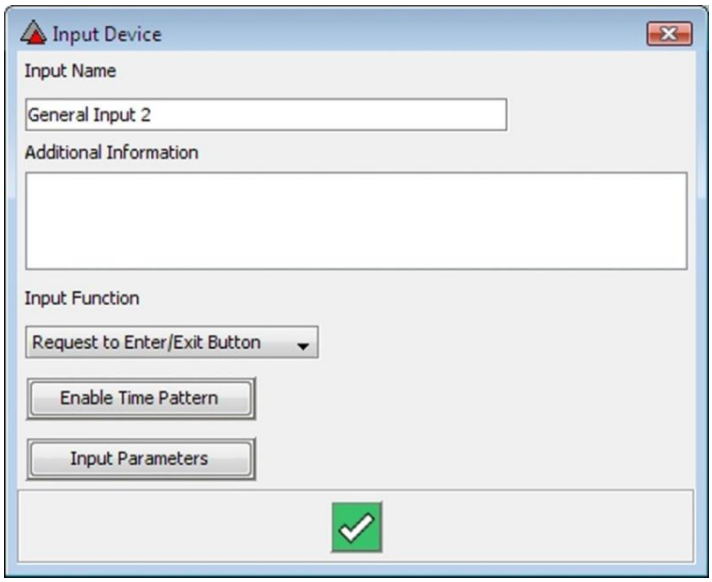


Figure 17 – Input Device Dialog

4. Enter an **Input Name**, or use the default name.

5. Select an **Input Function** from the drop-down list.

The following options are available:

- **Not Used**—select if the input is unused.
- **Request to Enter/Exit Button**—select if the input is connected to a Request To Enter or Exit (RTE) button.
- **Door Open Sensor**—select if the input is connected to a Door Open Sensor (DOS).
- **Alarm Input**—select this option if the Input is connected to a third-party alarm system.
- **Inhibit Scanner**—disables a Tag Reader from reading Tags.
- **Emergency**—switches on Emergency Mode.
- **Lockdown**—switches on Lockdown Mode.
- **Alarm Armed**—arms or disarms the Zone.
- **Alarm System Ready**—puts the Zone into Ready Mode.

Enable Time Patterns

Time Patterns determine when a Terminal Input is active. To configure Time Patterns, proceed as follows:

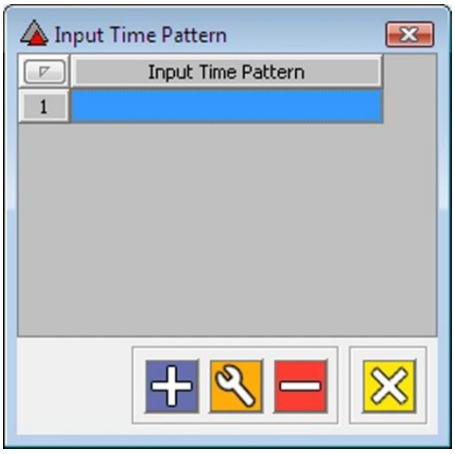


Figure 18 – Input Time Pattern Dialog

1. On the **Input Device** window, click the **Enable Time Pattern** button.
2. Click on the or button.
3. In the **Device Time Patterns** dialog, select the record.
4. Click on the button.
5. Click the button.
6. Click the button.

Input Parameters

The Input Parameter setting provides options for the selected **Input Function**. Proceed as follows to configure Input Parameters:

1. On the **Input Device** window, click the **Input Parameters** button.

For the **Request to Enter/Exit Button** Input Function, the following options are available:

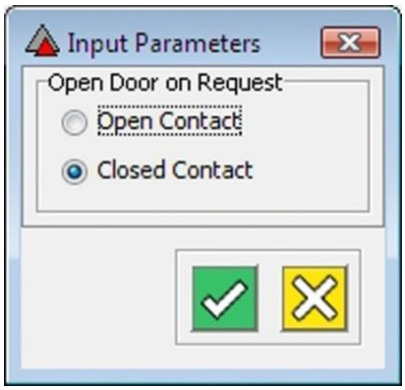


Figure 19 – Request to Enter/Exit Input Parameters

- **Open Contact**—the Door opens when the Input receives an open-contact signal.
- **Closed Contact**—the Door opens when the Input receives a closed-contact signal.

For the **Door Open Sensor** Input Function, the following options are available:

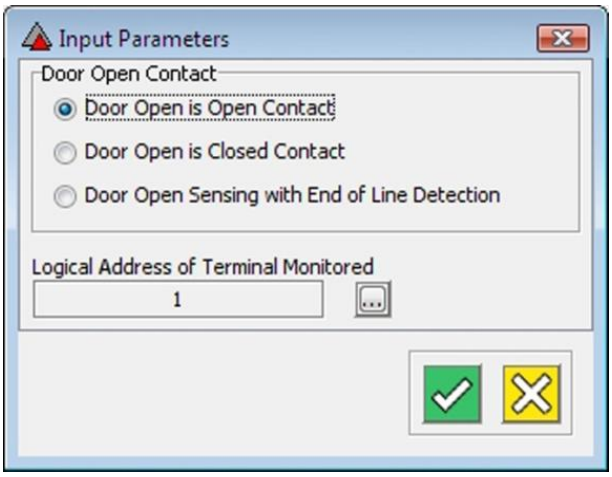


Figure 20 – Door Open Sensor Input Parameters

- **Door Open is Open Contact**—the Input reports that the Door is open when an open-contact signal is received.
- **Door Open is Closed Contact**—the Input reports that the Door is open when a closed-contact signal is received.
- **Door Open Sensing with End of Line Detection**—enables the End-of-line Sensing option.

- Click the button to select the Logical Address of the Terminal Monitored.

The **Inhibit Scanner** Input Function disables a Tag Reader from reading Tags. For IXP400i Sites, using ImproNet V7.60 onwards, the Input Parameters dialog gives the added functionality of setting the inhibit function across MULTIPLE Terminals.

The ability to inhibit multiple units, as shown in Figure 21, is only available on sites using EC^{II} Controllers (IXP400i Sites). In configurations using AC's, IC's or EC's (IXP300 and IXP400 Sites) the dialog only lets you inhibit a single unit.

The following **Inhibit Scanner** options are available:

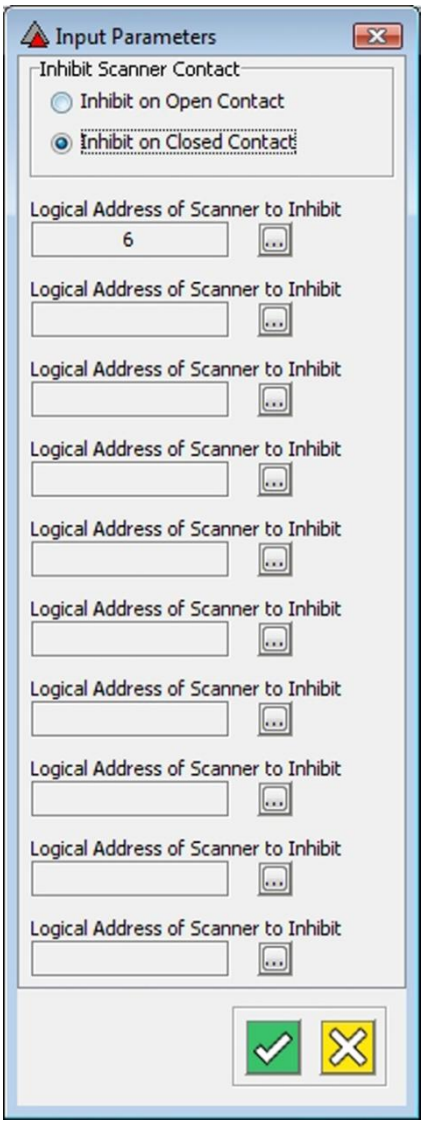


Figure 21 – Inhibit Scanner Input Parameters

Inhibit Scanner Contact

- **Inhibit on Open Contact**—the Reader does not read Tags if the Input detects a Door open-contact signal.
- **Inhibit on Closed Contact**—the Reader does not read Tags if the Input detects a Door closed-contact signal.

Scanner Selection Section

For the first **Logical Address of Scanner to Inhibit** textbox, activating the Inhibit Scanner feature selects, by default, the Terminal being edited. If selecting a Terminal (other than the default) click the button to select the Logical Address to Inhibit.

For the remaining Logical Address of Scanner to Inhibit textboxes, click the button to select the Logical Address to Inhibit.

The text fields remain blank until you select a Terminal's Logical Address.

Selecting the same Logical Address more than once only saves the Logical Address once.

For the **Alarm Input** Function, the following options are available:

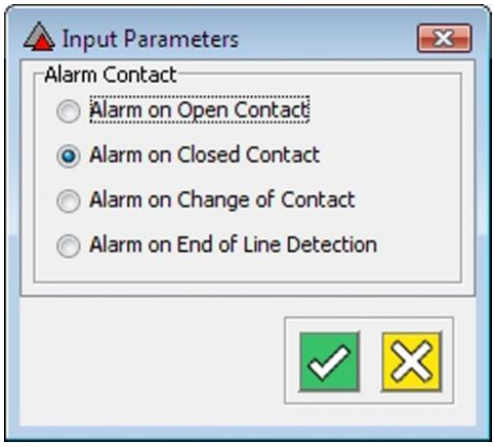


Figure 22 – Alarm Input Parameters

- **Alarm on Open Contact**—an Alarm event is generated if the Input receives an open-contact signal.
- **Alarm on Closed Contact**—an Alarm event is generated if the Input receives a closed-contact signal.
- **Alarm on Change of Contact**—an Alarm event is generated if the Input receives a change-in-contact-state signal.
- **Alarm on End of Line Detection**—an Alarm event is generated if the Input receives an End-of-line-detection contact signal. This option is recommended for the ImproX I16 Terminal.

2. Click the button to accept.

Ensure that you click the button when you exit the Input Device window.

End-of-line Sensing for the ImproX TT

End-of-line Sensing on the ImproX TT is only possible if Door Open Sensing is configured. Only Inputs 1 and 3 on the ImproX TT have end-of-line sensing functionality. Configure the Input as a **Door Open Sensor**, and select **Door Open Sensing with End of Line Detection** from the input parameters list.

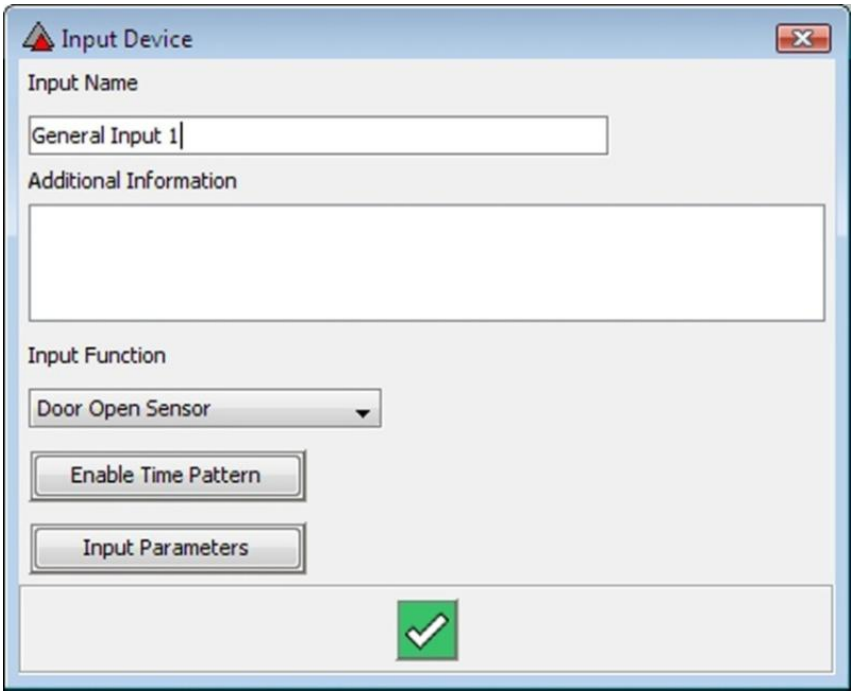


Figure 23 – Input Device Dialog

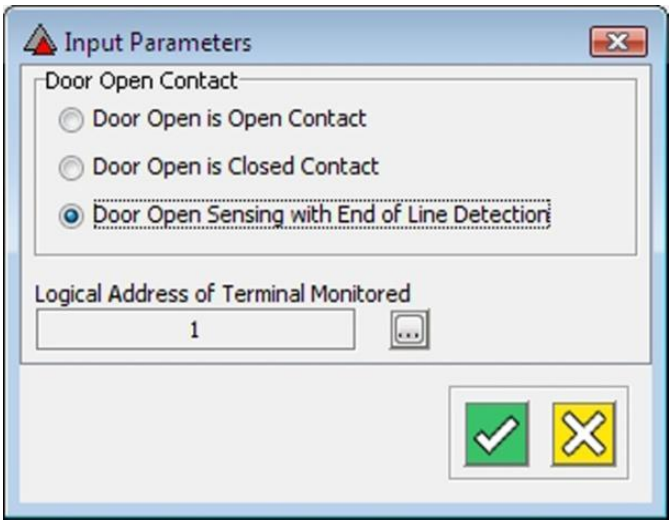


Figure 24 – Input Parameters Dialog

Outputs

The **Outputs** tab enables you to configure a Terminal's LED and Relay states for different Terminal Modes.

We recommend setting different LED states for different Terminal Modes, as this will help Tagholders identify Terminal Mode changes.

To configure Terminal Outputs, proceed as follows:

1. In the Main Pane, select the **Output** tab.
2. Select an Output row.
3. Click the button.

The content in the Output Device dialog is one of the following depending on the function of the selected output device.

- General Relay
- Status LED

General Relay

If the output device is a General Relay, select a **Relay Contact State** for each of the following:

- Relay during Locked Mode
- Relay during Unlocked Mode
- Relay during Tag Mode
- Relay during Emergency Mode
- Relay during Lockdown Mode

Click either the associated Mode's **Query** button or the **Configure Outputs** button to edit the available Relay Contact States. The following **Relay Contact States** are available:

- Do NOT Drive Relay in this Mode
- Drive Relay in this Mode

Status LED

If the output device is a Status LED, select a **Status LED State** for each of the following:

- Status LED during Locked Mode
- Status LED during Unlocked Mode
- Status LED during Tag Mode
- Status LED during Emergency Mode
- Status LED during Lockdown Mode

Click either the associated Mode's **Query** button or the **Configure Outputs** button to edit the available Status LED States. The Status LED States appear as shown in Figure 25.

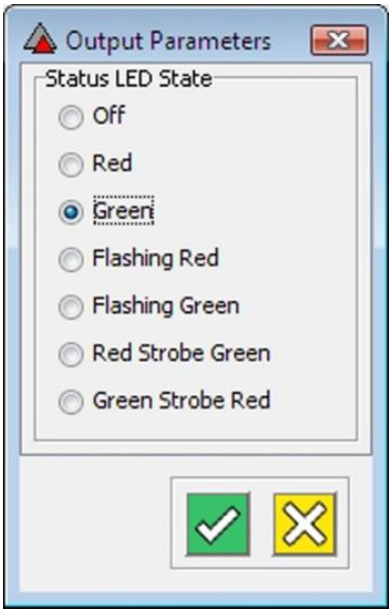


Figure 25 – Output Parameters Dialog

Actions

About Actions

ImproNet enables you to define Actions for Terminals and in some cases, Controllers. Actions are instructions stored in a Controller's memory, and are triggered by **Events** or by the **Time Triggered Actions** function. The following are examples of common Actions:

- Driving a Relay
- Sounding a Buzzer
- Changing LED state
- Displaying LCD message

When a Terminal is assigned to a Location, default actions for the Terminal are created. Figure 26 displays the default actions created for the **On Valid Tag** event, and for the **On Invalid Tag**. These Actions are executed when a Tag is presented at the Terminal.

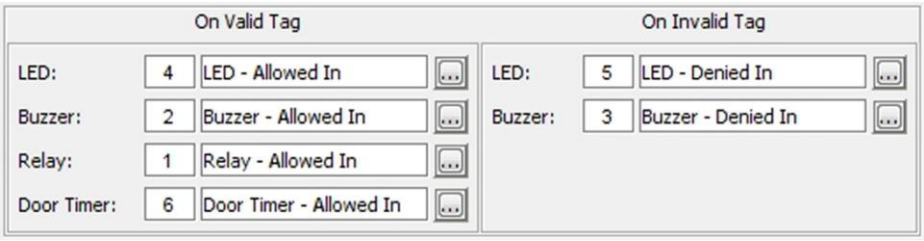


Figure 26 – Default Terminal Actions

The **On Valid Tag** event encompasses *all* valid Tag Events. Therefore, the **On Valid Tag** section on the Terminal tab enables you to configure actions to all valid Tag Events in a bulk procedure. Similarly, the **On Invalid Tag** event encompasses *all* invalid Tag Events. Therefore, the **On Invalid Tag** section on the Terminal tab enables you to configure actions to all invalid Tag Events in a bulk procedure.

To customize the settings of the default actions, proceed as follows:

1. On the Terminal tab, click the button next to the Action that you want to edit.
2. Change the settings as necessary.
3. Click the button to accept.

*The **Actions** tab lists all Actions currently assigned to the selected Terminal and enables you to assign additional actions to the **On Valid Tag** and **On Invalid Tag** events.*

About Events

System Events are activated by a Controller when a particular procedure or process is performed.

For example, when a Reader detects a Tag, the Tag is validated by the Controller, and the Event **Allowed_Normal_In** or **Allowed_Normal_Out** is activated. In this example, the actual Event depends on whether the Reader is an Entry or Exit Reader.

When an Event is generated, the Controller executes the Actions linked to the Event.

Active System Events

The **Active System Events Editor** enables you to link Actions to *Allowed* Events and *Denied* Events. You can have up to five of the following Action types per Event:

An Action is not created for a Terminal if the hardware does not support the Action.

Action	Optional	Description
Buzzer	×	Created by default when you specify a Terminal as an Entry or Exit Reader.
Status LED	×	Created by default when you specify a Terminal as an Entry or Exit Reader.
Buzzer—Armed Out of Sequence	×	Created by default when you set up Alarm Arming (see Part V – Advanced Configuration for more information).
Buzzer—Failed to Arm	×	
Buzzer—Failed to Arm All Zones	×	
Buzzer—No Arm Authority	×	
Buzzer—Zone Already Armed	×	
Buzzer—Zone Armed	×	
Buzzer—Zone Not Ready	×	
LED—Armed Out of Sequence	×	
LED—Failed to Arm	×	
LED—Failed to Arm All Zones	×	

Action	Optional	Description
LED—No Arm Authority	×	Created by default when you set up Alarm Arming (see Part V – Advanced Configuration for more information).
LED—Zone Already Armed	×	
LED—Zone Armed	×	
LED—Zone Not Ready	×	
Buzzer—Already Disarmed	×	
Buzzer—Disarm Failed	×	
Buzzer—Disarmed Emergency Unlock	×	
Buzzer—Disarmed out of Sequence	×	
Buzzer—No Disarm Authority	×	
Buzzer—Zone Disarmed	×	
LED—Already Disarmed	×	
LED—Disarm Failed	×	
LED—Disarmed Emergency Unlock	×	
LED—Disarmed out of Sequence	×	
LED—No Disarm Authority	×	
LED—Zone Disarmed	×	
Relay	×	Created by default when you specify a Terminal as an Entry or Exit Reader.
LCD	✓	An LCD Action displays a user-configurable text message on a Terminal or Controller with an LCD.
Emergency Mode	✓	Emergency Mode Actions are only executed on Controllers and Terminals that have been configured for Emergency Mode.
Door Open Timer	✓	The Door Open Timer Action is created by default for ImproX PT and TT Terminals. However, it is not enabled until a Terminal Input is configured as a Door Open Sensor (DOS). A Door Open Timer Action prevents a Door Forced Alarm Event from being activated if a Door is opened under the following conditions: – A valid Tag Event precedes the Door opening – A valid RTE Event precedes the Door opening
Multiple Actions	✓	A Multiple Action groups up to five other Actions together so that they execute as a single Action. Multiple Actions are useful for Lift (Elevator) Control.
Reset Digital Inputs	✓	Resets Digital Inputs.
Raise System Event	✓	Raise Event triggering Action.
Reset Zone Count	✓	Resets the Zone count (count of Tagholders in the Zone).

Action	Optional	Description
Arm Alarm System Relay	×	The Relay for use in arming the alarm system for the specified Zone.
Disarm Alarm System Relay	×	The relay for use in disarming the alarm system for the specified Zone.
Send SMS	✓	Used for sending an outgoing SMS to the phone number(s) specified in the message.

Table 3 – Actions

Configure Active System Events

On the **Actions** tab, click the **Active System Events** button. The Active System Events Editor enables you to assign up to five Actions to the **On Valid Tag** and **On Invalid Tag** events. Available Actions are listed in sequence. If the middle block of an Action is empty, the action is unused.

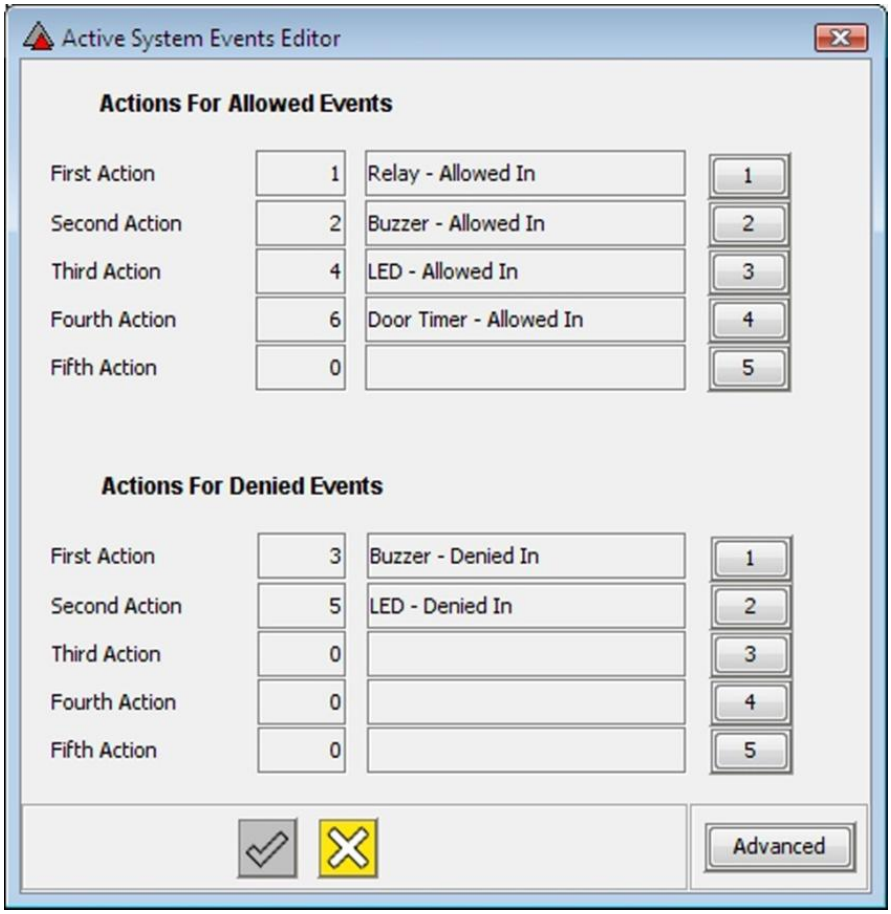


Figure 27 – Active Systems Event Editor

To assign new Actions to an Event, proceed as follows:

1. Click the number button to the right of an unused Action.
2. Click an Action to select it.
3. Click the button.

Advanced Active Systems Events

The **Active Systems Events** window enables you to assign up to five Actions to any system Event. To access this facility, click the **Advanced** button on the **Active Systems Event Editor** dialog, and select an Event from the **Active System Event** drop-down list.

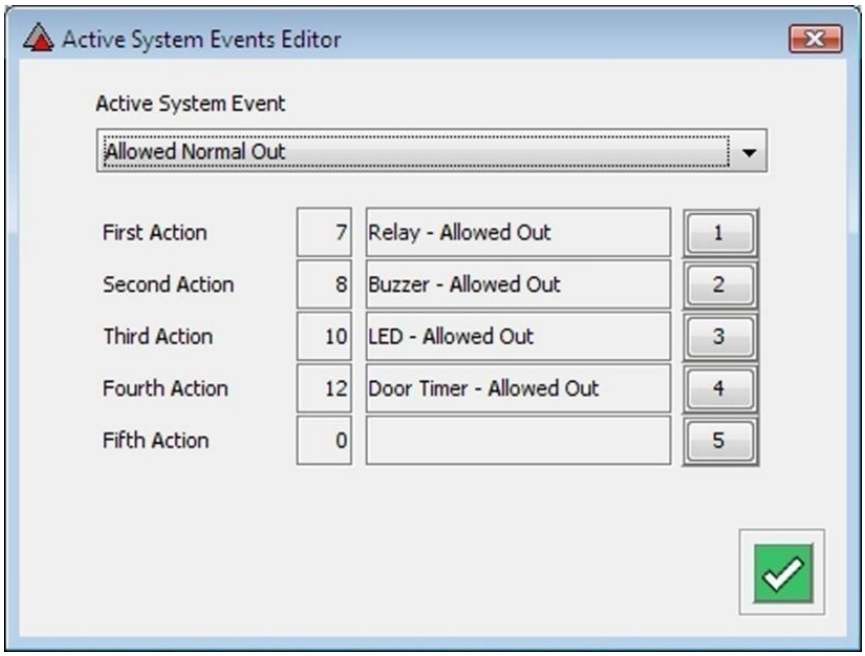


Figure 28 – Advanced Active Systems Events Editor Dialog

Access Time Patterns

Access Time Patterns specify times when access is permitted. Tagholders Access Groups are assigned one or more Access Time Pattern. When an **Access Time Pattern** and an **Area** are linked, they form an **Access Description**.

Terminal Modes override Access Time Patterns. For example, if a Tagholder has access from 6 am to 6 pm, but the Terminal is locked from 5:30 pm, the Tagholder will be denied in after 5:30 pm.

Access Time Patterns regulate Tagholder access times, and have no start and end dates. Device Time Patterns regulate Terminal operation times.

Configure Access Time Patterns

To configure an Access Time Pattern, proceed as follows:

1. In the Navigator Pane, click the icon. In the Main Pane, the Default Access Time Pattern displays.
2. Do one of the following:
   - Select an Access Time Pattern, and click the button. The **Edit Access Time Pattern** dialog displays.
   - Click the button to create a new Access Time Pattern.

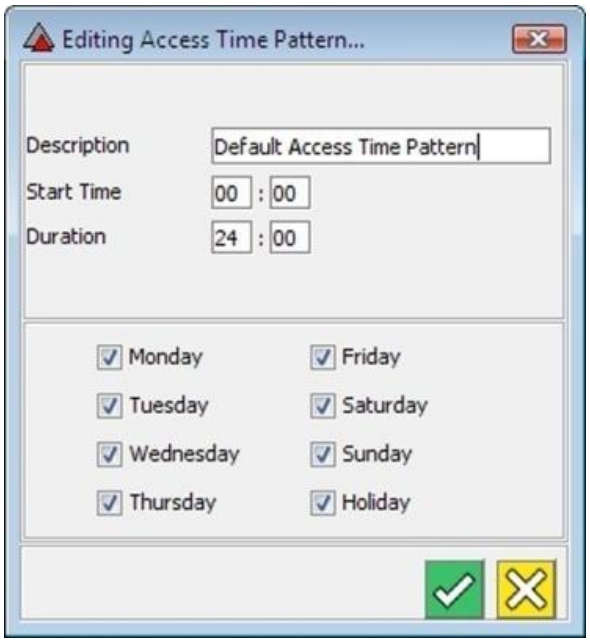


Figure 29 – Edit Access Time Pattern Dialog

3. Enter a **Description** for the Access Time Pattern.
4. Enter a **Start Time**—this is the time of day when the Access Time Pattern becomes active.

5. Enter the **Duration** in hours and minutes—this is how long after the start time, the Access Time Pattern is active.
6. Select the days of the week when the Access Time Pattern is enabled.
7. Create as many Access Time Patterns as necessary.

If a lockout period between regular access periods is required, you need to create two Access Time Patterns. For example, to disable access during a lunch hour, you need to create an Access Time Pattern that ends when lunch starts, and another Access Time Pattern that starts when lunch ends.

Areas

An Area consists of a number of Locations grouped together to form a logical unit. An Area is *not* a physically bounded building or place; it is a collection of Locations that a group of Tagholders has access to.

The purpose of an Area is to group Locations with the *same access requirements* together. This enables you to assign the same access rights to multiple locations at the same time. Figure 30, illustrates the concept of Areas. In the schematic, Locations are assigned to the **Management**, **Factory Workers**, or **Design Staff** Areas. Note that a single Location can be assigned to more than one Area.

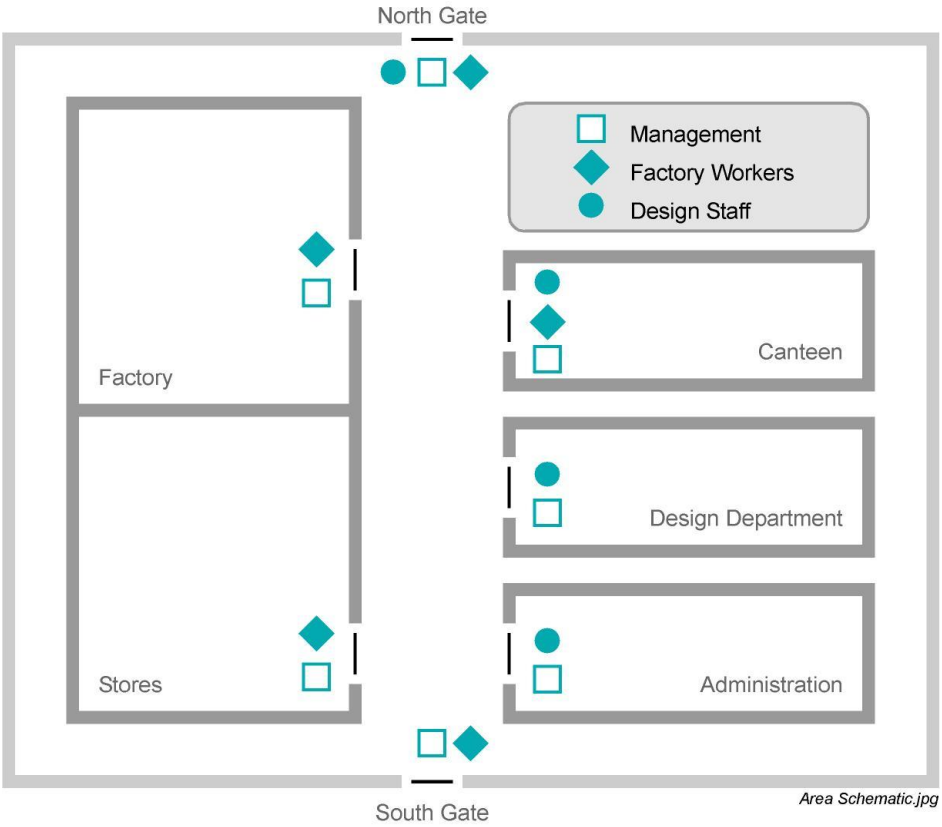


Figure 30 – Area Schematic

Select Area

To select an existing Area, proceed as follows:

1. In the Navigator Pane, click the icon.
2. Select an Area from the **Area Name** drop-down list.

An Area that has no Locations assigned to it displays the icon only. A configured area displays a tree of locations. If a Location is visible, then it is assigned to the selected Area.

Create Area

To create an Area, proceed as follows:

1. In the Navigator Pane, click the icon.
2. In the Main Pane, click the button.
3. Enter an Area Name and Area Description.

Delete Area

To delete an Area, proceed as follows:

1. In the Navigator Pane, click the icon.
2. Select an Area from the **Area Name** drop-down list.
3. Click the button.
4. Click the button. A confirmation dialog displays.
5. Click **Yes.**

Assign Locations to Areas

To assign Locations to an Area, proceed as follows:

1. In the Navigator Pane, click the icon.
2. Select an Area from the **Area Name** drop-down list.
3. Click the button.
4. In the **Edit** window, select a Location by clicking it—Select multiple Locations by holding down the **Ctrl** key while you click.

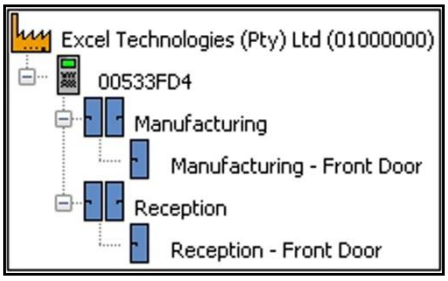


Figure 31 – Assign Locations to Areas

5. Click the button to save.

Access Groups

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

Item	ImproX IC IXP300	ImproX AC IXP400	ImproX EC IXP400	ImproX EC^{II} IXP400i
Tagholder Access Groups per Site	256	1 024	1 024	10 000
Access Descriptions per Tagholder Access Group	3	3	3	3
Tagholder Access Groups per Tag	3	3	3	10

AGSysConfigParameters.jpg

Figure 32 – System Configuration Parameters

Access Descriptions

An **Access Description** defines the Time and the Area where access is permitted.

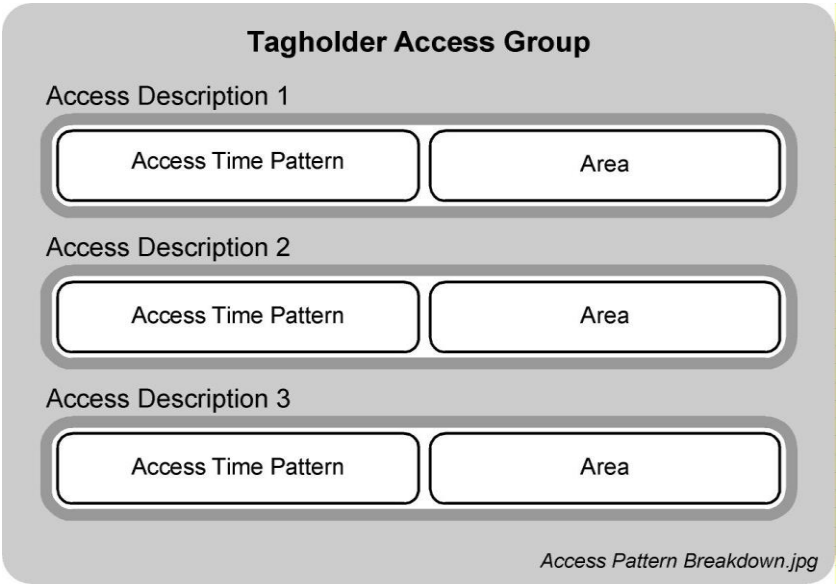


Figure 33 – Tagholder Access Group Breakdown

There are two types of Tagholder Access Groups:

- **General**—used for permanent staff.
- **Visitor**—used for visitors.

Configure Tagholder Access Groups

The Tagholder Access Group screen displays available Access Groups in the left-hand panel, and their Access Descriptions in the right-hand panel.

Select a Tagholder Access Group

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

1. In the Navigator Pane, click the icon.
2. Select a Tagholder Access Group from the **General** tab in the left-hand panel. Alternatively, click the **Visitors** tab and select a Visitors Access Group.

The selected Access Group's **Access Descriptions** are displayed in the right-hand panel of the Tagholder Access Group screen

Create a Tagholder Access Group

To create a Tagholder Access Group, proceed as follows:

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.
4. Click the button to save.

Delete a Tagholder Access Group

*Remove all **Tags** assigned to the Tagholder Access Group before you delete the Group.*

*Remove all **Access Descriptions** from the Tagholder Access Group before you delete the Group.*

To delete a Tagholder Access Group, proceed as follows:

1. In the Navigator Pane, click the icon.
2. Select a Tagholder Access Group.
3. Click the button. A confirmation dialog displays.
4. Click **Yes**.

Edit a Tagholder Access Group

To edit a Tagholder Access Group, proceed as follows:

1. In the Navigator Pane, click the icon.
2. Select a Tagholder Access Group.
3. Click the button.

Configure Access Descriptions

The **Access Descriptions** dialog has three tabs—one for each Access Description per Access Group. The **Access Description 1** tab is displayed by default.

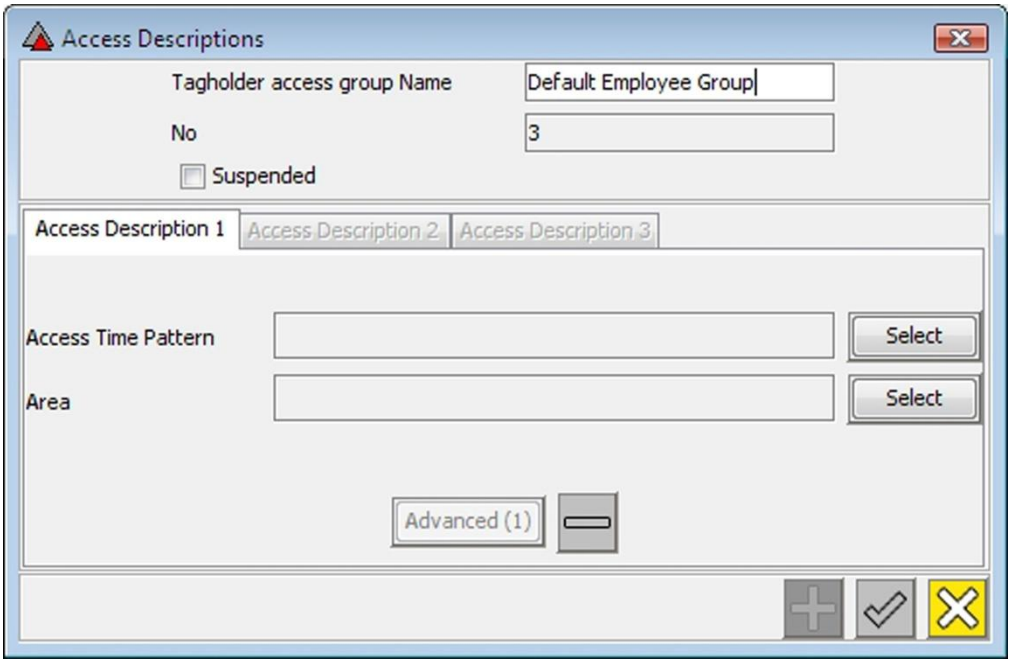


Figure 34 – Access Descriptions Dialog

Assign Access Time Patterns

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

Assign Areas

4. Alongside the Area textbox, click the **Select** button.
5. Click a **Time Pattern Name** to select it.
6. Click the button to accept.

Three Access Descriptions are available per Access Group. However, you only need to configure one of them to save an Access Group.

Advanced Settings

Click the **Advanced Settings** button on the **Access Descriptions**. Additional settings are displayed on the following tabs:

- **Reporting**—click the checkbox to log all transactions for the selected Access Description.
- **Start & Expiry Date**—click the edit buttons and enter dates to control when the Access Description is active.

- **Supervisor Unlock**—select the Supervisor who is required to be inside the Area before other Tagholders are permitted entry.

*The **Supervisor Unlock** facility is only applicable to Areas comprising a single zone set to **Strict Anti-passback**.*

- **Actions**—click the Select buttons to assign actions for when Tagholders are entering (**Coming In**), or exiting (**Going Out**) the Area specified in the Access Description.
- **Alarm Arming**—(only available on Employee Tagholder Access Groups, when unlocked for Alarm Arming) 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 options 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.

Visitor Access Group

Visitor Access Groups are displayed on the **Visitors** tab on the Tagholder Access Groups screen. They operate the same as other Access Groups. Note that Visitor Tags can be assigned to Visitor Access Groups only.

Tagholders – Assign Access to Tags

A Tagholder is any person who uses a Tag to access a Site. Visitors are Tagholders with restricted access rights. Before you can assign access to a Tag, you must first assign the Tag to a Tagholder. The Tagholder screen enables you to do the following:

- Add Tagholders to a Site
- Edit existing Tagholder information
- Search for Tagholders
- Read Tags

Add or Edit a Tagholder

To add or edit a Tagholder, proceed as follows:

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.

Quick Search for Tagholder

To search for a Tagholder, proceed as follows:

1. In the Navigator Pane, click the icon.
2. Enter some text into the **Find** textbox.

Figure 35 – Find Tagholder

3. Select the search criteria from the **on Column** drop-down-list. The results display in the Main Pane.

Configure Tagholder

The **Edit Tagholder** dialog enables you to create or edit a Tagholder's information and assign Tags. Only the **First Name** and **Last Name** fields are required. However, we recommend entering as much information as possible.

To create or edit a Tagholder, proceed as follows:

1. Enter the Tagholder's **First Name** and **Last Name**.
2. Complete other personal information as necessary.
3. Select the **Current** checkbox to enable the Tagholder (selected by default). If this **Current** checkbox is unchecked, the Tagholder is inactive in the system.
4. Use the **Notes** text area to enter other information about the Tagholder.
5. Enter a PIN-code of up to 5 digits if the Tagholder is required to use keypad-type Readers.

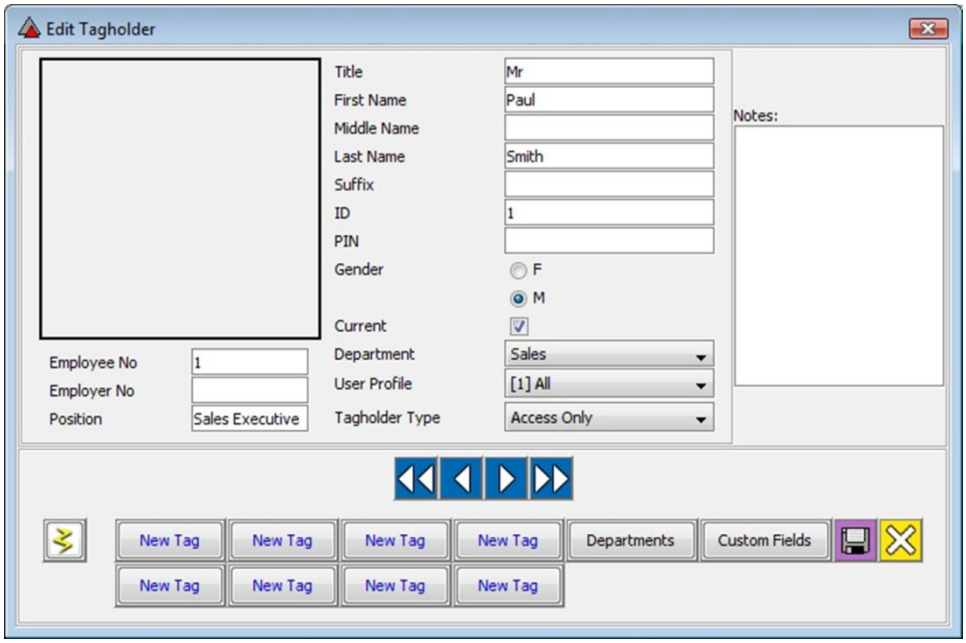


Figure 36 – Edit Tagholder Dialog

Departments

Select the Tagholder's Department from the **Department** drop-down list. To add new values or to edit the Department list, proceed as follows:

1. Click the **Departments** button. The **Department Editor** dialog displays.

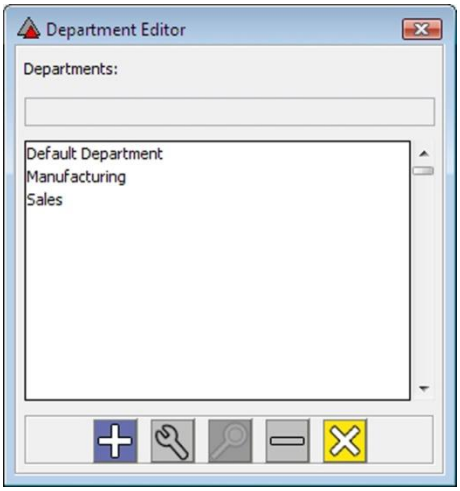


Figure 37 – Department Editor Dialog

2. Do one of the following:
   - Click the button to add a new Department.
   - Click the button to display Tagholders belonging to the selected Department.
   - Select a Department and click the button to edit it.
   - Select a Department and click the button to delete it.

Custom Fields

This feature lets you create any extra fields you may need. For example, there is no field in Access where you may enter the Tagholders home address or telephone number.

Add Custom Fields

1. In the Edit Tagholders dialog, click on the **Custom Fields** button.
2. In the Custom Fields dialog, click on the **Advanced** button.
3. Click the button.
4. In the **Field Name** field, type in a name for your custom field.
5. In the **Field Description** field, type in a description of your custom field.
6. Click the **Required Field** checkbox, if this field's information is required for every Tagholder entry.
7. Click the button to accept.
8. Click on the button.

Now when you click on the Custom Fields button, the Custom Fields dialog displays your newly created fields.

Edit Custom Fields

1. In the Field Creator dialog, double click on the fields name.
2. Edit the details as necessary.
3. Click the button to accept.
4. Click on the button.

Third-party Applications

Once a single Third-party Application is assigned, pressing this button launches a third-party application from Access.

This button only appears in the Edit Tagholder dialog.

1. In the Edit Tagholder dialog, click on the button.
2. In the Third-party App dialog, select the button alongside the Path field.
3. Choose the **exe** or **bat file** you wish to run.
4. Click the Open button.
5. Click the button to accept.

The path entered above is stored in the Access Properties file. If you want to change the path, either edit the Properties file or, in the Edit Tagholder dialog, hold down the Ctrl key and click on the button.

User Profile

User Profiles are configured when Operator Security is required.

Configure Tag Details

A Tagholder can have 4 Tags assigned to them in IXP300 or IXP400 Systems and 8 Tags assigned in IXP400i Systems.

To assign Tags to a Tagholder, proceed as follows:

1. On the Edit Tagholder dialog, click any of the New Tag buttons.
2. 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.
3. Configure the following:
   - **APB Override**—Tags are not subject to APB rules.
   - **Report Always**—All Transactions for the Tag are written to the Database.
4. Assign the Tagholder to a Site by selecting a value from the Site Assigned drop-down list.
5. Assign the Tagholder to one or more Tagholder Access Groups by selecting values from the **Group1** to **10** drop-down lists.

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

Repeat procedure for additional Tags if necessary.

Read the Tag

1. Present a Tag to an Enrollment Reader and click the **Read Tag** button. The Tag Type is usually detected automatically.
2. 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.

When ImproNet detects a Tag, a Tag number displays in the **Tag Code** textbox.

*To create a Personal Access Code (PAC) only, select the **Personal Access Code** option from the **Tag Type** drop-down list and enter the PAC in the **Tag Code** textbox.*

Multiple Tags do not work in an Anti-Passback Zone; if you enter a Zone with one Tag, and exit the Zone using a different Tag, APB is not enforced.

Specify Start and End Dates

1. If the Tagholder is temporary, click the **Pick Start Date** and **Pick End Date** buttons to select a Start Date and Expiry Date. To select dates, proceed as follows:
   – Select a **Month** and a **Year** using the and arrow buttons
   – Select a **Day** by clicking it. Alternatively, click **Zero Date** to set no date
2. Click the button to accept.

Set the Default Card Template

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

*The procedure for Setting the **Default Card Template** is described in Part VI – Modules, of this manual, in the Card Designer chapter.*

Batch Enrollment of Tags

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

Start Batch Enrollment

Proceed as follows to open Batch Enrollment and start adding Tags:

1. On the ImproNet Access Menu, select **Configuration**>**Batch Enrollment**.

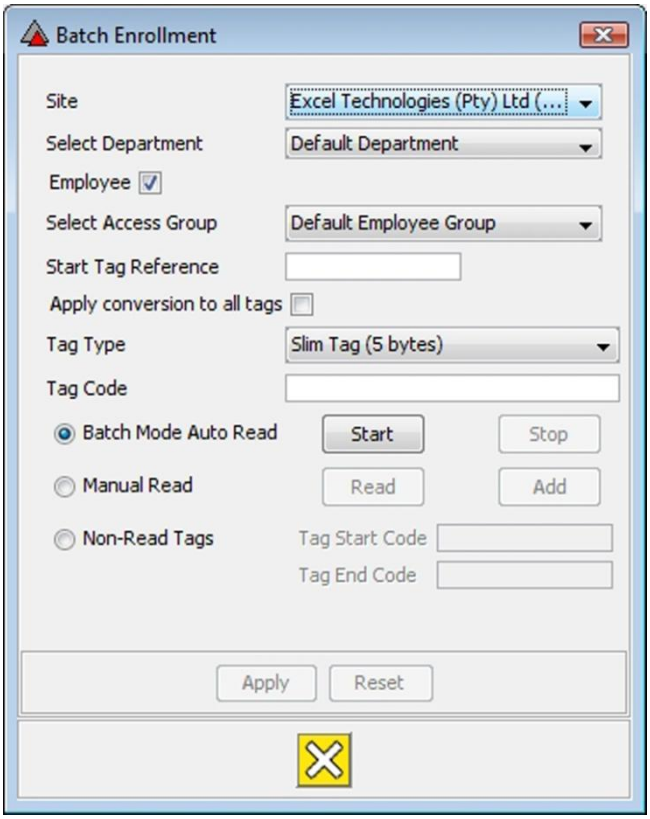


Figure 38 – Batch Enrollment Dialog

2. Select a **Site** to assign the Tags to.
3. Select a **Department** if necessary.
4. Select the **Employee** checkbox if the Tags are for employees. Or deselect the **Employee** checkbox if the Tags are for Visitors.
5. Select an **Access Group**.
6. Enter a **Start Tag Reference** number if required. The Start Tag Reference number is any number or identification that you can use to temporarily identify the Tags.
7. Select one of the following to start the Batch Enrollment process:
   - Batch Mode Auto Read
   - Manual Read
   - Non-read Tags

Batch Mode Auto Read

This Mode enables you to scan a batch of Tags in quick succession.

1. Select the **Batch Mode Auto Read** option.
2. Click the **Start** button.
3. Present Tags to the Enrollment Reader one at a time.
4. Click the **Stop** button.
5. Once the **Apply** button becomes enabled, click **Apply**.

Manual Read Mode

Manual Mode lets you scan a batch of Tags one at a time. It is useful if an Enrollment Reader is not within reach of the Host PC.

1. Select the **Manual Mode** option.
2. Present a Tag to the Enrollment Reader.
3. Click the **Read** button. The Tag is read when its number displays in the **Tag Code** textbox.
4. Click the **Add** button.
5. Repeat steps 1 to 4 for additional Tags.
6. After you've scanned all the Tags, click **Apply**.

Non-read Tags Mode

This Mode enables you to add a batch of sequential Tag codes.

1. Select the **Non-read Tags** option.
2. In the **Tag Start Code** textbox, type in the Tag code for the first Tag in the sequence.
3. In the **Tag End Code** textbox, type in the Tag code for the last Tag in the sequence.
4. Once the **Apply** button becomes enabled, click **Apply**.

*Use this feature when enrolling a group of Tags in sequence. For example where you have 5 Tags, (1011, 1012, 1013, 1014 and 1015). Enter Tag code **1011** into the **Tag Start Code** textbox and Tag code **1015** into the **Tag End Code** textbox.*

Convert Slim Tags to ASCII Type

To convert a batch of Slim Tags to the ASCII Tag type, continue as follows:

First Tag

1. Select the **Apply Conversion to all Tags** checkbox.
2. Select the **Manual Read** radio button.
3. Present a Slim Tag to the Enrollment Reader and click the **Read** button.
4. From the Tag Type drop-down list, select the **Ascii, Biometric, Magstripe** option.
5. When the dialog pops up, select the required option from the following:
   - **Accept Full Tag Code**
   - **Convert Code to Slim Tag Without Customer Code (32 bits)**
   - **Convert Code to 32 bit Wiegand Without Site Code (24 bits)**
   - **Convert Code to 26 bit Wiegand Without Site Code (16 bits)**
6. Click the **Add** button.

Remaining Tags

1. Select the **Batch Mode Auto Read** radio button.
2. Click the **Start** button.
3. Present each Tag individually to the Enrollment Reader.

At this stage you may present various Tag types to the Enrollment Reader. The "Convert Slim Tags to ASCII Type" change only affects the Slim Tags.

4. Click the **Stop** button.
5. Click the **Apply** button.

Advanced Search

To search for a Tagholder, proceed as follows:

1. In the Navigator Pane, click the icon.
2. In the Main Pane, click the button. The **Select** dialog displays.

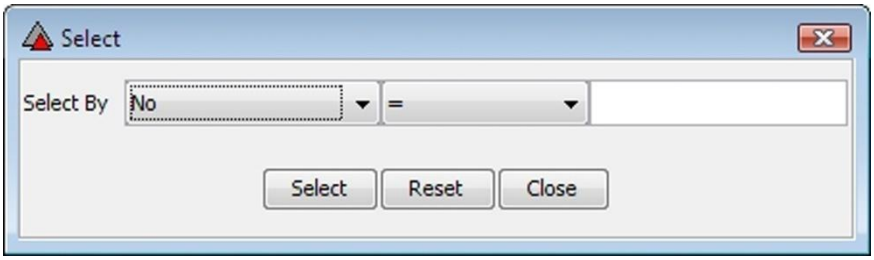


Figure 39 – Select Search Window

3. In the first drop-down list, select a field to search.
4. In the second drop-down list, select an *operator*—see the next section for details.
5. Enter keywords in the textbox on the right.
6. Click the **Select** button to start the search. The results display in the Main Pane.
   - Click **Reset** to display the original Tagholder list in the Main Pane
   - Click **Close** to exit the Search window

Search Operators

- **=** means the **same as**—use **=** to search for exact matches to your keyword
- **!=** means **not equal to**—use **!=** to search for Tagholders that do *not* match your keyword. For example, use **!=** to search for Tagholders that are *not* in a particular Department
- **LIKE** means **same first character**—use **LIKE** to search for Tagholders if you are unsure of a spelling. For example, if you know that a Tagholders Last Name is Johnson, but you are unsure how to spell it, enter the character **J** into the keyword textbox. All Tagholder records that have Last Names beginning with a J are returned

Available Search Fields

The first drop-down list in the **Select Search** window contains the following fields:

Field Name	Description	Search Criteria
No	Tagholder's *unique ID* assigned by ImproNet	Number
Title	Tagholder's title. For example, Mr, Mrs, or Prof.	Text
First Name	Tagholder's first name	Text
Second Name	Tagholder's second or middle name	Text
Last Name	Tagholder's last name	Text
Suffix	Tagholder's name suffix. For example, John Doe *Jr*	Text
ID	Number of Tagholder's ID Document or Passport	Number
Gender	Male or Female	M or F
Pin	PIN-code for use with Keypad Terminals	Number
Type	Tagholder type, 0 (Employee) or 1 (Visitor)	Number
Current Employee	The Tagholder is currently employed, that is 0 (Not Current) or 1 (Current)	Number
Position	Tagholder's status in the company	Text
Department	Tagholder's department	Text
Employee Number	Tagholder's number assigned by their company	Number

Table 4 – Available Search Fields

Device Time Patterns

A Device Time Pattern (DTP) determines *when* a device is physically operational. Create Device Time Patterns on the **Device Time Pattern** screen, and assign them when you set up Terminals. You can also link Device Time Patterns to other functions including the following:

- Time Triggered Actions
- Inputs
- Random Search

A Device Time Pattern has the following settings:

- **DTP Name**—unique name.
- **Start Date**—date when DTP starts operating.
- **End Date**—date when DTP stops operating.
- **Start Time**—time of day when DTP starts operating, configurable on a per day basis.
- **Duration**—the length of time when the DTP is active.
- **Day of the Week**—the days of the week when the DTP is active.

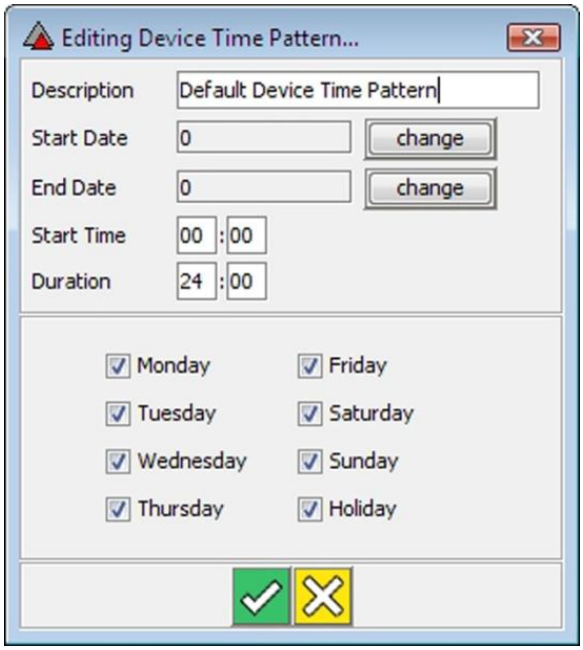


Figure 40 – Editing Device Time Pattern Dialog

Create a Device Time Pattern

To create a new Device Time Pattern, proceed as follows:

1. In the Navigator Pane, click the icon.
2. In the Main Pane, click the button.
3. Configure the new Device Time Pattern as specified in the Configure Device Time Patterns section on page 63.

Open a Device Time Pattern

To open a Device Time Pattern, proceed as follows:

1. In the Navigator Pane, click the icon.
2. In the Main Pane, select a **Time Pattern Name**.
3. Click the button.
4. Configure the new Device Time Pattern as specified in the section below, Configure Device Time Patterns.

Configure Device Time Patterns

To configure the Device Time Patterns, proceed as follows:

1. Create a new Device Time Pattern, or open an existing one.
2. Enter a **Description** that describes the Device Time Pattern.

Configure Dates

If the Device Time Pattern is not required permanently, you can specify a start date and an end date. The default value for Start Date and End Date is **Zero Date**—this means that the Device Time Pattern begins immediately and does not expire.

Specify a Start Date as follows:

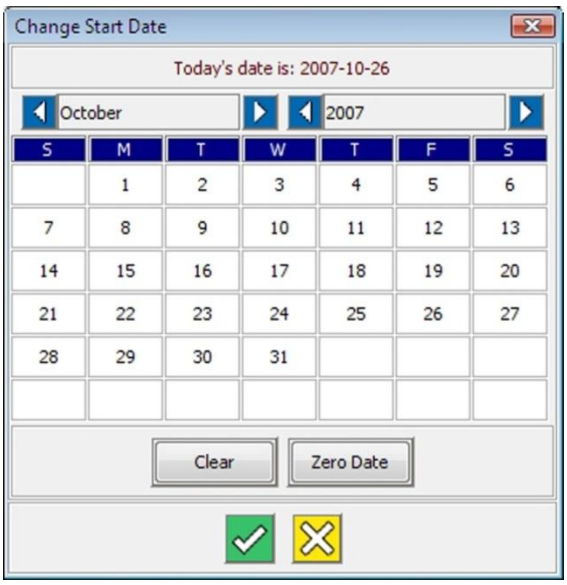


Figure 41 – Change Date Dialog

1. Click the **Change** button for the **Start Date**.
2. Select a **Month** and a **Year** using the and arrow buttons.
3. Select a **Day** by clicking it.
4. Alternatively, click the **Zero Date** button to enable the default value.
5. Click the button to accept.

Now, Specify an End Date as follows:

1. Click the **Change** button for the **End Date**.
2. Select a **Month** and a **Year** using the and arrow buttons.
3. Select a **Day** by clicking it.
4. Alternatively, click the **Zero Date** button to enable the default value.
5. Click the button to accept.

Configure Times

Configure operating times as follows:

1. Enter a **Start Time**—this is the time of day when the Device Time Pattern becomes active.
2. Enter the **Duration** in hours and minutes—this is how long after the start time, the Access Time Pattern is active.

Configure Days

Configure days as follows:

1. Select the **days of the week** when the **Device Time Pattern** is enabled.
2. Click the button to accept the Device Time Pattern.

Multiple Device Time Patterns

You can create up to 128 Device Time Patterns per Site. Additionally, multiple Terminals can share a single Device Time Pattern.

Holidays

Holidays are days or periods when access to a Site is restricted to Administrators. If the **Holiday** checkbox in an Access Time Pattern is selected, then Tagholders assigned to that Access Time Pattern have access to a Site on or during Holidays.

Add, Edit, or Delete a Holiday

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

1. In the Navigator Pane, click the icon.
2. In the Main Pane, do one of the following:
   - Click the button to **Add** a Holiday.
   - Click the button to **Delete** a Holiday.
   - Click the button to **Edit** a Holiday.

Configure Holidays

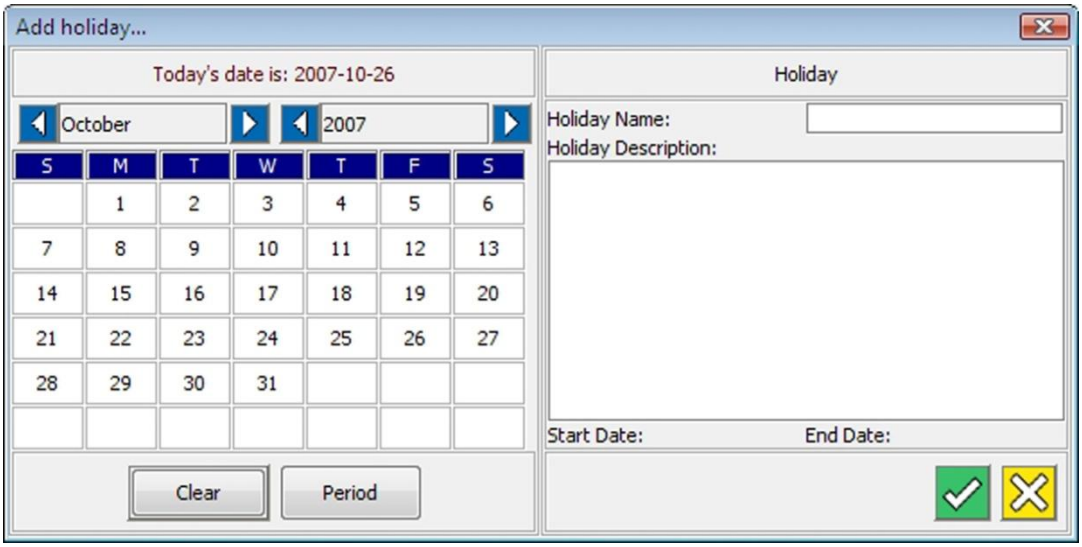


Figure 42 – Add Holiday Dialog

The **Add Holidays** dialog enables you to select the day or days to specify as a Holiday. To do this, proceed as follows:

1. Enter a **Holiday Name**.
2. Enter a **Holiday Description**.
3. Select a **Month** and a **Year** using the and arrow buttons.
4. Select a **Day** by clicking it.
5. Click the **Period** button to select a period of more than one day.
6. Click the button to accept.

Time Triggered Actions

Time Triggered Actions are actions triggered by a Controller at the Start Time of a specified Device Time Pattern. They continue for the duration of the Device Time Pattern. To specify a Time Triggered Action you must assign a **Device Time Pattern** and an **Action**.

Add a Time Triggered Action

Figure 43 – Create Time Triggered Action Dialog

To add a Time Triggered Action, proceed as follows:

Ensure that the information captured below is correct, as you cannot edit this information after capture.

1. In the Navigator Pane, click the icon.
2. In the Main Pane, click the button.
3. In the Create Time Triggered Action dialog, edit the default **Action Name**.
4. Click on the button alongside the **Trigger Time** field.
5. Select and click on a **Device Time Pattern** record from those displayed.
6. Click the button.
7. Click on the button alongside the **Execute Action** field.
8. Select and click on an **Action** record from those displayed.

After linking one or more Actions to a Time Triggered Action, ensure that you do NOT change the Readers Position setting (that is Entry or Exit). Changing this setting after linking results in an Error dialog displaying.

9. Click the button.
10. In the Create Time Triggered Action dialog, click the button.

Delete a Time Triggered Action

To delete a Time Triggered Action, proceed as follows:

1. In the Navigator Pane, click the icon.
2. In the Main Pane, select a Time Triggered Action and click the button.
3. Confirm the deletion.

Actions

When a Terminal is assigned to a Location, default Actions are created and linked to default Events. For example, the **Normal Allowed In** Event is automatically linked to the Action **Relay Allowed In**.

ImproNet Access enables you to create additional Actions and link them to Events.

*Most Actions are created and configured on the Action tab of the Terminals screen. Refer to the Actions section on page **41** for details.*

It is possible for Events on one Terminal to activate Actions on other Terminals.

Edit and Delete Actions

Actions are created when Terminals are assigned to Locations. Therefore, the Actions screen only enables you to edit or delete Actions.

To open the **Actions** screen, click the icon in the Navigator Pane.

Edit an Action

To edit an Action, proceed as follows:

1. In the Main Pane, select an **Action** row.
2. Click the button.

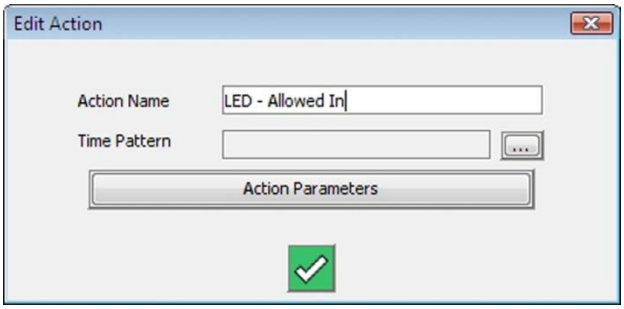


Figure 44 – Edit Action Window

3. Edit the **Action Name** if necessary.
4. Click the **Action Parameters** button. An **Action Parameters** window corresponding to the Action type displays.
5. Edit the parameters as required.
6. Click the button to accept.
7. In the **Edit Action** dialog, click the button to apply the changes.

Delete Action

There is no undo for this procedure.
Deleting an Action can result in a Terminal or Location functioning incorrectly.

To delete an Action, proceed as follows:

1. In the Main Pane, select an **Action** row.
2. Click the button. A delete confirmation dialog box displays.
3. Click **Yes**.

Inputs

When a Terminal is assigned to a Location, default Inputs Functions are created. For example, if a Terminal has a Request to Exit (RTE) facility, a **General Input** for the Terminal is created.

The Inputs screen enables you to configure existing Inputs created during Terminal assignment.

*We recommend using the **Inputs** tab on the **Terminal** screen to configure Inputs. Refer to the Inputs section on page **33** for details.*

Outputs

When a Terminal is assigned to a Location, default Output Functions are created. For example, an Output function that controls the Terminal's LED status is created.

The Outputs screen enables you to configure existing Outputs created during Terminal assignment.

*We recommend using the **Outputs** tab on the **Terminal** screen to configure Outputs. Refer to the Outputs section on page **40** for details.*

Common Zones

Terminals on different Controllers can be assigned to Common Zones. However, you must first create a Common Zone in the **Common Zones** screen before it is available in the Terminal screen.

Refer to Part V, Advanced Configuration, for details on Common Zones.

Moving Employees (Tagholders)

This dialog lets you move employees (Tagholders) from one Site to another, if for example you added an employee (Tagholder) to the wrong Site.

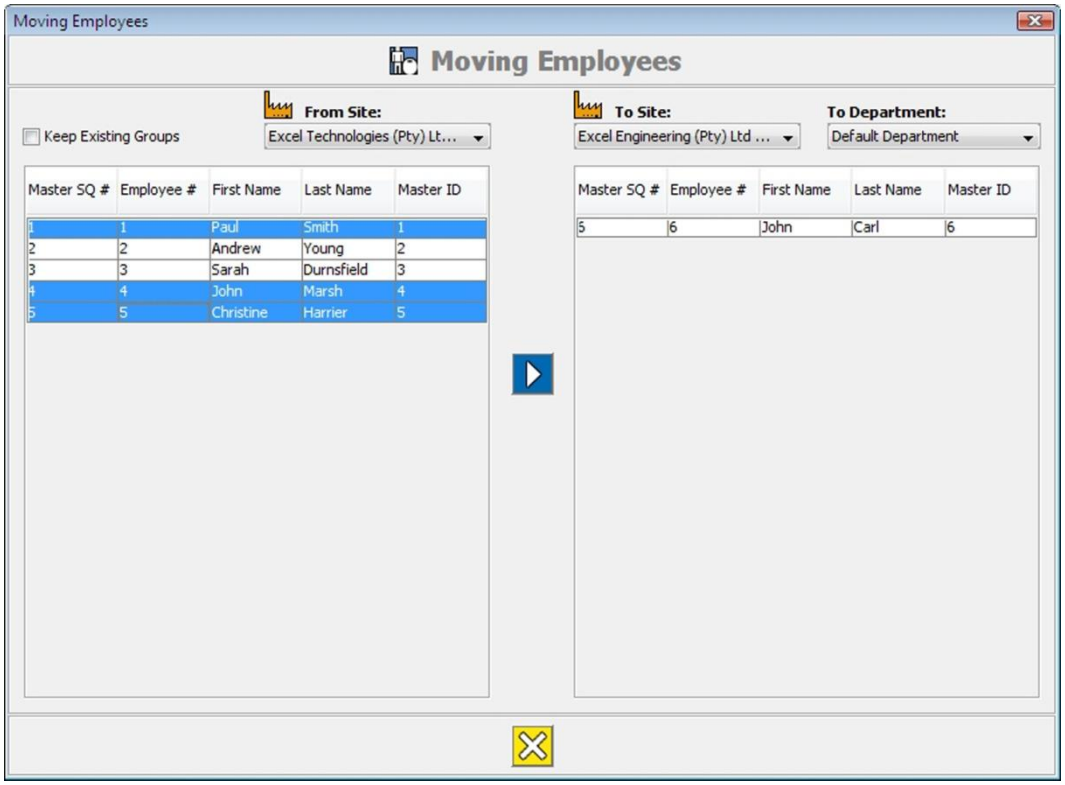


Figure 45 – Moving Employees Dialog

1. In Access, from the Menu Bar, select **Configuration**>**Moving Employees**.
2. In the **Moving Employees** dialog:
   a. Select the Site the *employees are currently on*, from the **From Site** drop-down list.
   b. Select the Site you *want to move the employees to*, from the **To Site** drop-down list.
3. Select the department you want the employees to join, from the **To Department** drop-down list.
4. From the **From Site** table, select the Employees you would like to move.

*Use **Ctrl** select or **Shift** select when selecting multiple employee names.*

5. Click on the button.
6. Confirm the move.

*If you selected the **Keep Existing Groups** checkbox (in the upper left-hand side of the Moving Employees dialog), the Moving Tags – Site: dialog will NOT appear. Instead all existing Tagholder Access Groups for the Tags remain.*

If the employee already had Tags assigned, the **Moving Tags – Site:** dialog appears.

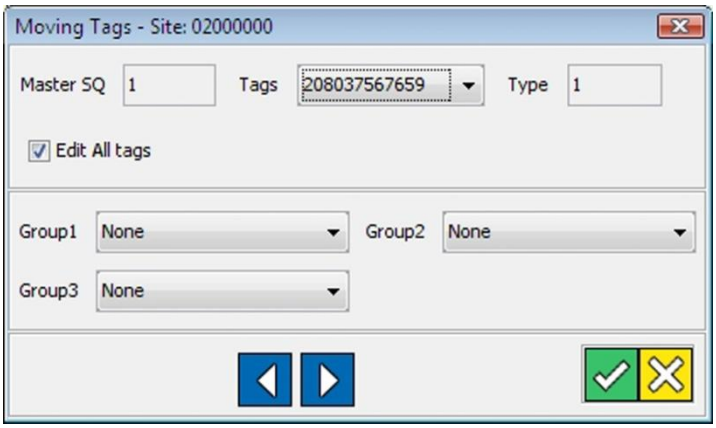


Figure 46 – Moving Tags – Site: Dialog

Once you apply your changes to a Tag, the Tag no longer appears on the Tags drop-down list (see Figure 46). With this in mind, make sure of your changes before clicking the button.

7. From the **Tags** drop-down list, select the Tag Code.
8. If the employee has multiple Tags, select the **Edit All Tags** checkbox.

*The **Edit All Tags** checkbox allows you to select groups for each Tag individually instead of assigning default groups across all the Tags for that employee.*

9. Assign the Groups from the **Group1** to **Group3** drop-down lists.

Ensure that you click the button for each Tag when selecting groups. If you scroll to the next employee, without applying your changes, the settings are lost.

The previous and next buttons allow you to scroll between the various employees you selected for moving.

*The **Moving Tags – Site:** dialog closes once you've edited all the Tags (and employees) selected and clicked the button for your last Tag.*

10. When you return to the **Moving Employees** dialog, click on the button.

Replacing Controllers and Terminals

Keep ImproNet Engine running when you replace a unit.

When removing Controllers or Terminals from their bus, perform the following procedure:

1. Physically disconnect and remove the old hardware.
2. Physically connect and mount the new hardware.
3. Configure the new hardware configuration in ImproNet Access.

Replace Controller

1. Remove the **old Controller** from the Controller bus.
2. Connect the **new Controller** to the Controller bus.
3. In Windows®, click **Start**>**Programs**>**ImproNet**>**Access**.

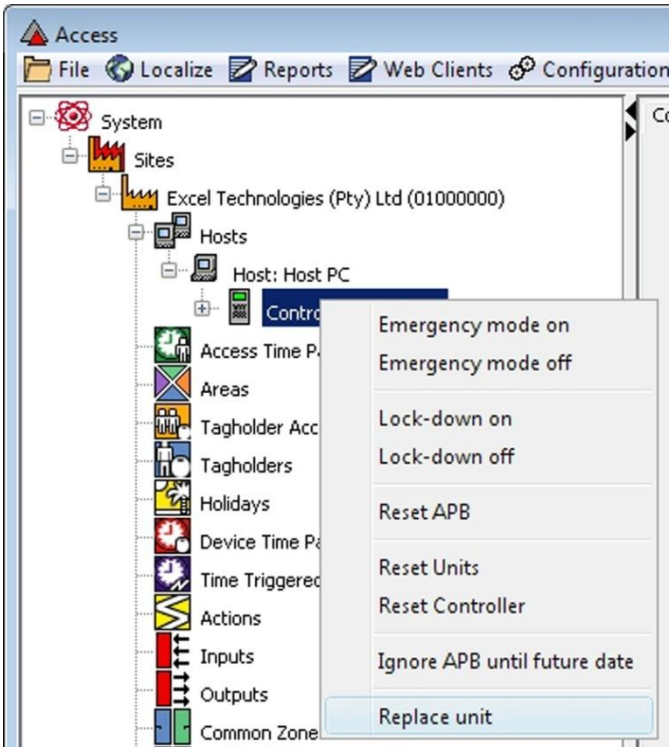


Figure 47 – Replacing the Controller

4. In the **Navigator Pane**, click the **old Controller** to select it.
5. Right-click the Controller and select the **Replace Unit** option.
6. From the **Unit Type** drop-down list, select the new Controllers unit type.
7. Enter the **new Controllers Fixed Address**.
8. Click the button.

Replace Terminal

Ensure that the replacement Terminal is of the same type as the original Terminal.

1. Remove the **old Termina**l from the Terminal bus.
2. Connect the **new Terminal** to the Terminal bus.
3. In Windows®, click **Start**>**Programs**>**ImproNet**>**Access**.
4. In the **Navigator Pane**, click the **old Terminal** to select it.
5. Right-click the Terminal and select the **Replace Unit** option.
6. Enter the **new Terminals Fixed Address**.
7. Click on the button.

Database Maintenance

Firebird General

General

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

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

Firebird 1.5 is a full-featured SQL database engine. Firebird is powerful, yet lightweight, with the smallest possible configuration and administration needs. It's easily scalable from single-user, single-database use up to company-wide enterprise purposes. A single Firebird server can handle multiple independent databases, each with multiple client connections. And best of all: it’s true Open Source, thus free of any license fees even for commercial use.

We publish all our Software with the Firebird Database as our standard offering. The ImproNet Software suite also offers support for Windows SQL Server 2000 and 2005. The purpose of this document is to aid you in running Systems on the Firebird Database. Administrators running Systems on the Windows SQL Server must have the right training for the administration of those Databases.

This section will address the following topics:

- Firebird Utilities
- Database Backups
- Database Restore
- Database corruption
- General Impro Database maintenance

Suggested Maintenance Schedule

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

1. Perform regular backups using the tools and techniques described under the section Database Backups.
2. Perform regular test restores on the backup files, using the tools and techniques described under the section Database Restore.
3. At regular intervals, take the working database off-line and carry out a Backup and restore. This ensures that the working database does not contain any corrupt data or tables. Refer to the section Recovering a Corrupt Database for more information.

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

Figure 48 below shows an example of a monthly maintenance schedule: This organisation needs daily backups as data is critical.

September

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

Figure 48 – Example of a Monthly Maintenance Schedule

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

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

Firebird Utilities

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

An Introduction to IBConsole

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

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

The first step in connecting to an Impro Database is registering the Database Server. The following examples refer to the default Database **impronet.fdb** used by the ImproNet Software suite. The default locations for the Databases and the IBConsole Utility varies dependant on the Access Control System used.

Start the IBConsole Software
In Windows®, go to **Start**>**Programs**>**ImproNet**>**Utils**>**IBConsole**.

Register the Server

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

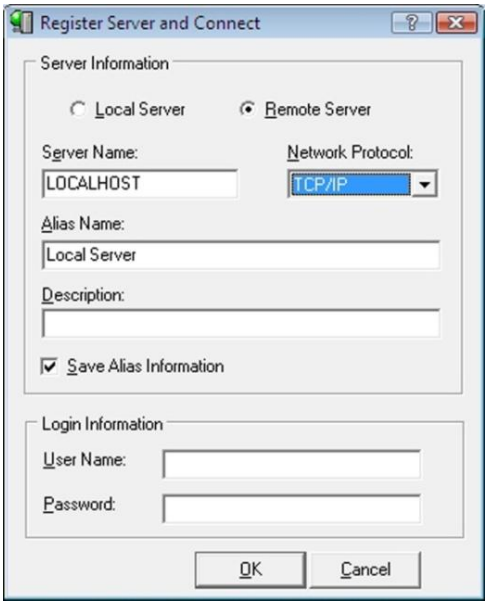


Figure 49 – Register Server and Connect Dialog

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

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

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

Login to the InterBase Server

1. From the Hierarchical Tree, select your InterBase Server (based on the example in Figure 49 select Local Server).
2. From the Server drop-down menu, select the **Login** choice.
3. In the Server Login dialog, enter the **Username** and **Password**.

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

4. Click the **Login** button.

Register the Database

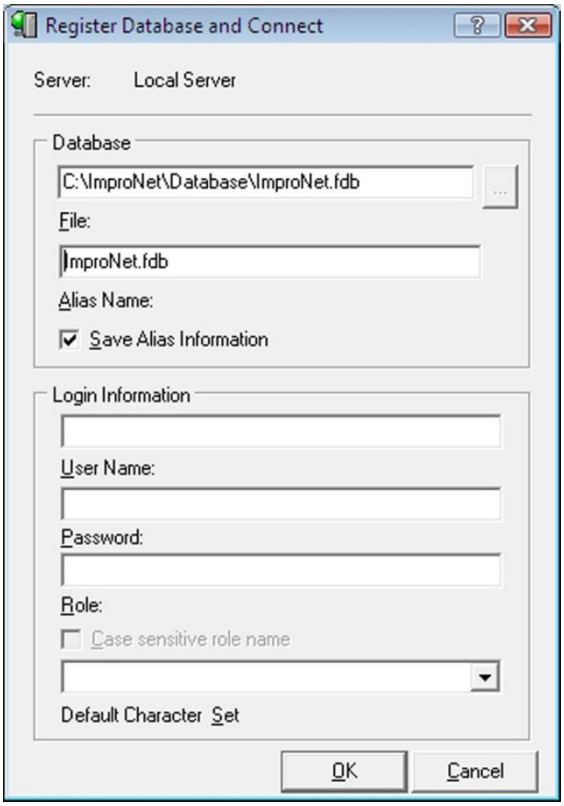


Figure 50 – Register Database and Connect Dialog

1. From the Database drop-down menu, select the **Register** choice.
2. In the Register Database and Connect dialog, In the **Database** textbox, enter the full file path to your Database (see Figure 50).
3. Click your mouse pointer in the **File** textbox, the Database's file name automatically appears.
4. Leave the remaining fields unchanged.
5. Click the **OK** button.

The default Database path for the ImproNet Software suite is: ***C:\ImproNet\databse\impronet.fdb****.*

6. In the Hierarchical Tree, double-click on the **Impronet.fdb** file, starting the Database.

Database Backups

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

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

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

The preferred method of making a backup is to use the built in (automatic) backup features in the ImproNet Software.

Scheduling the backup of an ImproNet Database

1. In Windows®, go to **Start**>**Programs**>**ImproNet**>**Engine**.
2. From the Configuration drop-down menu, select **Backup**.

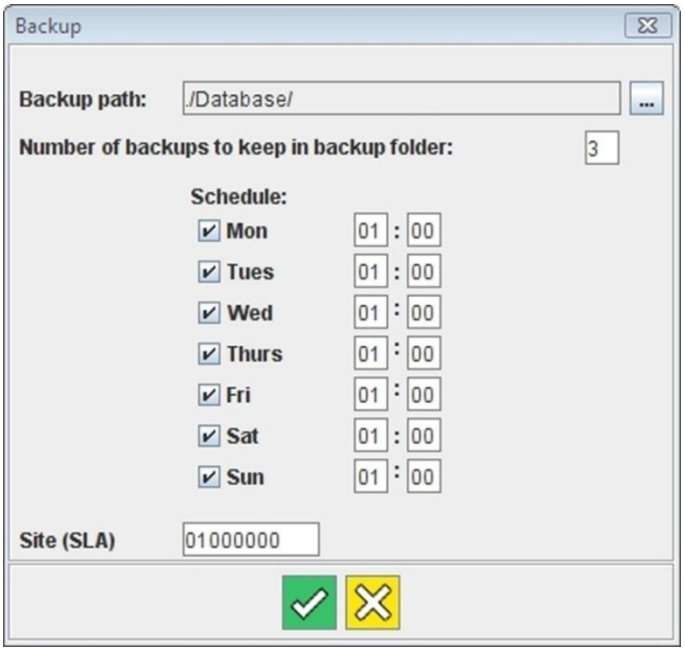


Figure 51 – Backup Dialog

3. In the Backup dialog, alongside the Backup Path textbox, click on the button.

The backup path automatically defaults to the local workstation. For storage purposes, ensure that you change this backup path to a remote server.

4. In the **Number of Backups to keep in Backup Folder** textbox, enter a suitable number.
5. From the Schedule group specify the **days** and **times** you wish to perform the backups.
6. Click on the button.

Ensure that you schedule the backups when Engine is open and running.

7. Shutdown and restart the Engine module for the changes to take effect.

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

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

For unscheduled backups use either of the following choices:

- Backup the ImproNet Database using IBConsole.
- Backup the ImproNet Database using a Batch File.

Backup the ImproNet Database using IBConsole

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

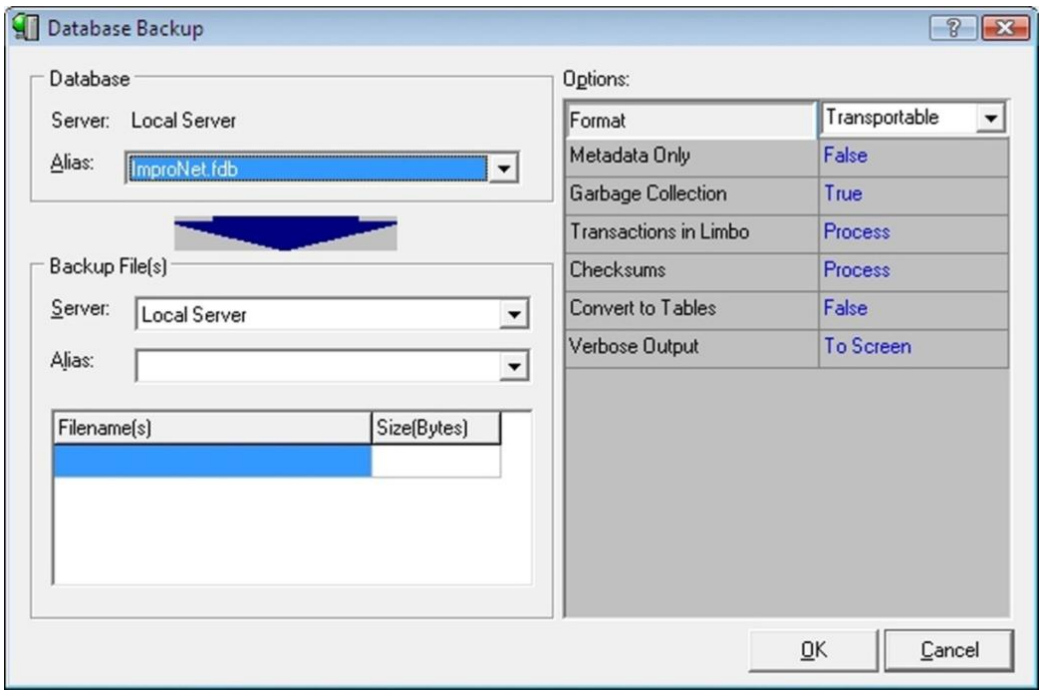


Figure 52 – Database Backup Dialog

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

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

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

Backup the ImproNet Database Using a Batch File

Create the ".bat" File

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

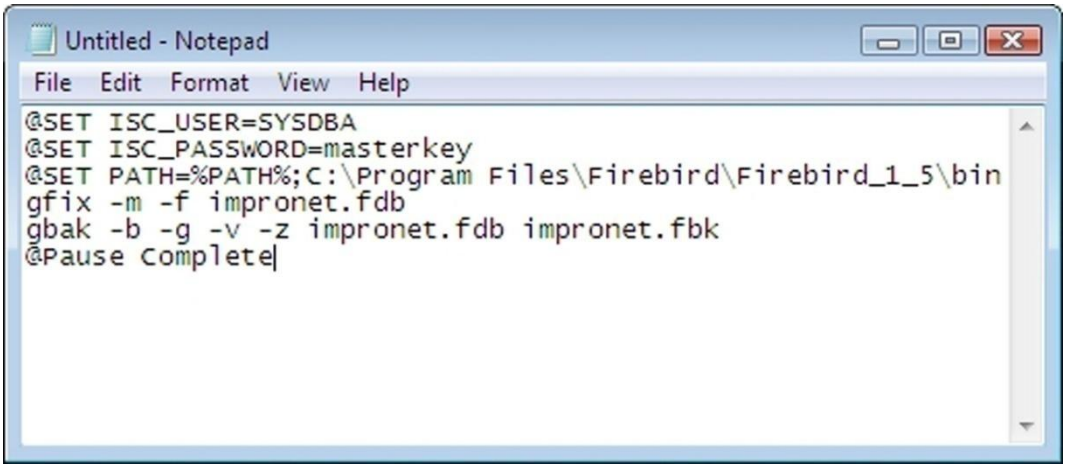


Figure 53 – Backup Using a Batch File

Settings explained:

- ***@SET ISC_USER=SYSDBA**—this sets the user name as SYSDBA, thus ensuring the backup utility connects to the Database.*
- ***@SET ISC_PASSWORD=MASTERKEY**—this sets password. If you changed the default password, ensure that you use the new password.*
- ***@SET PATH=%PATH%;C:\Program Files\Firebird\Firebird_1_5\bin**—indicates the path to the GBAK backup utility. If the GBAK backup utility does not appear in this directory, set the path accordingly.*
- ***gfix -m -f impronet.fdb**—repairs minor database corruption.*
- ***gbak -b -g -v -z impronet.fdb impronet.fbk**—creates the backup file impronet.fbk. To change the name of the target database, simply change the impronet.fbk file to another name, keeping the fbk file extension.*

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

Run the ".bat" Batch File

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

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

Database Restore

Perform a Database restoration for the following reasons:

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

Restoring the ImproNet Database Using IBConsole

Disconnect from the Database

1. In Windows®, go to **Start>Programs>ImproNet>Utils>IBConsole**.
2. From the Hierarchical Tree, click on the **Impronet.fdb** file.
3. From the Database drop-down menu, select **Maintenance>Shutdown**.

Restore the Backup

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

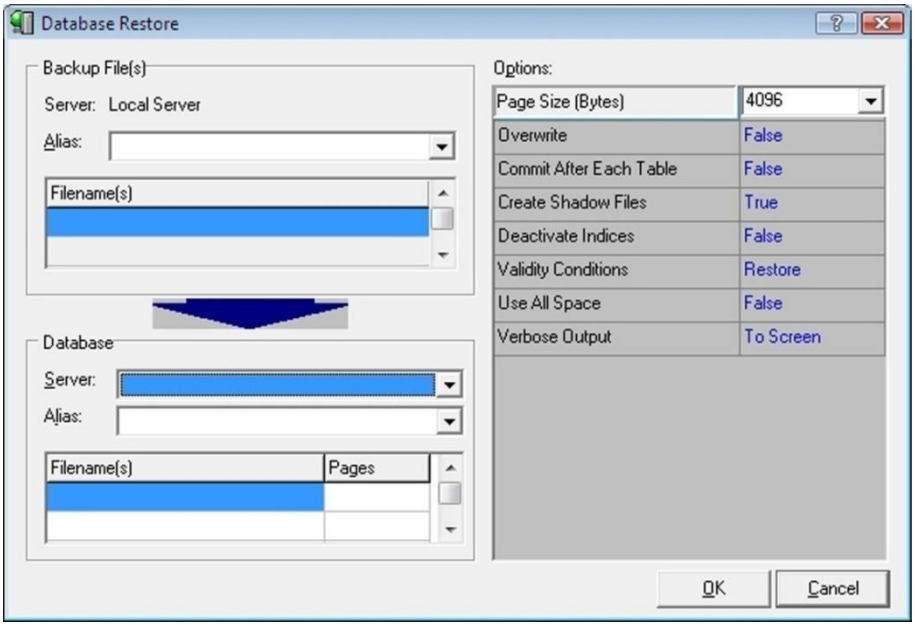


Figure 54 – Database Restore Dialog

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

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

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

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

Reconnect to the Database

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

Restoring the ImproNet Database Using a Batch File

Create the ".bat" File

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

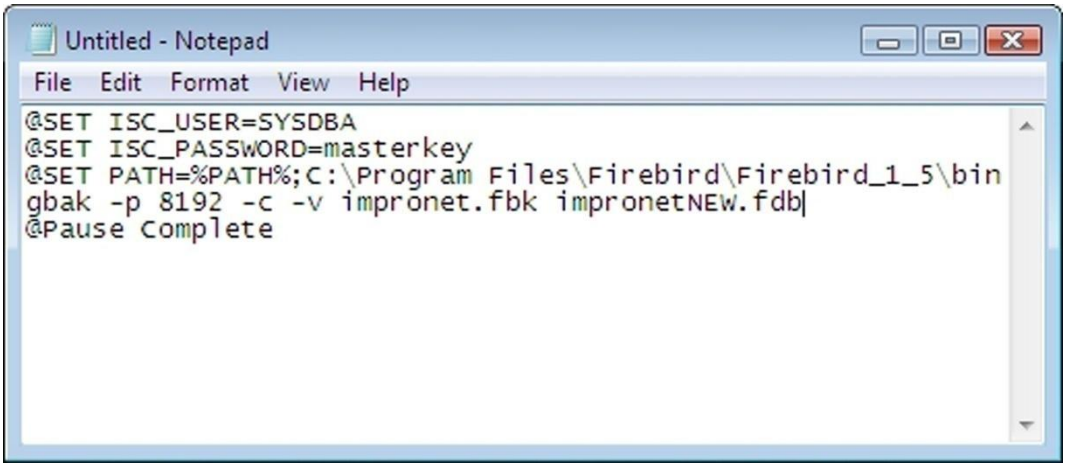


Figure 55 – Restore Using a Batch File

Settings explained:

- ***@SET ISC_USER=SYSDBA**—this sets the user name as SYSDBA, thus ensuring the backup utility connects to the Database.*
- ***@SET ISC_PASSWORD=MASTERKEY**—this sets the password, if you changed the default password, ensure that you use the new password.*
- ***@SET PATH=%PATH%;C:\Program Files\Firebird\Firebird_1_5\bin**—indicates the path to the GBAK backup utility. If the GBAK backup utility does not appear in this directory, set the path accordingly.*
- ***gbak -p 8192 –c -v impronet.fbk impronetNEW.fdb**—restores the impronet.fbk file to the name of impronetNEW.fdb.*

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

Run the "restore.bat" File

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

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

Database Corruption

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

A Corrupt Database does not always mean a loss of data. Usually, you can recover the Database using a combination of the tools described earlier, as well as the Pump Utility shipped with ImproNet.

There are various indicators of a corrupt Database:

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

Causes of Database Corruption:

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

1. **Abnormal or incorrect shutdown of the server**, especially during power failures. Ensure that the server has a working uninterrupted power supply.
2. **Server defects and hardware faults**, especially with hard disk drives, disk controllers, main memory of the PC and cache memory of raid controllers.
3. **Copying the Database while the servers running**.
4. **Hard disk drive or Operating System corruption**.
5. **Poor Database design**.
6. **Sharing the Database folder** (allowing access over the network) is a security risk, and increases the chance of database corruption. Firebird cannot tolerate other applications locking sectors of the Database file.
   - DO NOT use Windows Explorer (or command line 'Copy' or 'Xcopy') when copying the Database file on a live Database. In practice, these utilities may lock the sector they're copying. So merely copying the **impronet.fdb** file with Windows Explorer is enough to corrupt the Database.
   - DO NOT use any arbitrary backup tool or archiving tool to make a backup copy of the Database. The only safe way to make a backup copy of the Database is to use the backup facility we provided with ImproNet, or use Firebird's GBAK tool. This creates a '.gbk' or '.fbk' backup file, suitable for safe copying after finishing the backup process. Alternatively, the Firebird Server on the server must be stopped to copy the '.fdb' file, and it must be restarted afterwards.
   - Check for other processes trying to read the Database file. These are typically Virus and Spy-ware scanners, common on corporate PC's.
7. **The bigger the size of the Database file**, the more likely is it to become corrupt because of one of the reasons mentioned above.

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

Checking and Repairing Minor Database Corruption

Follow these steps when checking and repairing minor corruption:

Carry out these steps regularly, for example every 2 or 3 months.

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

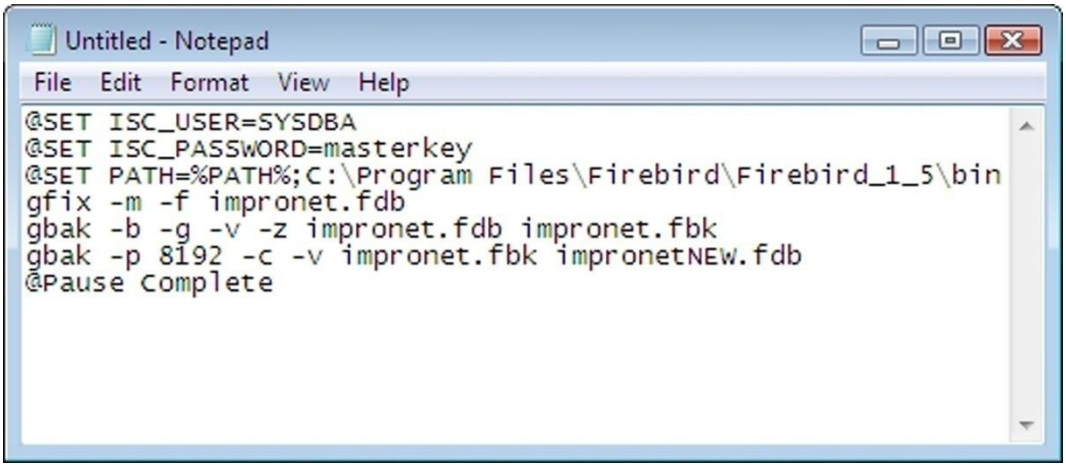


Figure 56 – "repair.bat" Batch File

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

Run the "repair.bat" File

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

This process mends and backs-up the Database to the same directory as where the batch file ran from. Once complete, the restore process runs resulting in an impronetNEW.fdb Database file. If successful, you may use the restored Database as a direct replacement for the existing Database. If the restore fails for any reason, perform the steps described in the Recovering a Corrupt Database section below.

Recovering a Corrupt Database

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

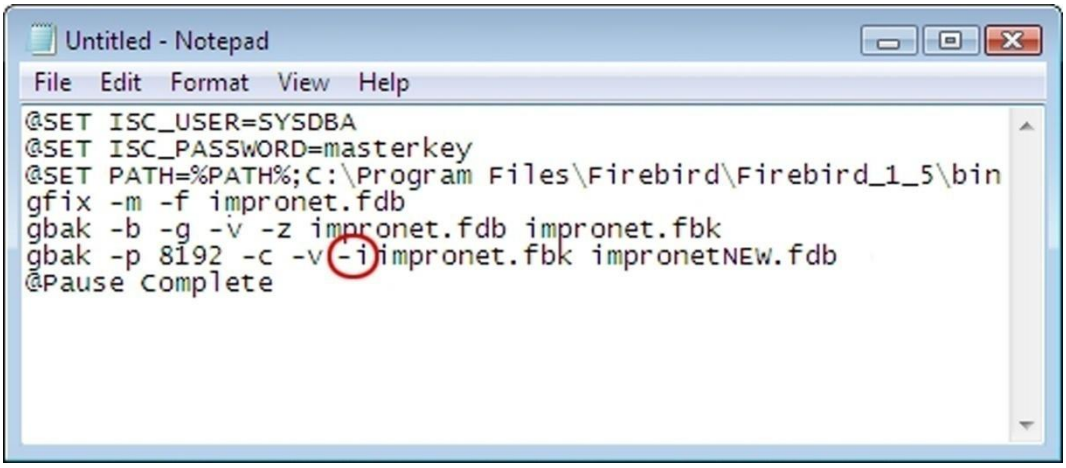


Figure 57 –Batch File

*The **-i** option highlighted in **gbak -p 8192 –c –v -i impronet.fbk impronetNEW.fdb**—restores the Database without indexes.*

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

Run the Batch File

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

This process mends and backs-up the Database to the same directory as where the batch file ran from. Once complete, the restore process runs resulting in an impronetNEW.fdb Database file. If successful, you may use the restored Database as a direct replacement for the existing Database. If the restore fails for any reason, contact your nearest Impro support representative.

Run the Database Pump Utility

The Pump Utility lets you flush out and correct a "muddled" or overloaded Database. When executed, the Pump takes all the Tagholders, Visitors and Transaction data and pumps this into a fresh Database.

Before using the Pump Utility, ensure that you close all other applications. For large Databases carry out the Pump action over a quiet period, as completion could take many hours.

1. In Windows®, go to **Start**>**Programs**>**ImproNet**>**Utils**>**Pump**.
2. Enter your **Username** and **Password**.

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

3. Click on the **OK** button.
4. In the **Pump Database** dialog, click the **Start** button.

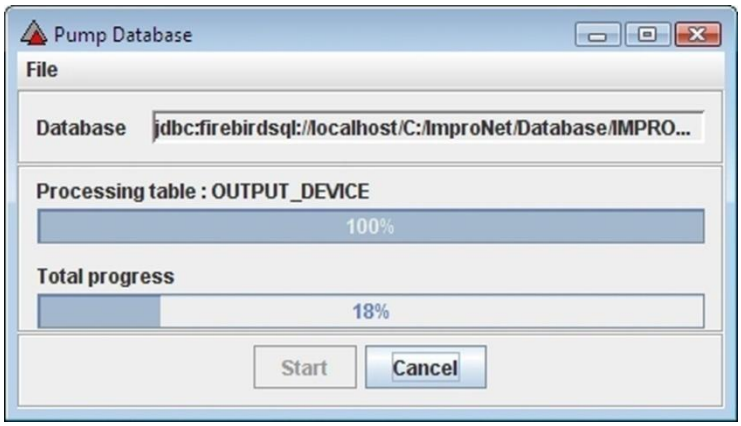


Figure 58 – Logon to Database Dialog

5. In the **Message** dialog, click the **OK** button.

An Introduction to IBFirstAID

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

Accessing the IB Surgeon Web Site

1. Open your chosen **Internet browser**.
2. In the **Address** bar, type in the URL: **http://www.ib-aid.com/**.
3. On the **Home** page, select the **Products** tab.
4. From the **Recovery or Optimization Products** group, click on the **IBFirstAID** link.

From here you may read up on the Software, or buy a copy for use.

Archiving Transactions

The maximum recommended Database size for ImproNet is **2 GB**.

To keep your Database, below this limit, we recommend that you archive transactions using the ImproNet's Archive Utility.

This Archive action has two major benefits:

- Manages the size of the Database, freeing up space on the PC
- Keeps a cleaner, uncluttered Database

For full details on using the Archive Utility go to ***Part VII – Utilities***.

Archiving Tagholders

The **Archive Tagholders** choice lets you archive Employee and Visitor Tagholder and transaction information.

To do this, continue as follows:

Archive Employee Tagholders

1. In Access, from the Menu Bar, select **Configuration**.
2. Click on the **Maintenance** menu choice.
3. Select the **Archive Tagholders** radio button.
4. Click the button to accept.

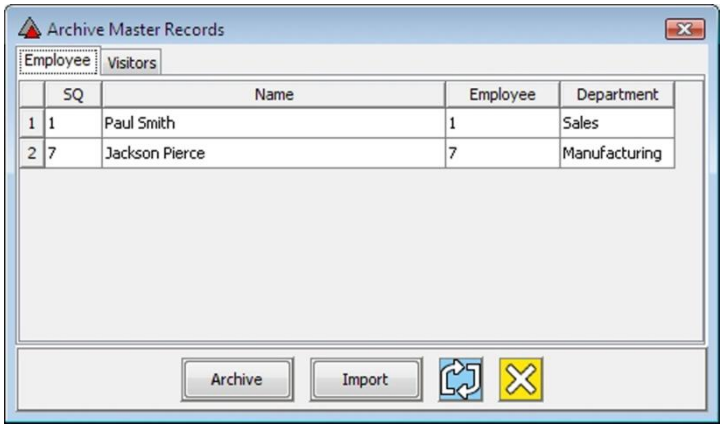


Figure 59 – Archive Master Records Dialog

5. In the **Archive Master Records** dialog, select the **Employee** tab.
6. Select either a **single Tagholder** or **multiple Tagholders** from the list of displayed records.
7. Click the **Archive** button.

*The same steps apply when you archive **Visitor Tagholders**, however, instead of selecting the Employee tab, select the **Visitor** tab.*

Import Employee Tagholders

1. From the Menu Bar, select **Configuration**.
2. Click on the **Maintenance** menu choice.
3. Select the **Archive Tagholders** radio button.
4. Click the button to accept.
5. In the **Archive Master Records** dialog, select the **Employee** tab.
6. Click the **Import** button.
7. In the **Please Select a Tagholder Archive** dialog, double-click on the **Archive** folder.
8. Double-click the **Tagholders** folder.
9. Select the Tagholder for importing.
10. Click the **Open** button.

Figure 60 – Import Transactions Dialog

11. In the **Import Transactions** dialog, confirm whether to import the Tagholders transactions, click either the **Yes** or **No** button.

*The same steps apply when you import **Visitor Tagholders**, however, instead of selecting the Employee tab, select the **Visitor** tab.*

Events and Actions

Many of the Events referred to in the text have multiple value possibilities. Not every Event is repeated below, as it would entail printing a repeated increasing value for such events. Therefore, the first of the series has the value limits stated such as “Door open too long 1 to 16”. This means there are in fact, 16 different events available.

Event Statement	Event Description
EV_Allowed_Exceptional_In	Tagholder allowed IN.
EV_Allowed_Exceptional_Out	Tagholder allowed OUT.
EV_Allowed_Normal_In	Tagholder allowed IN.
EV_Allowed_Normal_Out	Tagholder allowed OUT.
EV_Allowed_Normal_On	Manually added clocking added by T&A systems.
EV_Allowed_Normal_Off	Manually added clocking added by T&A systems.
EV_Allowed_Keyboard_Clock_On	Manually added clocking added by T&A systems.
EV_Allowed_Keyboard_Clock_Off	Manually added clocking added by T&A systems.
EV_Allowed_Keyboard_Allowed_In	Manually added clocking added by T&A systems.
EV_Allowed_Keyboard_Allowed_Out	Manually added clocking added by T&A systems.
EV_Allowed_APB_Override_In	Allowed APB Override IN, if Ignore APB until Future Date is set on the Controller.
EV_Allowed_APB_Override_Out	Allowed APB Override OUT, if Ignore APB until Future Date is set on the Controller.
EV_Allowed_APB_Violation_Out	Allowed APB Violation OUT, if the zones been set to relaxed APB.
EV_Allowed_Time_or_Day_Violation_Out	Allowed Time or Day Violation OUT, while the Tagholders in a zone and the ATP ends.
EV_Allowed_Visitor_In	Visitor allowed IN.
EV_Allowed_Visitor_Out	Visitor allowed OUT.
EV_Allowed_Duress_In	Tagholders allowed entry by pressing a duress code after presenting a Tag.
EV_Allowed_Duress_Out	Tagholders allowed exit by pressing a duress code after presenting a Tag.
EV_Authentication_Failure	Tag not authenticated by the Controller.
EV_Counter1_Threshold_In	Counter reached threshold IN level.
EV_Counter1_Threshold_Out	Counter reached threshold OUT level.
EV_Counter2_Threshold_In	Counter reached threshold IN level.
EV_Counter2_Threshold_Out	Counter reached threshold OUT level.
EV_Counter3_Threshold_In	Counter reached threshold IN level.
EV_Counter3_Threshold_Out	Counter reached threshold OUT level.
EV_Counter1_Has_Zeroed_In	Counter reached zero IN level.

Event Statement	Event Description
EV_Counter1_Has_Zeroed_Out	Counter reached zero OUT level.
EV_Counter2_Has_Zeroed_In	Counter reached zero IN level.
EV_Counter2_Has_Zeroed_Out	Counter reached zero OUT level.
EV_Counter3_Has_Zeroed_In	Counter reached zero IN level.
EV_Counter3_Has_Zeroed_Out	Counter reached zero OUT level.
EV_Counter1_Is_Zeroed_In	Counter is zero IN level.
EV_Counter1_Is_Zeroed_Out	Counter is zero OUT level.
EV_Counter2_Is_Zeroed_In	Counter is zero IN level.
EV_Counter2_Is_Zeroed_Out	Counter is zero OUT level.
EV_Counter3_Is_Zeroed_In	Counter is zero IN level.
EV_Counter3_Is_Zeroed_Out	Counter is zero OUT level.
EV_Denied_APB_In	Denied Access IN, APB active, no access with Tag.
EV_Denied_APB_Out	Denied Access OUT, APB Active, Tag already used.
EV_Denied_Interleading_Zone_Routing_In	Denied Access IN, Tag requires Zone route sequence to be followed.
EV_Denied_Location_In	Denied Location IN, Tagholder does not have access to that specific location.
EV_Denied_Location_Out	Denied Location OUT, Tagholder cannot exit from that specific location.
EV_Denied_No_Supervisor_In	Denied No Supervisor IN, Supervisor Unlock, Tagholder denied because there is no supervisor in the zone.
EV_Denied_Last_Supervisor_Out	Denied Last Supervisor OUT, No supervisor to validate exit.
EV_Denied_Tag_Blacklisted_In	Denied IN, Tag blacklisted.
EV_Denied_Tag_Blacklisted_Out	Denied OUT, Tag blacklisted.
EV_Denied_Tag_Suspended_In	Denied IN, Tag suspended.
EV_Denied_Tag_Suspended_Out	Denied OUT, Tag suspended.
EV_Denied_Tag_Expired_In	Denied IN, Tag expired
EV_Denied_Tag_Expired_Out	Denied OUT, Tag expired
EV_Denied_Time_or_Day_In	Denied IN, Tagholder out of range of their Access Time Pattern for their Access Group.
EV_Denied_Time_or_Day_Out	Denied OUT, Tagholder out of range of their Access Time Pattern for their Access Group.
EV_Denied_Zone_Count_Exceeded_In	Tagholder denied access if the zone is at its maximum capacity of Tagholders. Initiate Zone count first.
EV_Denied_Site_In	Tagholder does not have access to this site.
EV_Denied_Site_Out	Tagholder does not have permission to exit this site.
EV_Denied_External_In	Reserved for R/W, not currently used.
EV_Denied_External_Out	Reserved for R/W, not currently used.
EV_Denied_No_Host_for_Visitor_In	Denied entry because Host has not entered first.
EV_Denied_No_Host_for_Visitor_Out	Denied exit because Host has not entered first.

Event Statement	Event Description
EV_Denied_Multiple_Tags_Req_In	More than one Tag is required for access.
EV_Denied_Multiple_Tags_Req_Out	More than one Tag is required for access.
EV_Denied_Unknown_Tag_In	Denied IN, unrecognised Tag, this Tag does not exist in the Database.
EV_Denied_Unknown_Tag_Out	Denied OUT, unrecognised Tag, this Tag does not exist in the Database.
EV_Denied_Location_Locked_In	Denied IN, Entry unit locked.
EV_Denied_Location_Locked_Out	Denied Out, Exit unit locked.
EV_Denied_Location_No_Tag_Time_In	Reserved for R/W, not currently used.
EV_Denied_Location_No_Tag_Time_Out	Reserved for R/W, not currently used.
EV_Denied_Inhibited_by_Input_In	The event is raised when an input is configured to block a scanner, and a Tag is presented at the Reader. The input may for example be connected to a vehicle detector embedded into the road.
EV_Denied_Inhibited_by_Input_Out	The event is raised when an input is configured to block a scanner, and a Tag is presented at the Reader. The input may for example be connected to a vehicle detector embedded into the road.
EV_Denied_Unknown_In	Random Tagholder denied access.
EV_Denied_Unknown_Out	Random Tagholder denied access.
EV_Denied_Pin_In	Tagholder denied entry, incorrect PIN-code entered on the keypad.
EV_Denied_Pin_Out	Tagholder denied entry, incorrect PIN-code entered on the keypad.
EV_Denied_Wrong_Routing_In	Tagholder has not followed routing sequence.
EV_Denied_Wrong_Routing_Out	Tagholder has not followed routing sequence.
EV_Biometric_Allowed_In	For use in third-party validation.
EV_Biometric_Allowed_Out	For use in third-party validation.
EV_Biometric_Denied_In	For use in third-party validation.
EV_Biometric_Denied_Out	For use in third-party validation.
EV_Single_Key_Pressed	Single Key Pressed, reserved – not currently used.
EV_Dual_Key_Pressed	Dual Key Pressed, reserved – not currently used.
EV_Special_Key_Code_1	Raised when a Terminal specific PIN-codes been typed in. Each Terminal can have two PIN-codes.
EV_Special_Key_Code_2	Raised when a Terminal specific PIN-codes been typed in. Each Terminal can have two PIN-codes.
EV_Anti_Tamper	A units being tampered with.
EV_Terminal_Timeout	A Terminals off-line.
EV_Host_Timeout	Hosts off-line.
EV_Unit_Power_up	Units received power.
EV_RTE_1-16	Request To Enter 1-16, Button pressed requesting access.
EV_DOS_Door_Forced_1-16	Door Open Sensor, Door Forced 1-16.
EV_DOS_Door_Open_Too_Long_1-16	Door Open Too Long 1-16.
EV_DOS_Door_Open_Normal_1-16	Door Open Normally 1-16.

Event Statement	Event Description
EV_DOS_Door_Not_Opened_1-16	Door Not Opened 1-16.
EV_Input_Alarm_1-16	Input Alarm 1-16.
EV_Raised_Event_1-16	Raised Event 1-16.
EV_Zone_Count_Is_Zero_1-64	Zone 1-64: Count is Zero.
EV_Zone_Count_Is_NonZero_1-64	Zone 1-64: Count is Non Zero.
EV_Zone_Count_Is_Max_1-64	Zone 1-64: Count is maximum – Count at its limit.
EV_Zone_Count_Is_MaxMinusOne_1-64	Zone 1-64: Count is maximum minus one.
EV_Reason_Code_0-99	Reason Code 0-99.
EV_DOS_Door_Closed_1-16	Door Closed 1-16.

EV_Host_Allowed_Normal_In	Host Allowed Normal IN.	Normally used with Third-party Integrations
EV_Host_Allowed_Normal_Out	Host Allowed Normal OUT.	
EV_Host_Allowed_APB_Override_In	Host Allowed APB Override IN.	
EV_Host_Allowed_APB_Override_Out	Host Allowed APB Override OUT.	
EV_Host_Allowed_APB_Violation_Out	Host Allowed APB Violation OUT.	
EV_Host_Allowed_Time_Day_Violation_Out	Host Allowed Time Day Violation OUT.	
EV_Host_Allowed_Exceptional_In	Host Allowed Exceptional IN.	
EV_Host_Allowed_Exceptional_Out	Host Allowed Exceptional OUT.	
EV_Host_Allowed_Vistor_In	Host Allowed Vistor IN.	
EV_Host_Allowed_Visitor_Out	Host Allowed Visitor OUT.	
EV_Host_Allowed_Duress_In	Host Allowed Duress IN.	
EV_Host_Allowed_Duress_Out	Host Allowed Duress OUT.	
EV_HFB_Allowed_Normal_In	Host not available, Host Fall Back to Controller allows IN.	
EV_HFB_Allowed_Normal_Out	Host not available, Host Fall Back to Controller allows OUT.	
EV_HFB_Allowed_APB_Override_In	Host not available, Host Fall Back to Controller allows APB override IN.	
EV_HFB_Allowed_APB_Override_Out	Host not available, Host Fall Back to Controller allows APB override OUT.	
EV_HFB_Allowed_APB_Violation_Out	Host not available, Host Fall Back to Controller allows APB violation OUT.	
EV_HFB_Allowed_Time_Day__Violation_Out	Host not available, Host Fall Back to Controller allows Time/Day violation OUT.	
EV_HFB_Allowed_Exceptional_In	Host not available, Host Fall Back to Controller allows Tag exception IN.	
EV_HFB_Allowed_Exceptional_Out	Host not available, Host Fall Back to Controller allows Tag exception OUT.	
EV_HFB_Allowed_Visitor_In	Host not available, Host Fall Back to Controller allows Visitor Tag IN.	
EV_HFB_Allowed_Visitor_Out	Host not available, Host Fall Back to Controller allows Visitor Tag OUT.	
EV_HFB_Allowed_Duress_In	Host not available, Host Fall Back to Controller allows Duress code IN .	
EV_HFB_Allowed_Duress_Out	Host not available, Host Fall Back to Controller allows Duress code OUT.	

Event Statement	Event Description
EV_Allowed_Special_1_In	Allowed Special 1 IN – Property set on Tag.
EV_Allowed_Special_1_Out	Allowed Special 1 OUT – Property set on Tag.
EV_Allowed_Special_2_In	Allowed Special 2 IN – Property set on Tag.
EV_Allowed_Special_2_Out	Allowed Special 2 OUT – Property set on Tag.
EV_Tables_Initialised	Raised when the Controller initiates all internal tables. They all become blank.
EV_Tables_Corrupt	Raised when the Controller detects a corrupt table.
EV_Trans_Buffer_75_Full	Transaction buffer in the Controllers 75% full.
EV_Trans_Buffer_90_Full	Transaction buffer in the Controllers 90% full.
EV_Trans_Buffer_100_Full	Transaction buffer in the Controllers 100% full.
EV_3rd_Party_Event_1-16	Action of a third-party event.
EV_Inter_Controller_Comms_Error	Inter Controller Comms Error.
EV_Bell_Button	Bell Button pressed on the KMA Antenna Reader.
EV_Input_Cut_1-16	Input Cut 1-16.
EV_Input_Shorted_1-16	Input Shorted 1-16.
EV_Denied_Biometric_In	Denied Biometric IN.
EV_Denied_Biometric_Out	Denied Biometric OUT.
EV_Scanner_Inhibited	Scanner Inhibited.
EV_Scanner_Enabled	Scanner Enabled.
EV_Pending_Allowed_Normal_In	Dual Tag Pending, Allowed Normal IN.
EV_Pending_Allowed_APB_Override_In	Dual Tag Pending, Allowed APB Override IN.
EV_Pending_Allowed_Normal_Out	Dual Tag Pending, Allowed Normal OUT.
EV_Pending_Allowed_APB_Override_Out	Dual Tag Pending, Allowed APB Override OUT.
EV_Pending_Allowed_TimeDay_Violation_Out	Dual Tag Pending, Allowed Time or Day Violation OUT.
EV_Pending_Allowed_APB_Violation_Out	Dual Tag Pending, Allowed APB Violation OUT.
EV_Allowed_Interleading_In	Allowed Interleading IN.
EV_Allowed_Interleading_Out	Allowed Interleading OUT.
EV_Controller_Timeout	Controller Timeout.
EV_Input_Emergency_Mode_On	Input Emergency Mode ON.
EV_Input_Emergency_Mode_Off	Input Emergency Mode OFF.
EV_Input_Lockdown_Mode_On	Input Lockdown Mode ON.
EV_Input_Lockdown_Mode_Off	Input Lockdown Mode OFF.
EV_Input_Alarm_Restore_1-16	Input Alarm Restored 1-16.
EV_Power_Failure	Power Failure.
EV_Power_Restored	Power Restored.
EV_Battery_Low	Battery Low.
EV_Battery_Ok	Battery OK.
EV_Arm_No_Authority	The Tag used does not have zone arming authority.

Event Statement	Event Description
EV_Arm_Already_Armed	Zone already armed.
EV_Arm_Zone_Not_Ready	Zone not ready for arming.
EV_Arm_Zone_Armed	Raised on successful arming operation.
EV_Arm_Failed	Arm operation failed, zone not armed.
EV_Arm_Failed_Arm_All	Failure arming all zones.
EV_Arm_Request	Places the Controller in the middle of an arming sequence, and tries to Arm the zone (carries out the 'Arm Alarm System Relay' action).
EV_Arm_Out_Of_Sequence	Raised when the 'Armed Input' activates suddenly (with no Arming Request), the zone immediately goes into Armed Mode.
EV_Disarm_No_Authority	The Tag used does not have disarm authority for the zone.
EV_Disarm_Already_Disarmed	Zone already disarmed.
EV_Disarm_Zone_Disarmed	Raised on successful disarm operation.
EV_Disarm_Failed	The disarm operation failed, zone not disarmed.
EV_Disarm_Emergency_Unlock	Raised when a zone is in Armed Mode and an Emergency Unlock request is made. Emergency Unlock has a higher priority than Armed Mode. No disarm request is made to the Alarm Panel. All Readers exit Armed Mode and go into Emergency Unlock Mode.
EV_Disarm_Request	Places the Controller into the middle of a disarming sequence and tries to disarm the zone. Carries out the 'Disarm Alarm System Relay' action.
EV_Disarm_Out_Of_Sequence	Raised when the 'Armed Input' suddenly becomes inactive (with no Disarming Request). The zone immediately exits Armed Mode.
EV_Denied_Terminal_Armed_In	Terminal denies entry while in Armed Mode.
EV_Denied_Terminal_Armed_Out	Terminal denies exit in Armed Mode.
EV_SMS_Action_Performed	This status transaction keeps a record of actions performed via SMS.
EV_Comms_Message_Failure	Raised when sending a template to a B-SHO Terminal fails.

Table 5 – Table of Events and Actions

USER NOTES