integriti
INTEGRATED SOLUTIONS

SYSTEM CONFIGURATION HANDBOOK

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

ASIAL MEMBER
AUSTRALIAN SECURITY INDUSTRY ASSOCIATION LIMITED
GOLD MEMBER

Certified System
Quality
ISO 9001

INNER RANGE recommends that all Inner Range systems be installed & maintained by FACTORY CERTIFIED TECHNICIANS.

For a list of Accredited Dealers in your area refer to the Inner Range Website.
http://www.innerrange.com

UPDATES AND ADDITIONAL INFORMATION:

Check the Website regularly for:

- Additional applications and tables not included in this manual.
- Updates and/or changes to existing documents.
- New documents added to this manual.

Advanced Tech Support:

- http://www.onlinetraining.innerrange.com/
  (Restricted downloads)
- http://www.onlinetraining.innerrange.com/login/signup.php
  (Restricted account creation)
- http://www.innerrange.com.au/support.php
  (Support contacts)

Home Page:

- http://www.innerrange.com

Please send or fax any comments regarding this manual to:

- "Publications" at the Head Office address. (See front cover)
  – Or –
- e-mail to: Publications@innerrange.com

Disclaimer:

1. The manufacturer and/or its agents take no responsibility for any damage, financial loss or injury caused to any equipment, property or persons resulting from the correct or incorrect use of the Inner Range system and its peripherals.
2. Whilst every effort has been made to ensure the accuracy of this manual, Inner Range Pty Ltd assumes no responsibility or liability for any errors or omissions. Due to ongoing development the contents of this manual are subject to change without notice.

System Configuration Handbook

Table of Contents

1. HARDWARE AND SOFTWARE PREREQUISITES 8

1.1 MINIMUM SYSTEM REQUIREMENTS 9

1.1.1 Client workstation specifications: 9

1.1.2 Server workstation specifications: 9

1.2 INTEGRITI SPECIFICATIONS 11

2 INSTALLING THE SOFTWARE 12

2.2 INSTALLATION OPTIONS 12

2.2.1 Registration 13

3 LOGIN 15

3.1 INTEGRITI SERVICES 16

3.2 LOG UTILITY 16

4 USER INTERFACE 17

4.1 THE REVIEW PANEL 17

4.2 THE ACTIONS PANEL 19

4.3 EDITOR WINDOWS 20

4.3.1 Toolbar 21

4.3.2 Hyperlinks 22

5 SETTING UP AN INTRUDER SYSTEM 23

5.1 INTRODUCTION AND PROGRAMMING SUMMARY 23

5.2 INPUTS & INPUT BEHAVIOUR 24

5.3 SETUP INPUTS 24

5.4 SET UP AREAS 25

5.5 SET UP A SYSTEM AREA 27

5.6 CONFIGURE PSTN REPORTING 29

5.7 CONFIGURING DIALLER TEST REPORTS 30

5.8 USER SECURITY PERMISSIONS 32

5.8.1 Area Lists 32

5.8.2 Menu Groups 33

5.8.3 Permission Groups 33

5.8.4 Users 36

5.9 USING THE INTRUSION SYSTEM 38

5.9.1 Arming / Disarming… 38

5.10 ADVANCED 39

5.10.1 Auto arm / disarm by Time Period 39

5.10.2 Defer area arming 40

6 SETTING UP AN ACCESS SYSTEM 43

6.1 INTRODUCTION AND PROGRAMMING SUMMARY 43

6.2 CARD TEMPLATE 45

6.3 DOOR CONFIGURATION 45

6.4 READER MODULE CONFIGURATION 46
6.5 USER ACCESS PERMISSIONS 46
6.5.1 Door Lists 46
6.5.2 Menu Groups 47
6.5.3 Permission Groups 48
6.5.4 Credentials (Cards & RF fobs) 48
6.6 USING THE ACCESS CONTROL SYSTEM 51
6.6.1 Locking / Unlocking 51
6.7 ADVANCED ACCESS CONTROL 51
6.7.1 Time based door control 51
6.7.2 Disabled access 53

7 CREDENTIALS 54

7.1 CARD FORMAT 54
7.2 CARD TEMPLATES 57
7.3 CARDS 57
7.4 RF REMOTE TEMPLATES 59
7.5 RF REMOTES 60
7.6 CARDS 61

8 SCHEDULING 64

8.1 TIME PERIODS 64
8.2 SCHEDULES 66
8.3 HOLIDAYS 67
8.4 SCHEDULED TASKS 68

9 AUTOMATION 71

9.1 COUNTING INPUT TYPES 71
9.2 AUXILIARIES 72
9.3 AUXILIARY LISTS 73
9.4 COMPOUND ENTITIES 73
9.5 NAMED ACTIONS 74
9.6 MACROS 76
9.6.1 Macro characteristics 76
9.6.2 Controlling / Running macros 77
9.6.3 Creating a new macro 78
9.6.4 Statements 78
9.6.5 Execute Modified Action… 79
9.6.6 Macro Expressions 81
9.7 GENERAL VARIABLES 83
9.8 GENERAL TIMERS 84

10 HARDWARE AND LAN MANAGEMENT 85

10.1 CONTROLLER CONFIGURATION 85
10.2 ENROLLING CONTROLLERS 86
10.2.1 Automatic controller discovery (Method 1) 87
10.2.2 Manual controller enrolment (Method 2) 92
10.2.3 Controller enrolment using the SkyTunnel service (Method 3) 93
10.3 MAINTAINING FIRMWARE 95
10.3.1 Upgrading module & controller firmware 97
10.4 MODULE PROGRAMMING 98
10.4.1 Adding New Modules 99
10.4.2 Deleting Modules 99

11 CCTV 100

11.1 INSTALLING INSIGHT DVR PLUGINS 100
11.2 ENROLLING VIDEO SYSTEMS 100
11.3 CCTV CAMERA CONFIGURATION 102
11.4 ASSOCIATING CAMERAS WITH ENTITIES 102
11.5 VIEWING ASSOCIATED VIDEO FROM ASSOCIATED ENTITIES 102
11.6 VIEWING ASSOCIATED VIDEO WITH REVIEW 103
11.7 VIEWING VIDEO FROM SCHEMATICS 103

12 PHOTO ID 104

12.1 CREATING A PHOTO ID DESIGN 105

13 SCHEMATICS & ELEMENT PRESENTERS 106

13.1 ELEMENT PRESENTERS 107
13.1.1 Condition 108
13.1.2 Icon Format 109
13.1.3 Shape Format 109
13.1.4 Label Format 112
13.2 CONFIGURATION OF SCHEMATIC MAPS 115
13.2.1 Map properties 116
13.2.2 Schematic map toolbar 117
13.2.3 Map Element Properties 119

14 LAYOUTS & EDITORS 126

14.1 LAYOUTS 126
14.2 CREATING AND SAVING LAYOUTS 127
14.3 EDITOR LAYOUT SETS 128

15 COMMUNICATIONS TASKS 131

15.1 SERIAL CHANNEL 131
15.2 COMMUNICATIONS TASKS: 133
15.2.1 Integriti 133
15.2.2 Monitor 133
15.2.3 Dialler 133
15.2.4 GSM 133
15.2.5 Automation 133
15.2.6 EMS 134
15.2.7 Securitel 134
15.2.8 Intercom 134

16 COMMUNICATIONS HANDLERS 135

16.1 REVIEW RECEIVER 135
16.2 REVIEW SENDER 135
16.3 REST/XML WEB SERVICE 135

17 ALERTS 136

ALERT DEFINITIONS 137
17.1 ALERT GROUPS 138
17.2 ALERT VIEWS 139
17.3 RESPONSE PLANS 140
17.3.1 Delete Selected Item 140
17.3.2 Information Box Item 141
17.3.3 Information Display Item 141
17.3.4 Alert Custom Field 142
17.3.5 Action Button 142
17.3.6 Alert Details 142

17.3.7 Response History Item 143
17.3.8 Add Operator Response Item 143
17.3.9 CCTV Stream 144
17.3.10 Browser Item 144
17.3.11 Creating a new Response Plan 144

18 IMPORTING DATA 145

18.1 IMPORTING CSV FILES - MANUALLY 145
18.2 IMPORTING CSV FILES – IMPORT CONFIGURATION 148
18.2.1 To use the newly created Import Configuration: 149

19 INTEGRITI SERVER MANAGEMENT 150

19.1 LICENSE MANAGEMENT 150
19.2 OPERATORS AND OPERATOR TYPES 151
19.3 OPERATOR TYPE 151
19.3.1 Type Permissions 152
19.3.2 Extra Permissions 156
19.3.3 Features 157
19.4 OPERATOR 159
19.5 CUSTOM FIELDS 161
19.6 SYNCHRONIZATION WARNINGS 164
19.7 CROSS REFERENCES 166
19.8 AUDIT TRAIL 167

APPENDICES 168

A. INTEGRITI LOG VIEWER 170

B. GLOSSARY OF TERMS 174

C. IDENTIFYING THE INTEGRITI CONTROLLER SERIAL NUMBER 180

D. RANDOM NUMBER 181

E. FILTER STACKS 182

F. ACTION TYPES 183

G. ENTITY STATES 200

H. ENTITY TYPES 204

I. CALIBRATIONS 206

J. DEFAULT ENTITIES 209

K. SYSTEM INPUT PROCESS GROUP DEFAULTS 213

L. INTEGRITI PROGRAMMING EXAMPLES 214

M. LICENSES 219

1. Hardware and Software Prerequisites

The Integriti suite consists of Server and Client software. Integriti software installation files contain all of the client and server software in one package for easy deployment. The entire software suite can be installed on a single machine for typical installations or as one server and *n* clients.

We recommend the use of a dedicated computer for the purpose of running the Integriti server.

Supported 32bit operating systems:

- Windows Vista SP2
- Windows 7 SP1
- Windows Server 2003 SP2
  - Requires Windows Imaging Component (WIC) prior to installing version 4.5 of the .NET Framework
- Windows Server 2008 SP2
  - Including R2

Supported 64bit operating systems:

- Windows Vista SP2
- Windows 7 SP1
- Windows 8
  - Excluding Windows 8 RT
- Windows Server 2003 SP2
  - Requires Windows Imaging Component (WIC) prior to installing version 4.5 of the .NET Framework
- Windows Server 2008 SP2
  - Including R2
- Windows Server 2012

Unsupported operating systems:

Windows XP is not officially supported; however Integriti has been known to work on windows XP SP 3. Users will need to install the Windows Imaging Component (WIC) prior to installing version 4.5 of the .NET Framework.

Supported MS SQL versions:

- SQL Server 2008
- SQL Server 2008 R2
- SQL Server 2012 (all editions)

1.1 Minimum system requirements

All machine specifications should include the following:

- A screen resolution of 1024x768 or higher. A 22" WSXGA+ monitor at 1680x1050 (or better) is recommended.
- The Integriti software management suite requires both a keyboard and pointing device to operate.
- It is the responsibility of the system administrator to ensure the machine specifications are adequate for the operating system and version of MS SQL selected.

1.1.1 Client workstation specifications:

At the time of writing, almost any PC purchased today should easily run the Integriti client software.
These specifications are also suitable for installations where there is one PC and one Controller in use.

- Any of the operating systems listed above.
- 2GHz or higher quad core processor.
- 4GB DDR II memory or higher.
- 500GB SATA HDD or higher.
- Gigabit Ethernet adaptor.

Older machines may be able to run Integriti software, please contact your support representative for more details.

1.1.2 Server workstation specifications:

Small sites consisting of 1 – 10 Integriti controllers and up to 5 client workstations:

The following specifications are suitable for a PC used as a dedicated Integriti server.
Additional client workstations should have specifications equal to or better than the client workstation specifications listed above.

- Any of the above operating systems.
- 2GHz or higher quad core processor.
- 4GB DDR II memory or higher.
- 500GB SATA HDD or higher.
- Gigabit Ethernet adaptor.

Medium sites consisting of no more than 50 Integriti controllers and up to 5 client workstations:

The following specifications are suitable for a PC used as a dedicated Integriti server. Additional client workstations should have specifications equal to or better than the client workstation specifications listed above.

- Any of the above operating systems.
- A core i5 family or higher processor.
- 6GB DDR III memory or higher.
- 1TB SATA HDD or higher.
- Gigabit Ethernet adaptor.
- SQL Server 2008 Standard edition is recommended for sites consisting of more than 25 controllers.
- Please contact the Inner Range technical support team for assistance with your project.

Large sites consisting of more than 50 Integriti controllers and more than 5 client workstations:

The following specifications are suitable for a PC used as a dedicated Integriti server. Additional client workstations should have specifications equal to or better than the client workstation specifications listed above.

- Windows Server 2008.
- A core i7 family or higher processor.
- 12GB DDR III memory or higher.
- 1TB SATA HDD or higher.
- Gigabit Ethernet adaptor.
- SQL Server 2008 Standard edition or higher.
- Please contact Inner Range to discuss your project in detail.

1.2 Integriti specifications

Approximate disk usage:

- ~100MB - Integriti software management suite
- 550MB – 10GB - SQL Express 2008[1]

Running processes:

- ~120MB - IntegritiSystemDesigner.exe
- ~42MB - IntegritiControllerServer.exe
- ~35MB - IntegritiApplicationServer.exe

There will also be additional SQL processes running. Memory usage and process names will vary depending on the SQL instance name, database size and version of SQL server. For more information please refer to the Microsoft SQL documentation.

Ports used:

- 44000 - TCP Client ↔ Application server communications
- 4711 - TCP Controller ↔ Controller server communications

By default, Integriti uses the Microsoft SQL 2008 R2 Express database engine, which limits the database to 10 GB of data.

Whilst the installation itself only takes approximately 600MB of hard disk space, the SQL Express database can grow to 10GB over time with the storage of your controllers' historic review data. If up to 4 or 5 million review events are expected over a 12 month period and SQL Express is required to host the Integriti database, then 5GB of free hard disk space is recommended. The 10GB database will allow room for more than 6 million review events, but note that a moderate to busy site could easily generate that number of events every year. For large / busy sites, (more than 6 million review events per year) you may need to purchase the full version of SQL Server 2008 (or newer).

Contact the manufacturer for hardware specifications when the recommended number of review events will be exceeded.

[1] Database size can vary dramatically due to a number of factors such as the version of MS SQL or number of Integriti controllers and Integriti controller activity.

2 Installing the Software

Before installing Integriti, please make sure your computer hardware specifications meet the minimum hardware requirements as explained above.

Integriti should only be installed by someone logged on to the machine locally as an administrative user.

2.1 Installation packages available

There are two installation packages available – the full installer and the web installer.

The full installer is the larger of the two and contains all of the files and resources required to install the Integriti software management suite on your computer without the use of internet connectivity.

The web installer is much smaller and quicker to download, but requires an internet connection for the duration of the installation process and may take a little longer to install depending on the dependencies required for your computer.

The web installer is a good option when upgrading an existing Integriti installation.

To begin the Integriti installation, double click the Integriti setup executable:

Integriti_Pro_Full_x*XX*_setup_(*XXXXX*).exe – or – Integriti_Pro_web_setup_(*XXXXX*).exe

Make sure you have the latest version of Integriti before installing. Visit http://www.onlinetraining.innerrange.com/login/index.php *(login required).*

2.2 Installation options

After accepting the license agreement and reviewing the release notes you will have the following options:

- Installation path
- Components to install
  - Server & Client
  - Client Only
  - Stand Alone Controller Server
- Where should setup create the database?
  - Upgrade my existing database
  - In a new SQL Express Instance
  - I will specify an existing SQL Instance (advanced)

2.2.1 Registration

On first use of the Integriti management software, you will be presented with the software activation wizard. You will be required to enter a valid product key before continuing with the registration process.

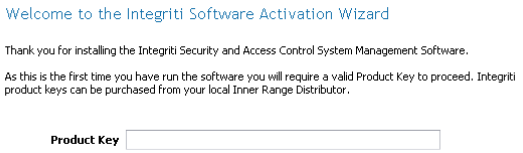


Figure 1

Upon entering your license key you will have the option of selecting from one of three registration methods:

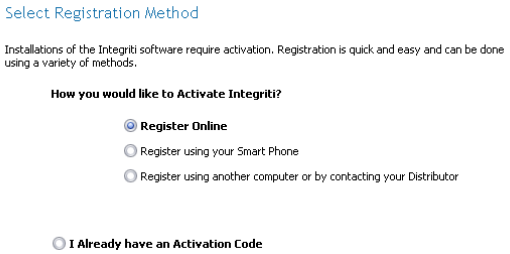


Figure 2

2.2.1.1 Register online (Default, recommended option).

If the machine has access to the internet, you can register online. Once you have provided some basic site details, the software will automatically register itself.

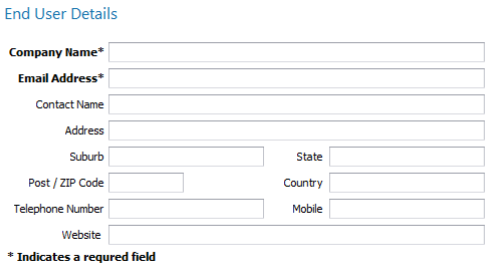


Figure 3

2.2.1.2 Register using your smart phone.

If the machine does not have access to the internet, you have the option to register the software using your mobile device.

Using your mobile device, take a photo of the QR code shown on the screen (not the one in this document). The QR code will translate to a URL on your mobile device. This web page will request the same information as if you were registering online.

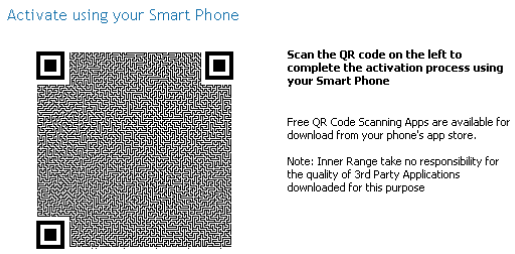


Figure 4

When the registration page has been completed, you will be given a unique activation code. Enter this code in to register your copy of the software using the method below.

2.2.1.3 Register using another computer or by contacting your distributer.

If you are unable to register the software due to security or connectivity issues, this option allows you to go through the process by either contacting your distributor or by using another computer that has internet access.

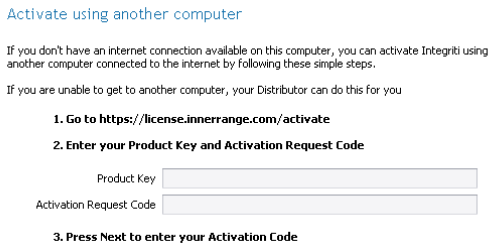


Figure 5

2.2.1.4 I Already have an Activation Code.

If you have already been through the registration process and have been given your activation code, you can select the 'I Already have an Activation Code' option to register your copy of the software.

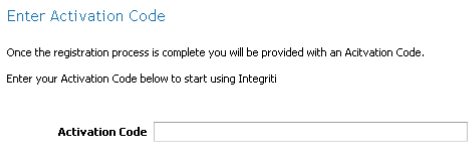


Figure 6

3 Login

Operators are presented with a login dialog when they run Integriti. To log in, simply enter your operator name and operator password then click the Login button.

Operator credentials are defined within the Integriti management software.

The default Integriti operator login is a user name of 'installer' with the default password of 'installer'. It is strongly recommended that you remove this operator or change the password as soon as possible.

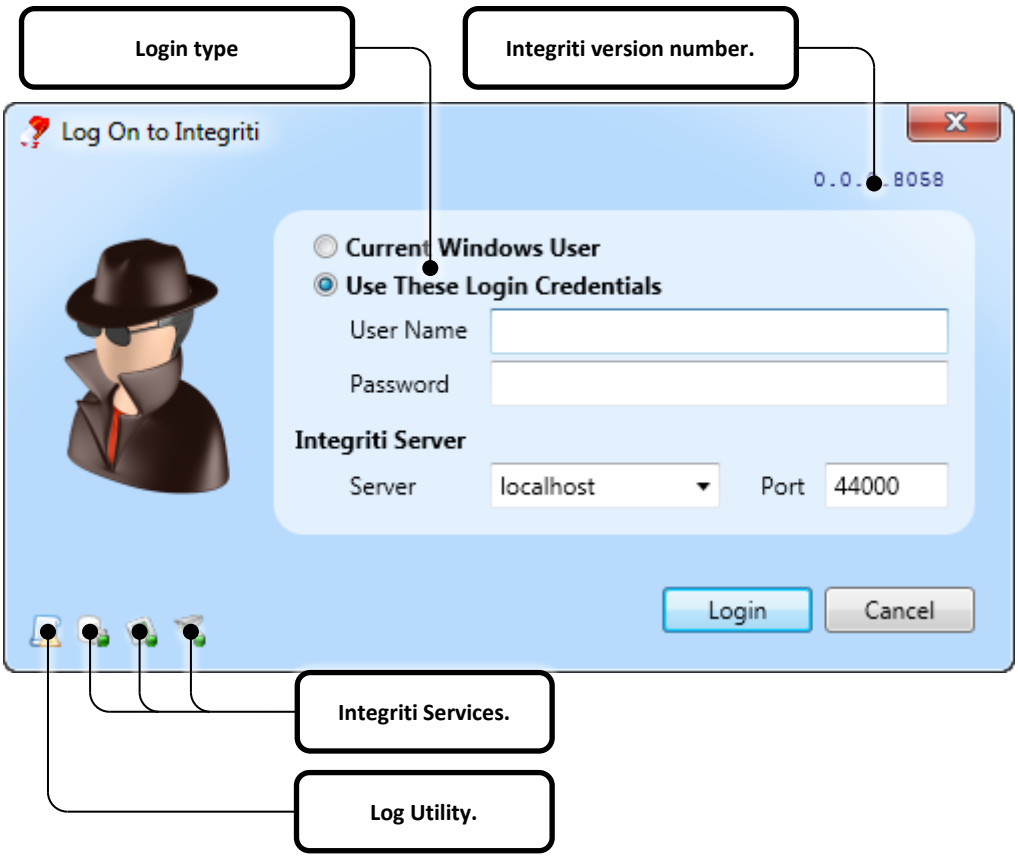


Figure 7

Make sure the Integriti services are running before you attempt to log in. See Integriti Services on page 16.

3.1 Integriti Services

The Integriti services should be running before you log in to Integriti. If they are not, right-click the service icon and click Start.

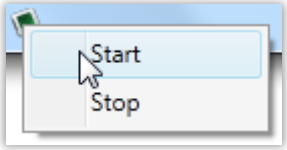


Figure 8

The service icon should appear solid (with a green indicator), indicating that the service is running:

	Stopped	Stopping	Starting	Running
Integriti controller server				
Integriti application server				
Integriti Integration server				

Table 1

3.2 Log Utility

The log utility is used for diagnostic / fault finding purposes. You can access the log utility by clicking the icon either in the login dialog or in the Integriti title bar. For more information on the log utility, see the section titled 'Integriti log viewer' towards the end of this document.

4 User Interface

Please read the document titled “Interface Elements for Integriti” for more information on how to make good use of the user interface.

4.1 The Review Panel

The review panel is located at the bottom left of the Integriti window by default. At a glance, operators can see events as they occur and action them if required.

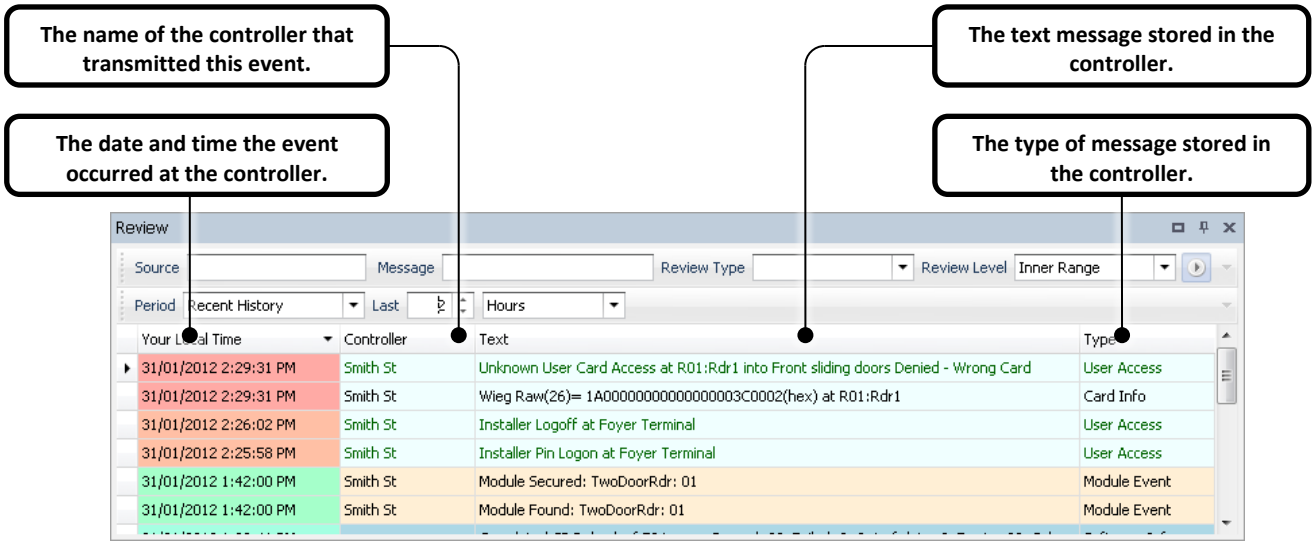


Figure 9

The review panel has a 'heat signature' feature which allows the operator to see the age of the displayed review events. The background colour of the review events in the first column 'Your Local Time' represents the age.

Present Past

Your Local Time	Controller	Text
21/11/2011 8:33:50 AM		Controller 'New Controller (PT000031)' disconnect
21/11/2011 8:18:28 AM	New Controller (...	Module UnSecured: Front Entry & Car Park
21/11/2011 8:18:28 AM	New Controller (...	Module Found: Front Entry & Car Park
21/11/2011 8:03:16 AM	New Controller (...	System Date/Time set to Nov 21 2011 08:02:50 U
21/11/2011 8:03:16 AM	New Controller (...	Timezone set to UTC+11:00 by Integriti 01 (Integ
21/11/2011 8:03:16 AM	New Controller (...	Comms Task 02 (Integriti) - Integriti Connected du

Figure 10

The single greatest advantage of this feature is the ability to notice how review events are grouped without reading individual timestamps. ***Figure 10*** is a simple example of this feature.

Your Local Time	Controller	Text
21/11/2011 9:58:06 AM	New Controller (...	System Date/Time set to Nov 21 2011 09:58:36 U
21/11/2011 9:58:06 AM	New Controller (...	Timezone set to UTC+11:00 by Integriti 01 (Integ
21/11/2011 9:58:05 AM	New Controller (...	Comms Task 02 (Integriti) - Integriti Connected du
21/11/2011 9:00:00 AM	New Controller (...	Working Hours became Valid (TP00001)
21/11/2011 9:58:35 AM		Controller 'New Controller (PT000031)' connected

Figure 11

In the example above an older event has been placed in between newer events. This scenario can occur when communications to one or many controllers has been (re-)established. Review filtering and organisation occurs at the time the filter is applied.

4.2 The Actions Panel

The actions panel will display various action types as they occur and their status. For instance, if you were to upgrade the firmware of a controller, a progress bar will appear in the actions panel indicating the firmware upgrade progress.

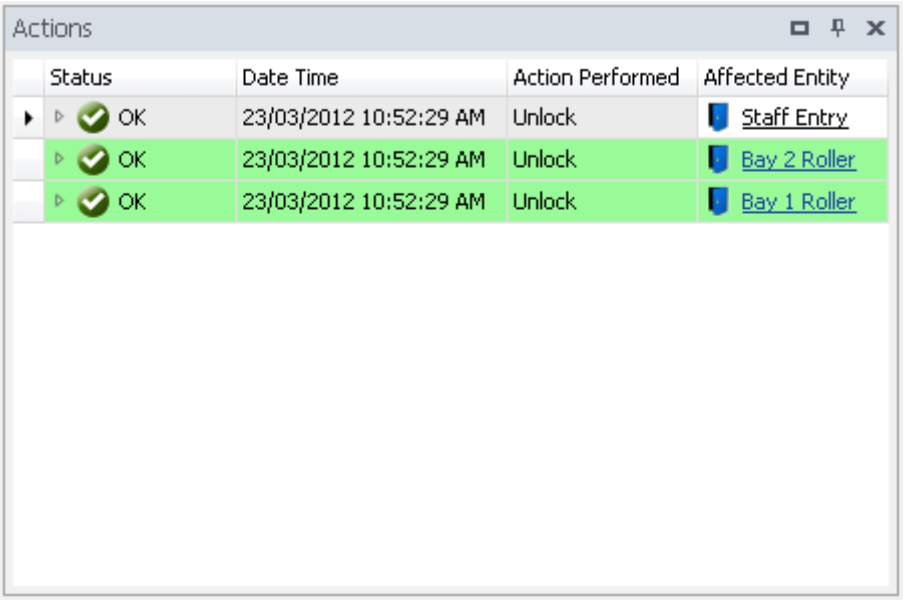


Figure 12

4.3 Editor windows

Most editor windows will look like the following example…

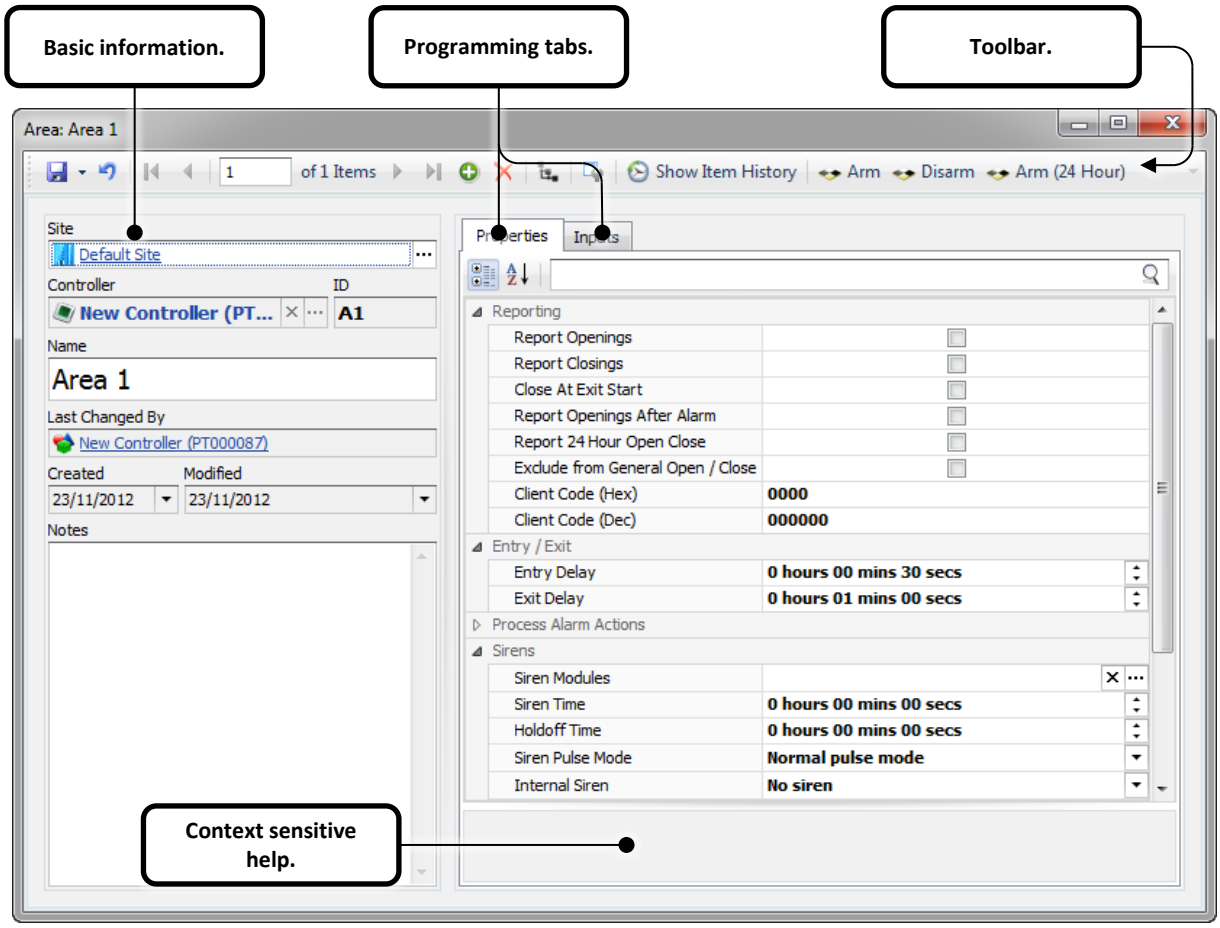


Figure 13

The left side of the editor window contains items relevant to all programmable entities within the Integriti management software.

The right side of the editor window contains a number of programming tabs (usually two). The first tab (e.g. 'Properties') will contain all of the required programmable items relevant to the entity. Other tabs will usually contain advanced options or lists to associate other entities with the currently programmed item (e.g. inputs to an area).

Context sensitive help will appear at the bottom right hand corner of the editor window for items selected under the programming tabs.

Depending on the editor window position and layout, not all of the information contained in the context sensitive help box may be visible. You can adjust the size of the context sensitive help box by clicking and dragging the top section of the box (*Figure 14*).

Figure 14

4.3.1 Toolbar

The toolbar contains the following buttons:

Save	Save the currently displayed record settings.
Undo	Undo the last change since the window was opened.
First Record	Go to the first record in the series.
Previous Record	Go back one record.
Next Record	Go forward one record.
Last Record	Go to the last record in the series.
New Record	Create a new record.
Delete Record	Delete the currently displayed record.
Property page view	Change the view to the default property page layout.
Show Cross References	Open a dialog with a tree view that displays the references to and references from this entity.
Show Synchronisation Warnings	Displays the synchronisation warning panel.
Audit	Open a new window displaying the entire history of changes made to this record.
Customize Layout	Change the layout of the editor window.

Table 2

Other buttons specific to the current entity may be visible on the toolbar.

You can toggle an automatic save feature by clicking on the save button dropdown followed by 'Auto Save'. The Save icon will change to a green icon when the automatic save feature is active.

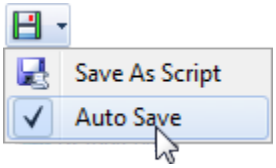


Figure 15

4.3.2 Hyperlinks

Integriti has the added convenience of hyperlinks. Hyperlinks are blue text labels that allow you quickly navigate between related items, without using the ribbon and panels to manually locate them. To follow a hyperlink, simply click on it. Clicking on a hyperlink will open a window with the properties for the clicked item.

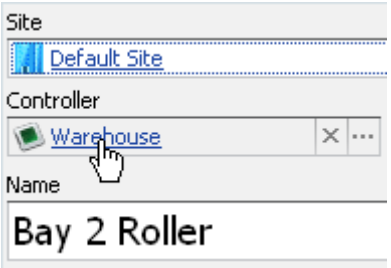


Figure 16

5 Setting up an intruder system

The following will step you through what is required to commission a basic intrusion system.

It is assumed that the operator is logged in to the System Designer. An Integriti controller with the necessary modules attached should already be online, communicating with the server.

The instructions provided are based on the default layout.

5.1 Introduction and programming summary

Areas

Security management operation is designed around the concept of Areas. Areas are groups of Inputs such as movement detectors that can be collectively enabled when the Area is turned on or disabled when the Area is turned off.

The system determines which Areas each User can control during which times and with which options.

Inputs

An Area can contain one or more detection devices or other devices (wired to Zone Inputs) and/or one or more System Inputs. If a Zone detects an intruder or a System Input is activated (e.g. Low Battery, Cabinet Tamper, etc.) it will only be actioned if the Area that the Input is in, is turned on. The action which is taken when an Input is activated in a particular Area (e.g. activate Siren/s, activate Auxiliaries, report to Central Station, etc.) is determined by how that Input is programmed in that particular Area.

An Input can be programmed into more than one Area. The Alarm action taken by an Input when in the Alarm condition is dependent on how that Input is programmed in each Area, and on the Area/s being turned on.

This allows a particular Input alarm to be actioned in different ways depending on what Areas it is assigned to, and which of those Areas are on.

Process Groups

Defining how an Input will be actioned in each Area is primarily done by allocating an appropriate Process Group, to every Input in each Area that it is assigned to. Process Group programming includes defining the Input states (Seal/Alarm/Tamper/Isolate/…) that will be recognised, Entry/Exit delay processing options, Reporting & message options, and Auxiliary and Siren control options.

Programming summary

Inputs are assigned to areas with a process group. Input programming records cover the physical attributes of the input on the module. Process group programming records contain the rules that govern how the input will behave within the assigned area.

Recommended programming sequence:

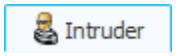
- Configure Inputs
- Create and populate Areas
  - Set up Area reporting
  - Assign Sirens to Areas
  - Assign Inputs to Areas and Assign Process Groups
- Create Telephone Number records
- Configure a Communications Task for monitoring
  - Assign Telephone Numbers to a Communications Task
- Create an Area List
- Create a Menu Group
  - Give arming permissions to a Menu Group
- Create a Permission Group
  - Adding Areas and Area Lists
  - Adding Menu Groups
- Create Users
- Assigning Permissions to Users
  - User PIN codes

5.2 Inputs & input behaviour

On some Modules, a number of the Zone Inputs have pre-defined functions. These can only be used as general purpose Zone Inputs if the operation relating to the pre-defined function is not being implemented.

5.3 Setup inputs

All inputs should be named according to their application and some additional options may need setting.

1. Click on the 

tab followed by

.
2. Double-click an input to program. The Editor Window for the input should appear.
3. Change the name of the input to something more appropriate.
   - e.g. "`Front Door Reed Switch`"
4. On the right-hand side of the window, expand-out Options.

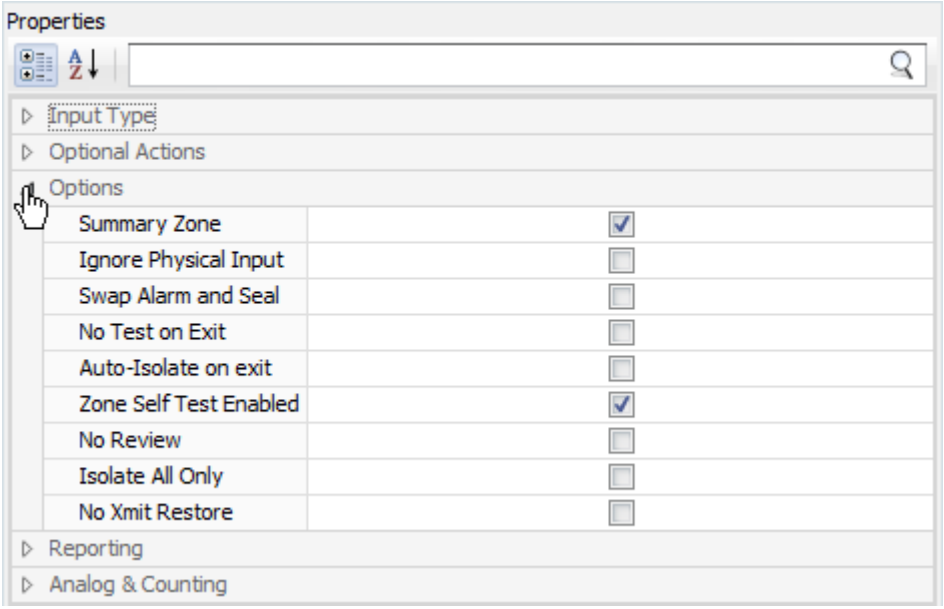


Figure 17

5. If there is a possibility that the input will be in an unsealed state at the time of arming, then click "No test on exit".
6. If the input is physically wired to a normally open device then you might need to tick the "Swap Alarm and Seal" option.
7. Save and close the editor window for the Input.
8. Repeat steps **2** - **6** for the other inputs you are using.

The input item editor, like all item editor windows in Integriti contains a context sensitive help box at the lower right which can help remind users of the effect of each option.

5.4 Set up areas

Once all of the Inputs have been programmed, you can configure the Areas.

1. Click on the Intruder tab followed by Areas.
2. Click Add New. The Editor Window for a new area should appear.
3. Give the Area a name.

Under the Properties tab…

4. Expand-out reporting.
   a. If openings for the area should be reported, click the "Report Openings" option.
   b. If closings for the area should be reported, click the "Report Closings" option.
   c. Enter the Client Code in "Client Code" field provided by the monitoring centre.
5. Expand-out Entry / Exit.

a. If an entry delay is required, fill in the “Entry Delay” option.
b. If an exit delay is required, fill in the “Exit Delay” option.

6. Expand-out Sirens

a. To make use of the sirens, click on the ··· to the right of Siren Modules.

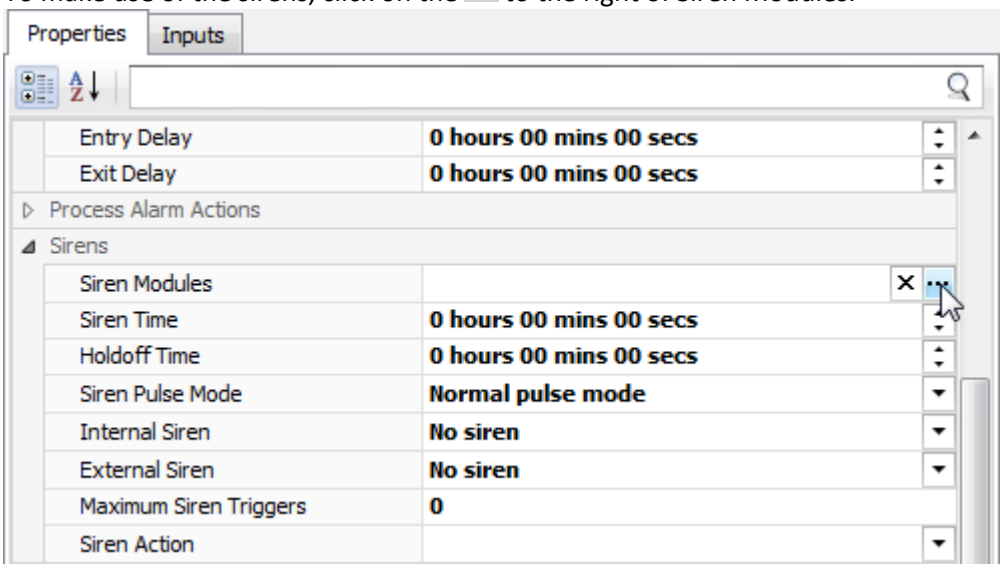


Figure 18

b. A new window “Siren Modules” should appear. Click on the Add button.
c. From the window that appears, select the required siren module(s) and click OK.
d. Verify that all of the required siren modules have been selected and click OK.
e. Change the siren time option as required. (Note local laws etc…)
f. Click on the “Internal Siren” drop-down and select the mode of operation for the siren modules internal siren.
g. Click on the “External Siren” drop-down and select the mode of operation for the siren modules external siren.
h. If required, adjust the “Maximum Siren Triggers” that can occur before a siren is disabled.

Under the Inputs tab…

7. Click on Add to add inputs to the area.

8. From the window that appears, select the input(s) you want to add to the area and click OK. If you have a large list of available inputs, you may wish to filter the list by typing into the filter row at the top of the Input selection window. The Controller, ID, and Name fields are particularly useful here.
Pick a Process Group that defines how each input will operate. See the section titled ‘Default entities’ for a summary of the process groups and their behaviour.

9. Change the Process Group of an input (if required) by selecting the input and clicking Change Process Group.

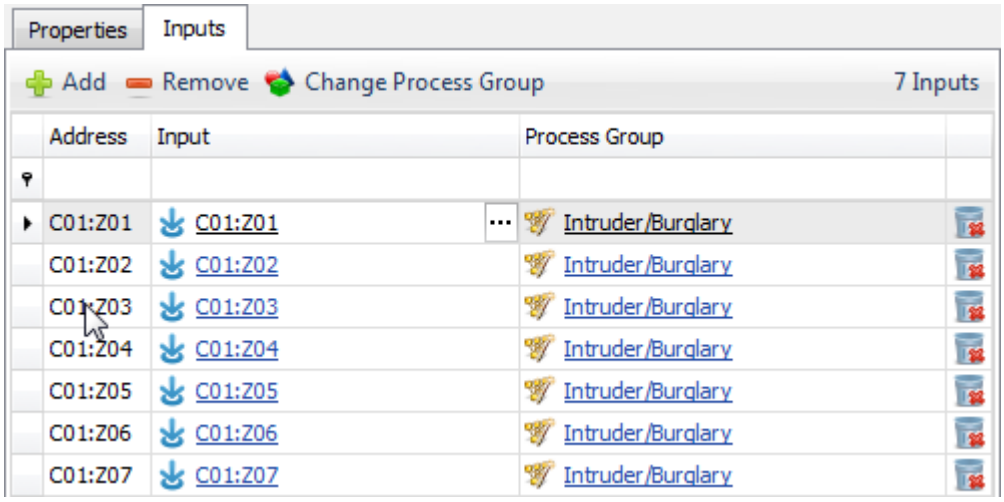


Figure 19

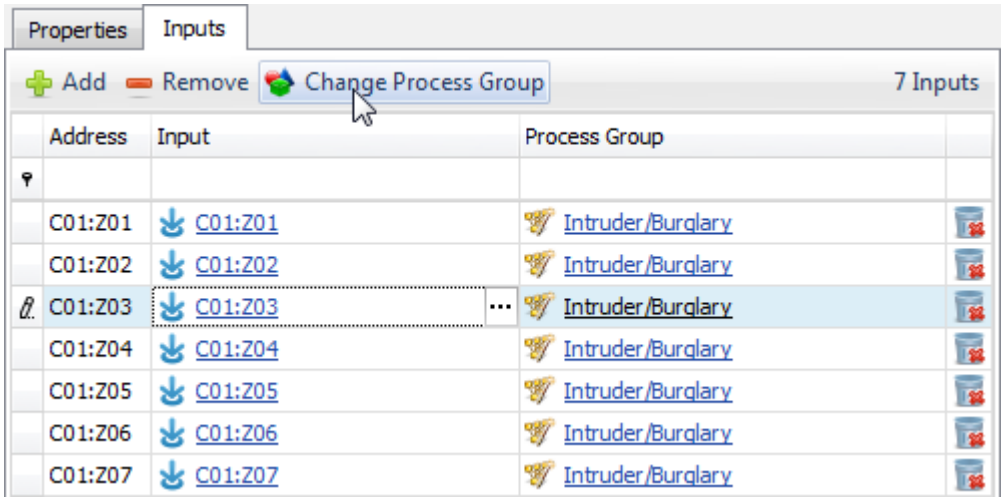


Figure 20

10. Save and close the editor window for the area.

5.5 Set up a System Area

The Integriti security controller has various system input types which should be placed in to an area for local alarms and reporting purposes. Alarms such as AC failure, Low battery, LAN communications failure and cabinet tampers are some of the types of system inputs that should be included in a system area.

Integriti has a feature in area programming that allows you to automatically populate a designated system area with the inputs you specify. To do this you will need to create a Systems area and using the 'Assign System Inputs' feature, enter the systems input types for all of the required Integriti/Concept 4000 LAN modules.

This systems area can be any area you choose, and the below step by step guide shows you how to create this Systems area.

Creating a new System Area…

1. Click on the Intruder tab followed by Areas.
2. Click Add New. The Editor Window for a new area should appear.
3. Give the area a name such as 'System Area'.
4. Give the Area a new name and enter any necessary notes in the Notes field.
5. Establish what Systems inputs will be required for available LAN modules. Refer to the 'System Input Process Group Defaults' in the appendix for more information on what process group is appropriate for each individual system input.
6. Click on the Inputs tab.
7. Click on Assign System Inputs. The following window should appear…

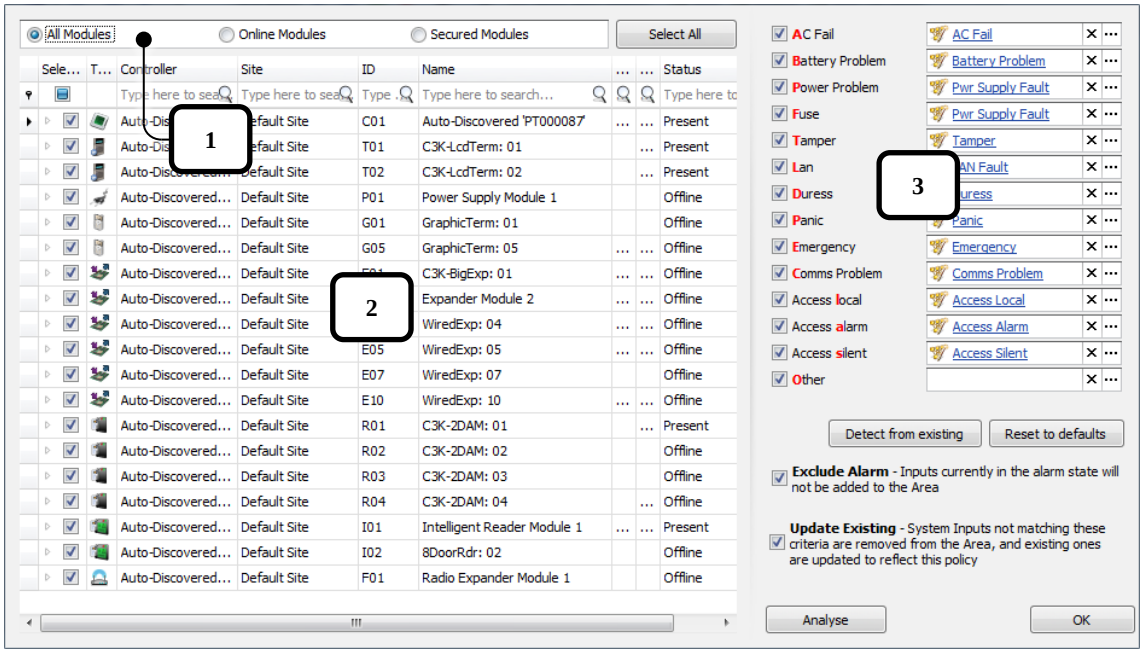


Figure 21

8. Select what module category you will be assigning inputs from (1).
9. Select (or unselect) modules as required in the list below (2).
10. Select the Process Groups based the various input types you want to assign to this area (3). Usually intrusion and access system inputs are divided in to two separate system areas for easier system wide control and monitoring.
    - Detect from existing is used in cases where system inputs are being updated or appended to an area with pre-existing inputs. If the Process Group selected for a particular type of input was something other than factory default, Integriti will use that Process Group instead (e.g. The 'Duress' Process Group was used for 'Panic' Inputs).
    - Clicking Reset to defaults will change the Process Groups for the various input types to factory default.

- Checking the Exclude Alarm option will exclude any inputs that are in alarm at the time the button was pressed from the area.
- If Update Existing is checked, inputs assigned to this area will be updated or appended (if they do not already exist).

11. Click Analyse to display a total of all of the inputs that will be added (or updated) to the area. Totals for each Input type will also appear.

12. Click OK.

13. Add any additional area processing you may require, such as reporting options for open and close etc…

14. Ensure access to the System Area is restricted to the integrator and/or on site technician.

15. Save and close the editor window for the system area.

5.6 Configure PSTN reporting

To setup reporting via the telephone dialler you will need to configure Telephone Number(s) and a Communications Task.

Configuring the Telephone Number…

1. Click on the Intruder tab followed by Telephone Numbers.

2. Click Add New. The Editor Window for a new phone number should appear.

3. Give the telephone a name.

4. Enter the phone number on the right-hand side of the phone number editor window.

5. Save and close the editor window for the telephone number.

6. Repeat steps **1** - **5** if additional telephone numbers are required.

Configuring the Communications Task…

1. Click on the Intruder tab followed by Comms Tasks.

2. Click Add New. The Editor Window for a new communications task should appear.

3. Give the communications task a name.

4. On the right-hand side under Comms Task Setup, click on the “Type” dropdown and select “Dialler”.

5. On the right-hand side under Dialler Programming.

6. Expand-out Reporting.

a. Change the “Format” to “Contact ID”.

Contact ID is common however; IRFast is preferred when the Central Station supports it as more information is available to aid in achieving an appropriate response. SIA, 4+2 and other less common formats are also available if desired.

b. Enter the Client Code in "Client Code" field provided by the monitoring centre.

c. Click on the ... to the right of the Telephone number fields to open the Telephone number selection window.

d. Select the Telephone number from the list and click OK.

e. Repeat for the second phone number if required.

7. Expand-out Contact ID.

a. The "Standard" map is the default used for Contact ID. If necessary, change the format here.

8. Save and close the editor window for the Communications Task.

5.7 Configuring dialler test reports

Monitoring centres usually ask for a routine dialler test to be configured on the controller to test the integrity of the communications path and to ensure the controller is still online and functional.

To configure the Integriti controller for a dialler test report you will need to change controller settings, program an area and assign the Time Report input to the area.

Configuring the Time Report…

1. Click on the Hardware tab followed by Control Module.

2. Double-click the controller. The Editor Window for the controller should appear.

3. Click on the Module Details tab.

4. Expand-out Time Report.

5. Enter the hour of the day that the controller should send a dialler test report to the monitoring centre.

6. Tick the day(s) of the week that the controller should send dialler test reports to the monitoring centre.

7. Tick Holidays to allow dialler test reports on holidays.

8. Save and close the editor window for the controller.

9. Click on the Intruder tab followed by Areas.

10. Click Add New. The Editor Window for a new Area should appear.

11. Give the Area a new name and enter any necessary notes in the Notes field.

12. Click on the Inputs tab.

13. Click the Add to open the Input selection window.

14. Type “time” in to the filter row under the Name column.

	T...	Controller	Site	ID	Name
		Type here to sea	Type here to sea	Type .	time
				C01:S16	C01 Time Report

15. Select the Time Report system input from the list and click OK.

16. Type “time” in to the filter row under the Name column of the process group assignment window.

	T...	Site	ID	Name
		Type here to sea	Type .	time
			PG25	Time Report

17. Select the Time Report process group from the list and click OK.

18. Save and close the editor window for the area.

5.8 User security permissions

5.8.1 Area Lists

Area lists provide convenience and functionality. Example usage of area lists:

- Assigning the same areas to a number of users.
- Assigning many areas (more than 8) to users.
- Controlling a number of areas using a named action.

Creating Area Lists…

1. Click on the Intruder tab followed by Area Lists.
2. Click Add New. The Editor Window for a new area list should appear.
3. Give the Area List a name.

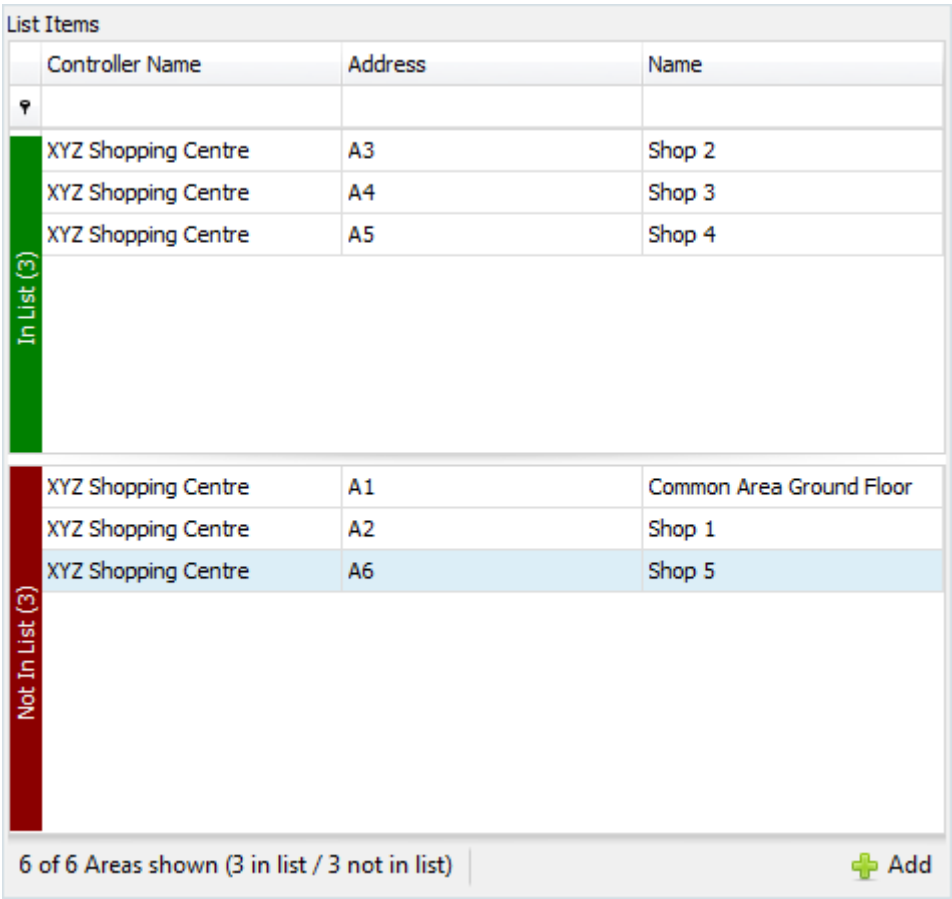


Figure 22

4. Items in the top section of the window are in the area list. Items in the bottom section are not. Double click items to move them from one section to the other.
5. Save and close the editor window for the Area List.

5.8.2 Menu Groups

Menu Groups are permission sets used to grant or deny user's terminal access to the Integriti controller.

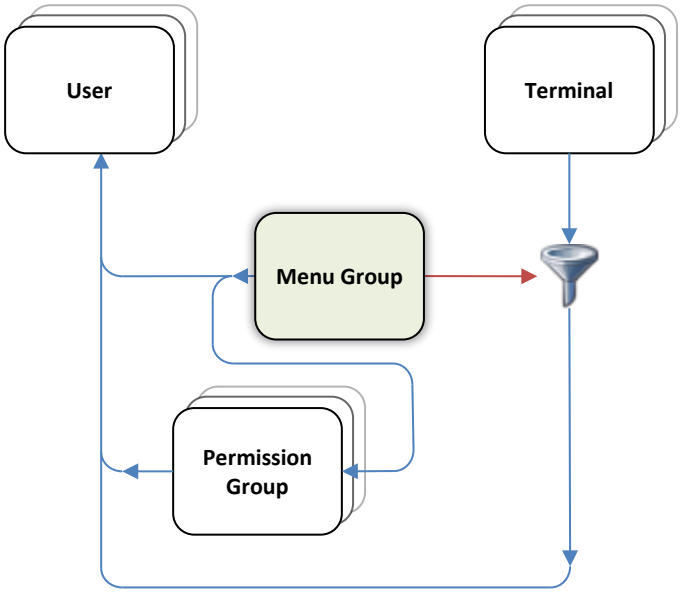
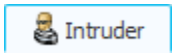
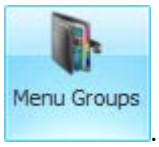
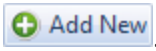


Figure 23

Menu groups can be assigned to compound entities, permission groups and users.

Menu Groups…

1. Click on the  tab followed by  .
2. Click  . The Editor Window for a new menu group should appear.
3. Give the Permission Group a name.
4. On the right-hand side under Properties.
5. Expand-out Main Menu Items.
   a. Tick the "Area" option.
6. Save and close the editor window for the Menu Group.

5.8.3 Permission Groups

A permission group can contain a list of areas, area lists, doors, door lists, menu groups and other permission groups from all of the accessible controllers within Integriti.

Instead of individually assigning the same individual permissions to every user, you can assign these permissions to a permission group. The permission group is then assigned to

users. Changing the permissions for all of the users with the same permission group is simple as the only change required is in the permission group.

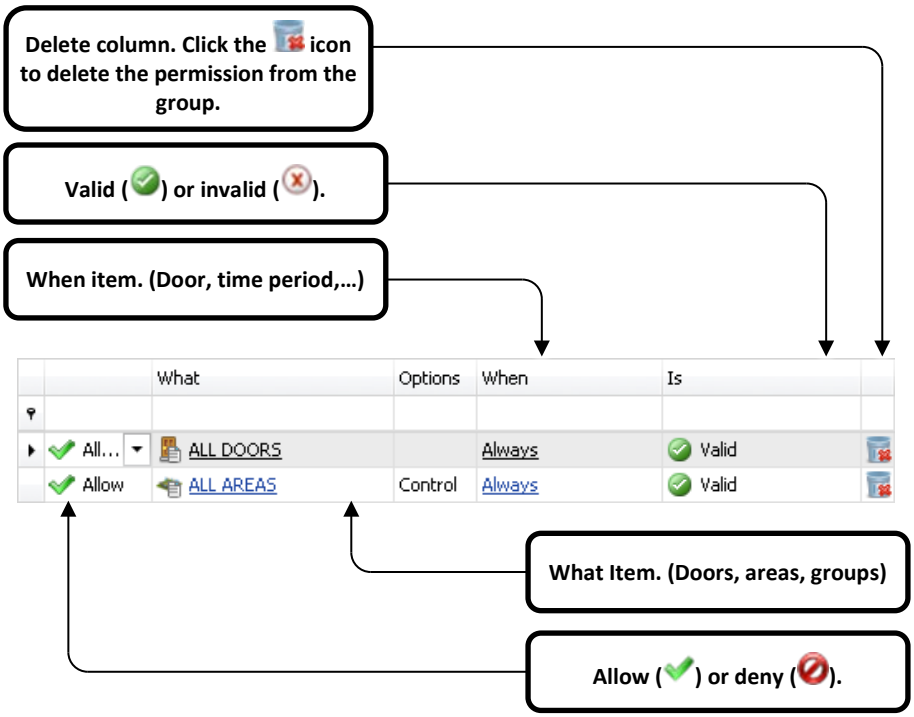


Figure 24

Permission Groups can have a maximum of 16 permissions.

Permission Groups can contain other permission groups but they are not permitted to create cyclic references.

Permission Groups can only go 4 levels deep from the top level entity.

Example:

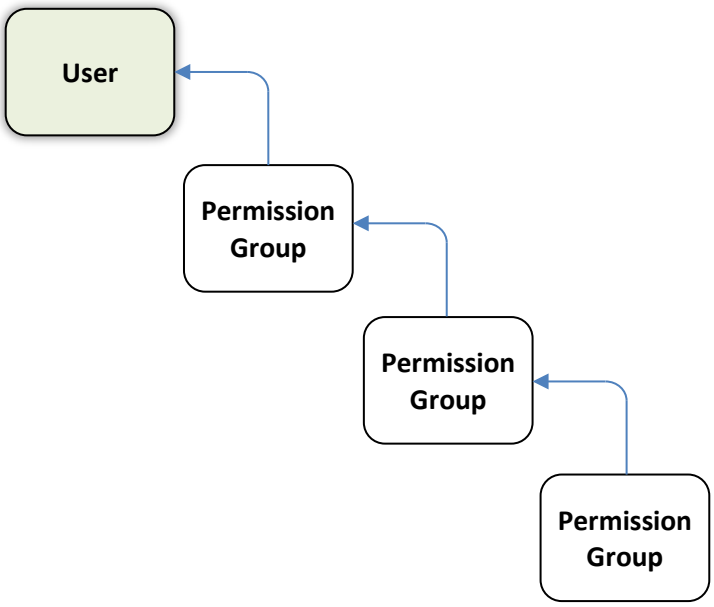


Figure 25

5.8.3.1 Using Allow and Deny permissions

Most permission groups will only contain 'allow' permissions as they are created for a large group of users that need these permissions assigned to them. There may be applications where the permission group could be assigned to other users but might include a few too many permissions.

This can be solved by assigning the permission group to the user and then adding an extra deny permission to filter out the permission.

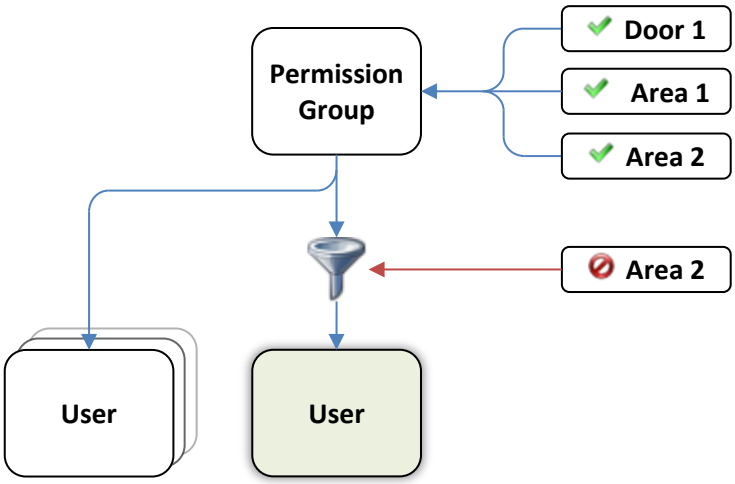


Figure 26

The highlighted user in the figure above has the same permission group as other users. However, the extra deny permission for area 2 will ensure the highlighted user only has access to Door 1 and Area 1.

	What	Options	When	Is
Deny	Area 6	Control	Always	Valid

Figure 27

1. Click on the Intruder tab followed by Permission Groups.
2. Click Add New. The Editor Window for a new permission group should appear.
3. Give the Permission Group a name.
4. On the right-hand side, click on Add. A new window should appear.
5. On the left side of the window, select Areas or Area Lists.

6. Select the area / area list on the right side and click OK.
7. The permission group will have a new row added to it under permissions. In the left-hand column, select whether the permission is allowing access or denying it.
8. The "What" column is the selected door, door list, area, etc…
9. Depending on the entity selected in the "What" column, the "Options" column may have a drop-down selection available. ***Figure 28*** is an example of the area control options.

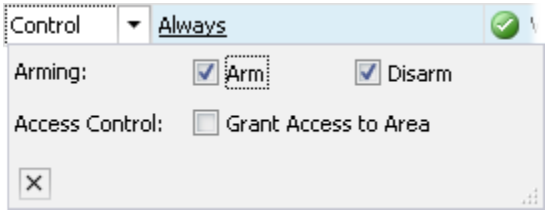


Figure 28

10. The "When" column is an optional qualifier for the permission itself. Its default value is "always". Permissions are often qualified by times (e.g. Time Periods or Holidays, but can also be qualified by many other things, like the state of doors or areas.
11. The "Is" column determines whether the optionally selected qualifier ("When") needs to be valid or invalid. Permission
12. Repeat steps **4** - **12** and make sure you add the Menu Group you created earlier. If additional areas or area lists are required, repeat the steps again accordingly.
13. Save and close the editor window for the Permission Group.

5.8.4 Users

Users within the Integriti management software are global. This means that the user record is only created the one time and individual permissions will tie the user to one or many controllers.

Qualify PIN codes may be used in association with cards for access control to provide a "something you have plus something you know" method of user authentication, in a card and PIN system. Many users can have the same Qualify PIN codes (just like an ATM card).

Security PIN codes are unique codes (passwords) used to identify users. These PIN codes are used to log in to the Integriti controller and perform various tasks. Because individual PIN codes are used to identify users at the controller, duplicate PIN codes are not permitted.

You can add individual permissions to a user by clicking the Add button within the User Programming dialog or if many users are likely to have the same permissions, permission groups should be used.

Permissions that can be added to a user are Doors, Door Lists, Areas, Area Lists, Menu Groups and Permission Groups.

Each User record has a default Permission Group. Permission Groups are an optional resource used for organisation of granular user permissions.

There are two methods used to create new users:

Creating a new user by duplicating an existing record:

If an existing user has the same configuration as the new user you are about to create then the easiest method of creating that new user is by clicking the existing user you want to duplicate followed by the Duplicate button. A new dialog window will appear with the new user details.

Assigning permissions to users…

1. Click on the Intruder tab followed by Users.
2. Click Add New. The Editor Window for a new user should appear.
3. Give the User a name.
4. Give the user a Security PIN.
   Users have two PIN codes. The Qualify PIN is used for access control purposes where a PIN qualification is required for access control. This number can be duplicated across the system.
   The purpose of the Security PIN is to log in to the terminal. This PIN code must be unique. If a duplicate PIN is entered, the PIN will not be allowed and the original owner of the PIN will be notified when they log in next that their PIN has been discovered.
5. On the right-hand side of the window, click on the ... to the right of Primary Permission Group.
   The primary permission group should contain most (if not all) of the required permissions for the user to control areas, doors and other items with relevant access from a terminal or external interface (e.g. web interface).
6. Select the Permission Group you created earlier from the window that appears and click OK.
   In cases where the primary permission group does not cover all of the required permissions for the user, extra permissions can be used to give additional permissions or deny permissions that were allowed but not required within the primary permission group.
7. Save and close the editor window for the User.

5.9 Using the intrusion system

5.9.1 Arming / Disarming…

5.9.1.1 Terminal access

Arming an area from the terminal…

1. Enter your PIN followed by OK: **[0], [1], [Ok]**
2. Go in to the area menu: **[Menu], [0]**
3. Use the up/down directional arrows to select an area: **[▲] / [▼]**
4. Turn the area on by pressing ON: **[On]**

5.9.1.2 Software access

Arming Areas…

1. Click on the Intruder tab followed by Areas.

- Method 1
  2. Right-click an area from the list.
  3. Click Arm or Disarm.
- Method 2
  2. Double-click the area from the list.
  3. Click Arm or Disarm in the toolbar.

Arming Area Lists…

1. Click on the Intruder tab followed by Area Lists.

- Method 1
  2. Right-click an area from the list.
  3. Click Arm or Disarm.
- Method 2
  2. Double-click the area from the list.
  3. Click Arm or Disarm in the toolbar.

24 Hour Areas…

Arming and disarming 24 hour areas is the same as the procedures listed above for arming and disarming areas.

5.9.2 Isolating

There are three isolation options available, isolate, sticky isolate and de-isolate. When an input is isolated its states are ignored.

Isolating an input will result in states of that input being ignored until any area that the input is associated with is disarmed.

Sticky Isolation is more permanent. By sticky isolating an input, the input will remain isolated until something or someone de-isolates it.

Isolating the input…

1. Click on the Intruder tab followed by Inputs.

- Method 1
  2. Right-click an input from the list.
  3. Click Isolate, Sticky Isolate or De-Isolate.
- Method 2
  4. Double-click the input from the list.
  5. Click Isolate, Sticky Isolate or De-Isolate in the toolbar.

5.10 Advanced

5.10.1 Auto arm / disarm by Time Period

Automatic arming and disarming of an area can be achieved by using named actions. You will need to create a time period defining the when the area will automatically arm and/or disarm before creating the named action.

Creating a Time Period…

1. Click on the Home tab followed by Time Periods.
2. Click Add New. The Editor Window for a new Time Period should appear.
3. Give the Time Period a name.

Under the Time Periods tab…

4. Click on Add to create a new row for the Time Period.

5. Click on the Start Time and enter the time that the area should arm.
6. Click on the End Time and enter the time that the area should disarm.
7. Click on the days which this time should apply to. Note that you can enter any number of start / stop time pairs and that these can occur on different days if desired (e.g. 9am – 12pm and 1pm to 5 pm on weekdays and 9am to 12:30 pm Saturday)
8. If this time is to ignore holidays then tick the Ignore Holidays check box at the end of the row.
9. Save and close the editor window for the Time Period.

Creating a Named Action…

1. Click on the Automation tab followed by Named Actions.
2. Click Add New. The Editor Window for a new Named Action should appear.
3. Give the Named Action a name.
4. On the right-hand side under Properties.
5. Expand-out Action.
   a. Click on the drop-down arrow to the right of Action to Take.
   b. Select Control Area from the list that appears.
   c. Click on the ··· to the right of the Area field to open the Area selection window.
   d. Select the Area from the list and click OK.
6. Expand-out Optional Trigger.
   a. Click on the ··· to the right of the Entity field to open the Entity selection window.
   b. Click on Time Qualifiers on the left side of the window.
   c. Select the Time Period that was created earlier from the list and click OK.
7. Save and close the editor window for the Time Period.

5.10.2 Defer area arming

Defer area arming is used in applications where automatic re-arming of an area is required to ensure an area remains secure. Users with defer arming enabled will be able to disarm areas but will start a timer that when expired will re-arm said area. This is also often used as an alarm in a lone worker scenario.

The following procedure assumes that an area has already been created and a user has access to this area.

Enabling Defer arming for the Area…

1. Click on the Home tab followed by Areas.
2. Double-click the area to enable defer arming on. The Editor Window for the area should appear.
3. On the right-hand side under Properties.
4. Expand-out General.
   a. Tick the Defer Area check box.
   b. Change the Defer Time to an appropriate value. Make sure you factor in the exit delay time for the area (if any).
5. Save and close the editor window for the Area.

Enable Defer arming for the Menu Group…

1. Click on the Intruder tab followed by Menu Groups.
2. Double-click the Menu Group given to the users that have permissions to disarm the area to be Defer armed. The Editor Window for the Menu Group should appear.
3. On the right-hand side under Properties.
4. Expand-out Area Control Permissions.
   a. Tick the Initiate Defer check box.
5. Save and close the editor window for the Menu Group.

5.10.3 Process Groups

Defining how an Input will be actioned in each Area is primarily done by allocating an appropriate Process Group to every Input in each Area that it is assigned to. Process Group programming includes defining the Input states (Seal/Alarm/Tamper/Isolate/…) that will be recognised, Entry/Exit delay processing options, Reporting & message options, and Auxiliary and Siren control options.

Figure 29

A large number of predefined process groups exists (see 'Default entities') for common use cases or you can create your own process group if unusual functionality is desired.

5.10.4 24 Hour Areas

Each individual area has its own 24 hour area. The 24 hour area is for inputs using a process group with the Process 24 Hour option set.

Normally, zone inputs and system inputs that require the alarm condition to be processed 24 hours a day (e.g. Smoke detectors, duress buttons, LAN communications problems, AC failure, etc…) must be assigned to an area that is always turned on.

Inputs associated with an area using the process group option “Process 24 Hour” allows a zone input alarm to be processed in an area that is off; or a system input alarm to be processed as an alarm rather than a tamper in an area that is off. If the process group option “Process 24 Hour” is set, then an alarm condition on the zone/system input is processed as an alarm even if the area is turned off.

This option allows for 24 Hour alarm inputs such as fire, duress, emergency, etc… to be assigned to the same area as other inputs (e.g. intruder alarms) that are only processed when the area is on.

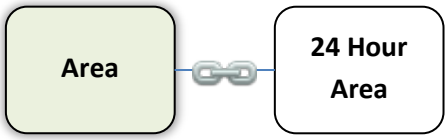


Figure 30

6 Setting up an Access System

The following will step you through what is required to commission a basic access control system.
It is assumed that the operator is logged in to the System Designer. An Integriti controller with the necessary modules attached should already be online, communicating with the server.
The instructions provided are based on the default layout.

6.1 Introduction and programming summary

The Integriti range of products integrates Access Control, Security Management and Building Automation. Access Control functionality and Building Automation operations can be kept completely separate from Security Management or can be fully integrated, if desired. Access Control operation is designed around the concept of Doors. The system simply determines which Users are allowed to use which Doors, at which times and with which options or restrictions.
Security Management operation is designed around the concept of Areas. Both Access Control and Security come together at Doors. For each Door in the system, one side is defined as the "outside" Area and the other side as the "inside" Area. Each Door can optionally be programmed as to which Area is on the outside and/or inside of the Door. If Area/s are programmed at a Door, then access at that Door will also be controlled by security considerations (via Areas).
e.g.

1. A User requiring access at a Door may be denied access because the Area they are about to enter is turned on, and they are not allowed to turn that Area off. If the User was allowed to turn that Area OFF then this may be done automatically on un-locking the Door, if programmed.
2. A User requesting access at a Door may be denied because the system has not seen the User leave the Area they are attempting to enter (Anti-Passback).

Doors

When designing an access system, Doors are the logical place to start. Each Door is numbered from Door 001 (D001), to the maximum available on your system. Each Door is individually programmed to define the functionality (via an Access Group) and the related Area/s, Auxiliaries and Timers, etc.

Access Modules

These Modules are required whenever access Cards are required, such as Proximity, Wiegand, Mag swipe, etc.

- Single Door Access Modules can control 1 Door with an Entry Reader.
- 2 Door Access Modules can control either 1 Door fitted with Entry and Exit Readers OR 2 Doors with Entry Readers.
- Intelligent 4 Door Access Modules can control 4 Doors with Entry and/or Exit Readers for all 4 Doors.

Each Access Module is individually programmed to define the Door/s controlled, Off-line operation, Zone input and Auxiliary options, Area control options and the direction (in or out), format, read mode, etc. for each Reader.

LCD Terminals

LCD Terminals can be used for Door Access Control if access to a Door is to be gained via a PIN code. Each Terminal may be individually programmed to define the Door controlled, Zone input & Auxiliary options & the direction (in or out).

Access Groups when Applied to Doors

Access Groups are a set of options that can be applied as a group to a Door. The typical system may have up to 32 Access Groups (depending upon system configuration) and each group may be individually programmed. A Door is assigned one of these Access Groups to use in determining the basic access control at the Door. The basic options that can be programmed for each Access Group are the modes of operation for Entry and Exit readers, Anti-passback options, REN/REX button options, Area control options, etc.

Time Periods

A Time Period can be used by any programming item that needs to be made Valid/Invalid according to the time of day and/or day of the week. A Time Period, once programmed, can be assigned to more than one item.

Holidays

A holiday comprises a start date and an end date and is used to set specified Time Period in-valid when a holiday occurs.
Each holiday can be defined as to which Time Period it will effect.

Programming summary

This section will take you through the creation of a basic access control system.

- Card template
- Door configuration
    - Reader module selection
    - Door types
- Reader module configuration
- User access permissions
    - Door lists
    - Permission Groups
    - Menu Groups
    - Credentials

6.2 Card Template

In cases where proximity technologies are used, a card template is required to define how the data on the proximity device will be interpreted. Card Templates also store the Site Code.

Creating a card template…

1. Click on the Access Control tab followed by Card Templates.
2. Click Add New. The Editor Window for a new Card Template should appear.
3. Give the Card Template a name.
4. On the right-hand side under Properties.
5. Expand-out Card Format.
   a. Click on the ··· to the right of the Format field to open the Card Format selection window.
   b. Select the Card Format from the list and click OK.
6. Expand-out Site Code.
   a. Enter the Site Code in decimal or hexadecimal in either one of the Number fields.
7. Save and close the editor window for the Card Template.

6.3 Door configuration

Creating a door…

1. Click on the Access Control tab followed by Doors.
2. Click Add New. The Editor Window for a new Door should appear.
3. Give the Door a name.

Under the Door Programming tab…

4. Click on the ··· to the right of the Module field to open the Reader Module selection window.
5. Select the Reader Module from the list and click OK.
6. Click on the ▾ to the right of the Relay field and select the desired lock relay from the list.
7. Click on the ▾ to the right of the Door Type field and select the desired door type from the list.
8. Under the Outside heading
   a. Click on the ▾ to the right of the Reader field and select the desired reader (or PIN device) from the list.

9. If you have chosen an Internal (Read In / Read Out Door) you will want to set up the internal reader or PIN Device as well.
10. Save and close the editor window for the Door.

6.4 Reader module configuration

Reader modules usually require little or no configuration changes. Most of the programming had been taken care of when the Door was created and assigned to the reader module.

Reader Module configuration…

1. Click on the Access Control tab followed by Reader.
2. Double-click a Reader Module. The Editor Window for the Reader Module should appear.
3. Give the Reader Module a name.
4. On the right-hand side under Properties.
5. Expand-out Readers followed by Reader 1.
   a. Click on the ··· to the right of the Card Format field to open the Card Format selection window.
   b. Select the Card Format from the list and click OK.
6. Save and close the editor window for the Reader Module.

6.5 User access permissions

6.5.1 Door Lists

Creating a Door List…

1. Click on the Access Control tab followed by Door Lists.
2. Click Add New. The Editor Window for a new Door List should appear.
3. Give the Door List a name.

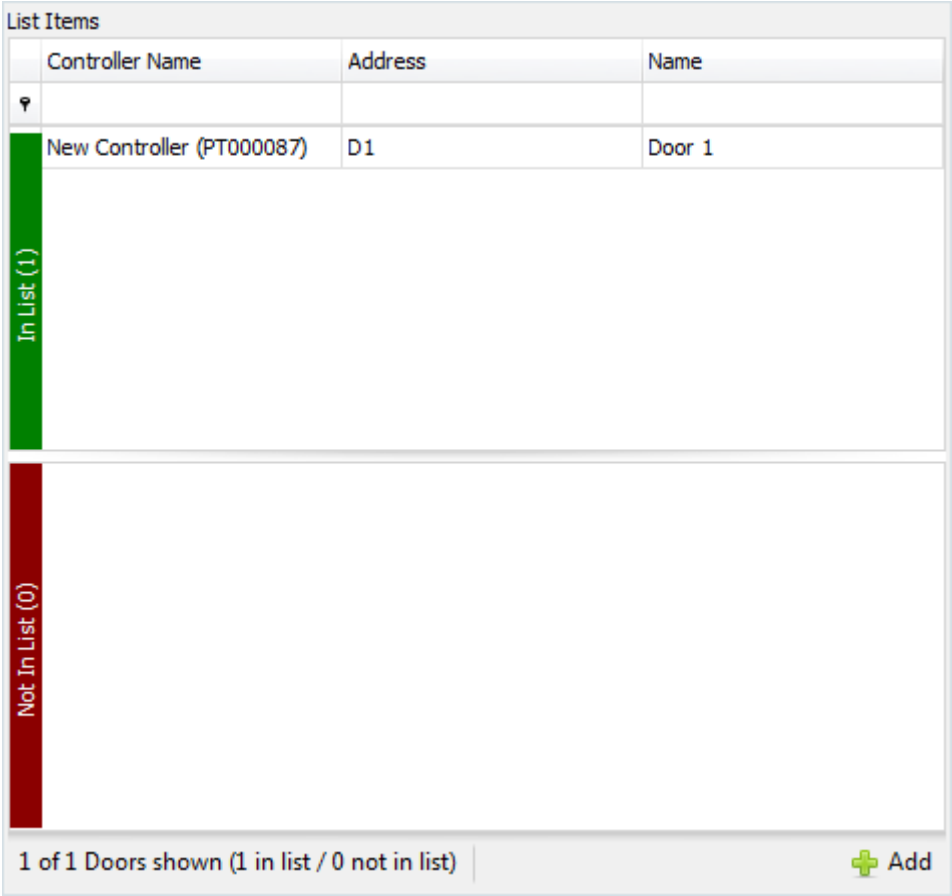


Figure 31

4. Items in the top section of the window are in the Door List. Items in the bottom section are not. Double click items to move them from one section to the other.
5. Save and close the editor window for the Door List.

6.5.2 Menu Groups

Menu Groups…

1. Click on the Access Control tab followed by Menu Groups.
2. Click Add New. The Editor Window for a new menu group should appear.
3. Give the Permission Group a name.
4. On the right-hand side under Properties.
5. Expand-out Main Menu Items.
   a. Tick the “Access” option.
6. Save and close the editor window for the Menu Group.

6.5.3 Permission Groups

Creating Permission Groups…

1. Click on the Access Control tab followed by Permission Groups.
2. Click Add New. The Editor Window for a new permission group should appear.
3. Give the Permission Group a name.
4. On the right-hand side, click on Add. A new window should appear.
5. On the left side of the window, select Doors or Door Lists.
6. Select the Door / Door List on the right side and click OK.
7. The permission group will have a new row added to it under permissions. In the left-hand column, select whether the permission is allowing access or denying it.
8. The "What" column is the selected door, door list, area, etc…
9. Depending on the entity selected in the "What" column, the "Options" column may have a drop-down selection available. ***Figure 32*** is an example of the Door control options.

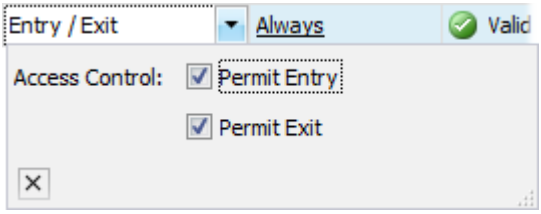


Figure 32

10. The "When" column is an optional qualifier for the permission itself. Its default value is always.
11. The "Is" column determines whether the optionally selected qualifier ("When") needs to be valid or invalid.
12. The last column is a button to allow you to remove the individual permission. Double-click this if you want to remove the row.
13. Repeat steps **4** - **12** and make sure you add the Menu Group you created earlier. If additional areas or area lists are required, repeat the steps again accordingly.
14. Save and close the editor window for the Permission Group.

6.5.4 Credentials (Cards & RF fobs)

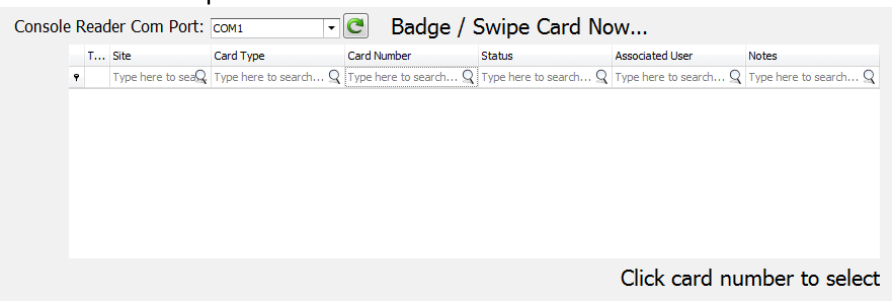
You can associate multiple credentials with a single user. A credential can be one of a number of things including but not limited to a swipe card, proximity card or wireless fob.

Assigning permissions to users…

1. Click on the Access Control tab followed by Users.
2. Click Add New. The Editor Window for a new user should appear.
3. Give the User a name.
4. Give the user a Security PIN.
5. On the right-hand side of the window, click on the ... to the right of Primary Permission Group.
6. Select the Permission Group you created earlier from the window that appears and click OK.

To add a new credential to a user:

- Click on the Cards tab for swipe/proximity cards or RF Remotes tab for wireless devices.
- If you selected the Cards tab you have 3 options for adding a credential to the user record.
  - Using Acquire Card...
    1. Clicking Acquire Card... will open a new window where you have the option to select cards from Review or from a Console Reader. Select one of these two items.
    2. If you selected Console Reader, You might need to change the serial communications port.



  - Using Enter Number ...
    1. Selecting this option allows you to directly enter the card number.

Figure 33

2. Select the desired card template.
3. Enter the card number.
4. Click OK.

- Using Existing Card...
  1. Clicking this button will open a new window. The default view will display all of the Available Cards. By clicking All Cards, you will be able to see cards belonging to users.
  2. Select a card from the list and click OK.

> *Selecting a card that has already been allocated to a user will generate a synchronisation warning (users can not share the same card).To resolve this issue, go to the other user record and remove the card from the Cards list.*

- If you selected the RF Remotes tab.
  - Using From Review...
    1. A find remote window will appear.
    2. Once the window is open, press a button on the remote. It should then appear in the list.
    3. Double-click the remote in the list.
  - Using Existing Remote...
    1. A find remote window will appear.
    2. Select a remote from the list and click OK.

Removing a credential from a user is as simple as double-clicking on the button to the right of the credential. Click the button to commit these changes.

7. Save and close the editor window for the User.

6.6 Using the access control system

6.6.1 Locking / Unlocking

Locking Doors…

1. Click on the Access Control tab followed by Doors.

- Method 1
  2. Right-click an door from the list.
  3. Click Unlock, Unlock (Timed) or Lock.
- Method 2
  2. Double-click the door from the list.
  3. Click Unlock, Unlock (Timed) or Lock in the toolbar.

Unlocking Doors…

1. Click on the Access Control tab followed by Door Lists.

- Method 1
  2. Right-click an door from the list.
  3. Click Unlock, Unlock (Timed) or Lock.
- Method 2
  2. Double-click the door from the list.
  3. Click Unlock, Unlock (Timed) or Lock in the toolbar.

6.7 Advanced access control

6.7.1 Time based door control

Timed door access requires the configuration of a Time Period and a Named Action. The Named Action will use the Time Period as an optional trigger to control the Door (or Door List).

Creating a Time Period…

1. Click on the Home tab followed by Time Periods.
2. Click Add New. The Editor Window for a new Time Period should appear.
3. Give the Time Period a name.
   See "Time Periods" for details on setting up a time period.

Under the Time Periods tab…

4. Click on Add to create a new row for the Time Period.
5. Click on the Start Time and enter the time that the area should arm.
6. Click on the End Time and enter the time that the area should disarm.
7. Click on the days which this time should apply to.
8. If this time is to ignore holidays then tick the Ignore Holidays check box at the end of the row.
9. Save and close the editor window for the Time Period.

Creating a Named Action…

1. Click on the Automation tab followed by Named Actions.
2. Click Add New. The Editor Window for a new Named Action should appear.
3. Give the Named Action a name.
4. On the right-hand side under Properties.
5. Expand-out Action.
   a. Click on the drop-down arrow to the right of Action to Take.
   b. Select Control Door from the list that appears.
   c. Click on the ··· to the right of the Door field to open the Door selection window.
   d. Select the Door from the list and click OK.
6. Expand-out Optional Trigger.
   a. Click on the ··· to the right of the Entity field to open the Entity selection window.
   b. Click on Time Qualifiers on the left side of the window.
   c. Select the Time Period that was created earlier from the list and click OK.
7. Save and close the editor window for the Time Period.

6.7.2 Disabled access

To give a disabled user extended access to a door you will need to configure the Handicapped Unlock Time of the Door and change the User to a Handicapped User.

Change the Handicapped Unlock Time of a Door…

1. Click on the Access Control tab followed by Doors.
2. Double-click a Door to program. The Editor Window for the Door should appear.
3. On the right-hand side under Properties.

Under the Advanced tab…

4. Expand-out Advanced Door Configuration.
   a. Change the Handicapped Unlock Time.
5. Save and close the editor window for the Door.

Changing a User to a disabled User…

1. Click on the Access Control tab followed by Users.
2. Double-click a User to program. The Editor Window for the User should appear.
3. On the right-hand side under Properties.
4. Expand-out User Options.
   a. Click on Handicapped User.
5. Save and close the editor window for the Time Period.

7 Credentials

This section covers the creation and management of credentials. You can associate multiple credentials with a single user. A credential can be one of a number of things including but not limited to a swipe card, proximity card or wireless fob.

7.1 Card Format

Within each card format is a card type, and this will tell the reader how to operate, including whether to expect Magnetic card data or Wiegand card data, whether it needs to convert the raw data to site code, card number and issues number, or if it needs to hash or decrypt the card data. Some of these operations are done by the reader module and some by the control module. Different Card Types selected in the Card Format dialog of the software should display different fields where relevant, i.e. display site code bit lengths and offsets for Wiegand Custom Sitecodes and display Secure 40 scheme type for IR Secure 40.

All Card Formats that use a Wiegand type can also take a parameter called Wiegand Card Type. This can be N Bit meaning any bit length is allowed or it can be set to a particular bit length. N Bit will always return all the bits read. For fixed bit lengths, the behaviour varies between legacy Concept and new Integriti modules. For legacy modules, for cards equal to or longer than the bit length, it will return the first n bits, as if the card read were n bits long. If the card is shorter than the bit length, it is ignored. For Integriti modules if the card is not equal to the bit length, it is ignored completely.

Most of the common card formats have been added to the Integriti System Designer for convenience.

Card Types…

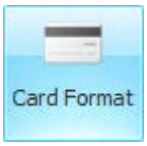
None	The Card Format will be unusable with this setting.
Wiegand Raw	For direct entry wiegand cards of any length. Credential is number of bits read followed by 11 bytes of data with the card data right justified and the rest of the filled padded with 0's. If no format is specified on the door then this is the format that will be used.

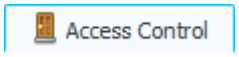
Wiegand Site	Allows user credentials to be entered as site code and card number providing the format is known for that user (i.e. HID 26 bit H10301), including migrations from Concept and other systems. Assumes that the bits that don't form the site code and card number (i.e. start and stop parity bits) conform to a manufacturer's specification that Inner Range was aware of at the time we implemented the SW/FW. There is an option in these formats called "encoding" which allows for different parity schemes than the standard one we assume from a particular card length, although none have been added as yet. All the underlying credentials are actually compared and stored as wiegand Raw.
Wiegand Custom Sitecode	Allows for site code formats unknown to Inner Range. This is now the recommended format when only one card format is used throughout the system. User credential stored is actually just the site code, card number and issue number, not the raw data. Parity and other unused bits are discarded and not compared.
Mag Raw 40	This magnetic swipe card format read the first 10 characters (40 bits) from a mag card, nibble swapping each byte (i.e. swapping each character pair). This allows for compatibility in migrations where Concept Mag Direct was used.
Mag Site	Reads mag cards in character mode. Like Wiegand Custom Sitecode allows user definable site code, except lengths and offsets are specified in characters instead of bits. Unlike IRMag, the cards are assumed to not be encrypted. Credentials are store as site code, not raw data.
Mag Hash 5	Reads the first 22 characters from a mag card and generates a 5 byte hash from this, using the same algorithm as the Concept "Credit Card" format.
IR Mag Swipe	Decrypts a Concept Secure Mag card and returns its site code, card number and issue number. Although site code parameters are user definable for this format, the decryption part will probably only work if it follows the IRMag Secure scheme.

IR Secure40	Decrypts an IR Secure 40 card and matches it on site code and card number. Only needs to be put in the card template of the user. If the reader is set to this format it will operate as a wiegand raw format. In the format the scheme in use must be chosen, whether Standard, Registered Site or Enterprise.
Mag Raw 88	Reads up to the first 22 characters of a mag card, until it gets an end or separator sentinel character. This usually reads financial cards as the number is written on them (no nibble swap) prepended with the number of bits read (4 per character) and 0's.
Mag Site (bits)	This format makes the reader return the binary data from the card instead of the characters. For most mag cards (i.e. financial cards) this is 4bits for the character and one bit of parity. This supports hypothetical cards where the site info is stored as binary data instead of characters
Wiegand 3K Raw	Reads the wiegand card data, removes the start bit and puts the data in a 5 byte field and left justifies that data. It then prepends the credential with "28000000000000" For instances, the 26bit wiegand card with binary data '1100111100000111101010100 0' (Wiegand Raw (26) = 1A00000000000000033C1EA8(hex)) would be read as per the next column. This helps migrations from concept direct entry wiegand systems where the start bit was not used (99% of all sites).

Table 3

Creating a new Card Format…

1. Open the 

panel from the 

tab.
2. Click the

button to create a new Card Format.
3. Give the Card Format a new name and enter any necessary notes in the Notes field.
4. Expand-out Options and select the desired Card Type from the drop down list. Refer to Table 3 for details.
5. Expand-out Card Programming and select the bit length of the card in the Wiegand Card Type field. If the bit length is variable or unknown, 'N Bit' can be used.
6. Expand-out Site Code Parameters (Card Type dependant).
   a. Enter the bit length of the card format in the Total Bits field.
   b. Enter the offset from the first bit where the site code begins in the bit stream.
   c. Enter the total bit length of the site code in the Site Code Length field.
   d. Enter the offset from the first bit where the card number begins in the bit stream.

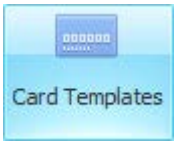
e. Enter the total bit length of the card number in the Card Number Length field.
f. Enter the offset from the first bit where the card issue number begins in the bit stream.
g. Enter the total bit length of the card issue number in the Issue Number Length field.
h. If the selected Card Type is Secure 40, there are three schemes to choose from:
   - Standard
   - Registered Site
   - Enterprise

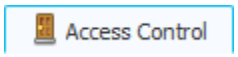
7. Save and close the editor window for the Communications Task.

7.2 Card Templates

Card Templates have been created to make life easier when adding new credentials to the Integriti system.

To create a new Card Template…

1. Open the 

panel from the 

tab.

2. Click the

button to create a new Card Template.

3. Give the Card Format a new name and enter any necessary notes in the Notes field.

4. Expand-out Card Format and select the desired Card Format for this Card Template.

5. Expand-out Site Code and enter the Site Code for the credentials you will be adding to the system in either binary or decimal.

6. Save and close the editor window for the Communications Task.

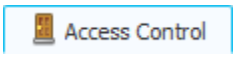
7.3 Cards

User credential (proximity card, swipe card, fob…) programming only requires a card template selection and data. The data field commonly refers to the card number (or issue number) of the credential that is to be issued to the user.

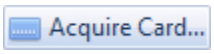
Card templates are created using a card format. Card formats contain detail explaining where data is situated on a card.

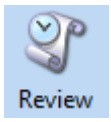
To add a new credential to a user:

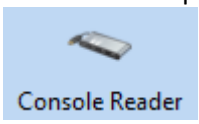
1. Open the

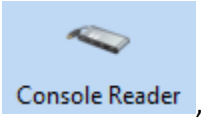
panel from the 

tab
2. Double-click a user for editing.
3. Click on the

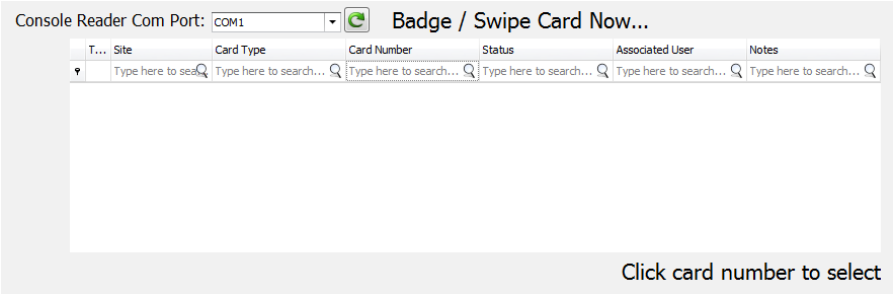
tab for swipe/proximity cards
   - Click 

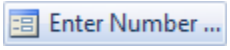
to open the card acquire window.
     a. Click on 

or 

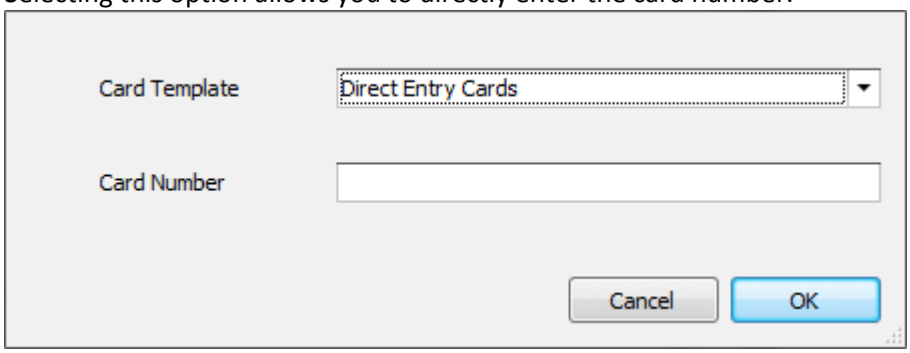
to select your card acquisition source.
        - If you selected 

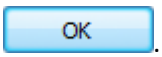
, You might need to change the serial communications port.



     b. Present the card to a reader attached to the controller (if you selected Review) or to the enrolment station.
     c. Double-click the card that appears in the list.
   - Click 

for manual card entry.
     a. Selecting this option allows you to directly enter the card number.



     b. Select the desired card template.
     c. Enter the card number.
     d. Click 

.
   - Click on

to select an existing card in the system. A new card selection window will appear.

a. The default view will display all of the Available Cards. By clicking All Cards, you will be able to see cards belonging to users.

b. Select a card from the list and click OK.

> *Selecting a card that has already been allocated to a user will generate a synchronisation warning (users can not share the same card).To resolve this issue, go to the other user record and remove the card from the Cards list.*

- Removing a credential from a user is as simple as double-clicking on the button to the right of the credential.

4. Click the button to commit these changes.

7.4 RF Remote Templates

RF Remote Templates map the various messages sent from the RF remote to actions, inputs and area control on the Integriti controller.

To map a button, you will need to observe the messages displayed in review for information on what button was pressed. RF expanders will need to have the option 'Log RF Remote Details' ticked.

To enable logging on the RF expander…

1. Open the Radio Expander panel from the Hardware tab.
2. Double-click the RF expander to open for editing.
3. Expand-out Misc.
4. Tick the option 'Log RF Remote Details'.
5. Save and close the editor window for the RF Expander.

Pressing buttons on the RF remote will result in review messages similar to the following:

```
Unknown User Paradox REM2 Prg1 button Unlicensed…
Unknown User Paradox REM2 Arm1 button Unlicensed…
```

In the two example review lines above, you can see Prg1 and Arm1. These labels indicate the buttons being pressed. Review text containing 'Prg' indicate actions. e.g. Prg1 = Action1, Prg2 = Action2, etc…

Creating a new RF Remote Template…

1. Open the RF Remote Templates panel from the Access Control tab.

2. Click the Add New button to create a new RF Remote Template.
3. Give the RF Remote Template a new name and enter any necessary notes in the Notes field.
4. Expand-out Button Definitions
   a. Drop-down actions 1-4 and select an action as required for each button available on the RF Remote.
   b. Click on the ... to the right of the Area fields to open the Area selection window.
   c. Select the Area from the list and click OK.
   d. If the RF Remote reports input states, click on the ... to the right of the Input fields to open the Input selection window.
      - Inputs mapped using RF Remote Templates should have the option 'Ignore Physical Input' set.
5. Paradox REM3 RF Remotes support PIN codes. There are three options available for these remotes. Expand-out Options.
   a. Ticking 'Needs 6 Digits' sets a requirement for all PIN codes used with a REM3 must be 6 digits.
   b. Ticking 'Needs PIB for Programming' sets a requirement for PIN entry to control Actions (Action 1-4).
   c. Ticking 'Needs PIN for Area On/Off' sets a requirement for PIN entry to control Areas (Area 1-2).
6. Save and close the editor window for the RF Remote Template.

7.5 RF Remotes

There are two methods available for creating RF remotes. The simplest method is to create a new RF remote by enrolling a remote to a user. The alternative method is manual entry.

RF Remotes need to have an RF Remote Template.

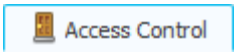
To create a new RF Remote (enrolling to a user)…

1. Open the Users panel from the Access Control tab
2. Double-click a user for editing (The user you want to enrol the RF Remote to).
3. Click on the RF Remotes tab for wireless devices.
4. Click on From Review... to open the find remote window.
5. Once the window is open, press a button on the remote. It should then appear in the list.
6. Double-click the remote in the list.
   - Alternatively you can use Existing Remote... to open a list of enrolled RF Remotes.
   - Select a remote from the list and click OK.
7. Save and close the editor window for the User.

Selecting a remote that has already been allocated to a user will generate a synchronisation warning (users can not share the same remote).To resolve this issue, go to the other user record and remove the remote.

To create a new RF Remote (manual entry)…

1. Open the

panel from the 

tab
2. Click the

button to create a new RF Remote.
3. Give the RF Remote a new name and enter any necessary notes in the Notes field.
4. Expand-out Credential.
5. Enter the unique serial number of the remote in the Remote Data field.
6. Click on the ··· to the right of Remote Template.
7. Select the appropriate RF Remote Template from the list and click OK.
8. Save and close the editor window for the RF Remote.

The unique ID of the RF Remote can be determined by looking at the end of a RF Remote review message. Pressing a button on the RF Remote will produce a review event similar to the following:

```
Unknown Paradox Door Alarm at C3K-RadioExp: 01 Sig=07
ID=00000B2B
```

You will need to ensure 'Log RF Remote Details' is enabled on the RF Expander. Details on how to set this option have been explained in the section titled 'RF Remote Templates'.

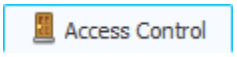
7.6 Cards

User credential (proximity card, swipe card, fob…) programming only requires a card template selection and data. The data field commonly refers to the card number (or issue number) of the credential that is to be issued to the user.

Card templates are created using a card format. Card formats contain detail explaining where data is situated on a card.

To add a new credential to a user:

1. Open the

panel from the 

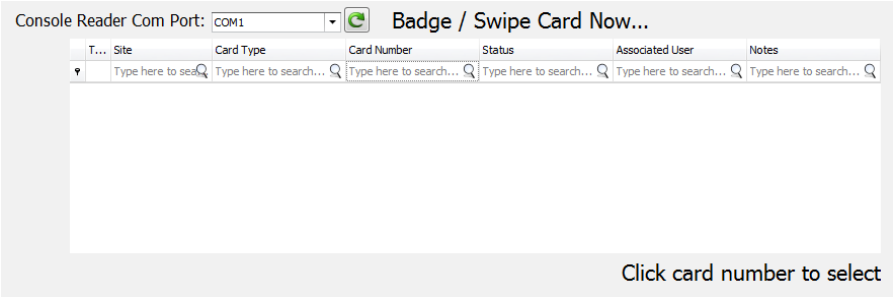
tab
2. Double-click a user for editing.

3. Click on the Cards tab for swipe/proximity cards

- Click Acquire Card... to open the card acquire window.

  a. Click on Review or Console Reader to select your card acquisition source.

  - If you selected Console Reader, You might need to change the serial communications port.

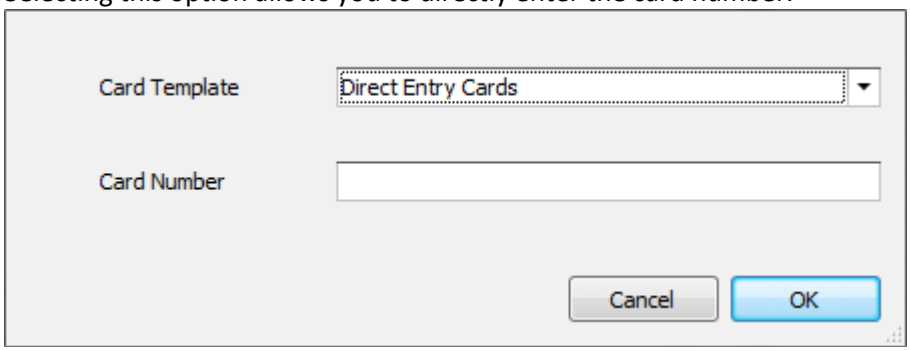


  b. Present the card to a reader attached to the controller (if you selected Review) or to the enrolment station.

  c. Double-click the card that appears in the list.

- Click Enter Number ... for manual card entry.

  e. Selecting this option allows you to directly enter the card number.



  f. Select the desired card template.

  g. Enter the card number.

  h. Click OK.

- Click on Existing Card... to select an existing card in the system. A new card selection window will appear.

  c. The default view will display all of the Available Cards. By clicking All Cards, you will be able to see cards belonging to users.

  d. Select a card from the list and click OK.

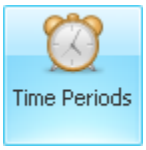
Selecting a card that has already been allocated to a user will generate a synchronisation warning (users can not share the same card).To resolve this issue, go to the other user record and remove the card from the Cards list.

- Removing a credential from a user is as simple as double-clicking on the button to the right of the credential.

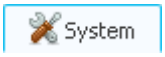
4. Click the button to commit these changes.

8 Scheduling

8.1 Time Periods



The time periods panel is accessible from the

and 

tabs.

Time periods are most commonly used as the “when” in permissions, but can also be used in named actions.

Time periods are created by adding a schedule period by clicking the

button directly below the schedule pane.

- Overlapping schedule periods do not impact one another.
- Only Holidays associated with the Time Period will have an effect on the validity of the Schedule Periods.
- Time Periods without the Holidays check box ticked will be invalidated when the Holidays associated with the Time Period are valid.

To create a new Time Period:

1. Open the time periods panel.
2. Click the Add New icon in the time periods Panel.
3. Give the Time Period a name and add any necessary details in the notes field.
4. Click the Add button and change the parameters of the newly created schedule period.
   - Ticking the Ignore Holidays option will cause any of the Holidays specified in the Holidays tab of this Time Period to be ignored.
5. Click on the Holidays tab followed by Add to add holidays to the Time Period.
6. Click the button and close the dialog.

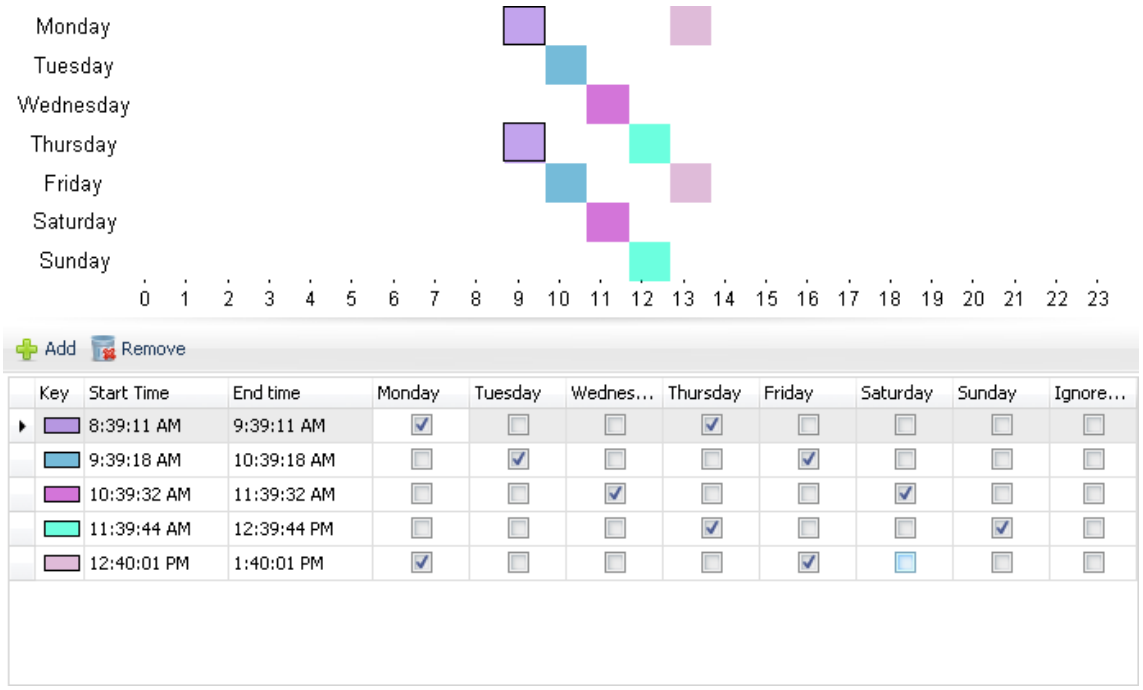
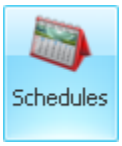
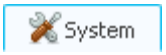


Figure 34

8.2 Schedules



The schedules panel is accessible from the 

tab.

Schedules allow for reoccurring events. Schedules can be set to trigger hourly, daily, weekly, monthly, yearly or weekday of month.

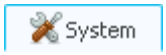
To create a new Schedule:

1. Open the schedules panel.
2. Click the

button in the schedules panel.
3. Give the Schedule a Name and add any necessary details in the Notes field.
4. If UTC time is used, tick the UTC check box.
5. Set the recurrence of the schedule as required.
6. Change the start date to that of the schedule.
7. Change the end date to that of the schedule.
8. Tick the days that the schedule is to be valid.
9. Click the button and close the dialog.

8.3 Holidays

The holidays panel is accessible from the

and 

tabs.

To create a new Holiday:

1. Open the holidays panel.
2. Click the

button in the holidays Panel.
3. Give the Holiday a Name and add any necessary details in the Notes field.
4. Change the start time and date to that of the holiday.
5. Change the end time and date to that of the holiday.
   – or –
   Change the Duration (Days) to the appropriate number of days the holiday is to last for.
6. If the holiday is to recur annually, tick the Recur Annually check box.
7. If UTC time is used, tick the UTC check box.
8. Click the button and close the dialog.

8.4 Scheduled Tasks

Scheduled tasks contain one or many actions that can be executed sequentially, parallel or a combination of both on predefined triggers.

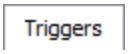
Scheduled Tasks are for automated actions in response to a trigger (which can be either time or review messages).

There are 15 action types to choose from:

- Backup Database
- Control Workstation
- Controller Action
- Escalate Alert
- Execute Code
- Execute Report
- Invoke Integrated Device Command
- Log Review
- Parallel Task List
- Pause
- Run External Program
- Send Communication Message
- Send Integrated Device Event
- Sequential Task List
- Synchronise Controller Time

Detail on these actions can be found in the section titled “Action types” in the appendix.

Triggers can be a combination of either Time or Review. Click

under the 

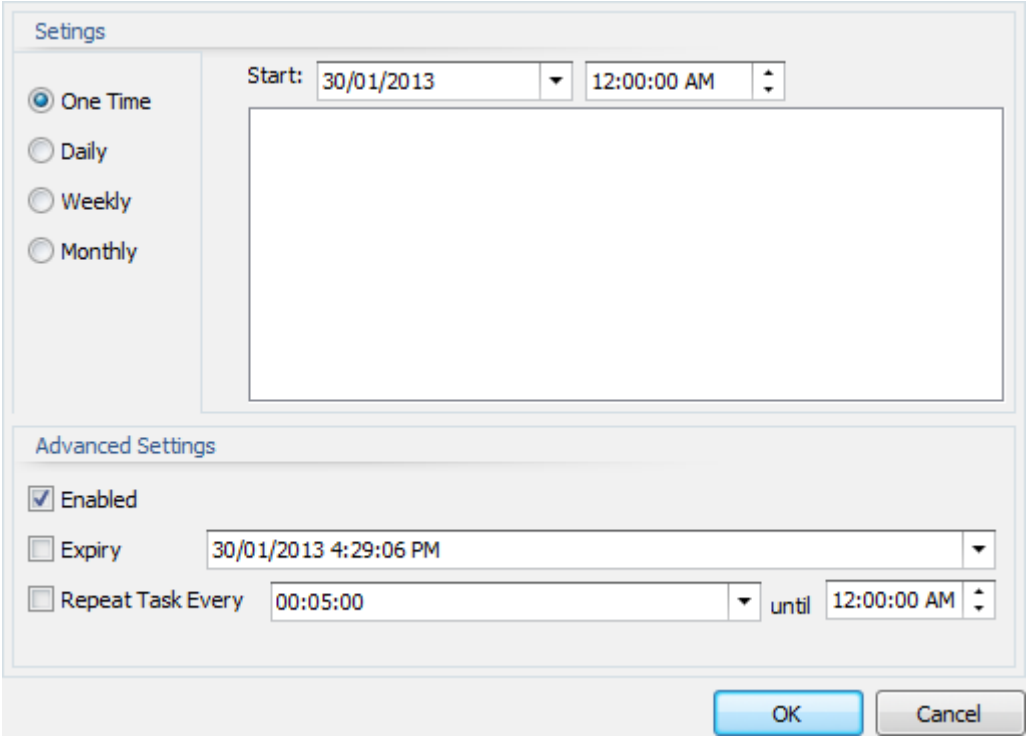
tab to add a new trigger.

Time Trigger

Time based triggers can be configured to activate once, daily, weekly or monthly.

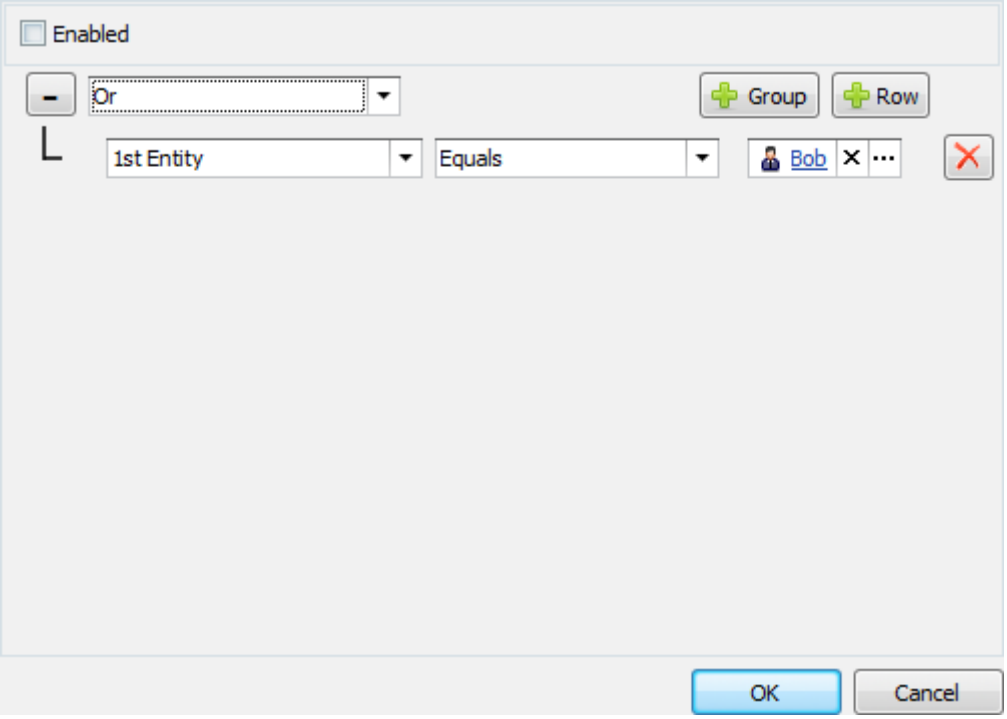
Time based triggers will only operate when the Enabled checkbox is ticked.

An optional configurable expiry can be set. The expiry can be adjusted to the minute.



Review Trigger

To add a new criteria to the Review Trigger, click the button. The first drop down list specifies the review component to test against. The Second drop down list specifies the criteria operator. The last drop down list is the operand value.



Creating Scheduled Tasks…

1. Click on the Administration tab followed by Scheduled Tasks.
2. Click Add New to create a new Scheduled Task.
3. Give the Scheduled Task a Name and add any necessary details in the Notes field.
4. Specify an action to take if the task is already running.
   - Do Nothing – The Scheduled Task will not execute.
   - Run After Completion – If the Scheduled Task was triggered while it was already running at the Scheduled Task will re-run immediately after completion.
   - Run In Parallel – The Scheduled Task will run immediately regardless of whether the task was already running or not.
5. If required, tick the Retry On Fail check box.
   a. Specify the Maximum Retry Attempts. Leaving this value set at 0 will cause the Scheduled Task to retry until it passes.
6. Add one or many Time or Review based triggers.
7. Add one or many Actions to the Scheduled Task.

9 Automation

9.1 Counting Input Types

There are four input types to allow for scenarios where counting is required.

Inputs with the 'Count up' or 'Count Down' type will have their own count value. Whenever the input transitions to the 'Alarm' state, the input will count up or down depending on the input type selected. Count inputs can be any value from 0 to 65535.

The 'Previous Count Up' and 'Previous Count Down' types will change the count value of the nearest 'Count Up' or 'Count Down' input type with a lower ID. 'Previous Count Up' and 'Previous Count Down' types must be on the same module as the 'Count Up' / 'Count Down' input.

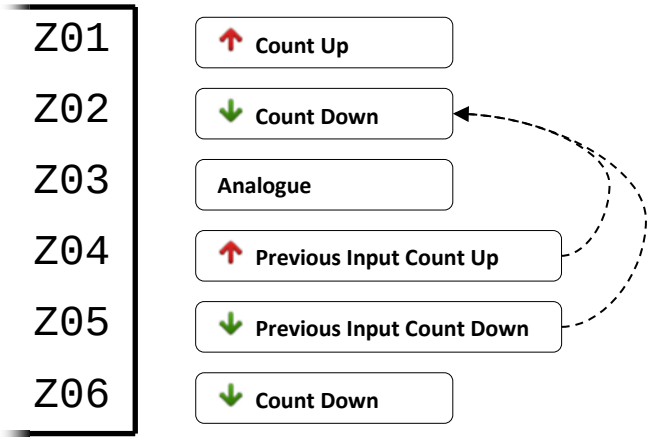


Figure 35

In the example above we can see that input 2 is affected by zones 4 and 5. Each time input 2 or 5 transitions to the alarm state, the count value of input 2 will decrease by 1. Each time input 4 transitions to the alarm state, input 2 will increase by 1.

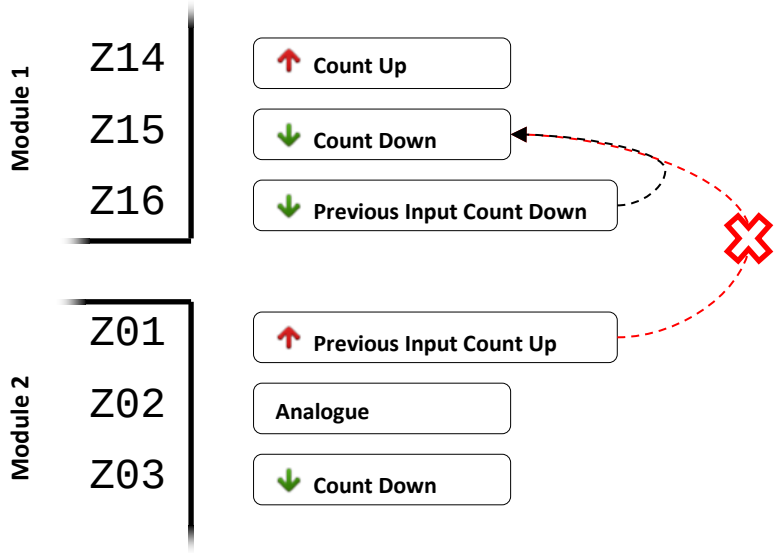


Figure 36

In the example above input 16 on module 1 will decrease the count of input 15 on module 1. However input 1 on module 2 will not increase the count of input 15 on module 2 because the inputs are not on the same module.

9.2 Auxiliaries

Auxiliaries are the digital outputs on the Integriti system. There are three different types of auxiliary that you can use.

Relay Output

Relay outputs are the most common and most practical of auxiliary output types. The relay output may provide an optional voltage out (jumper selection). The auxiliary relay ratings have different voltage and amperage ratings depending on the module used.

Open Collector

Open collector outputs are switched by a small semiconductor. . Open collector outputs are mainly found on Concept compatible LAN modules. As a result, the load can only be small. These types of outputs are good for LEDs and driving slave relays.

Phantom

Phantom auxiliaries are outputs that don't physically exist. They will still operate the same as a normal auxiliary. The Integriti controller has 30 phantom auxiliaries available unless expanded using UniBus relay expanders. LAN modules may also have auxiliaries available.

9.3 Auxiliary Lists

Auxiliary Lists can contain up to 16 auxiliaries. Auxiliary lists are particularly useful for applications where a number of auxiliaries may need to be controlled simultaneously.

9.4 Compound entities

Compound Entities represent the logical state of a collection of up to 8 entities. The state returned is a result of the logical relationship between them.

The logical relationship between entities is processed sequentially from lowest to highest.

Compound entities can be used to combine multiple controller entities for anything an entity is used as the source (e.g. as the "When" of a permission or permission group, the trigger for a named action, in an expression in a Macro).

Compound Entities can be used to combine multiple controller entities and trigger named actions (e.g. open a door, unsecure a floor, etc.).

Using Compound Entities to concatenate a time period and a schedule:

- Create a time period (e.g. "Opening Hours" 9:00 am to 5:00 pm Mon - Sat)
- Create a "never repeats" schedule that overlaps (e.g. "Extended Hours 1" 24/12/2013 4:50 p.m. to 10:00 p.m.).
  - Note: Don't start the schedule at the same minute that the time period expires as a race condition may ensue and an open door condition could get there just before a close door condition (for example).
- Create a compound entity (e.g. "Modified Trading hours" that is the OR of these two entities)
- Create a named action that performs the action you want (e.g. Control a door)
- Use the compound entity you created as the "Optional Trigger" for this action.

Note that to find the compound entity in the "Search for Entity of Named Action" window you will currently need to look in "Unfiltered Controller Items" and filter on either Name or ID.

In this way you can program up a named action with modified hours in advance.

If you chose, you could have more than 1 "Extended Hours" feature that occurred in the future.

Because you have set it up never to repeat, there's no need to clear these out after they've activated.

You can re-use them the next time you get a special event that you want to schedule.

In a similar way, Compound Entities can be used to combine multiple time periods, or time periods with other state (e.g. the state of an Aux).

Creating Compound Entities…

1. Click on the Automation tab followed by Compound Entities.
2. Click Add New. The Editor Window for a new Compound Entity should appear.
3. Give the Compound Entity a name.
4. On the right-hand side under Properties.
5. Expand-out Misc.
   a. Click on the ··· to the right of Entity 1.
   b. Select the entity from the window that appears and click OK.
   c. If the state of the entity needs to be inverted, click the Invert Entity 1 checkbox.
   d. Click on the ▾ to the right of Logical Relation 1.
   e. Select the relationship between entity 1 and entity 2 (none, AND, OR, XOR).
      - 'none' is only required if the entity is the last in the list.
   f. Repeat steps **a** - **f** for the remaining entities as required.
6. Save and close the editor window for the Compound Entity.

9.5 Named Actions

Named actions provide a means to perform an action on the controller. These actions can be controlled by the user or from a trigger (entity).

User access is controlled by Action Groups. Users with the appropriate Action Groups can view and control the Named Action.

Creating Named Actions…

1. Click on the Automation tab followed by Named Actions.
2. Click Add New. The Editor Window for a new Named Action should appear.
3. Give the Named Action a name.
4. On the right-hand side under Properties.
5. Expand-out Action and select an action to take from the drop-down list.
   More detail on Action types is available in the appendix.
6. If required, expand-out Optional Trigger.
7. Specify an optional trigger by clicking on the ellipsis to the right of Entity and select an entity from the list.
8. Optionally users can have direct control over Named Actions via the Terminal.
   a. Expand-out User Interface.
   b. Click on the drop-down list to the right of Interface Style and select the appropriate option based on the configured Action to Take.

c. If a Sense Entity is specified the state of the Named Action will reflect the state of the selected Sense Entity. If no entity is specified the state of the Named Action is determined by the entity controlled by the action.
d. Ticking the Invert Sense Entity will invert the reported state of the Named Action.
e. Allow Logged Off Access will allow terminal users to control the Named Action without logging in to the terminal.

9. Expand-out User Access followed by Action Groups.

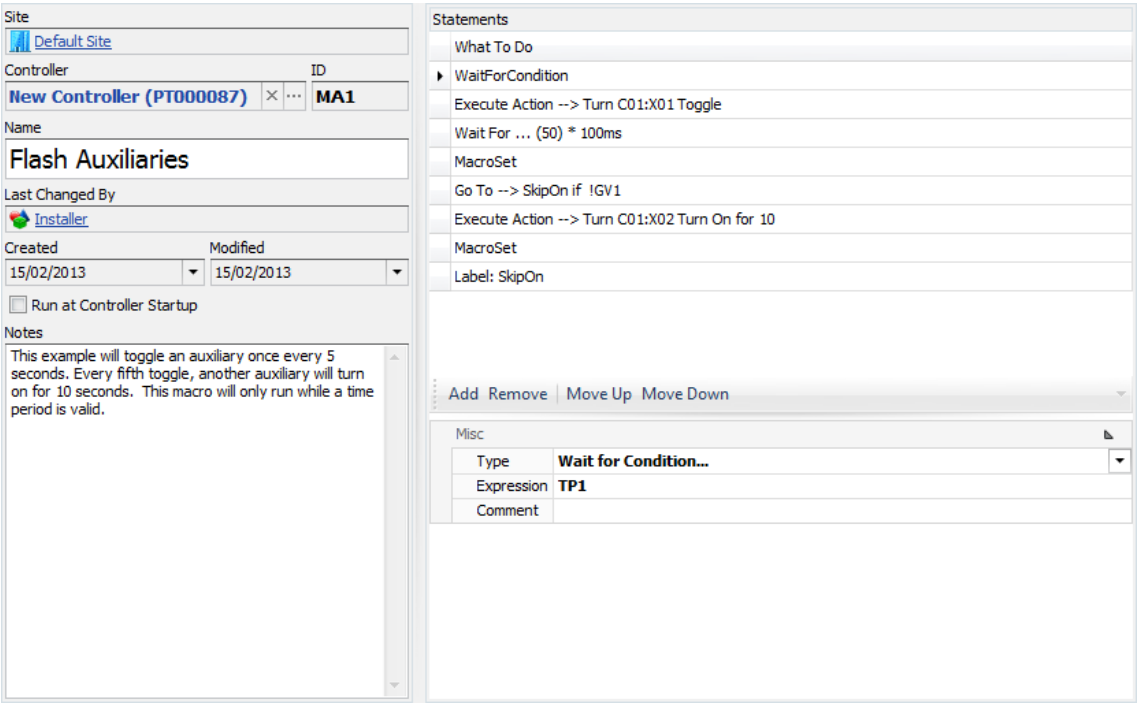
10. If no Action Groups are selected, any user can control the Named Action. If one or many Action Groups have been selected, users must have any one (or more) of the same Action Groups.

11. Save and close the editor window for the Named Action.

9.6 Macros

Macros within the Integriti controller provide an advanced level of flexibility where the use of actions is inadequate.

Programming of macros can only be created through the Integriti system management software.



9.6.1 Macro characteristics

All macros are implicitly looped –

Once a macro has started it will continue to run until stopped or the controller is restarted.

Macros can start automatically –

A macro can be configured to automatically start on controller start-up.

Actions are only asserted within macros –

'`Do an Action`' and '`Do an Action if`…' statement types will only assert the specified action.
The Dis-asserted option(s) are ignored.

Timing accuracy –

'`Pause for Time`…' statements are expressed in units of 100 milliseconds. Macro timings are accurate to roughly 100ms depending on the overall load on the Integriti controller.
Macro timing is affected by other higher priority processes taking place on the controller. Communications tasks and module communications are two examples of higher priority processes.

9.6.2 Controlling / Running macros

You can control macros from the Integriti management software or from the terminal (using 'Named Actions'). You can also configure macros to run on controller start-up or from an action.

Please refer to the section titled 'Named Actions' for more information on how to create a named action that will control a macro.

The section titled 'Actions' describes how to create an action with 'Run Macro' as the action.

9.6.2.1 Running macros from the Integriti management software

1. Open the macros panel.
2. Right-click the macro in the automation the macro panel and select 'Start'. (***Figure 37***)

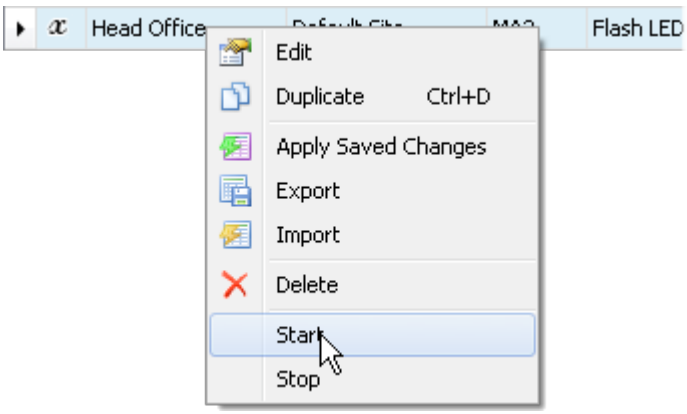


Figure 37

9.6.2.2 Running macros on controller start-up

1. Open the macros panel.
2. Double-click the macro.
3. Tick 'Run at Controller Startup'.
4. Save ( ) the macro and close the dialog.

9.6.3 Creating a new macro

1. Open the macros panel.
2. Click Add New in the Macro panel.
3. The properties window will appear with the usual basic options on the left side.
4. Tick 'Run at Controller Startup' if you need the macro to run once the controller is online.

To add a new statements to macros

- Click the Add button.

To remove a statements from macros

- Click on the statement you want to remove followed by the Remove button.

To relocate statements within macros

- Click the statement you want moved followed by the Move Up or Move Down button.

5. Save ( ) the macro and close the dialog.

9.6.4 Statements

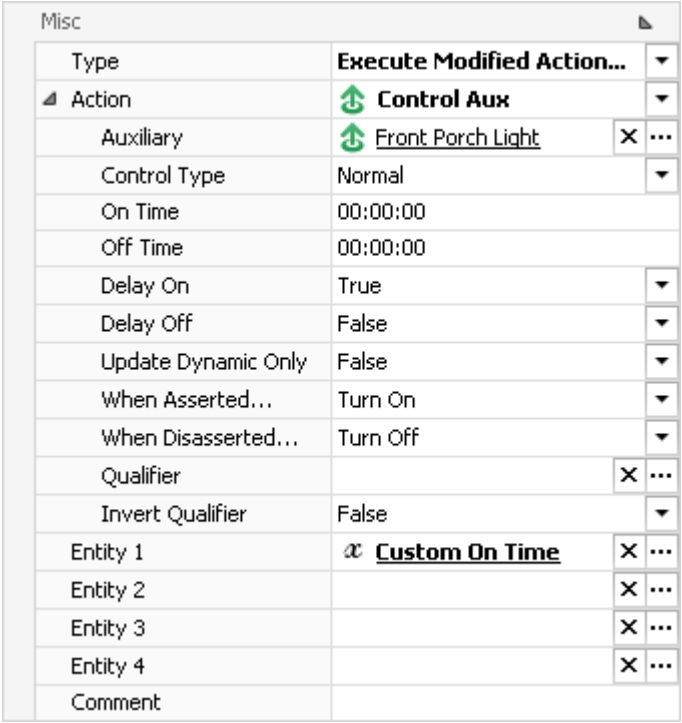
Each macro consists of one or many statements. At the very least an expression will have a type and a comment. Each statement must be one of the following types:

Statement type	Description
Do an Action	Perform the defined action.

Statement type	Description
Do an Action when the Expression Changes…	When this statement is evaluated for the first time it will perform the defined action. Every time the statement is evaluated after this, the defined action will only be performed if the result of the expression has changed.
Goto <label> if…	Go to a label defined elsewhere within the macro if an expression is true.
Pause for Time…	Suspend further execution of the macro for $n \times 100\text{ms}$.
Define a Label	A placeholder within a macro that execution can carry over to.
Set Entity To Expression…	Set an input to a specific count or analogue value.
Wait for Condition…	Further execution is suspended until the defined condition is met.
Execute Modified Action…	Perform the defined action using the values of entities to control the variables of the selected action.
End Current Macro	Terminates the macro.

9.6.5 Execute Modified Action…

This is a complex and powerful macro statement type. As described above, 'Execute Modified Action…' will perform the defined action using the values of entities to control the variables of the selected action.



Misc	
Type	**Execute Modified Action...**
Action	**Control Aux**
Auxiliary	Front Porch Light
Control Type	Normal
On Time	00:00:00
Off Time	00:00:00
Delay On	True
Delay Off	False
Update Dynamic Only	False
When Asserted...	Turn On
When Disasserted...	Turn Off
Qualifier	
Invert Qualifier	False
Entity 1	**Custom On Time**
Entity 2	
Entity 3	
Entity 4	
Comment	

Figure 38

Entities are associated with the variables of the selected action. In *Figure 38* there are two variables for the selected action (Control Aux). On Time will be controlled by the value of the global variable 'Custom On Time'. Off Time could be controlled by the value of Entity 2 (If set).

Control Aux & Control Aux List

- Entity 1 will control the On Time
- Entity 2 will control the Off Time

Control Door & Control Door List

- Entity 1 will control the Door Unlock Time

Trigger Input

- Entity 1 will control the Desired Global State
  - 0 All states sealed
  - 1 Alarm
  - 2 Sensor Mask
  - 3 Sensor Orientation
  - 4 Sensor Fault
  - 5 Sensor Range
  - 6 Tamper Low (e.g. short circuit)
  - 7 Tamper High (e.g. open circuit)
  - 8 General Tamper (e.g. Cabinet tamper)
  - 9 Zone self test fail
  - 10 Low battery
  - 11 Encryption fail on encrypted link
  - 12 Poll fail
  - 14 Input is in "soaking test"
  - 15 Input has failed a soak test

16 Input is isolated

Set Input Counters

- Entity 1 will control the Count value

Control Siren

- Entity 1 will control the Siren Time (value is multiples of 100ms)
- Entity 2 will control the Tone

9.6.6 Macro Expressions

Macro Expressions are represented as infix notation strings and have support for bracketing and operator precedence. They can include numeric constants (entered as decimal numbers) and entity references (entered in standard Inner Range address notation)

As with all things in Integriti, when an entity is evaluated in an expression it can have either an analogue (numeric) or Boolean value. The type used by a particular expression is chosen automatically by the controller based on context.

A few examples of valid macro expressions:

"`D03 && D05`"	= Both Door 3 and 5 are unlocked.
"`C01:X01 > 55`"	= C01:X01 has an analogue value greater than 55.
"`C01:X01 > C01:X02`"	= C01:X01 is greater than C01:X02.

Expressions are not sensitive to whitespace, so the expression "`((5+3)/7>C01:X01)&&D01`" is interpreted identically to "`( (5 + 3) / 7 > C01:X01) && D01`".

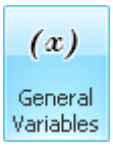
There are two special zone value modifiers. The 'hash' (#) modifier can be used to test the count value of an input entity. The 'at' (@) modifier can be used to test the analogue value of an input entity. To use the modifiers, place either one before the entity to be evaluated in the macro statement.

Example usage – Test the input count is above 5: "`#C01:Z01>5`".

The following table is a list of all operators, in order of precedence.

Operator	Name	Arguments	Argument Type	Return Type
!	NOT	1	Boolean	Boolean
*	Multiply	2	Numeric	Numeric
/	Divide	2	Numeric	Numeric
+	Plus	2	Numeric	Numeric
-	Minus	2	Numeric	Numeric
<<	Shift Left	2	Numeric	Numeric
>>	Shift Right	2	Numeric	Numeric
<	Less Than	2	Numeric	Boolean
<=	Less Or Equal	2	Numeric	Boolean
>	Greater Than	2	Numeric	Boolean
>=	Greater Or Equal	2	Numeric	Boolean
==	Equal	2	Numeric or Boolean	Boolean
&	Bitwise AND	2	Numeric	Numeric
^	Bitwise XOR	2	Numeric	Numeric
|	Bitwise OR	2	Numeric	Numeric
&&	Logical AND	2	Boolean	Boolean
||	Logical OR	2	Boolean	Boolean

9.7 General Variables



The general variables panel is accessible from the

tab.

General variables are used to store values for a number of applications. Values are assigned by other entities such as inputs, macros or named actions.

To create a General Variable:

1. Click the

button in the General Variable panel.
2. The properties window will appear with the usual basic options on the left side.
3. The only property that can be set is the optional test value.

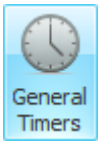
   The test value is used to determine whether the general variable evaluates to true or false when tested in a logic statement.

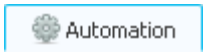
   For example:

   The general variable has been assigned a test value of 50.

   - If the general variable is equal to 50 or less, the general variable when tested will return false.
   - If the general variable is equal to 51 or greater, the general variable when tested will return true.

9.8 General Timers



The general timers panel is accessible from the 

tab.

General timers are used similarly to general variables. You can use another entity such as an input, macro or named action to set its value. The general timer will count back down to 0. The timer counts down every 100ms. When counting down, the general timer will be in an invalid state. When the general timer reaches 0 it will be in a valid state. General timers do not automatically restart.

To create a General Timer:

1. Click the

button in the General Variable panel.
2. The properties window will appear with the usual basic options on the left side.
3. Simply give the general timer a name, save the record and close.

10 Hardware and LAN management

Once Integriti hardware has been installed and is running, the next thing you will need to do is enrol controllers. Integriti controllers can be added (enrolled) either manually or automatically to the Integriti server.

If you are connecting a controller over the internet or between networks, you will need to ensure that TCP port 4711 is forwarded to the Integriti Controller Server.

10.1 Controller configuration

Before enrolling a controller, you will need to ensure it has been appropriately configured for the network it has been attached to.

Determining what IP address was given to an Integriti controller:

This procedure assumes the controller is connected to a LAN with a DHCP server and a terminal is attached to the device bus with its address set to 1.

If you can't determine if there is a DHCP server present on the network, follow this procedure through to step 7. If the displayed IP address is `0.0.0.0`, the controller was not issued with an IP address. Follow the procedure '*Manually assigning an IP address of the Integriti controller*' below.

1. After performing the pre-power up checks, turn the Integriti controller on.
2. Wait for the controller to start. When the controller is up and running, the Status 1 and Status 2 LEDs will flash in an alternating pattern (***Figure 39***).

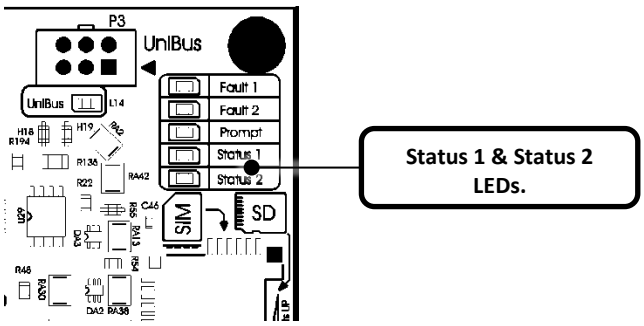


Figure 39

3. Log in to the terminal by pressing: **[0], [1], [Ok]**
4. Go in to controller information by pressing: **[Menu], [1], [9]**
5. Press **[▼]** once to display the controller serial number.
6. Press **[▼]** once more to display the controller MAC address.
7. Press **[▼]** two more times to reveal the controller IP address. (assuming the controller is connected to a network and a DHCP server has assigned an IP address to the controller)

Manually assigning an IP address of the Integriti controller:

This procedure assumes the controller is connected to a LAN without a DHCP server and a terminal is attached to the device bus with its address set to 1.

1. After performing the pre-power up checks, turn the Integriti controller on.
2. Wait for the controller to start. When the controller is up and running, the Status 1 and Status 2 LEDs will flash in an alternating pattern (*Figure 39 above*).
3. Log in to the terminal by pressing: **[0]**, **[1]**, **[Ok]**
4. Go in to controller NIC configuration by pressing: **[Menu]**, **[7]**, **[3]**, **[4]**
5. Press **[Ok]** once to configure NIC01.
6. Enter in the desired IP address for the Integriti controller followed by **[Ok]**.
7. Enter in the subnet mask followed by **[Ok]**.
8. Enter in the gateway address (if required) followed by **[Ok]**.
9. Enter in the primary DNS address (if required) followed by **[Ok]**.
10. Enter in the secondary DNS address (if required) followed by **[Ok]**.
11. The controller is configured to use DHCP by default. Press **[5]** to disable DHCP.

10.2 Enrolling controllers

Integriti controllers can connect to Integriti Controller Servers via Ethernet, USB or Modem. Ethernet connectivity can be direct or with the aid of the Inner Range SkyTunnel service.

With the exception of USB, at some point during the enrolment procedure you will need to decide how the data synchronisation is handled. Selecting a data synchronisation method will determine whether the data on the server or the data on the controller will take precedence in the event of a clash. When an entity within the controller does not match the corresponding entity in the Integriti server, one of the three options will occur:

Merge Changes –

Differences between the Software and Controller databases are merged, such that both the controller and server have a consistent database containing all programmed records. If there is a conflict on a particular record, the record from the Software will overwrite the record in the Controller.

This mode is suitable for single controller installations or installations where keypad programming is desired.

Disallow Changes From Controller –

All global entities in the Controller database are overwritten with the records from the Software database. This mode will NOT allow changes to global entities to be made via the keypad.

This mode is suitable for multi-controller installations where the system is centrally managed using the Integriti Pro Management Software.

Prefer Controller Changes –

Differences between the Software and Controller databases are merged, however records from the Controller database will overwrite records in the Software database.

This mode is suitable for situations where the only copy of the system programming is currently held within the controller and you wish to retrieve it.

If you are unsure about what option you should select, leave the default (recommended) setting- ' Prefer Controller Changes'.

10.2.1 Automatic controller discovery (Method 1)

The simplest method of adding controllers to Integriti is by using the 'Auto Discover new Controllers…' feature. This feature will only work if the controller is on the same subnet.

Please note that Automatic controller discovery can only work across the local network. To connect to controllers over the internet, see Method 4.

To access this feature, click on the Home tab followed by the Connect New Controller button (***Figure 40***).

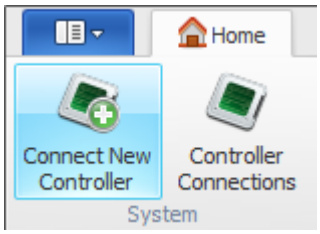


Figure 40

The 'Connect to Controller' window will appear.

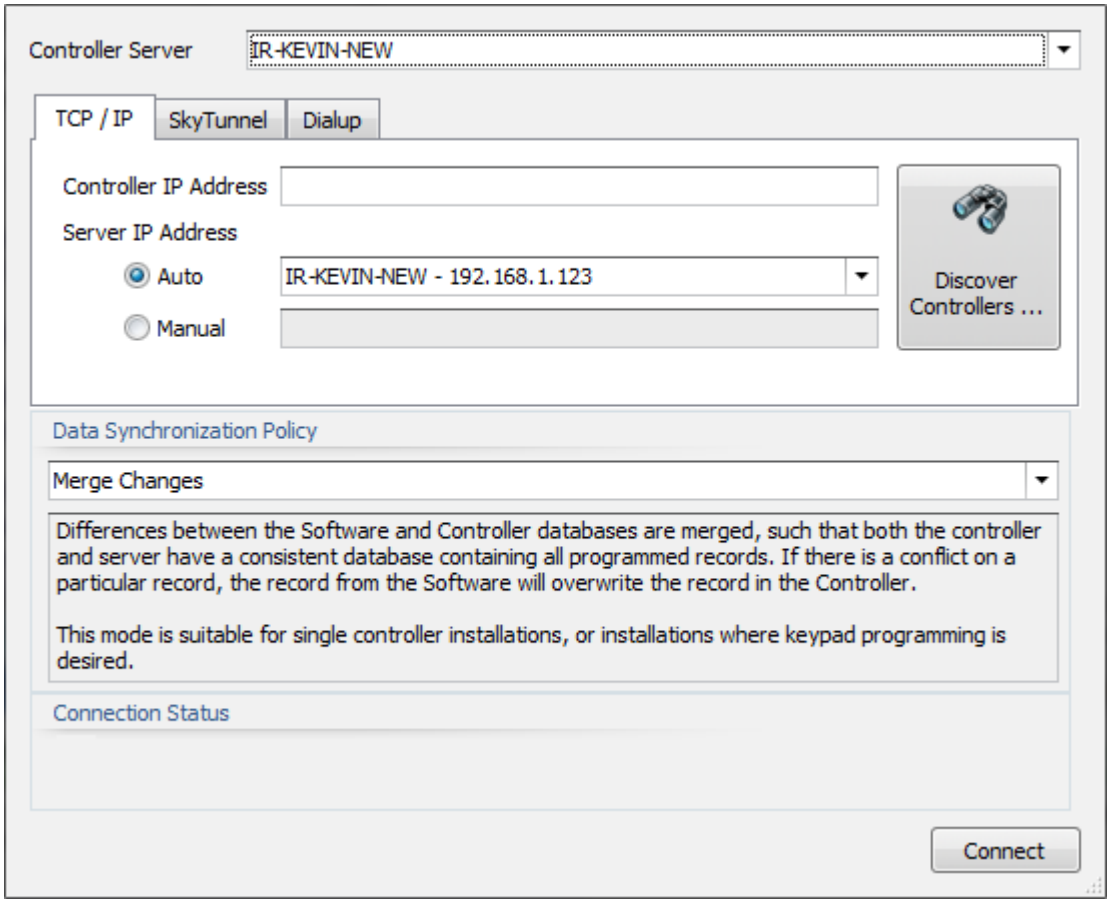
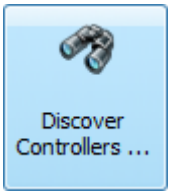


Figure 41

Click on the 

button and the 'Discover Controllers' window will appear. Automatic controller discovery will begin (*Figure 42*).

When the automatic controller discovery has completed the Integriti controllers will be listed in the upper section (Discovered Controllers) of the window (*Figure 42*).

The automatic controller discovery progress is displayed as a green progress bar to the right of the Integriti server under 'Scan Status'.

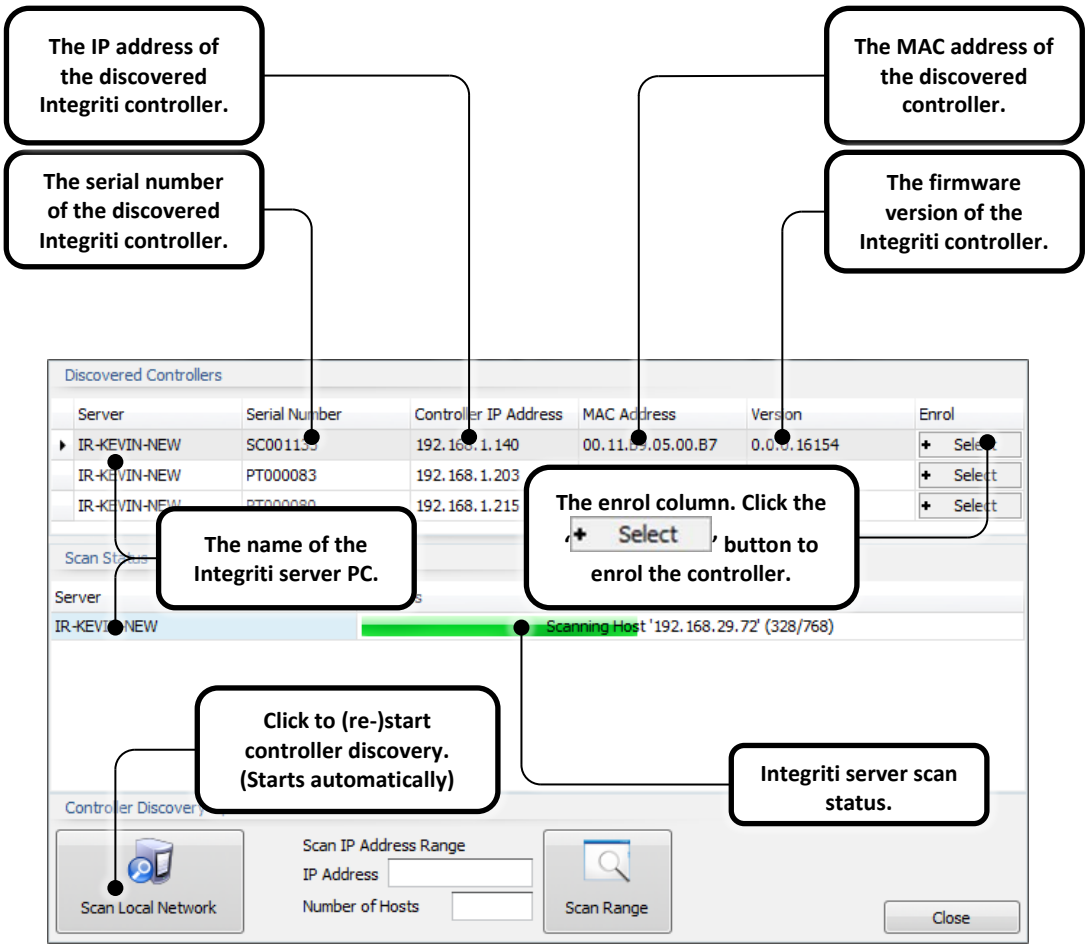


Figure 42

Each individual controller has its own unique serial number. The serial number and MAC address are printed on a label which is placed on the Integriti controller during production.

You can enrol controllers as soon as they appear in the 'Discovered Controllers' list. Simply click the + Select button to go back to the 'Connect to Controller' window (*Figure 43*).

There is no limit on the number of controllers you can enrol simultaneously. As soon as the controller is visible, you can begin enrolment.

Discovered controllers with a greyed out enrol button (+ Select) are controllers that have already been enrolled.

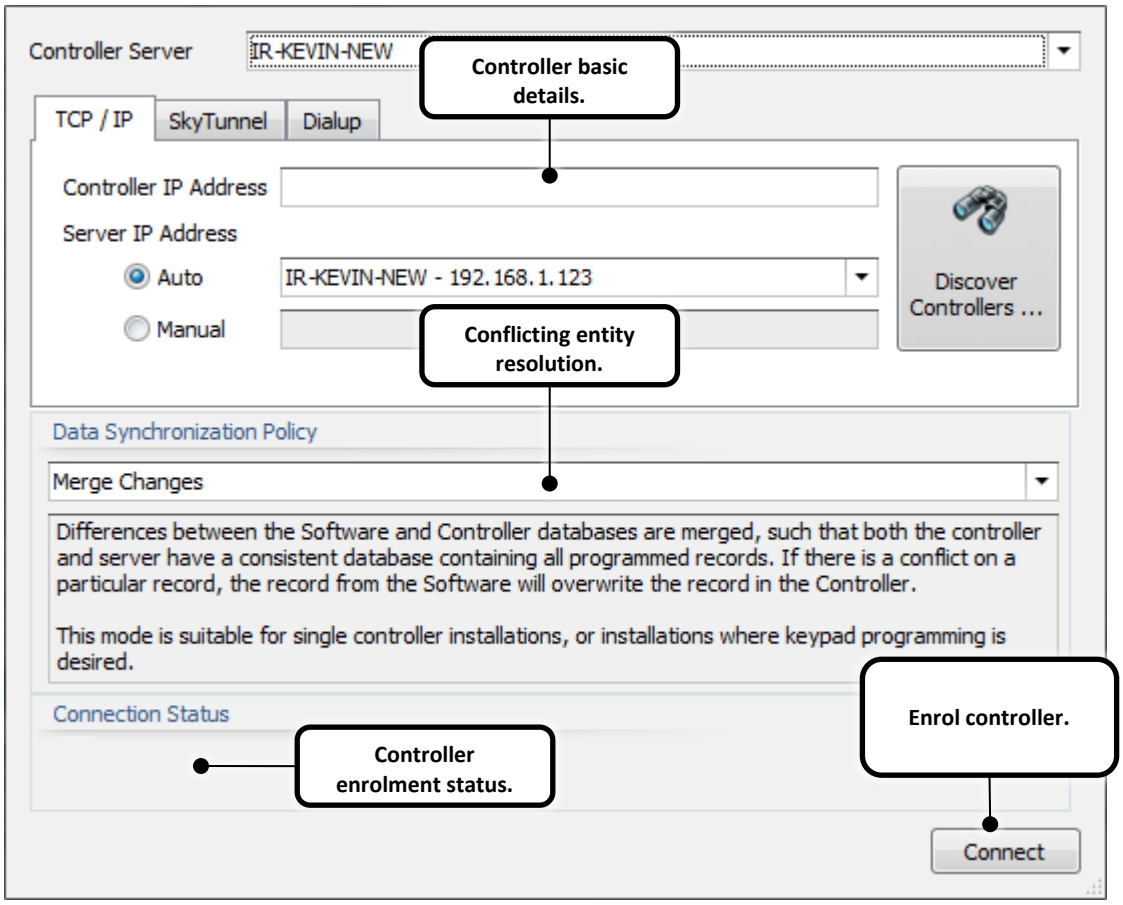


Figure 43

After clicking the + Select button, there is only one item that requires your attention before starting the enrolment process. You will need to select one of the three Data Synchronisation Policy options. See 'Enrolling controllers' (***above***) for detail on the synchronisation options available.

When you are ready to enrol the controller, click the Connect button.

10.2.2 Manual controller enrolment (Method 2)

Please note that there is no need for any port forwarding on the controller side.

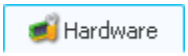
To manually enrol a controller, use the following procedure:

LCD Terminal specific instructions:

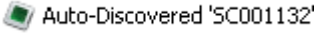
1. Log in to the terminal by pressing: **[0], [1], [Ok]**
2. Go in to controller communications task programming: **[Menu], [7], [3], [1]**
3. Configure communications task `CT01`: **[Ok], [9], [Ok]**
4. Select '`Integriti CT`' as the communications task type: **[►], [►], [Ok]**
5. Enter the exposed IP address of the server followed by **[Ok]**.
   - Values less than 3 digits should be entered with leading zeros.
6. Enter the Port used to connect to the server: **[0], [0], [4], [7], [1], [1], [Ok]**
7. Skip the DNS option: **[Ok]**
8. Set the encryption method to `AES128`: **[►], [Ok]**
9. Enable P under the Gip options: **[►], [►], [►], [►], [►], [►], [►], [9], [Ok]**
10. Leave the site fields blank: **[Ok], [Ok]**
11. Leave the GUID fields blank: **[Off], [Ok], [Off], [Ok]**
12. Leave the telephone number fields blank: **[Ok], [Ok]**
13. Select `Ethernet` for `Priority 1`: **[►], [►], [Ok]**
14. Skip the remaining priority options: **[Ok], [Ok], [Ok]**
15. Enable the C and A options: **[►], [►], [►], [►], [►], [►], [9], [9], [Ok]**
16. Skip the remaining C and A options: **[Ok], [Ok], [Ok]**
17. Skip the `Imodem` and `Emodem` options: **[Ok], [Ok], [Ok], [Ok]**
18. Enable the communications task and log out: **[9], [End]**

Software specific instructions:

1. Click on the

button under the 

tab.
2. The Controller panel should appear.
3. In the controller panel, the configured controller should appear automatically in the list of controllers as 'Auto-Discovered'.

   - If the controller does not appear in the list, check the following:
     i. Double-check your NIC and Comms Task programming options.
     ii. Check / update your licenses.
     iii. Verify the 'IR Integriti Controller Server' service is running.
     iv. Check your network configuration, firewall, port forwarding…

4. Select the auto-discovered controller and click Edit.
5. Change the name of the controller to something more appropriate.

Module Details

6. Under module details, expand out the Inputs group.
7. Click on the ellipsis ... to the right of each EOL configuration option and select Concept3K

Connection Details

8. The connection configuration changes required have been highlighted below:

Connectivity	
Connection Mode	**Auto**
Preferred Connection Type	**TCP**
Connection Timeout	**30000**
Connection Poll Time	**10000**
Modem Serial Port	
Modem Configuration string	
Modem Phone Number	
Synchronisation	
Review Synchronisation Mode	**Continuous**
Don't Sync Time Upon Connection	☐
Time Zone	**(UTC+10:00) Canberra, Melbourne, Sydney**
Enable Data Synchronisation	☑
Data Sync Mode	**Server to Controller**
Prevent State Syncing	☐

Figure 44

9. Click the button and close the window.
10. An icon ( ) should appear to the right of the controller in the Hardware panel indicating that the server is synchronising with the Integriti controller.

10.2.3 Controller enrolment using the SkyTunnel service (Method 3)

Inner Range has provided a service where controllers can be connected to the Integriti controller server provided there is internet connectivity at both ends.

To make use of this service, the controller must be configured to connect to the SkyTunnel service before the Integriti server can enrol it.

To connect a controller to the SkyTunnel service:

LCD Terminal specific instructions:

1. Log in to the terminal by pressing: **[0], [1], [Ok]**
2. Go in to the SkyTunnel communications task quick start: **[Menu], [8], [0]**
3. Start the SkyTunnel communication task: **[On]**
4. Write down the 8 digit password provided.
5. Log off: **[End]**

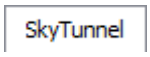
If you are using Integriti CS, you will need to change the Installer PIN code or create a new user with a PIN code other than 01. To do this, follow these instructions:

1. Log in to the terminal by pressing: **[0], [1], [Ok]**
2. Go in to user programming: **[Menu], [2], [1]**
3. Edit the Installer user: **[Ok]**
4. Change the user PIN: **[Ok], [Ok]**, *{enter a 2 to 8 digit PIN}*
5. Log off: **[End]**

To enrol a controller connected to the SkyTunnel service from the System Designer:

1. Click on the

button under the

tab.
2. The 'Connect to Controller' window should appear.
3. Click on the 

tab and enter the serial number of the controller in the 'Controller S/N' field provided.
4. Enter the randomly generated 8 digit password from the procedure above in the Sky Tunnel Password field.
5. Select the synchronisation method from the drop down list box. See 'Enrolling controllers' (***above***) for more detail.
6. Select either Server Authentication or User Login to connect to the controller.

10.2.4 Connecting directly to a controller using USB (Method 4)

Connecting to a controller using USB is very simple. After logging in to System Designer, connect your controller to an available USB port on the server. On the PC, you should notice the driver for the controller being installed automatically. Shortly after, the controller should appear under the 'Default' site as an 'Auto-Discovered' controller.

10.2.5 Connecting to a controller using a modem (Method 5)

In circumstances where any of the connection methods above cannot be achieved, controller connections using a dialler has been made available.

To configure the controller for a dialler connection:

LCD Terminal specific instructions:

1. Log in to the terminal by pressing: **[0], [1], [Ok]**
2. Go in to controller module programming: **[Menu], [7], [2], [0], [1]**
3. Change the number of rings to answer: **[◄], [0], [0], [0], [0], [6], [Ok]**

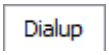
- If you are using 'User Login' to authenticate with the controller, follow the remainder of this procedure.

4. Go in to user programming: **[Menu], [2], [1]**
5. Edit the Installer user: **[Ok]**
6. Change the user PIN: **[Ok], [Ok]**, *{enter a 2 to 8 digit PIN}*
7. Log off: **[End]**

To enrol a controller connected via dialler from the System Designer:

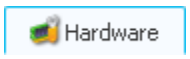
1. Click on the

button under the

tab.
2. The Connect to Controller window should appear.
3. Click on the 

tab.
4. Select the communications port that the modem is connected to.
5. Enter the telephone number of the controller.
6. If required for your specific make/model of modem, enter an initialisation string.
7. Select the synchronisation method from the drop down list box. See 'Enrolling controllers' (***above***) for more detail.
8. Select either Server Authentication or User Login to connect to the controller.

10.3 Maintaining Firmware

Controller and module firmware can be managed easily via the Integriti firmware manager under the 

tab.

Click

to open the update manager (***Figure 45***).

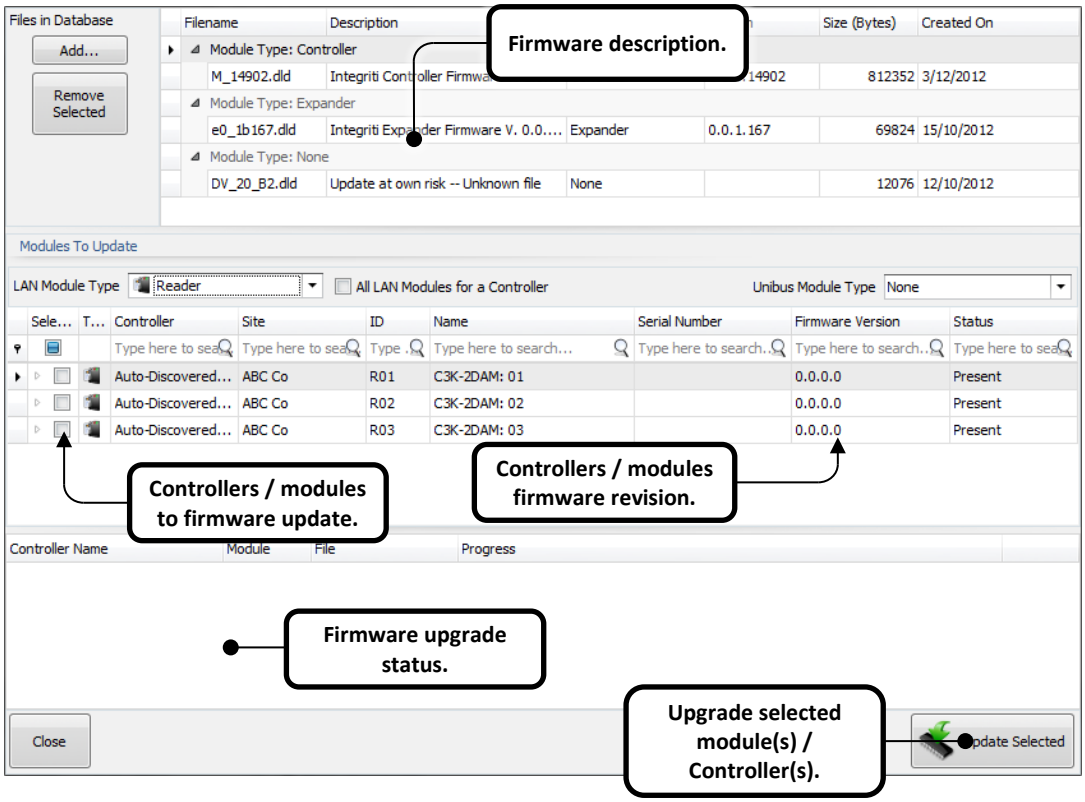


Figure 45

The available firmware list at the top of the window will display all of the firmware files you add to the update manager.
If you select a firmware file in the update manager you will see the list of modules to update change according to the type of firmware file selected.

Click Add... to add new firmware revisions to the update manager.

Updated firmware files are made available to qualified installers from time to time via the Inner Range support website.

The firmware upgrade status will indicate the progress of each individual controller / module being upgraded. The process is completed when the controller / module has come back online.

10.3.1 Upgrading module & controller firmware

1. Select the firmware revision you want to upgrade to from the list at the top of the update manager.
2. Select one or many controllers/modules from the modules to update list by ticking the appropriate check box(es).
3. Click

.

The time it takes to upgrade the firmware of a particular module or controller will vary depending on connectivity to the Integriti server. Please allow up to 30 minutes for the upgrade process to complete.

We recommend stopping, re-starting and testing communications tasks after controller firmware upgrades.

10.4 Module Programming

It is recommended that the Integriti controller LAN remains locked during normal operation. This will prevent the addition of new modules and the possibility of foreign modules interfering with the existing infrastructure.

To access the controller LAN settings, right-click the controller in the navigation panel:

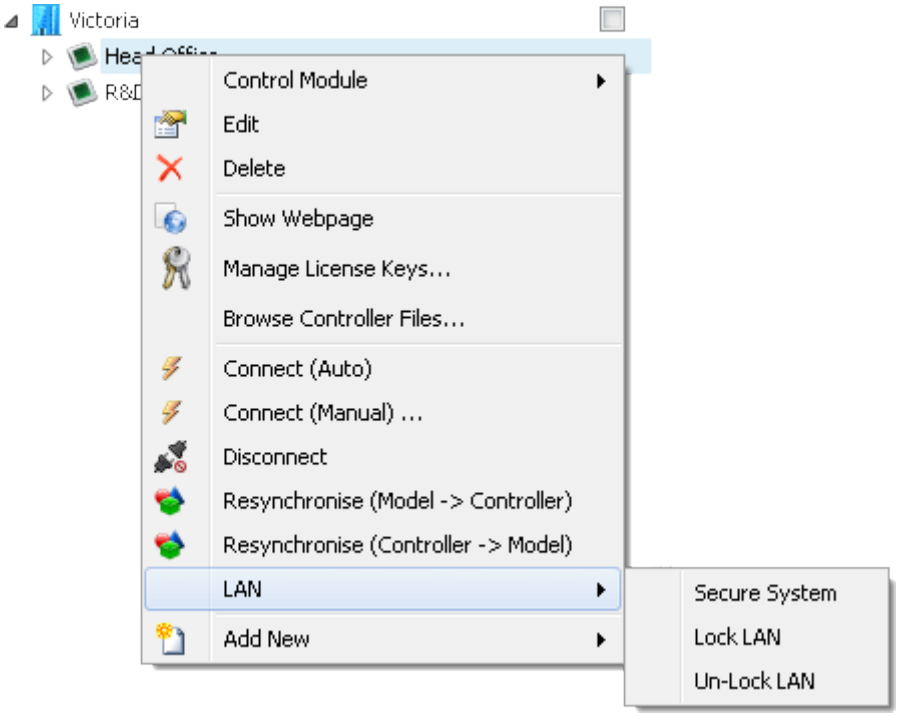


Figure 46

Secure System

Securing the LAN will send out a secure flag to all of the modules currently connected to the controller. The modules will remain secure until the next time the LAN is secured.

Modules that are not secured will have the status: "`Present (Unsecured)`". This usually occurs when a module has been attached to the LAN after secure system has been selected.

Lock LAN

Locking the LAN prevents any newly attached module from connecting to the Integriti controller. Modules that are not present at the time the LAN was locked will be ignored by the controller. The controller will log the presence of any foreign modules. This excludes new UniBus devices being attached to existing LAN modules.

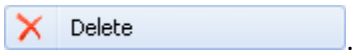
Un-Lock LAN

Unlocking the LAN is required before adding new modules to the Integriti controller.

10.4.1 Adding New Modules

Once a module has been attached to the Integriti LAN, the controller will detect the presence of the module and it will appear under the controller in the site navigation panel.

10.4.2 Deleting Modules

To remove and delete a module from an Integriti controller simply right-click the module and select 

.

11 CCTV

Integriti integrates with a large number of video surveillance products. Support for products is provided as a plugin installer. The plugin must be installed separately on the Integriti server and any clients that will be used to view images provided by the integrated device.

11.1 Installing Insight DVR plugins

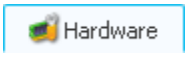
The Integriti software management suite can be used with Insight DVR plugins. Installing and using these plugins requires a slight change to the install procedure.

To install Insight Professional DVR plugins for use with Integriti:

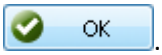
- Stop all Integriti services.
- Run the Insight DVR plugin installer and continue through until you get to the "Select Destination Location" dialog.
- Change the destination folder from the default to your Integriti installation folder. Typically this path is "`C:\Program Files\Inner Range\Integriti Pro\`" on a Windows 7 64bit platform.
- Complete the installation.
- Start all Integriti services.

If you click the browse button to select the destination folder location when installing Insight Professional DVR plugins, '`\Insight`' will be appended to the destination folder. You will need to remove this to continue.

11.2 Enrolling video systems

1. Click on the 

tab followed by

.
2. Select the DVR plugin from the list in the new dialog that appears and click 

.

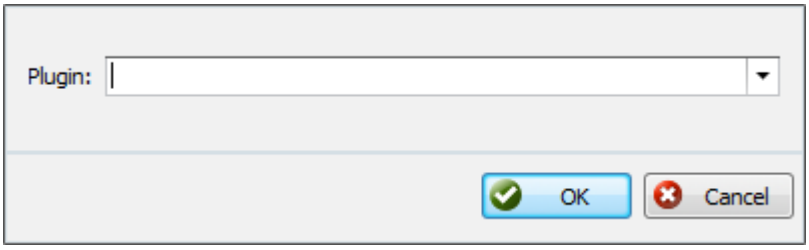


Figure 47

3. Enter the necessary connection settings for the plugin. These settings will vary from plugin to plugin but will mostly consist of an IP address, User name and Password.

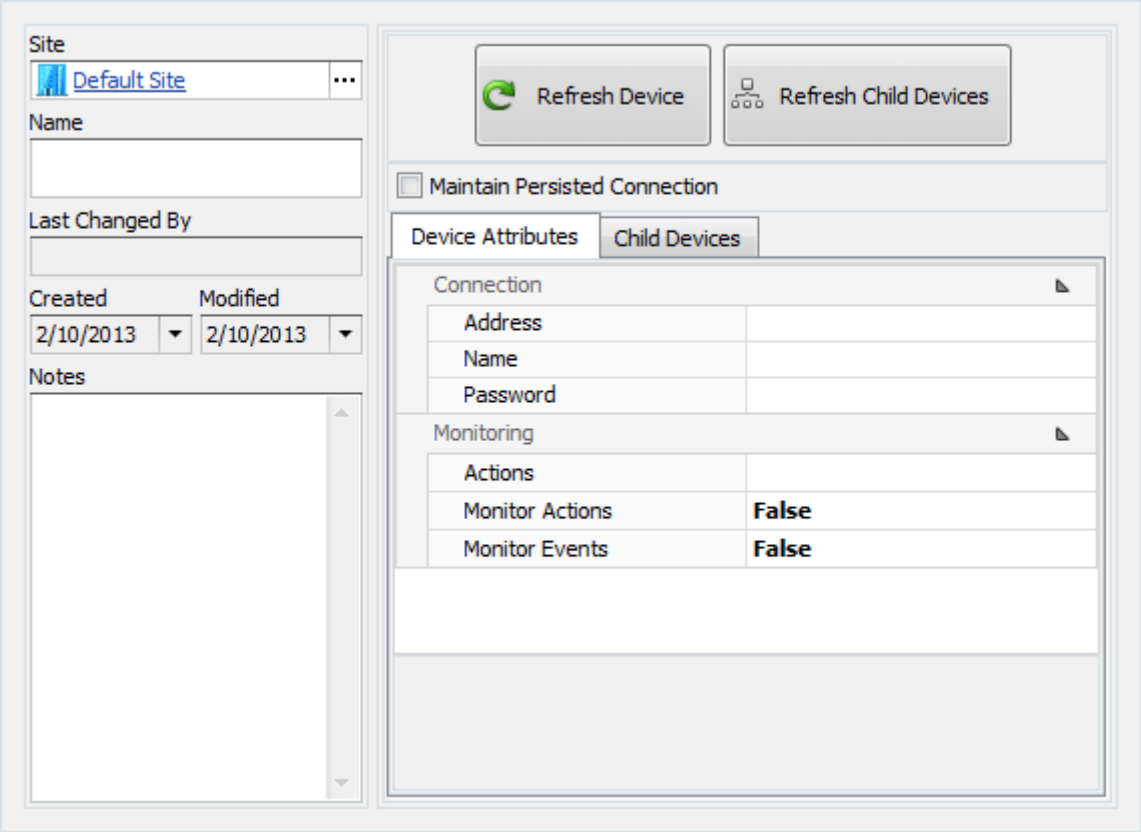
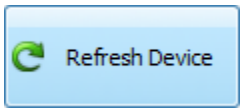


Figure 48

4. If available, click the  and buttons to ensure the actions, cameras and/or any other devices are detected and enrolled accordingly.
5. The option Maintain Persisted Connection is only required for situations where messages are sent and/or received from the device.
6. Save and close the editor window for the CCTV Recorder.

11.3 CCTV camera configuration

Once a video system has been enrolled, not all of the cameras may be required. Enabled cameras take up camera licenses.

Disabling CCTV cameras…

1. Click on the Hardware tab followed by CCTV Cameras.
2. Double-click a CCTV Camera to disable. The Editor Window for the CCTV Camera should appear.
3. On the right-hand side, click on Disable Device.
4. Save and close the editor window for the CCTV Camera.

11.4 Associating cameras with entities

By associating cameras with entities, operators can play back archived video from CCTV Recorders when review events are generated for the entity.

Associating cameras with entities …

1. Click on the Hardware tab followed by CCTV Cameras.
2. Double-click a Camera to associate entities to. The Editor Window for the Camera should appear.
3. On the right-hand side under Associated Entities, click on the Add button.
4. From the window that appears, select the entity to associate with the Camera.
5. Save and close the window.

11.5 Viewing associated video from associated entities

If an entity has been associated with one or many cameras, you can view live video by right-clicking the entity and selecting Show Video.
Live feeds will appear for all cameras associated with the entity.

11.6 Viewing associated video with review

If an entity has been associated with one or many cameras, you can view archived video by right clicking the entity and selecting Show CCTV Footage from review or filter windows.

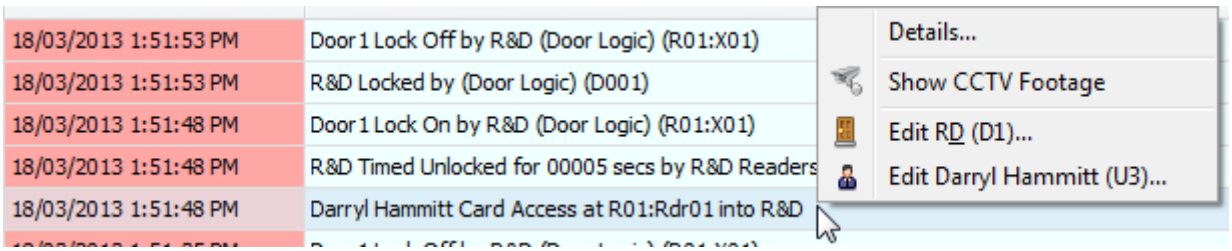


Figure 49

If more than one CCTV Camera has been associated with the one entity, clicking Show CCTV Footage will open a panel with a camera matrix.

The video will begin playback from the time that the entity appeared in review.

11.7 Viewing video from schematics

You can view video from a schematic using one of two methods:

1. Right-click an icon used to represent a camera and click on Show Video

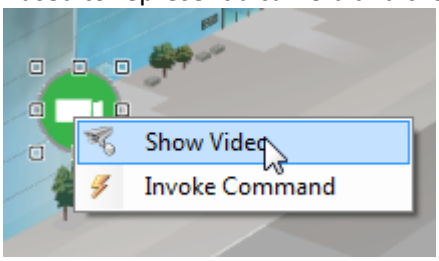


Figure 50

2. Click on an icon used to represent a camera then click on Show Video in the Commands toolbox.

Figure 51

12 Photo ID

Photo ID allows you to create Photo ID designs and print identification tags and badges for Users (employees, contractors, visitors, etc…)

The Photo ID designer features include rotation and flipping of images, creation of various arbitrary shapes, object alpha, support for double sided cards, barcodes, user photos and custom field images.

There is no restriction on the number of designs or design dimensions. Photo ID designs can be any one of a number of standard formats or user defined.

Printing ID cards is a two step process. First, you must create a Photo ID Design. Photo ID provides simple tools which allow you to customise the design by inserting the required graphics and fields into the card design and defining what fonts and colours will be used.

You can create and save as many different deigns as you like, each with a different layout. Designs may include images, simple graphics, text and user database information such as user names, company details and photos.

Once a design has been created, it can be used to print a batch of Users. To print designs, you first select the users who will be issued with the new Photo ID Design, then issue the print command from the context menu.

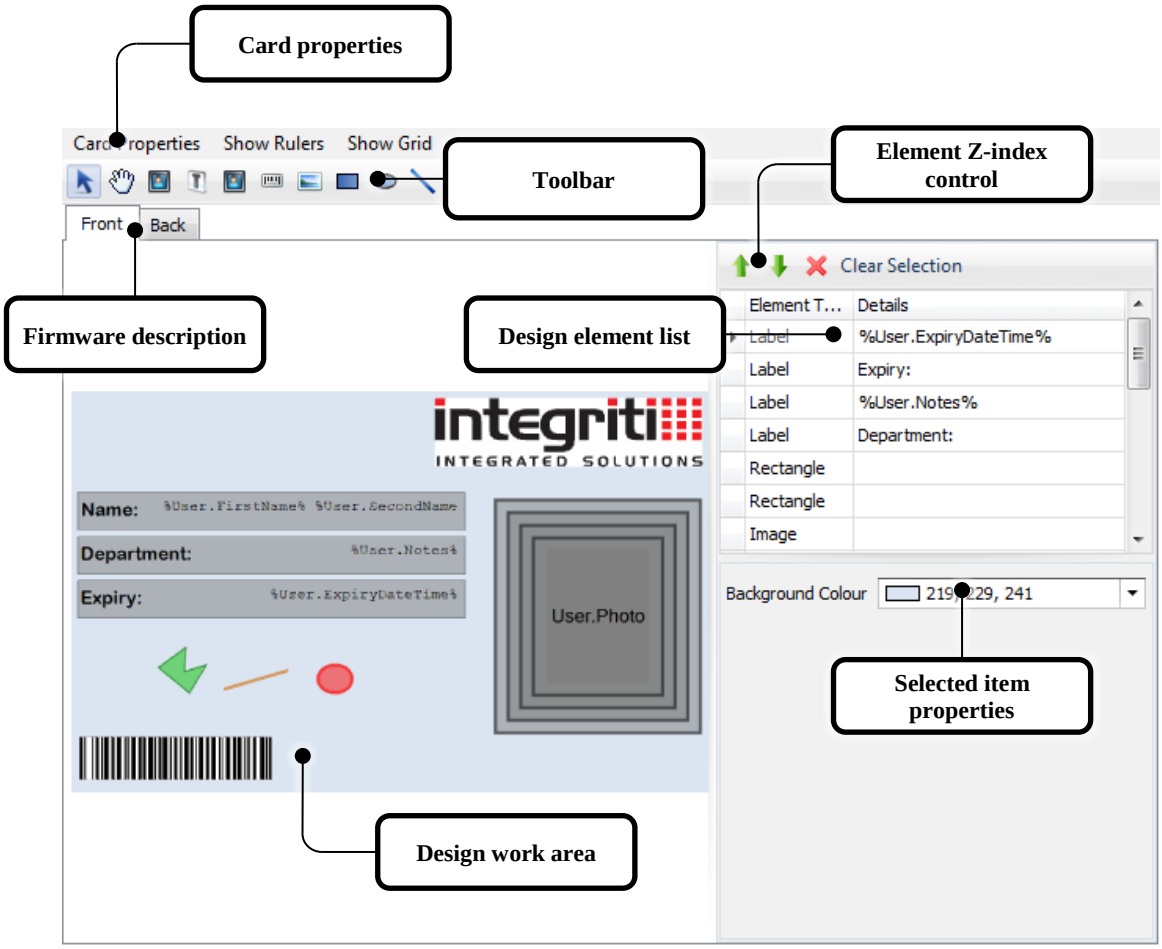


Figure 52

12.1 Creating a Photo ID Design

To create a Photo ID Design…

1. Open the Photo ID Designs panel from the Access Control tab.
2. Click the Add New button to create a new Photo ID Design.
3. Give the new design a name and enter a description in the notes field.
4. Click on Card Properties.
5. Specify whether the design will be single or double sided.
6. Select the card orientation.
7. Specify the card measurement units.
8. Select the physical dimension standard or custom from the Card Type drop-down list.
    a. If custom was selected, specify the Width and Height.
9. If required, adjust the DPI.
10. Click OK.
11. Place items on the design area.
12. Select an item from the toolbar.
    a. Click and drag in the design area to place a new design element.
    b. Adjust the placement of the newly placed design element by adjusting the element handles.
    c. Tweak the display element further by modifying the element properties to the right.
13. Continue creating items as required.
14. Save and close the editor window for the Photo ID design.

13 Schematics & Element Presenters

Schematic allows operators to monitor status and control entities via an intuitive interface based around graphical floor plans, site maps and mimic panels. Special items can be placed on each diagram that indicate the status of various entities such as inputs, areas and auxiliaries in real time.

Schematic can be used to:

- Import site plans
- Navigate between maps / diagrams
- Add entities to maps / diagrams
- Monitor site activity in real time
- View and acknowledge alarms
- Control items
- View video from associated CCTV sources.

Schematic maps, mimic panels and similar graphical interfaces are created using the Integriti System Designer. Schematic maps can then be viewed in either Gate Keeper or System Designer.

Items placed on the schematic are called map elements. Map elements are optionally linked to entities. These can either be icon based, or be drawn as shapes.

Map elements can be used to highlight items on the schematic or indicate the state of entities.

Map elements do not update when you are modifying or creating a schematic map.

Supported image formats used throughout Integriti:

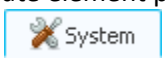
- BMP
- JPG
- GIF
- PNG

13.1 Element Presenters

A presenter is a collection of format settings and rules that govern how a map item will behave on the schematic. Presenters can only be assigned to a schematic map item if it is linked to an entity.

A significant number of element presenters with a common theme exist by default within the Integriti system, but there are occasions where the customer wants something a little more specific to their particular installation. Integriti includes the ability to create new presenters.

To create element presenters, click on the

button in the Schematics group under the 

tab.

Click on the

button to create a new element presenter.

Often, it is desirable to create a new element presenter, based on an existing one (we do not suggest editing default presenters as these may be over-written during software updates). To achieve this, right click on the presenter on which you wish to base a new presenter, select "Duplicate" and change the name, then edit the new presenter.

Double-click an existing element presenter to edit it.

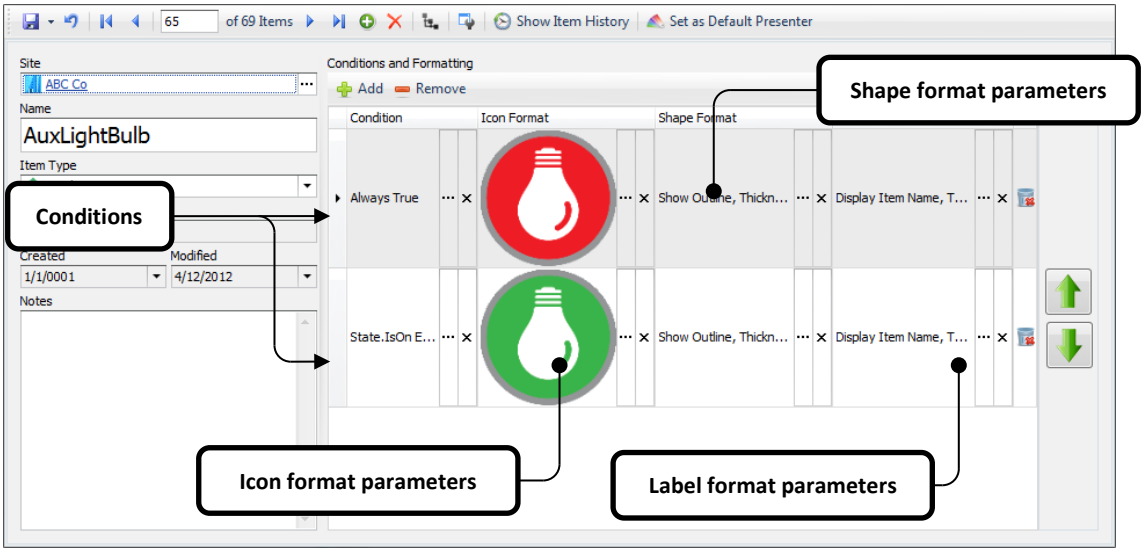


Figure 53

13.1.1 Condition

The condition under which the Icon, Shape or Label format will change to the values specified.

Clicking on the button will open the presenter rule/condition for editing.

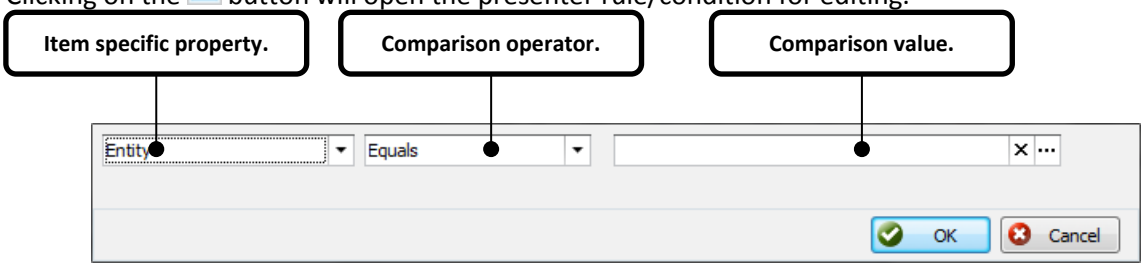


Figure 54

Depending on the selected item type of the presenter, options in the presenter rule editor will vary.

Examples of item specific properties for a door are:

- Is On
- Summary
- Last Updated
- Extended Status
- Entity

If a number of conditions are met, the icon shape or label format associated with the last (bottom-most) condition in the list is used. Because of this, it is often desirable to have, as the very topmost condition in the list, an “Always True” condition which will be displayed when none of the other conditions are met.

13.1.2 Icon Format

From here you can select an image for the specific condition.

Clicking on the ... button will open the icon format window.

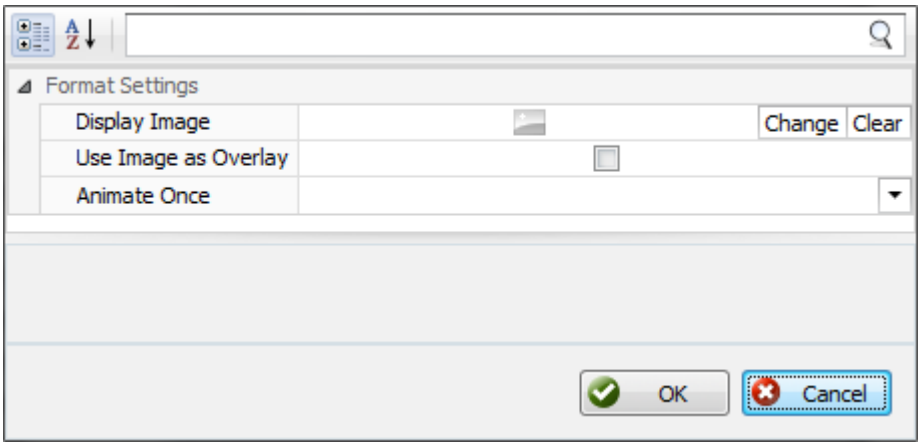


Figure 55

Click Change to select the desired image.

If the image is to be used to overlay other images of the element presenter, check the 'Use Image as Overlay' checkbox.

If the selected image is an animated GIF, you can change the 'Animate Once' to True to play the animation once or False to loop the animation.

13.1.3 Shape Format

Figure 56

13.1.3.1 Show outline

Default value: True

Setting this option to False will disable the outline of the item.

13.1.3.2 Outline Thickness

Default value: 5 pixels

The value specified here will determine the thickness of the border / outline. A value of 0 will leave a 1 pixel border.

13.1.3.3 Opacity 0-255

Default value: 128 (semi-transparent)

The opacity affects both the Interior and outline colour. Use a value of 255 for opaque and a value of 0 for transparent.

13.1.3.4 Interior colour:

Default value: Grey (128,128,128)

Colour selections are made up of a combination of 3 values (Red, Green and Blue) in the range of 0 and 255. The interior colour of the item can be a Web, System or Custom colour. You can manually enter the colour or click the drop down to select the colour from the colour picker.

Manual colour entry examples:

`0,0,255`	Blue
`255,0,0`	Red
`0,255,0`	Green
`0,255,255`	Cyan

If the colour value entered has the same value as any of the colours found under the Web or System colour picker tabs, it will automatically change to the colour name.

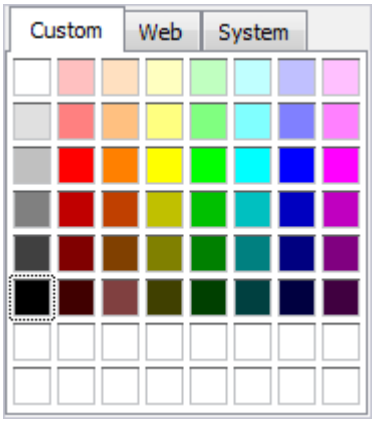


Figure 57

Right-click any of the colour squares in the bottom two rows of the Custom tab to add your own colour.

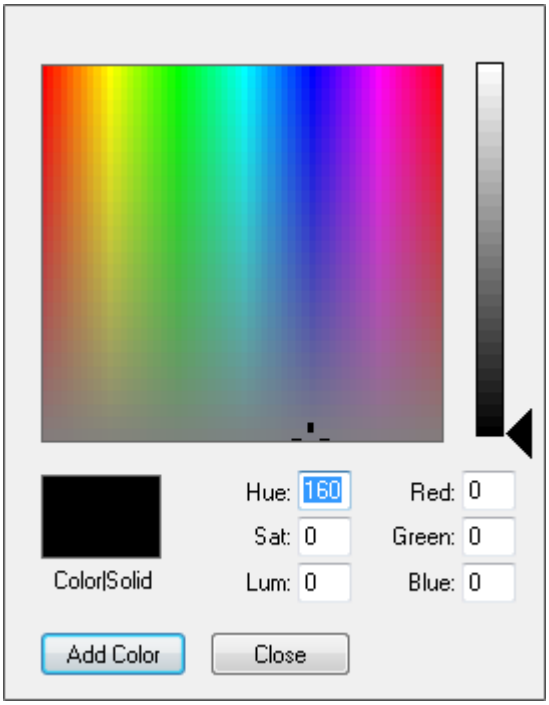


Figure 58

13.1.3.5 Outline color

Default value: Black (0,0,0)

The value specified here determines the colour of the outline/border surrounding the schematic map item.

If the border is transparent, only the opacity setting will affect the specified border width of the map item.

Example:

- Interior color – `Web -> Cyan`
- Opacity – `128`
- Outline color – `Web -> Transparent`
- Outline Thickness – `5`
- Show Outline – `True`

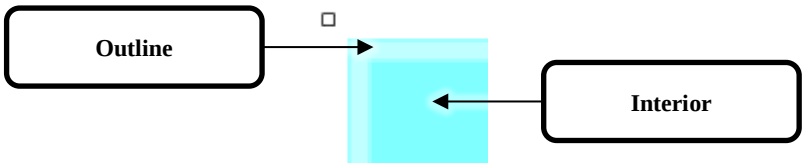


Figure 59

13.1.4 Label Format

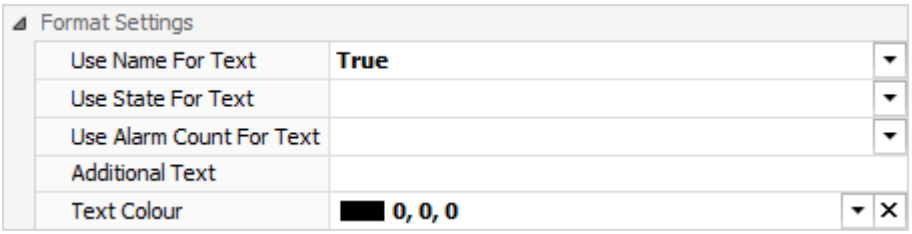


Figure 60

13.1.4.1 Use Name For Text

Default value: True

When set to True, the name of the item associated with the presenter will be displayed.

When set to False, the name of the item associated with the presenter will not be displayed.

13.1.4.2 Use State For Text

Default value: (Blank)

When set to True, the state of the item associated with the presenter will be displayed.
When set to False, the state of the item associated with the presenter will not be displayed.

13.1.4.3 Use Alarm Count For Text

Default value: (Blank)

When set to True, the alarm count of the item associated with the presenter will be displayed.
When set to False, the alarm count of the item associated with the presenter will not be displayed.
If the item associated with the presenter does not have an alarm count, setting this option has no effect.

13.1.4.4 Additional Text

Default value: (Blank)

Text entered in this field is appended to the end of the label for the associated map item. The text will be separated by a hyphen.

13.1.4.5 Text colour:

Default value: Black (0,0,0)

Colour selections are made up of a combination of 3 values (Red, Green and Blue) in the range of 0 and 255. The interior colour of the item can be a Web, System or Custom colour. You can manually enter the colour or click the drop down to select the colour from the colour picker.

Manual colour entry examples:

`0,0,255` Blue

255,0,0	Red
0,255,0	Green
0,255,255	Cyan

If the colour value entered has the same value as any of the colours found under the Web or System colour picker tabs, it will automatically change to the colour name.

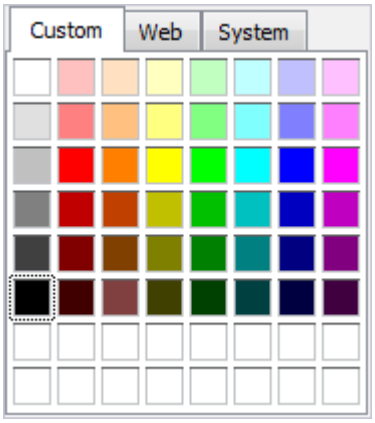


Figure 61

Right-click any of the colour squares in the bottom two rows of the Custom tab to add your own colour.

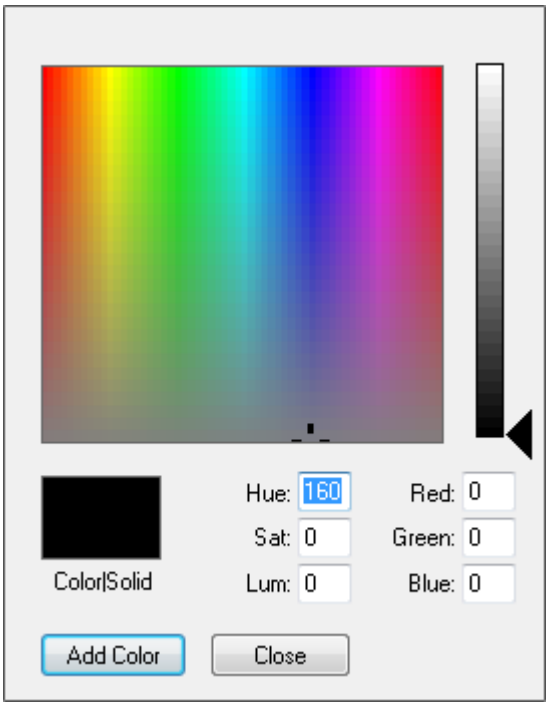


Figure 62

13.2 Configuration of Schematic Maps

Schematic maps are created, modified and removed through the Integriti System Designer. Schematic maps are found in the Schematics group under the System tab. Click the Schematic Maps button to open the schematic maps panel.

1. Click on Add New to open the schematic map designer.

To modify an existing schematic map:

1. Login to the Integriti System Designer.
2. Click on the System tab followed by Schematic Maps.
3. Double-click one of the existing the maps.

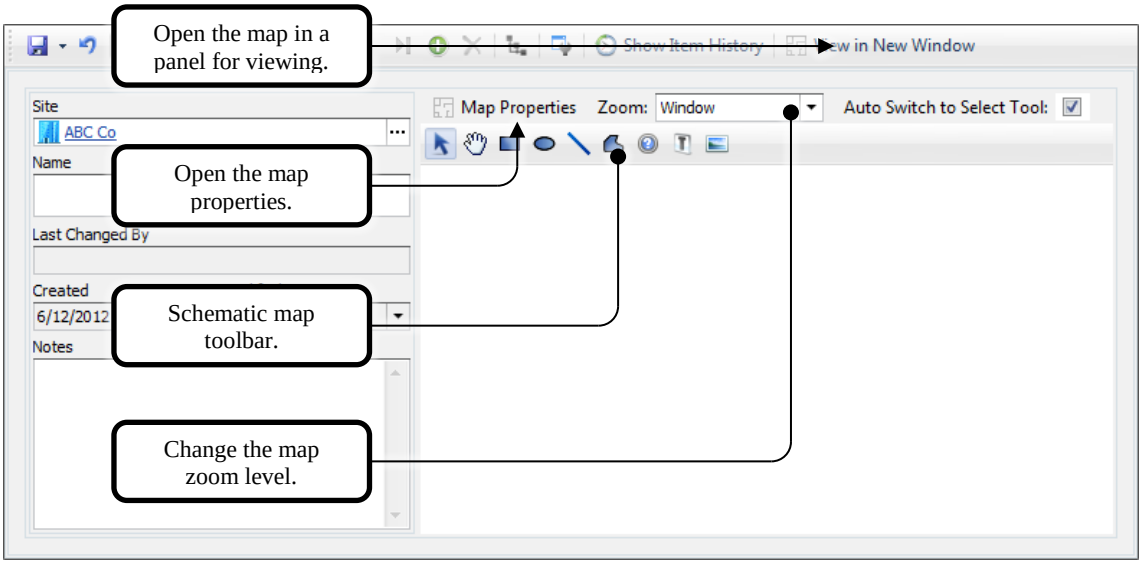


Figure 63

13.2.1 Map properties

Click the Map Properties button will open the schematic map properties.

13.2.1.1 Background

The map background width and height are determined automatically when loading a background image. You can adjust these values manually but this will stretch the background image (if one has been specified).

The background colour is white (255,255,255) by default. It is only visible if there is no background image or the image has transparent regions.

To load a background image, click on the Change button.
To remove the background image, click on the Clear button.

13.2.1.2 Grid Overlay

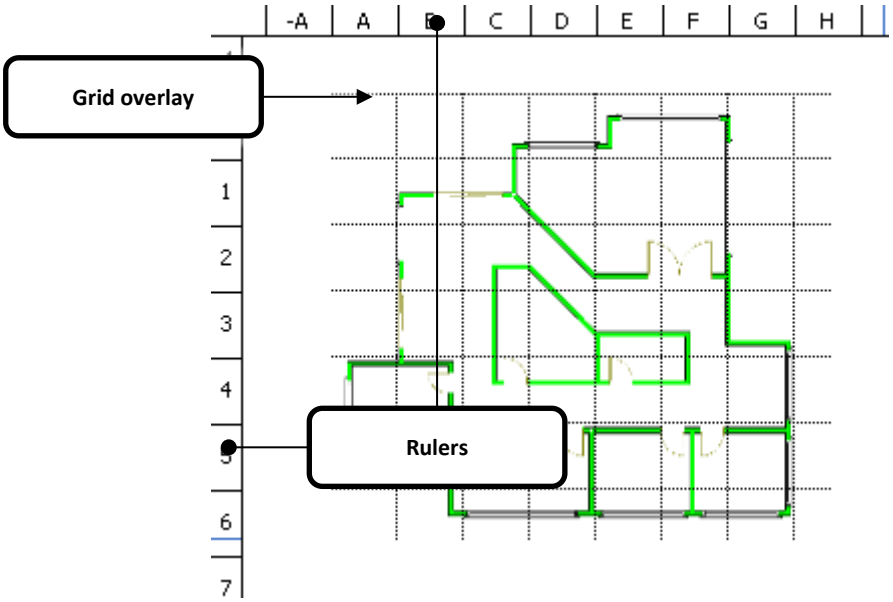


Figure 64

Enabling the grid overlay will place dotted grid lines over the schematic.
Enabling the rulers will place alphanumeric grid reference rulers to the top and left of the schematic map.

The grid block width and height are measured in pixels. The scale of the grid will vary with the schematic map zoom level.

13.2.1.3 Default Font

The default font used for schematic maps is Arial, 12pt. This can be adjusted by clicking on the ellipsis (...) and selecting your font preferences in the font selection window.

The default font will be used for all newly created schematic map items. Changing the default font will not override font settings for existing map items.

13.2.2 Schematic map toolbar

The schematic toolbar contains all of the controls necessary for creating the schematic.

Select tool

The select tool allows you to select and modify properties of items on the schematic. Ticking Auto Switch to Select Tool will cause the select tool to become active after a new item has been successfully added to the schematic.

Pan tool

If the schematic is at a zoom level larger than the screen, use this tool to move the schematic around the screen.

Rectangle tool

To draw a rectangle on the schematic:

1. Select the rectangle tool.
2. Click and drag to draw a rectangle. Where you press and release your mouse button will define the shape of the rectangle.
    - Pressing and holding shift for this step will allow you to create a square.
3. The Map Element Properties window will appear immediately after the element has been drawn.

Ellipse tool

To draw an eclipse on the schematic:

1. Select the eclipse tool.
2. Click and drag to draw an ellipse. Where you press and release your mouse button will define the shape of the ellipse.
    - Pressing and holding shift for this step will allow you to create a circle.
3. The Map Element Properties window will appear immediately after the element has been drawn.

Line tool

To draw a line on the schematic:

1. Select the line tool.
2. Click and drag to draw the line. Where you press and release your mouse button will define the position and length of the line.
3. The Map Element Properties window will appear immediately after the element has been drawn.

Freeform tool

To draw a freeform element on the schematic:

1. Select the freeform tool.
2. Click once at the starting point of where you want to create the freeform object.
3. Continue clicking on the schematic to place multiple points on the freeform element.
4. When you have finished, double-click.
5. The Map Element Properties window will appear immediately after the element has been drawn.

Once you have closed the Map Element Properties window, you can continue to fine tune the freeform element.
Click and drag your mouse along any freeform line to create a new node on the element.
Right-click any node on the freeform element to delete it.
You can click and drag any existing nodes on the freeform element.

Icon tool

Click where you would like to place the icon.

Label tool

Click where you would like to place a text label.

Image tool

Click where you would like to place the image.

13.2.3 Map Element Properties

Every item placed on the schematic map has its own set of properties.

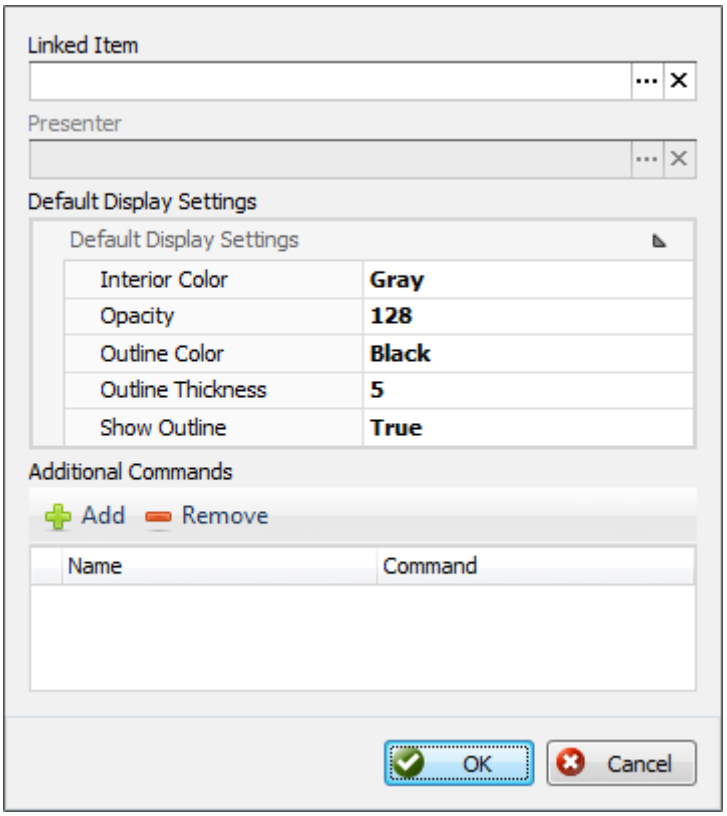


Figure 65

13.2.3.1 Linked Item

If a map element is linked to something, it will reflect the status of whatever it is linked to which is determined by the selected presenter.

To link the element to an item, click the ··· and select the item from the list that appears.

To remove the link, click on the ×.

13.2.3.2 Presenter

A presenter is a collection of format settings and rules that govern how a map item will behave on the schematic. Presenters can only be assigned to a schematic map item if it is linked to an entity.

When a linked item has been selected, an element presenter will automatically be associated with the schematic map item. If a default element presenter for the item type has not been designated, the element presenter that is automatically associated with the map item will be randomly selected.

Some presenters have been included with the Integriti software to cover common map item types. The included presenter item types are:

- Area
- Auxiliary
- Camera
- Controller
- Door
- Input
- LCD Terminal
- Macro
- Schematic Map

13.2.3.3 Default Display settings

13.2.3.3.1 Interior colour:

Default value: Grey (128,128,128)

Colour selections are made up of a combination of 3 values (Red, Green and Blue) in the range of 0 and 255. The interior colour of the item can be a Web, System or Custom colour. You can manually enter the colour or click the drop down to select the colour from the colour picker.

Manual colour entry examples:

`0,0,255`	Blue
`255,0,0`	Red
`0,255,0`	Green
`0,255,255`	Cyan

If the colour value entered has the same value as any of the colours found under the Web or System colour picker tabs, it will automatically change to the colour name.

Figure 66

Right-click any of the colour squares in the bottom two rows of the Custom tab to add your own colour.

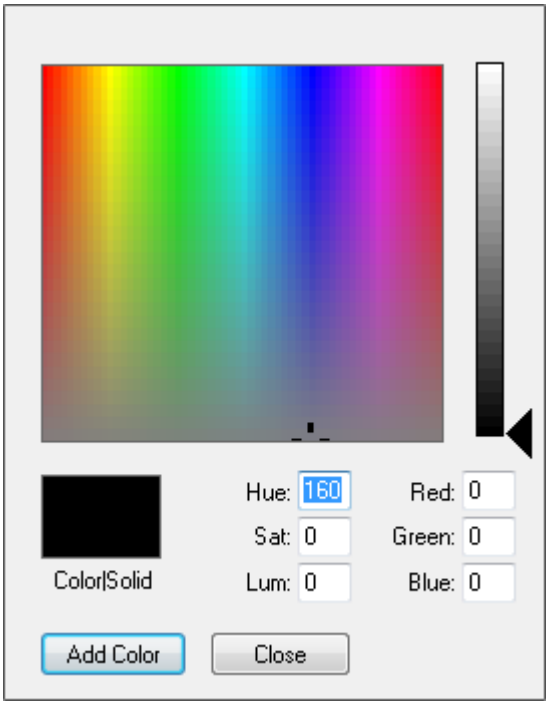


Figure 67

13.2.3.3.2 Opacity 0-255

Default value: 128 (semi-transparent)

The opacity affects both the Interior and outline colour. Use a value of 255 for opaque and a value of 0 for transparent.

13.2.3.3.3 Outline color

Default value: Black (0,0,0)

The value specified here determines the colour of the outline/border surrounding the schematic map item.

If the border is transparent, only the opacity setting will affect the specified border width of the map item.

Example:

- Interior color – `Web -> Cyan`
- Opacity – `128`
- Outline color – `Web -> Transparent`
- Outline Thickness – `5`
- Show Outline – `True`

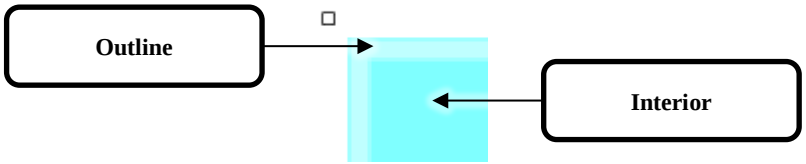


Figure 68

13.2.3.3.4 Outline Thickness

Default value: 5 pixels

The value specified here will determine the thickness of the border / outline. A value of 0 will leave a 1 pixel border.

13.2.3.3.5 Show outline

Default value: True

Setting this option to False will disable the outline of the item.

13.2.3.4 Additional Commands

Schematic map items can have custom commands assigned to them. When an operator clicks (or right-clicks) a schematic map item, a list of the available commands will be presented to them. Additional commands are appended to the end of the list.

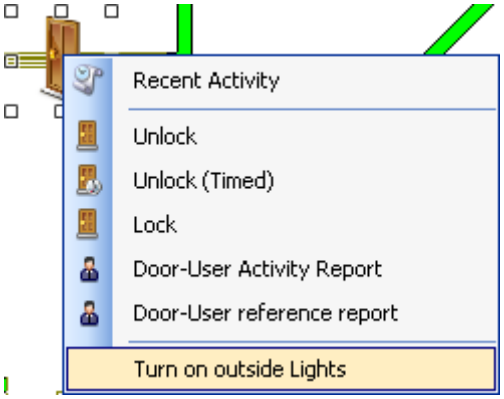


Figure 69

13.2.3.4.1 Creating additional commands

1. Click on Add to create an additional command in the additional commands list.
2. Click in the name field and give a name to the new command.
3. Click on the command field followed by ...
4. Select an option from the Action Type drop down list.
    - See the table below for more information.

None	Does not perform any action. Can be used as a place holder for future use or for entering notes.
ControllerAction	Can assert or dis-assert any action on the controller. Specify the action to send and the edge type.
DBBackup	Backup the entire database to a specified location. DB Backup has two options: • Include review data. • Append a date/time stamp the exported filename.
Delay	**Not used here.** This action type should only be used within a sequential list (below).
LogReview	Put a message in review. You can specify the review level and the message text.
ParallelList	Execute a list of commands in parallel. This will open a new Configure Task Action window where a list of actions can be executed in simultaneously.
SequentialList	Execute a list of commands in order. This will open a new Configure Task Action window where a list of actions can be executed in order.
SyncTime	Synchronise the time/date of one or many controllers. To update the time of all Integriti controllers, leave the controller field blank. To update a specific Integriti controller, open a controller for editing, copy its name and paste it in to this field.

14 Layouts & Editors

The layout of the entire management suite can be customised and stored. Stored layouts include:

- Positioning of each individual docking panel.
- Its own layout set. Which includes:
  - Positioning of each individual dialog window.
  - Content layout of each entity editor dialog window.

Layouts can be assigned to individual operators as required.

To customise an individual docking panel, open it and click the button.

Additional layout configuration settings are found under the Window tab.

Pressing the Reset Layout button will restore the entire layout back to the factory default settings.

14.1 Layouts

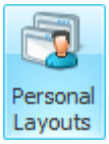
Layouts contain information about the panel(s) that are displayed and their position. Client workstations can be configured to automatically load a layout on start-up. There are two types of layouts – Personal and System.

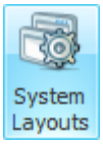
Personal layouts are tied to the individual operator. Where permitted, operators can create their own System Designer and Gatekeeper layout.

System layouts can be used as the 'default' or an 'enforced' layout by configuring operator type permissions.

Personal layouts are automatically associated with the operator who created them. They are intended to be used by "Power Users" who wish to define several layouts for their own personal use. System Layouts on the other hand can be associated with operators for whom it is desired that they have 1 fixed layout whenever they use the software. If you have already created a personal layout with your own operator, and need to change it into a System Layout, simply load the personal layout, then select the "Save Layout" button and press "System Layout". This can then be associated with another operator.

14.2 Creating and saving layouts

Click on the 

or 

buttons to open one of the layout managers.

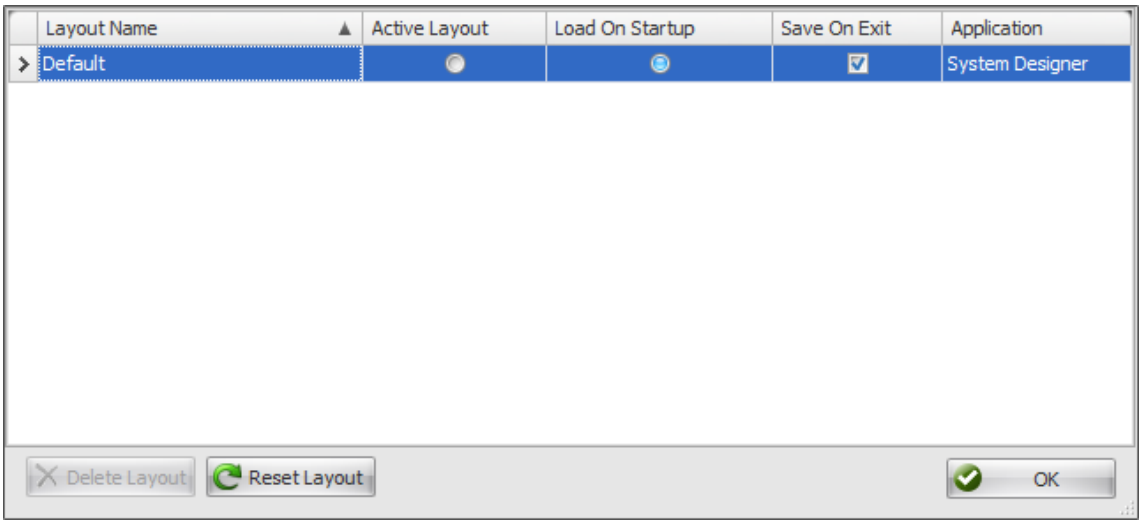
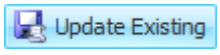


Figure 70

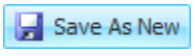
Each client can have its own layout that is loaded in start-up. To select the desired layout, click on the radio button in the 'Load On Startup' column to the right of the desired layout.

The active layout can be changed at any time by opening the layout manager and clicking on the radio button in the 'Active Layout' column to the right of the desired layout.

If the active layout has the 'Save On Exit' checkbox ticked, the layout will be saved when the Integriti software management suite is closed. Next time the layout is loaded, the layout will restore to the state it was in prior to Integriti closing.

Clicking the 

button will save the currently active layout over an existing layout.

Clicking 

will allow you to save the current layout as a new layout. A dialog window will appear prompting the user to enter a name for the new layout.

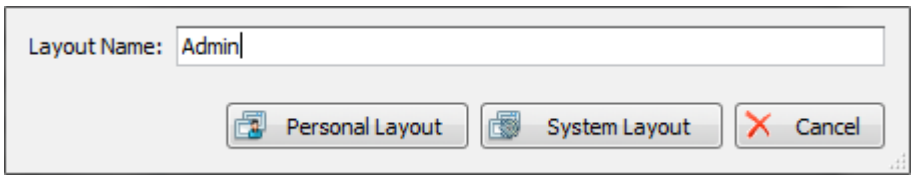
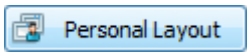
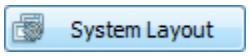


Figure 71

Enter the name of the layout then click on the 

or 

button to save.

Click on the

button to load a specific layout.

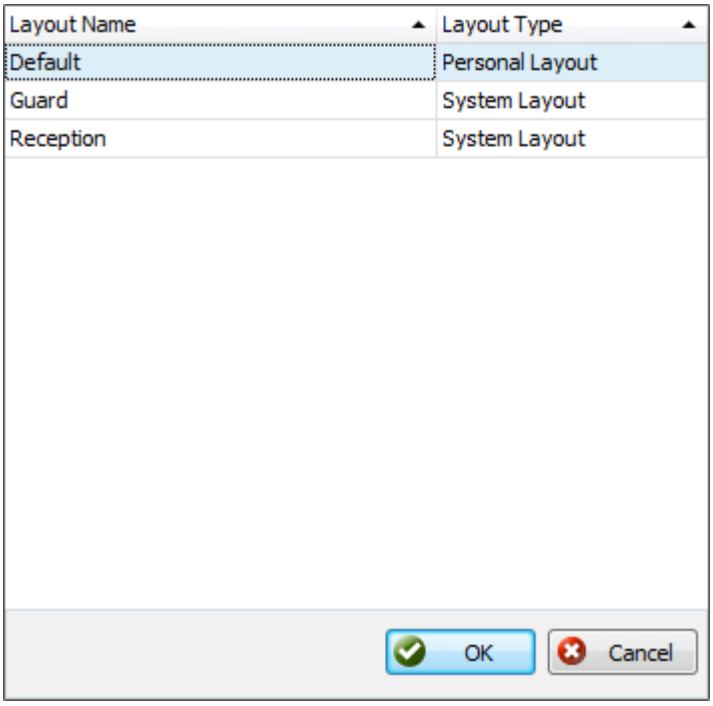


Figure 72

Click on the desired layout followed by

.

14.3 Editor layout sets

Click on the

button under the

tab to open the editor layouts panel.

The 'Default' editor layout set is suitable for most applications. The ability to create custom editor layouts allows you to:

- Hide unused / unnecessary portions of the layout.
- Rearrange each individual layout.
- Add custom content to layouts.

Editor layouts may be customised to suit individual operators or operator groups.

Double-click an editor layout set to re-configure it or click

to create a new one.

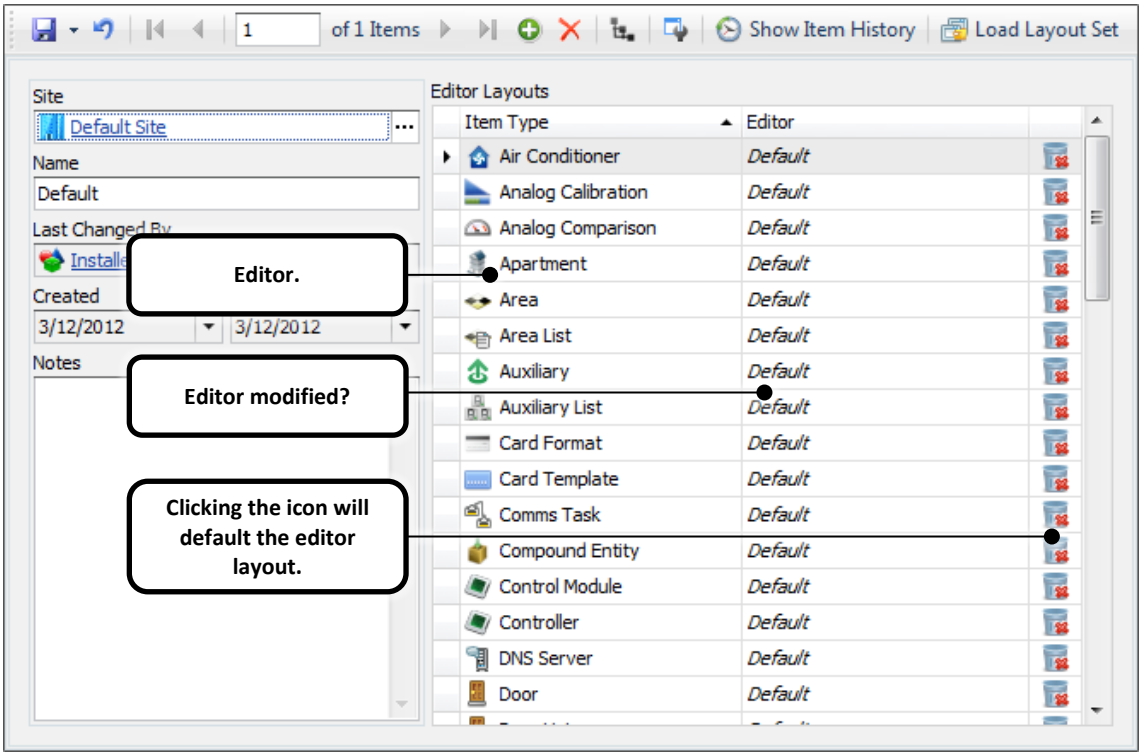


Figure 73

Individual editor layouts can be defaulted by clicking the icon.

To edit an editor layout, double-click it to open the editor dialog window in layout mode.

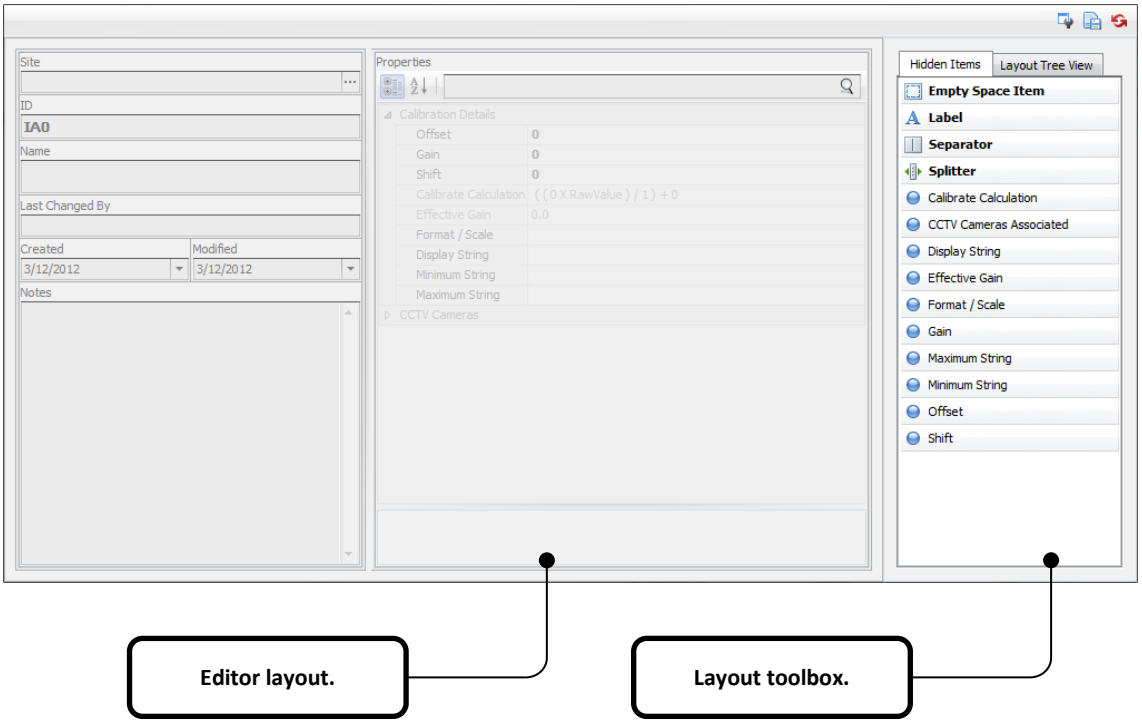


Figure 74

Please refer to the document titled 'Interface Elements for Integriti' for more information on how to use the layout manager.

	Toggle between the Editor and a preview of the
	Save the current layout.
	Restore the layout back to the factory default. (Click Save to commit changes)

Table 4

15 Communications Tasks

All external system communication is controlled by means of 'Comms Tasks'. As the name suggests a Comms Task is a communications task or job that you wish the system to carry out. Because there can be more than one Comms Task, it is also possible for more than one communications task to be operating at once.

e.g. To configure the system for a review printer you simply allocate one of the available Comms Tasks to perform the automation function. If you wish an alarms dialler to be operational as well, you simply assign another Comms Tasks the job of being a dialler format such as Contact ID.

The total number of available Comms Tasks available is ten (including the Integriti Comms Task). Comms Tasks can either be "active" or "idle". When the system is powered up, all programmed Comms Tasks are set to active so they can immediately start their intended function. If you wish to stop a Comms Task, for example abort a dialler format halfway through reporting, simply set that Comms Task to idle.

15.1 Serial Channel

Comms Tasks use communications ports to communicate with the outside world.

When a Comms Task is set to carry out a function, for example send data to a printer, it will be configured to use one of the available communications ports. For example a Comms Task programmed for automation may be configured to use "Unibus UART 1 (1)". This means that "Unibus UART 1 (1)" cannot be used for any other purpose unless the Comms Task is set to idle. Some Comms Tasks may share ports with other Comms Tasks. For example, Comms Tasks designed to be used with the modem can share the one communications port. Although these tasks may be configured to use the modem, when they are not reporting they are not using the port. If both tasks needed to use the modem for reporting at the same time, one Comms Task will use the port first and, when finished, the other Comms Task will use the port.

Comms Task types describe the job a particular Comms Task is to perform. For example, programming a Comms Task to Dialler will invoke a Contact ID, IR Fast, SIA or 4+2 dialler. The programming of options for the Dialler is unique to that Comms Task. If another Comms Task were also to be programmed to Dialler, the options for this Comms Task will be separate from those of the pre-existing one. This allows the commissioning of dual reporting with each Comms Task using its own Telephone Numbers and options. Listed below are the possible Comms Task types.

A maximum of 10 communication tasks can exist on the Integriti controller.

The number of serial channels available will depend upon the number of UniBus devices fitted to the Integriti controller.

Available Serial Channels:

- None
- Modem
- Onboard RS485 Reader Port
- UART 0
- Unibus UART 1 (1)
- Unibus UART 1 (2)
- Unibus UART 2 (1)
- Unibus UART 2 (2)
- Unibus UART 3 (1)
- Unibus UART 3 (2)
- Unibus UART 4 (1)
- Unibus UART 4 (2)
- USB Master
- USB Slave

15.2 Communications tasks:

15.2.1 Integriti

This communications task is usually present and active on an Integriti controller. The Integriti communications task is used to connect an Integriti controller its server. The Integriti communications task is usually the 1st communications task in the system.

15.2.2 Monitor

The Monitor communications task is reserved for use by Inner Range.

15.2.3 Dialler

This communications task uses the on board legacy modem to transmit messages back to the monitoring centre. Supported communications formats are:

- IRFast
- Contact ID
- SIA
- 4+2

15.2.4 GSM

The GSM Communications Task can interface with one of the many Inner Range FE3000 or Inner Range Multipath STU products. The Integriti Controller's GSM Communications Task is used to communicate reportable events to a Central Monitoring Station, to send reportable events via SMS message and/or to receive SMS control messages.

15.2.5 Automation

The automation communications task can be used for review printing and acknowledgement as well as control and interrogation of the controller. This communications task works over a serial UART or Ethernet.

Control and interrogation options require licensing.

15.2.6 EMS

Low and high level lift interfacing is available using this communications task. This is a licensed option.

15.2.7 Securitel

The Securitel network was a “direct-line” alarm transmission network that was supplied and maintained by Telstra. Alarm panels in the field were connected to a Subscriber Terminal Unit (a STU) and the STU would communicate events via the PSTN to Nodes that were hosted by Telstra. These events were then transmitted to a Central Monitoring Station for processing/actioning.

15.2.8 Intercom

The Integriti Controller has an Intercom Comms Task and an Apartment entity structure. The Integriti Controller’s philosophy for an Intercom system is that there is an Apartment that can grant access to a Call Location. An Apartment can optionally have a Floor defined as well as having an Intercom System Floor and an Intercom System Unit. Up to 32 Call Locations can be defined in the Intercom Comms Task and each can optionally have a Door and/or up to 4 Lift Cars defined. When the Intercom Comms Task detects that an Apartment has granted access to a Call Location, the defined Door and Lift(s) are temporarily unlocked/unsecured to allow access.

16 Communications Handlers

Communications Handlers work as a conduit between the Integriti Application Server service (the Integriti server) and other 3rd party products.

16.1 Review Receiver

Integriti 3rd party review receiver allows review to be streamed from a third party TCP client to the Integriti server for review logging.

Please refer to the document titled 'Integriti Communications Handlers - Review Receiver' for more information.

16.2 Review Sender

Integriti review sender allows review to be streamed to a third party TCP client.

Please refer to the document titled 'Integriti Communications Handlers - Review Sender' for more information.

16.3 REST/XML Web Service

The Integriti application server hosts a REST/XML based Web Service allowing integration with a wide variety of programming languages and environments in a stateless, query based fashion.

Please refer to the document titled 'Integriti Communications Handlers - REST XML Web Service' for more information.

17 Alerts

Alerts bring to the attention of one or many operators the change of state of one or many events.

Alerts consist of Alert Definitions, Alert Groups, Alert Views and Response Plans. Alert Definitions contain all of the information necessary to define the source of the alert and the appearance of the alert. Alert definitions can optionally invoke actions at various stages of the alerts lifecycle.

Alerts are created and configured in the Integriti System Designer. Alerts are actioned within Integriti Gate Keeper.

Alerts should only be used in situations where human intervention is required.
i.e. “An Operator must acknowledge an alert”
For automated actions, a Scheduled Tasks should be configured.

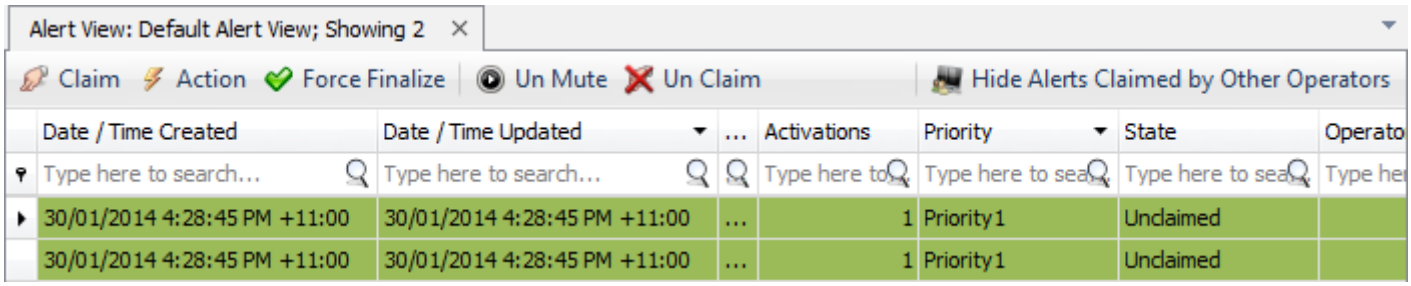


Figure 75

Alert Definitions

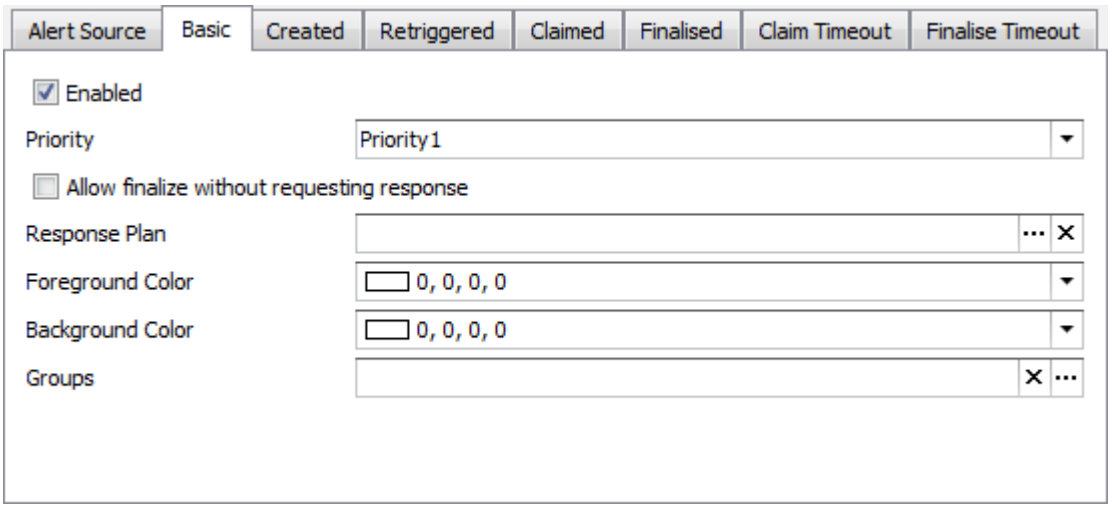
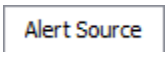
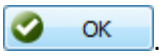


Figure 76

To create a new Alert Group…

1. Open the panel from the tab.
2. Click the button to create a new Alert Definition.
3. Give the new Alert Definition a name and enter a description in the notes field.
4. Click on the  tab.
   a. Select an alert source from the drop down list.
      - Intruder Events
        i. Three filters are available for intruder events. If a field is left blank then it is considered as 'all'. The three filters use AND logic.
        ii. Select one or many sites, areas or inputs by clicking the ··· to the right of the field to open a selection window.
        iii. Select one or many items from the list and click  .
        iv. The two 'Group Alerts by' buttons will group alerts of the same type in the alert view based on Areas, Inputs or both.
      - Review Filter
        i. Information on how to create filter stacks is available in the appendix under the section titled 'Filter Stacks'.
        ii. Tick 'Group All Active Alerts for this Alert Definition' to group alerts of the same type in the alert view.
      - Hardware Offline
        i. Two filters are available for hardware offline. If a field is left blank then it is considered as 'all'. The filters use AND logic.
        ii. Select one or many sites and/or modules by clicking the ··· to the right of the field to open a selection window.

iii. Select one or many items from the list and click OK.

iv. Tick the group alerts by bodules checkbox to group alerts of the same type in the alert view.

- The remaining tabs have their own action list that will execute at various stages of the alert.
  a. To execute all of the items in the list simultaneously, click on the Execute In Parallel button.
  b. To add actions to a list, click on the Add button.
     - For more information on the various actions available, see the section titled 'Actions'.
  c. If 'Supress if muted' is ticked under the Retriggered tab, actions in that list will not be executed.
- The Claim Timeout and Finalise Timeout tabs each have their own time out in hours, minutes and seconds. Setting these values will cause the actions in the list to be executed once the time specified has expired.

5. Click and close the Alert Definition.

17.1 Alert Groups

An Alert Group is a logical place holder for Alert Definitions. An Alert Group has no properties of its own. It is used for organising alerts only (such as in Alert Views).

To create a new Alert Group…

1. Open the Alert Groups panel from the Administration tab.

2. Click the Add New button to create a new Alert Group.

3. Give the new Alert Group a name and enter a description in the notes field.

4. Click and close the Alert Group.

17.2 Alert Views

Alert Views are lists containing Alerts belonging to the groups specified within the Alert View.

To create a new Alert View…

1. Open the Alert Views panel from the Administration tab.
2. Click the Add New button to create a new Alert View.
3. Give the new Alert View a name and enter a description in the notes field.
4. Expand-out Settings and click on the ··· to the right of groups.
5. In the window that appears, click on the Add button and select one or many Alert Groups from the list that appears.
6. Click OK to confirm your selection. Click OK once more to go back to the Alert View editor window.
7. Click and close the Alert View.

17.3 Response Plans

Response Plans can be used as an alternative to the default Finalize Response window. Response Plan windows can contain custom text in the form of instructions, checklists, buttons, alert details, response history and operator response items.

For more information on the Response Plan layout manager, please refer to the document titled 'Interface Elements for Integriti'.

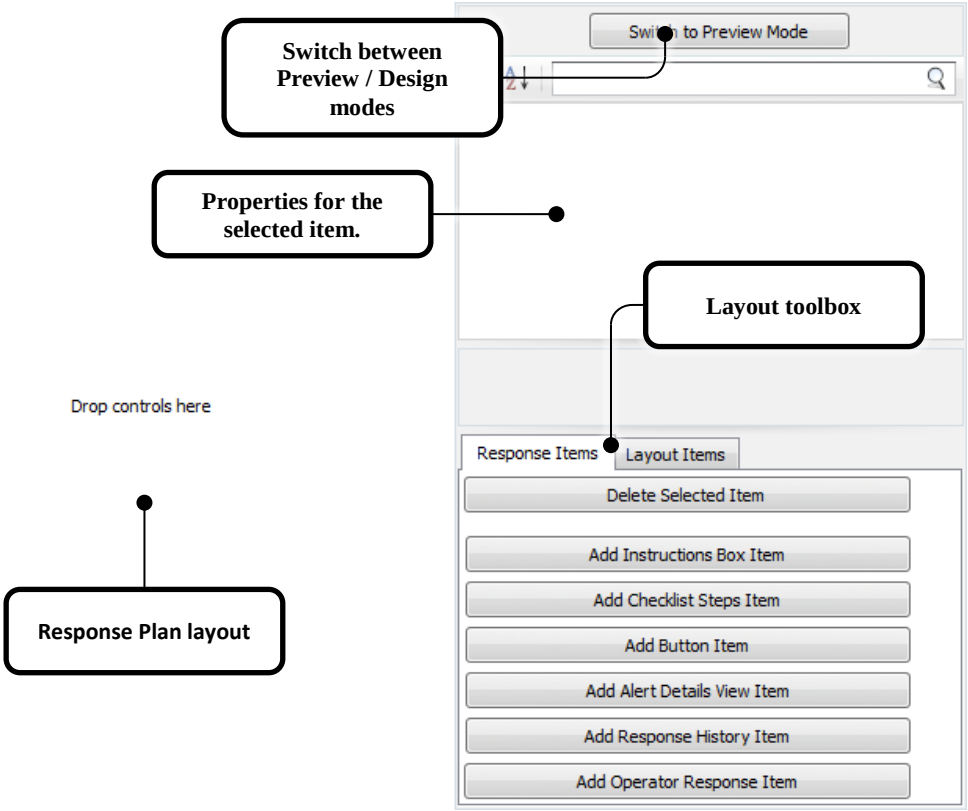
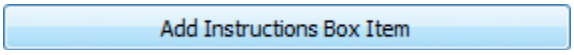


Figure 77

17.3.1 Delete Selected Item

Clicking this button will delete the selected item from the response plan layout.

17.3.2 Information Box Item



Selecting this and dragging it over to the Response Plan Layout designer on the left adds a text box containing configurable text.

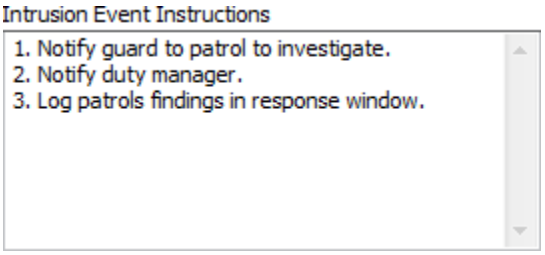


Figure 78

There are three configurable options available:
Information Text – Contains plain text. Format strings can be used here by clicking the ellipsis button.
Caption Text – This is an optional text label for the Instruction Box item.
Font – Set the type of font used.

17.3.3 Information Display Item

Selecting this and dragging it over to the Response Plan Layout designer on the left adds a box containing configurable important text. This text can be horizontally and vertically aligned, as well as have different sizes and formatting options.

Figure 79

There are five configurable options available:
Information Text –This can contain formatting tags and Format String Keywords alongside text. The Configure Format Strings form can be opened by clicking the ellipsis button.
Vertical Alignment – Allows setting of vertical alignment to Default, Top, Center, or Bottom.
Horizontal Alignment – Allows setting of horizontal alignment to Default, Top, Center, or Bottom.
Caption Text – This is an optional text label for the Checklist Step item.
Font – Set the type of font used.

17.3.4 Alert Custom Field

Selecting this and dragging it over to the Response Plan Layout designer on the left adds a field that is linked to a selectable Alerts Custom Field. This allows the operator experiencing the Response plan to add customisable input, which appears in Gatekeeper beside the alert.

17.3.5 Action Button

Add Button Item

Clicking this button adds a Button Item to the Response Plan. Response plan buttons can invoke any action in the section 'Action types'.

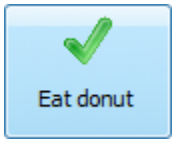


Figure 80

Button Action – Set the action for this button to invoke when clicked.
Button Text – Text for this button to display.
Button Image – Optional button image. Click the ··· to open a .bmp, .gif, .jpg, .png or .ico.
Button Text – Optional text displayed on the button
Image Width – The width of the image in pixels
Image Height – The Height of the image in pixels

17.3.6 Alert Details

Add Alert Details View Item

The Alert Details View Item displays review history that is directly related to the alert.

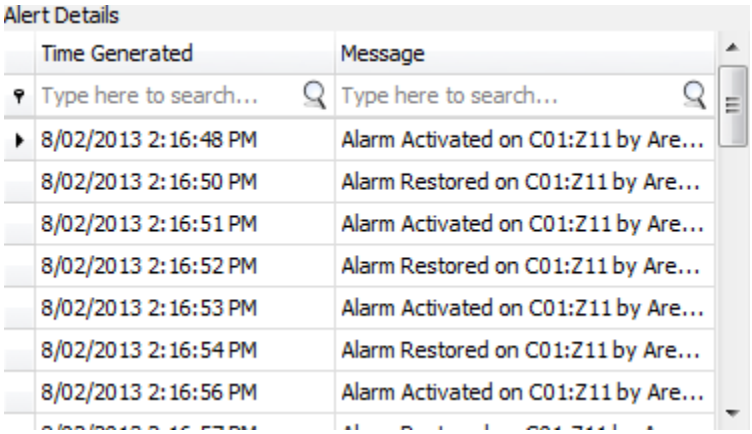


Figure 81

17.3.7 Response History Item

Add Response History Item

The Response History Item displays information regarding the alert such as the creation time, who claimed it, what checklist items have been given values and what response text operators have added to the alert.

Response History

Response Time	Message	Operator
Type here to search...	Type here to search...	Type here to sea
8/02/2013 2:16:49 PM	Alert was created	
12/02/2013 11:45:00 AM	Operator Installer claimed the alert	Installer
12/02/2013 11:45:03 AM	Operator Installer un-claimed the alert	Installer
12/02/2013 11:45:05 AM	Operator Installer claimed the alert	Installer

Figure 82

17.3.8 Add Operator Response Item

Add Operator Response Item

Clicking this button adds an Operator Response Item to the Response Plan. Operators can add their own text to the alert. Clicking the Submit Response will add the text to the Response History.

Operator Response

Found Ethan Hunt dangling in the middle of the server room.

Submit Response

Figure 83

There are two options available:
Caption Text – Text to display above the stream.
Text Font – Which font to use.

17.3.9 CCTV Stream

Selecting this and dragging it over to the Layout Designer will create an area which displays a CCTV camera feed when the response plan is shown. This will automatically show feed from the CCTV Camera which has been associated with one or more of the entities which functioned as the trigger for the Alert.

There are two options available:
Caption Text – Text to display above the stream.
Text Font – Which font to use for the caption.

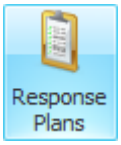
17.3.10 Browser Item

Selecting this and dragging it over to the Layout Designer will create a section which functions as a web browser displaying a single page when the response plan is shown. The URL can be configured via the 'Browser Url' setting of the item.

There are three options available:
Browser Url – The URL to open when the Plan is shown.
Caption Text – The text to display above the Browser Item.
Text Font – Which font to use for the caption.

17.3.11 Creating a new Response Plan

To create a new Response Plan…

1. Open the 

panel from the

tab.
2. Click the

button to create a new Response Plan.
3. Give the new Response Plan a name and enter a description in the notes field.
4. Using the information provided above, create your response plan layout. For information on layout editor usage, please read the document titled 'Interface Elements for Integriti'.
5. Click and close the Response Plan.

18 Importing Data

Operators with access to the Import data button (accessible from the administration tab) can sort data from a CSV file in to the Integriti database. This feature gives the operator the ability to create, modify or remove a number of records with ease.

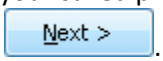
The import tool caters for CSV files with varying layouts and column placement. CSV exports from Insight or files provided by end users can be imported directly in to Integriti.

There are two methods used to import a CSV file. Users can manually import CSV files on a case by case basis or they can create CSV import settings if a known CSV format is going to be used regularly.

18.1 Importing CSV files - manually

1. Start by clicking on the

button under the

tab.
2. An open file dialog window will appear. Find and open your CSV file.
3. The following dialog will ask you to select your saved pre-set, from the list of options (if any), select 'Define settings as you go' and click 

.

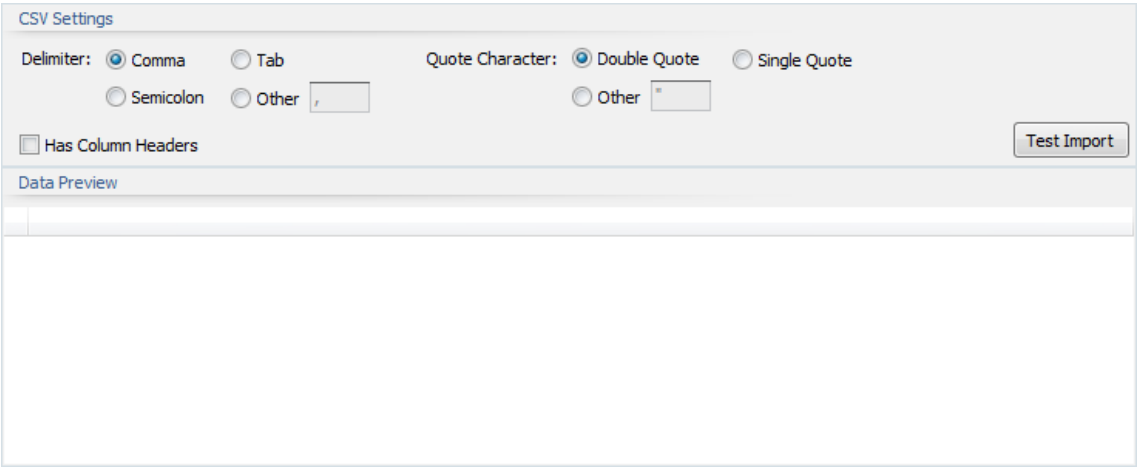


Figure 84

4. The CSV settings dialog window will appear (*Figure 84*). Click

to see if the CSV file will be imported correctly.

   If it does not look correct you have a few options:

   - You can attempt to open the CSV file yourself with a text editing program and see how the file is structured.
   - You can play with the CSV settings and use the

button to see if you can use a few educated guesses to determine the CSV layout.

- You can consult whoever issued you with this CSV file and see if they can provide details on the file structure.

Bad test import examples:

	Column0	Column1	Column2
▸	###	secondname	pin
	Installer		01
	Richie	Florencio	02
	Trenton	Buckalew	03
	Hugh	Sankowski	04
	Luci	Flesher	05

	Column0
▸	###,secon...
	Installer,,0...
	Richie,Flore...
	Trenton,Bu...
	Hugh,Sank...
	Luci,Flesher...
	Bertram...

Figure 85

A good example of what a test import should look like:

	###	secondname	pin
▸	Installer		01
	Richie	Florencio	02
	Trenton	Buckalew	03
	Hugh	Sankowski	04
	Luci	Flesher	05
	Bertram	Scargall	06

Figure 86

If you are importing from Insight, the settings required are Comma delimiter, Double quoted and Has column headers.

5. Click Next > to proceed to field mappings.

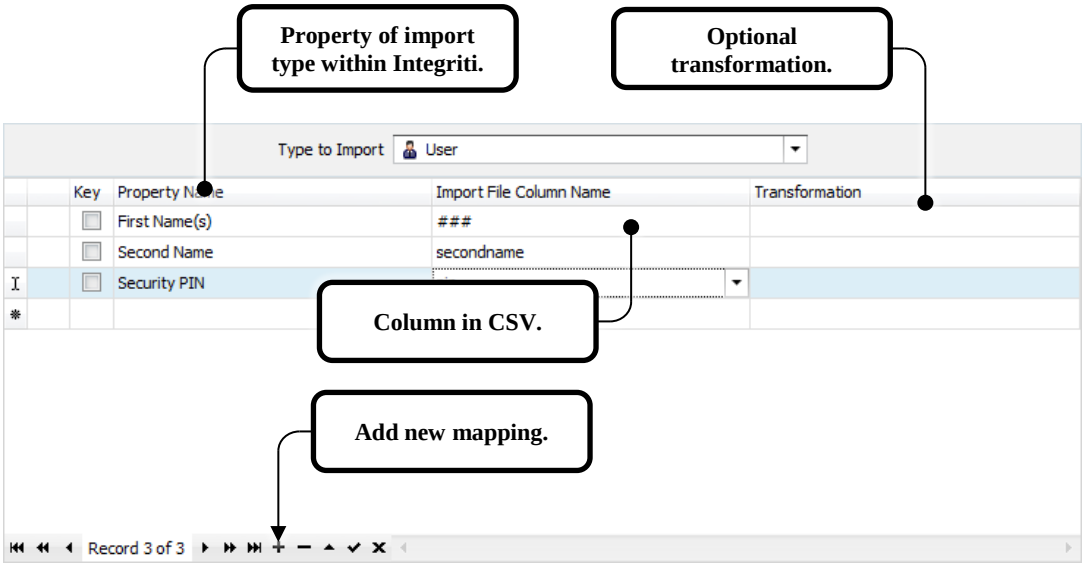


Figure 87

The field mappings dialog allows you to create a lookup table for as many fields in your CSV file as you require.

5.1. Select the type of data you will be importing from the CSV file.

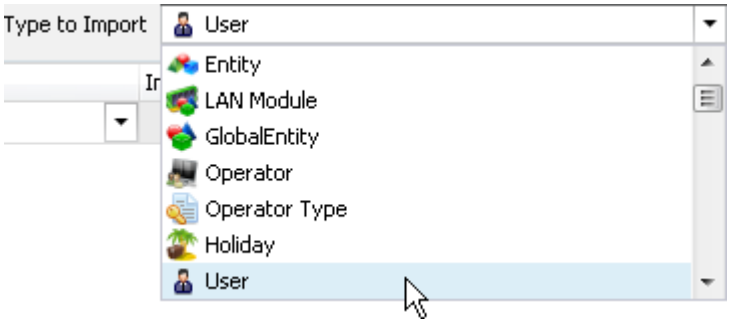


Figure 88

5.2. Begin filling in the lookup table by entering the 1st Property name of the import type.
5.3. Select the Import column to map to the CSV file.
5.4. Transformation is a powerful option that gives you the ability to govern how the data within the CSV field will be interpreted. In most cases you can leave this field blank.
5.5. Repeat steps **5.2** – **5.3** until the necessary mappings have been created.

6. When you are ready to proceed with the import, click Next > and the import process will begin.

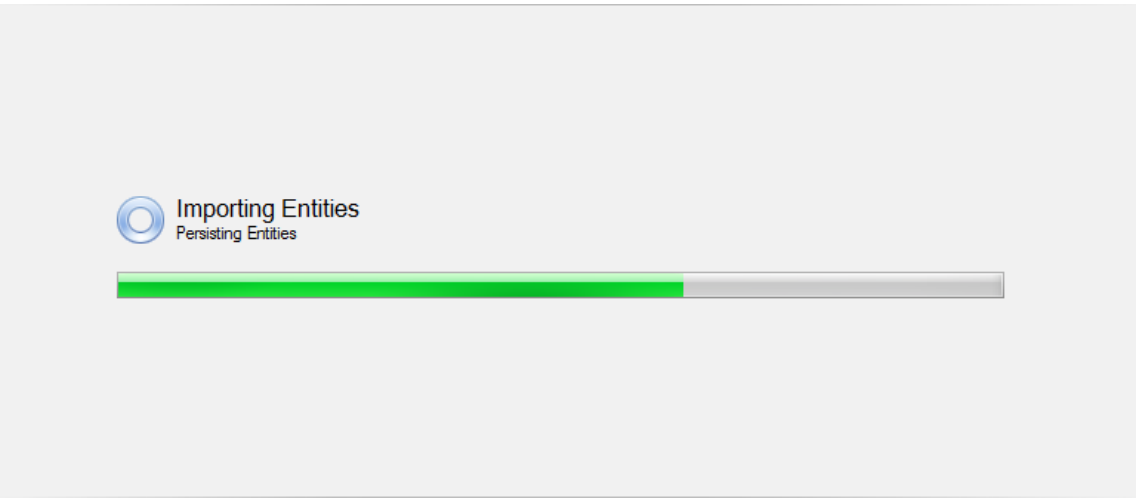


Figure 89

7. Click Finish.

18.2 Importing CSV files – Import Configuration

Import configuration allows you to save the import settings for use every time you need to import a file of the same type.

1. Start by clicking on the Import Configuration button under the Administration tab.
2. Click the Add New button in the Import Configuration panel.
3. Give the new Import Configuration a name and enter a description in the notes field.
4. Click the ... button and select the file that is to be opened and imported.
5. Just as in the manual import procedure above click the appropriate CSV settings.
6. Select the Type to Import.
7. Fill in the lookup table with the appropriate fields to match the imported file.
8. Click and close the Import Configuration.

18.2.1 To use the newly created Import Configuration:

1. Start by clicking on the

button under the

tab.
2. An open file dialog window will appear. Find and open your CSV file.
3. The following dialog will ask you to select your saved pre-set, from the list of options. Drop the list box down and select the pre-set (Import Configuration) you created earlier and click

.
4. Click

.
5. Click

.
6. Click

.

19 Integriti Server Management

19.1 License Management

Use the license manager to view, add and update licenses.

License key management is found under the Administration tab. Click on the License Manager button to open the license manager.

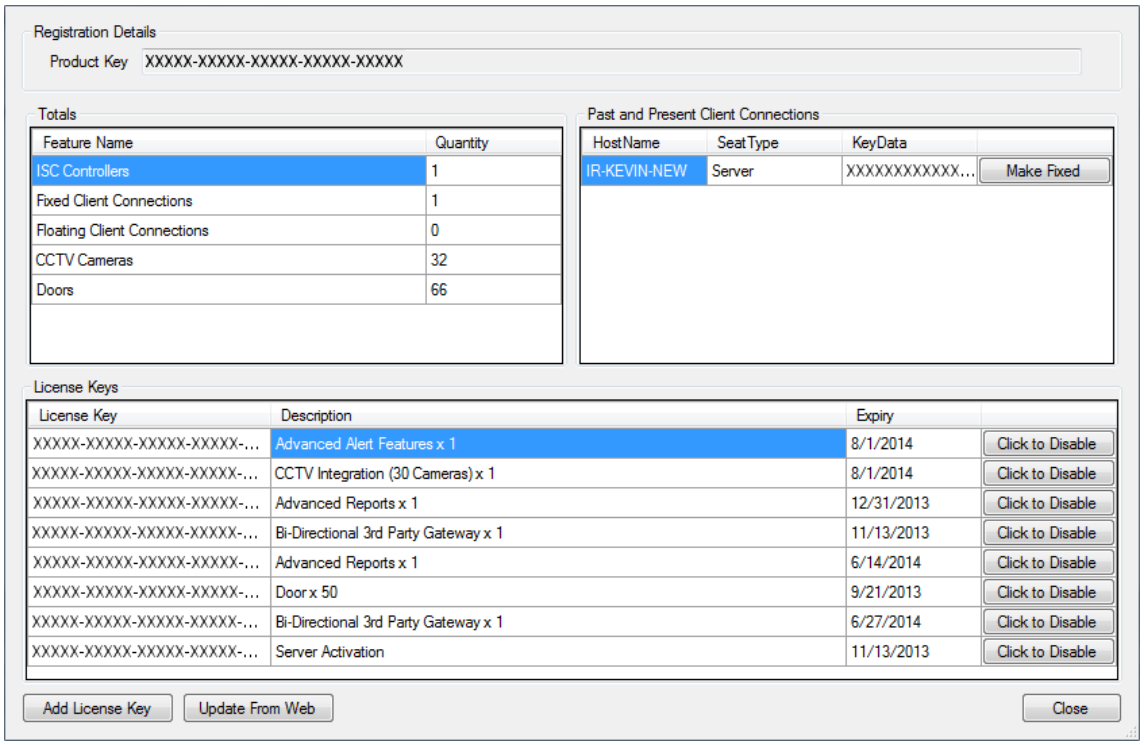


Figure 90

A summary of your license keys is displayed in the 'totals table' on the left side of the license manager.

Each individual license key is displayed in a list at the bottom of the license manager.

'Fixed Client Seats' are licenses allocated to client machines that are going to connect to the Integriti server.

Click Click to Disable to disable a license key. Once you have clicked the Click to Disable button, it will change to Click to Enable. To re-enable the license click Click to Enable.

Click Add License Key to open a new dialog and manually enter in your license key.

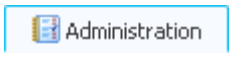
Click Update From Web to automatically update your license keys from the Integriti software license server.

19.2 Operators and Operator Types

Operators are used to access the Integriti software management suite. The Operator Types are groups of settings that define what content can be viewed, modified, removed, etc…

Each Operator is given an Operator Type that defines how much (or how little) they can access within the System Designer and Gate Keeper.

19.3 Operator Type

The Operator Types panel is accessible from the 

tab.

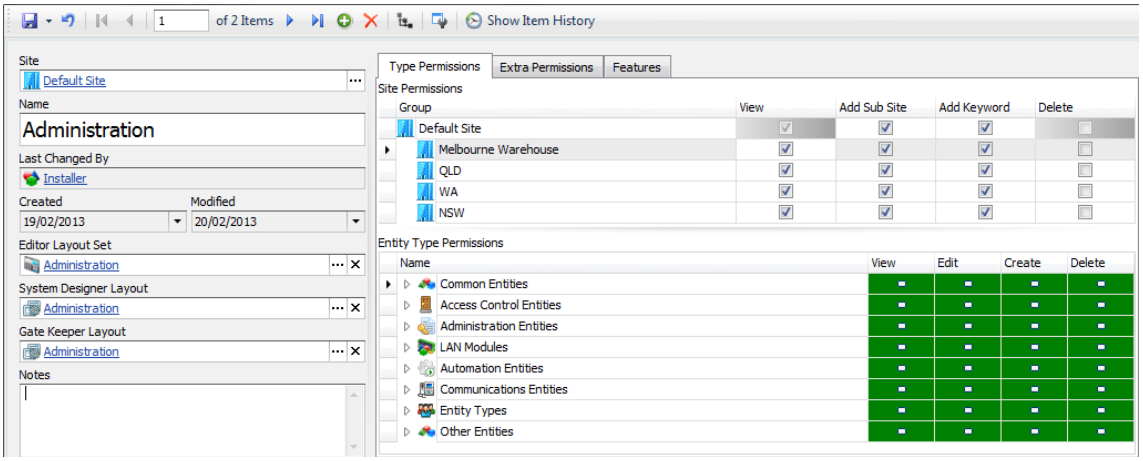


Figure 91

Each Operator Type can have an Editor Layout Set assigned to it. This gives the installer the opportunity to add, remove and re-arrange programming items on each individual editor page.

Custom System Designer and Gate Keeper layouts can also be assigned to the Operator Type.

19.3.1 Type Permissions

Type Permissions

Under the Type Permissions tab there are two sections - Site Permissions and Entity Type Permissions.

Site Permissions contains a list of all of the sites within the database and the option to set View, Add sub site, Add Keyword and Delete permissions.

19.3.1.1 Site Permissions

Site permissions are used to grant access to view, add entities, add to site, add keyword and delete from the navigation panel.

Clicking on the View, Add Entities, Add Sub Site, Add Keyword or Delete check boxes will allow/deny access to all of the entity type permissions that fall under the selected site.

Permission	Description
View	Operators with this permission can see the site.
Edit	Operators with this permission can modify entities belonging to this site.
Add sub site	Operators with this permission can create sub sites.
Add keyword	Operators can add keywords.
Delete	Operators with this permission can delete this site and / or items under it.

19.3.1.2 Entity Type Permissions

The Entity Type Permission tree defines four levels of access to entities within the Integriti system. These are:

Permission	Description
View	Operators can see the entity.
Edit	Operators can modify the entity.
Create	Operators can create new entities of this type.
Delete	Operators can delete entities of this type.

Table 5

Values set at the top level of the tree cascade through to every branch entity.

Name	Description	
	Use the inherited permission.	**Deny**
	Deny.	
	One or many of the deny permissions are inherited.	
	Use the inherited permission.	**Allow**
	Allow.	
	One or many of the allow permissions are inherited.	

Table 6

A blank / empty box indicates that the entities for the group are a mixture of allow and deny permissions.

19.3.1.2.1 Entity Type examples

The following illustration indicates that the Operator Type has allow permissions for all Entity Types excluding Communication Entities. Edit permissions have been revoked from one or many of the Communication Entity Types. This is indicated by the blank edit permission box.

Name	View	Edit	Create	Delete
Common Entities	✓	✓	✓	✓
Access Control Entities	✓	✓	✓	✓
Administration Entities	✓	✓	✓	✓
LAN Modules	✓	✓	✓	✓
Automation Entities	✓	✓	✓	✓
Communications Entities	✓		✓	✓
Entity Types	✓	✓	✓	✓
Other Entities	✓	✓	✓	✓

Figure 92

If we expand out the Communication Entities we can see that edit permissions have been removed from Comms Task entities.

Name	View	Edit	Create	Delete
Common Entities	✓	✓	✓	✓
Access Control Entities	✓	✓	✓	✓
Administration Entities	✓	✓	✓	✓
LAN Modules	✓	✓	✓	✓
Automation Entities	✓	✓	✓	✓
Communications Entities	✓		✓	✓
Comms Task	✓	✗	✓	✓
Telephone number	✓	✓	✓	✓
Telephone Number List	✓	✓	✓	✓
Network Interface	✓	✓	✓	✓
DNS Server	✓	✓	✓	✓
Entity Types	✓	✓	✓	✓
Other Entities	✓	✓	✓	✓

Figure 93

If at this point we were to add a new sub site, we would see the inherited permissions for the sub site appear like so.

Name	View	Edit	Create	Delete
Common Entities	▬	▬	▬	▬
Access Control Entities	▬	▬	▬	▬
Administration Entities	▬	▬	▬	▬
LAN Modules	▬	▬	▬	▬
Automation Entities	▬	▬	▬	▬
Communications Entities	▬	▭	▬	▬
Entity Types	▬	▬	▬	▬
Other Entities	▬	▬	▬	▬

Figure 94

If we were to expand out Communication Entities, we would see that edit permissions have been revoked from Comms Task Entities. These permissions were all inherited from the parent site.

Name	View	Edit	Create	Delete
Common Entities				
Access Control Entities				
Administration Entities				
LAN Modules				
Automation Entities				
Communications Entities				
Comms Task				
Telephone number				
Telephone Number List				
Network Interface				
DNS Server				
Entity Types				
Other Entities				

Figure 95

To override this inherited permission, click on the box to change it from deny to allow. You will notice that the Edit permission for Communication Entities will change to a , indicating that the group contains a mixture of allow permissions.

Name	View	Edit	Create	Delete
Common Entities				
Access Control Entities				
Administration Entities				
LAN Modules				
Automation Entities				
Communications Entities				
Comms Task				
Telephone number				
Telephone Number List				
Network Interface				
DNS Server				
Entity Types				
Other Entities				

Figure 96

19.3.2 Extra Permissions

Extra Permissions

This allows you to give an Operator specific access to an individual item, in any entity across the entire Integriti System. The interface is extremely granular and should not be used to create the majority of the Operator programming. Use this tab to fine tune access to specific entity items.

The checkboxes in the Deny, View, Edit, Delete and Change Permissions columns are there to help you filter your extra permissions. The Entity column can be filtered / sorted by text entered.

The Extra Permissions dialog has four states for each item added to the list:

Permission	Description
View	Operators can see the item.
Edit	Operators can edit the item.
Delete	Operators can delete the item.
Change Permissions	Operators can change the access other operators have to this item.

19.3.3 Features

Features

19.3.3.1 Administration

- Ticking the Import Data checkbox allows the operator to import records.

19.3.3.2 Review

- Operators with View Review ticked will be able to view review.
- Highest Review Level sets the detail / view level of the review data the operator can see

19.3.3.3 Controllers

- Ticking Send Actions allows the operator access to control controller items.
- Ticking Enrol Controllers gives the operator permission to enrol additional controllers.
- Ticking Upgrade Controller Firmware gives the operator permission to upgrade controller firmware.
- Ticking View Controller Data gives the operator permission to access version / hardware information.
- Ticking Lock/Unlock the LAN
- Ticking Remote Hard Reset Controller allows the operator to remotely restart the controller.
- Ticking Disable/Enable LAN modules allows the operator to enable or disable LAN modules.
- Ticking See Blank Entities allows the operator view records that have been 'blanked'.

19.3.3.4 Licensing

- Tick Can Manage Licenses to allow the operator to view, add and update license keys.

19.3.3.5 Layout

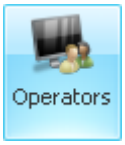
- Tick Change Dock Layouts to give operators permission to change dock layouts.
- Tick Can Switch Dock Layouts to give operators permission to use different dock layouts.
- Tick Can Use Personal Layouts to give operators permission to use their own layout.
    - The operator must have Can Switch Dock Layouts ticked to be able to use personal layouts.

- The operator must have Change Dock Layouts ticked to be able to customise personal layouts.

19.3.3.6 CCTV

- Tick Enrol CCTV Device to give operators permission to enrol new DVRs.

19.4 Operator



The Operators panel is accessible from the Administration tab.

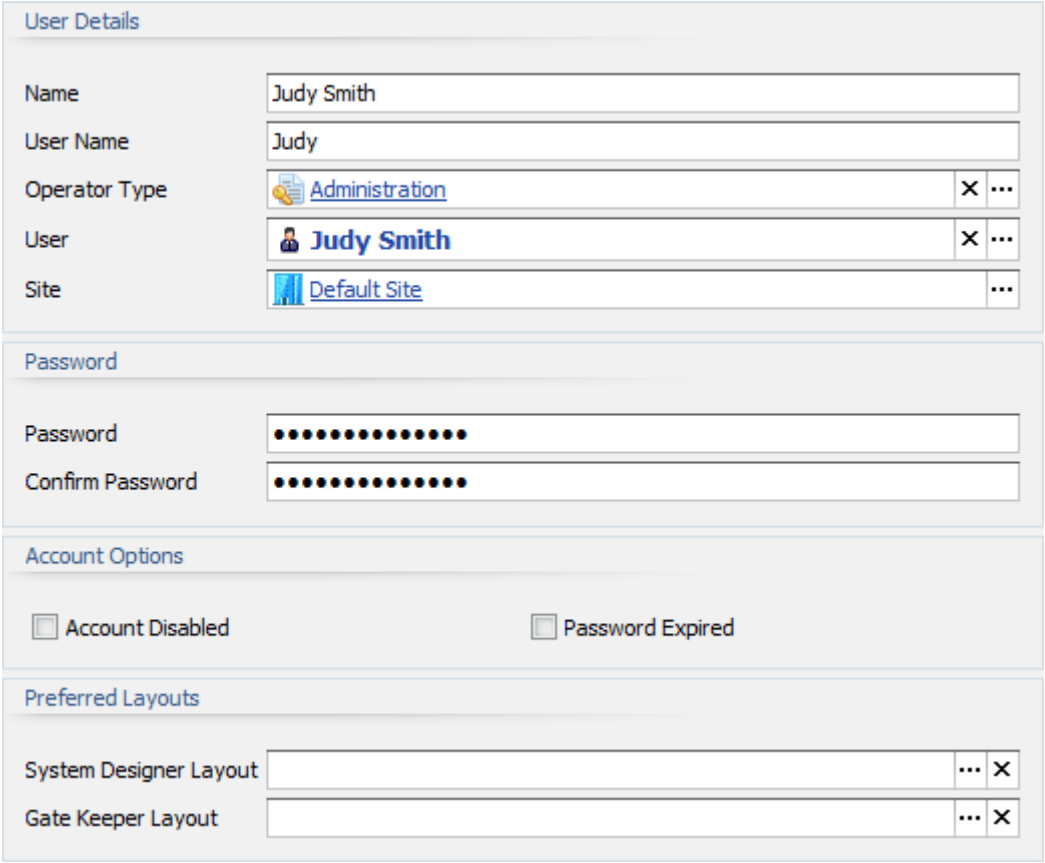


Figure 97

Operators consist of a few basic details:

Field	Description
Name	The actual name of the operator.
User Name	The name the operator enters when logging in to the Integriti client.
Operator Type	Configuration settings and permissions given to the operator.
User	Optionally, the operator can be associated with an Integriti controller user.
Site	
Password	The password the operator uses to log in to the Integriti client.
Account Disabled	Ticking this option will disable the operator account.
Password Expired	Ticking this option will force the operator to change his/her password next time they login to the Integriti client.
System Designer Layout	The default layout for the operator when using System Designer.
Gate Keeper Layout	The default layout for the operator when using System Designer.
Notes	Optional space for placing notes on the operator.

19.5 Custom Fields

Custom Fields provide a means through which the installer can add custom content to entity programming dialog windows.

Usage examples include but are not limited to:

- Users – Employee Payroll Number. (*Figure 100*)
- Users – Credit for goods and services available at a facility. (*Figure 100*)
- Powered modules – Date & Time the last service / battery change. (*Figure 99*)
- All modules – Photo / map of physical location of modules. (*Figure 99*)
- Air conditioner – A drop down editable list of the last mechanic to service the air conditioning.

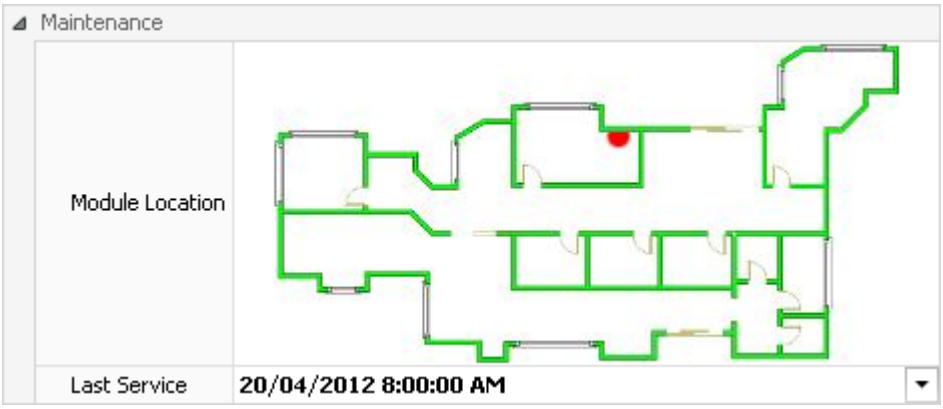


Figure 98

Custom fields can be configured by clicking on

under the

tab.

To create a new custom field:

1. Click

to open a new custom field dialog.
2. Enter a Name to describe the custom field.
3. Select the item type.
4. Enter a category name.
5. Enter a description describing the purpose of the custom field.
6. Select the field type.
    a. If one of the drop-down box options was selected, click

to add items to the custom field.

Once created, you cannot change the item type or the field type of custom fields.

Custom field descriptions appear at the bottom of the property grid.
If you create a custom field with the same category name as another property or custom field, the custom field will be grouped with it.

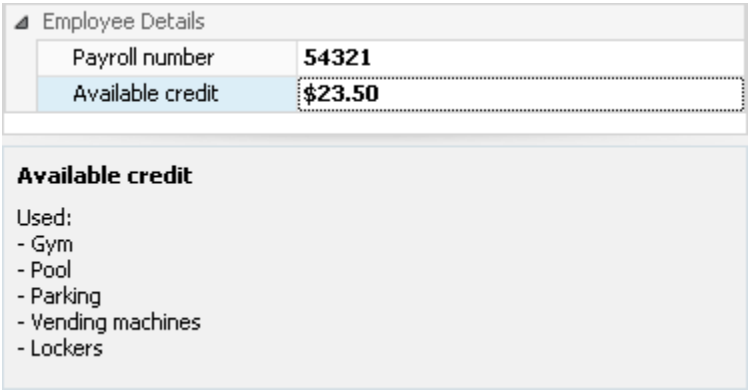


Figure 99

If the custom field type is an “editable drop down box” or “drop down box”, the values can be modified at any time. If an existing item with a custom field has a value that is modified at a later date, the item will retain the old value.

Field Type	Description
Text	A simple text field with up to 8000 characters.
Notes	A multiline text box with up to 8000 characters.
Integer	A number ranging from -2,147,483,648 to 2,147,483,647.
Decimal	A number with 15-16 decimal places ranging from -1.79769313486232E+308 to 1.79769313486232E+308.
Currency	A monetary value.
Date and Time	A combination of the following two field types.
Date	A date selector. From 01/01/0001 to 31/12/9999.
Time	A time selector. Hours, minutes, seconds, AM/PM.
Image	A BMP, GIF, JPG, JPEG, ICO or PNG image.
Check Box	Ticked or not.
Editable Drop Down Box	A drop-down list of selectable items. Custom text can be entered.
Drop Down Box	A drop-down list of selectable items.

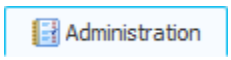
Large image sizes are supported but not recommended as they will impact Integriti client performance.

The checkbox will initially appear as because it is in an unknown state.

19.6 Synchronization warnings

Synchronization warnings usually occur when there is a conflict between one or many controllers and the Integriti server.

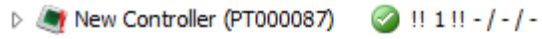
Clicking on the

button under the 

tab will display the synchronisation warnings panel.

Example:

Two users have been given the same security PIN. When both records are saved, the server will attempt to download these records to the appropriate controllers. The controllers will reject the last one of the two users that were sent. The server will report a synchronization warning.

- The affected controllers will appear with an exclamation mark next to them in the hardware navigation panel to indicate that something needs attention.
  

- The user that was not sent to the controller(s) will be highlighted in the Users panel.

	Default Site	U7	Julianne Wetherell	14/01/2013 10:25:44 AM

- A warning message will appear at the bottom of the users programming window (*Figure 101*).
- The synchronisation warning will also appear as an entry in the system warnings panel.

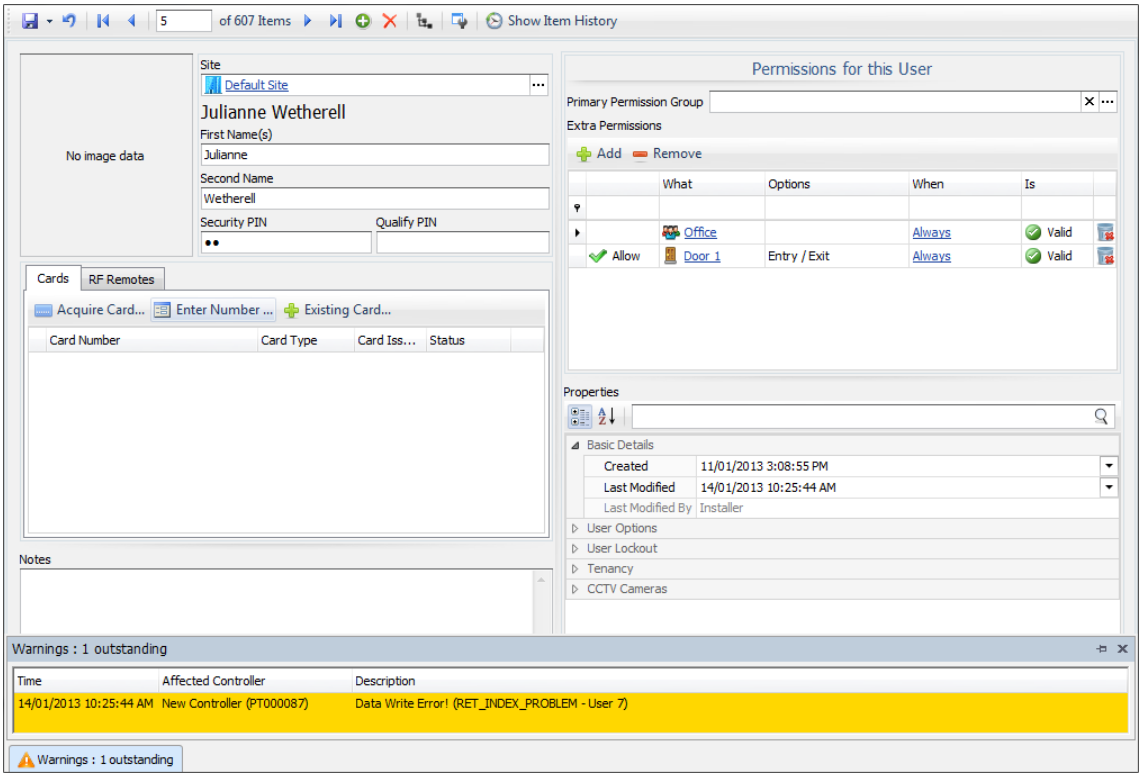

5
of 607 Items
Show Item History
No image data
Site
Default Site
Julianne Wetherell
First Name(s)
Julianne
Second Name
Wetherell
Security PIN
Qualify PIN
Cards
RF Remotes
Acquire Card...
Enter Number ...
Existing Card...
Card Number
Card Type
Card Iss...
Status
Notes
Permissions for this User
Primary Permission Group
Extra Permissions
Add
Remove
What
Options
When
Is
Office
Always
Valid
Allow
Door 1
Entry / Exit
Always
Valid
Properties
Basic Details
Created
11/01/2013 3:08:55 PM
Last Modified
14/01/2013 10:25:44 AM
Last Modified By
Installer
User Options
User Lockout
Tenancy
CCTV Cameras
Warnings : 1 outstanding
Time
Affected Controller
Description
14/01/2013 10:25:44 AM
New Controller (PT000087)
Data Write Error! (RET_INDEX_PROBLEM - User 7)
Warnings : 1 outstanding

Figure 100

19.7 Cross references

Cross references can be used to quickly discover what entities the current entity is referenced to or referenced from. Click the button to display the cross references for the entity.

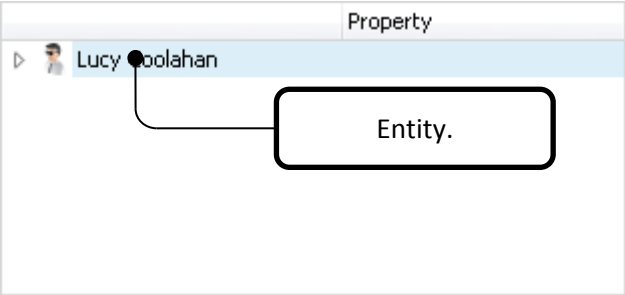


Figure 101

Clicking the triangle to the left of the entity displayed will expand-out said entity, displaying other entities referenced to/from.

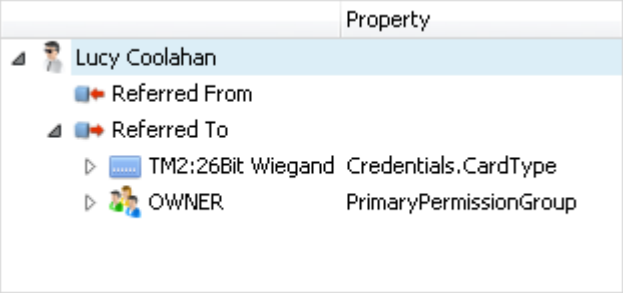


Figure 102

In *Figure 102* we can see that the user 'Lucy Coolahan' has been expanded out. There are two other entities that this entity refers to – a credential and permission group.

19.8 Audit Trail

The Audit panel contains a list of all changes made. Each individual change is logged within the Integriti database.

> Take advantage of the audit feature. If you've made a programming error, use audit to help review the changes you made.

You can view the audit trail of an individual item by going in to that item's programming screen and clicking the Show Item History button.

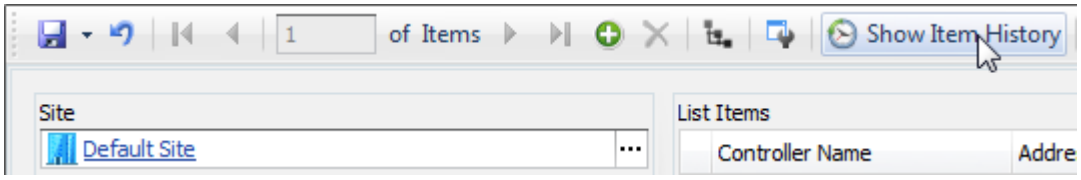


Figure 103

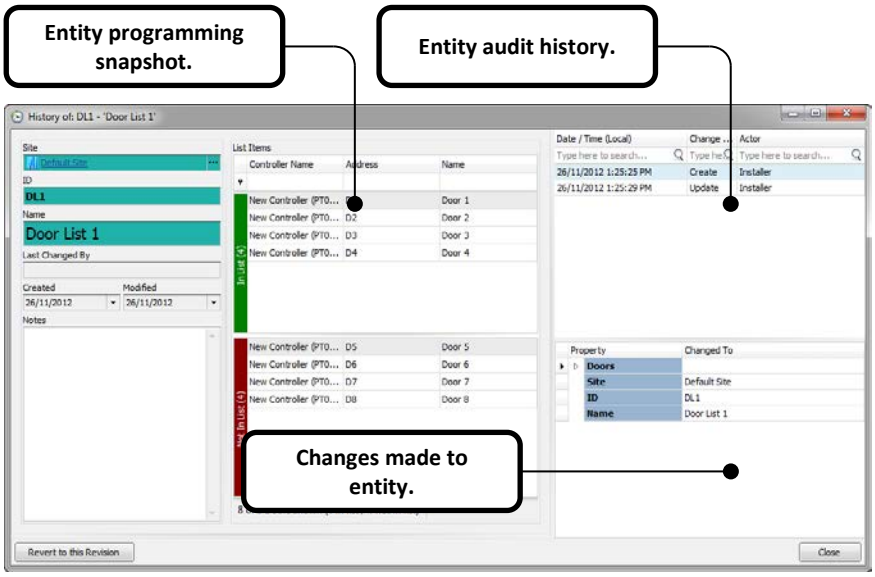


Figure 104

The entity audit history list will display the date / time, change type and actor for each event. Clicking on an item in this list will display a programming 'snapshot' of the entity at the selected time. A summary of the changes is easily viewed in the bottom right-hand corner of the screen.

Appendices

A. INTEGRITI LOG VIEWER 170

GUI LAYOUT 170
Log level 170
Search criteria 171
Log file selection / clear log 171
Log entry 171
Visible / Hidden entries 171
USING THE LOG VIEWER 171
Log file management 171
Using filters in the log viewer 172

B. GLOSSARY OF TERMS 174

C. IDENTIFYING THE INTEGRITI CONTROLLER SERIAL NUMBER 180

D. RANDOM NUMBER 181

E. FILTER STACKS 182

F. ACTION TYPES 183

CONFIGURE FORMAT STRING 183
BACKUP DATABASE 183
CONTROL WORKSTATION 185
CONTROLLER ACTION TYPES 186
Control Area & Control Area List 186
Control Aux & Control Aux List 186
Control Door & Control Door List 188
Secure/Unsecure a floor on a lift car, Secure/Unsecure a floor on a lift car list, Secure/Unsecure a floor list on a lift car & Secure/Unsecure a floor list on a lift car list 188
Trigger Input 189
Set Area User is in 189
Set Area User Count 189
Set Input Counters 189
Control Siren 190
Set Timer Variable 190
Set Variable 190
Control Airconditioning 190
Macro Control 190
Isolate 190
Comms Task Control 191
Grant Amnesty 191
Set Air-Conditioner Temperature 191
Call Floor 191
ESCALATE ALERT 192
LOG REVIEW 193
PARALLEL TASK LIST 194
PAUSE 194
RUN EXTERNAL PROGRAM 195
SEND COMMUNICATION MESSAGE 195

Message *196*
Recipients *196*
CLEANUP DATABASE 196
EXECUTE CODE 196
SEQUENTIAL TASK LIST 197
SYNCHRONIZE CONTROLLER TIME 198
EXECUTE REPORT 198

G. ENTITY STATES 200

H. ENTITY TYPES 204

I. CALIBRATIONS 206

OFFSET 206
GAIN 206
SHIFT 206
FORMAT / SCALE 207
DISPLAY STRING 207
MINIMUM & MAXIMUM STRING 208
CALIBRATION EXAMPLE 208

J. DEFAULT ENTITIES 209

PROCESS GROUPS 210
ANALOGUE CALIBRATIONS 211
CARD FORMATS 212

K. SYSTEM INPUT PROCESS GROUP DEFAULTS 213

L. INTEGRITI PROGRAMMING EXAMPLES 214

EXAMPLE 1 - FLASHING AUXILIARIES DURING A TIME PERIOD 214
EXAMPLE 2 - RANDOM BAG INSPECTIONS 217

M. LICENSES 219

SOFTWARE LICENSES 219
HARDWARE LICENSES (SMART CARD) 220

A. Integriti log viewer

It's important to understand how to use the Integriti log viewer in the event of an error. In most cases it is worthwhile for the administrator to read the most recent events in the log to diagnose errors.

GUI layout

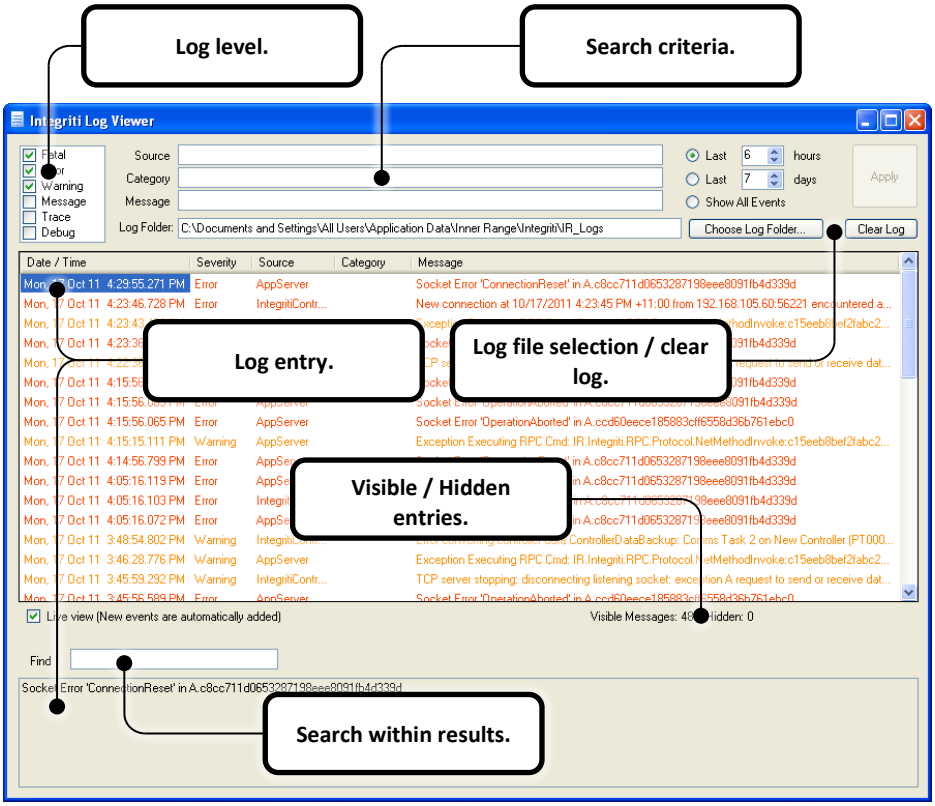


Figure 105

Log level

There are 6 log levels available – Fatal, Error, Warning, Message, Trace and Debug. By default only the first three items are ticked. Usually these items are all that is required to diagnose an error.

Search criteria

There are three search boxes available – Source, Category and Message. When applying your search criteria the returned results will match all three search boxes. The search boxes match the source, category and message columns in the list below.

Log file selection / clear log

Logs are simply groups of text files created with particular time & date stamps for organisation.

Log entry

Clicking on an individual log entry will reveal more detail in the box below.

Visible / Hidden entries

The total visible and hidden entries are filtered by the search criteria and the time frame selected.

Using the log viewer

Log file management

Clicking the [Clear Log] button will delete the log files in the currently selected directory. It is recommended that you clear your logs regularly. This will make searching your log files easier if an error occurs.

If you require a complete audit trail you can optionally move your log files on a scheduled basis with use of the Windows Task Scheduler.

Clicking the [Choose Log Folder...] button allows you to select another folder that contains log files.

Using filters in the log viewer

The log viewer search boxes (Source, Category, Message and Find) support the following delimiters:

; A semicolon can be used to separate search terms (logic OR).

- A dash (minus) can be used to exclude search terms (logic NOT).

Searches performed are not case sensitive.

Examples

- "`Initializing database`" will search for log entries containing "`Initializing database`" whereas "`Initializing;database`" will search for results with "`Initializing`" or "`database`".
- "`Initializing;-database`" will search for entries containing "`Initializing`" that do not include "`database`".

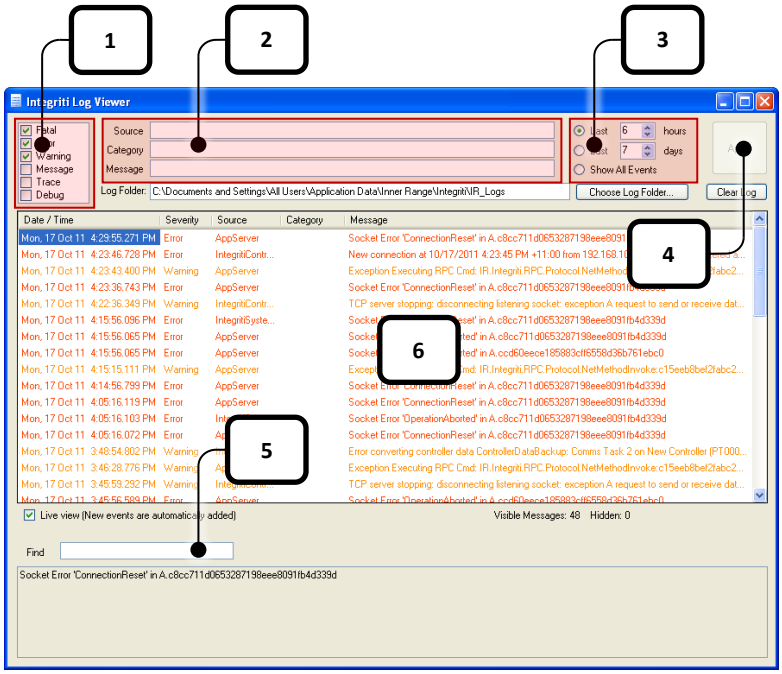


Figure 106

1. Select the desired log level.
2. Enter your search criteria.
3. Select the time period to search through.
4. Apply your search terms.
5. Optionally, use the "Find" box to narrow your search results.

Example usage

Search for errors where there was an issue initializing the database because the required services were not running in the last hour.

1. Ensure the Error checkbox is ticked. Un-tick the other checkboxes. (*Figure 106*)
2. Type "`AppServer`" in the Source search box.
    a. Type "`Initializing database`" in the message search box.
3. Select the Last Radio button. Type "`1`" in to the hours box to the right of the Last radio button.
4. Click Apply and wait for the results to be filtered.
5. If many results are returned you might want to search through the displayed results using the Find search box below the displayed results.
6. Click on a log entry to see more detail in the box at the bottom of the window.

B. Glossary of terms

ACCESS CONTROLLER (AC)	One type Integriti control module. (See also “CONTROL MODULE” and “SECURITY CONTROLLER”)
ADDRESS	A number allocated to every module in the system that is connected to a Control Module via the LAN. Allows the Control Module to identify each module.
ALARM	The condition of a zone or system input when it is in an abnormal condition and the system has been set to respond to that condition. i.e. Area/s turned ON.
ALPHA-SEARCH	Many items in the system are identified with text names (as well as ID number). The Alpha-search option allows the User to quickly locate items by using the digit keys of the LCD Terminal to jump to names beginning with a specific letter.
ANTI-PASSBACK	A system to monitor/prevent a user passing through a door into the same area as the system records them as being already in. e.g. Prevents a user from passing their card back under a door for another person to use.
AREA	Dividing a system into areas allows different parts of the system to be protected differently. i.e. Turned ON or OFF at different times, Reported separately, etc. Areas are named for easy identification. e.g. WORKSHOP, OFFICE, STORE, etc. See TWENTY-FOUR HOUR.
AUXILIARY	A device used to control an external device or indicate that a particular condition or conditions exist in the system. An auxiliary may be a physical output (Lock auxiliary, Entry warning device, Strobe, etc.), or a “phantom” auxiliary used in the programming to link two or more functions together.
CREDENTIAL	General term for Magnetic Stripe, Proximity, Wiegand cards & other devices such as Insert keys, Barcodes, etc. that can be utilized to operate the system.
CONTROL MODULE	The Control module stores all data, communicates with all modules connected to the system LAN, and reports alarms & system activity to the central station and/or computer.
DE-BOUNCE	See “Zone De-bounce”

DEFER AREA	Option to define specific Area/s that when turned Off by specific User Type/s, will start a timer running. When the timer expires, the Area will automatically turn On again, unless the User enters their code to “Defer” the Area On function and re- start the timer.
DOOR	An access point in a system that can be programmed to provide and restrict access to users as required, and monitored for abnormal conditions.
DOOR FORCED	A System Input for each Door to indicate when a Door is Locked and has been opened without a valid unlock command. i.e. Without valid User Access, REN / REX button, Auto unlock via Time Period, etc.
DOOR OPEN TOO LONG (DOTL) (or DOOR HELD)	A System Input for each Door to indicate when a Door is held open for too long when opened with a valid unlock command. The “Maximum Door Open Time” is programmable for each door.
DUAL USER	Requirement for two Users to present their Cards / PIN codes at specified Door/s before access is granted.
DURESS	PIN code/s can be programmed that will activate a System input on the Terminal where the code was used, to report a Duress condition to the Central Station. i.e. When a user is being forced to turn OFF the system by an intruder, they would do so using their “Duress” PIN code.
DVR	Digital Video Recorder.
EMS	Elevator Management System.
ENTRY DELAY	The maximum time that a user has to turn OFF an area, after entering the area and activating any detection devices nominated as “Primary Entry” types.
EXIT DELAY	The maximum time that a user has to exit the area after turning the area ON. Detection devices nominated as “Exit” types, will not generate alarms during this time.
HLI	High-level Lift Interface. Serial data protocol that allows communications between an Elevator Management System and an Access Control System.

HOLIDAY	Specific dates or periods may be programmed as "Holidays". Holidays may then be utilized in the "Time Periods" to specify whether the Time Period will be valid OR in-valid on the holiday date/s specified.
INPUT	An input may be a physical Zone Input on a Module, or a System input activated when specific conditions occur on a Module. (e.g. Low Battery, Line fault, Cabinet Tamper, Door Open Too Long, Illegal Card, etc.) Programming of Inputs and Areas will determine how (and if) the system will respond (generate an alarm, activate an auxiliary, etc.) when any input changes state. (See also "ZONE" and "SYSTEM INPUT")
INTERLOCK GROUP	A programming option allowing a List of Doors to be interlocked together. i.e. A Door will not un-lock unless all the other Doors in the List are locked and closed. Interlock Groups can also be programmed to check the status of a specific Area, Auxiliary or Zone before allowing access if required.
ISOLATE / DE-ISOLATE	Isolating enables faulty devices wired to Zone inputs, or System inputs that cannot be immediately restored, to be temporarily taken out of service in order to prevent them causing alarms when the area is turned ON. Once the problem is rectified, the device is De-isolated to restore normal operation.
LAN	(Local Area Network) Data communications network used in the system to connect modules (LCD terminals, Expander Modules, Reader Modules, etc.) into the system.
LCD	(Liquid Crystal Display) A display that allows information to be viewed in plain English text. The LCD used in the LCD Terminals is backlit to allow viewing in any lighting conditions.
LED	(Light Emitting Diode) A semiconductor light source used as an indicator lamp with the advantages of lower power, longer life and higher speed over conventional filament lamps. Used on module PCBs to indicate status and diagnose problems. Also used on Elite LCD Terminals to indicate Area status and/or other sys- tem conditions.

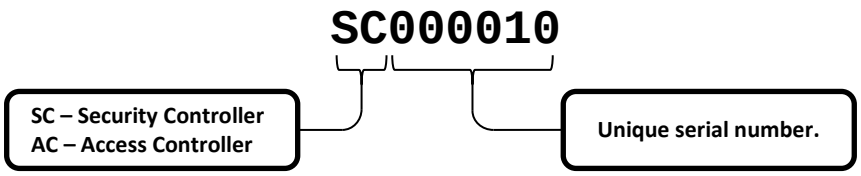
LIFT	A special access point in a system that can be programmed to provide and restrict user access to Lift Cars and Floors. This is achieved by enabling specific Floor selection buttons via a Reader in a Lift Car.
LISTS	Lists are used to simplify system programming. Once a List is created it can then be assigned in other programming options such as User Types, Time Periods, Calculated Auxiliaries and Named Actions, to define the items that are allowed to be controlled / accessed. There are 6 different types of Lists; Area, Siren, Door, Lift Car, Floor and Auxiliary Lists.
MCP	Main Control Panel. (See also “ACCESS CONTROLLER” and “SECURITY CONTROLLER”)
MENU GROUP	Menu Groups are programmed to define system operations & menu options allowed, and are then allocated to User Types and/or LCD Terminals to determine the control and menu access available.
MODULE	Module is the general term used for any device that connects to the system LAN to form part of the system, and includes LCD Terminals, Several types of Expander Modules, Reader (Door) Modules and Analogue Input Modules.
PANIC	A Panic alarm can be activated by a User by pressing the **[Help]** key 3 times in quick succession.
PIN CODE	A unique numerical code of 1 to 8 digits, allocated to any user in the system required to perform functions at an LCD Terminal or Keypad.
PRIMARY ENTRY ZONE	A type of Input (defined in the Process Group) that will start an Entry delay timer running when a User first enters an Area. (See “Entry Delay”)
PROCESS GROUP	Process Groups are programmed to define how Inputs (zones & system inputs) will be processed. Every Input in an Area is assigned a Process Group to deter- mine what processing (if any) will take place when the input changes state in that Area. (States include: Seal, Alarm, Tamper and Isolate)

PULSE COUNT	An option in Process Group programming that requires an Input to register a specified number of Seal to Alarm transitions within a specified time before it will be regarded as being in alarm. The number of pulses, and time are defined in Area programming if required.
READER	General term for a variety of card, insert key, biometric readers, etc. which may be utilized on the system to access Doors, access Lifts, Login, Logout, etc. Includes Magnetic swipe or insert, Proximity, Wiegand, Barcode, Hand geometry, Fingerprint, or scrambling Wiegand Keypads.
REED (or REED SWITCH)	(Also known as "Door Contact") Switch Contact activated with the presence of a magnetic field. Used to indicate the status of a Door/Window etc.
REN	(Request to Enter) Typically a button provided to unlock a door from the outside, bypassing the need to use a reader during low security periods.
REX	(Request to Exit) Typically a button provided to unlock a door from the inside either bypassing the need to use a reader during low security periods, or because an internal (exit) reader is not required. The "REX" device can also be a PIR or Photo-Electric beam to detect the User approaching the door.
REVIEW	Log of alarms and events that can be viewed at an LCD Terminal or PC. Each event is time/date stamped and programming options allow the installer to define which events are not logged.
SECURITY CONTROLLER (SC)	(Integriti Security Controller) See Control module.
SITE CODE	Used in conjunction with certain types of access control cards to identify a particular batch of cards when using the Site Code method. The system allows multiple Site Codes to be programmed.
SYSTEM INPUT	System inputs are activated when specific conditions occur on a Module. They are used to indicate situations such as Cabinet tamper, Siren tamper, AC fail, Low Battery, Fuse tamper, Communications problems, LAN problems, Panic, Duress, Door Open Too Long, etc. etc. Programming of Inputs and Areas will deter- mine how the system will respond (generate an alarm, activate an auxiliary, etc.) when any system input changes state.

TAMPER	An abnormal condition on a zone input or other device connected to the Integriti controller that indicates that interference or damage has occurred to the device or it's cabling. e.g. Open circuit or Short circuit condition. The system can be programmed to provide 24Hr monitoring for the tamper condition.
TERMINAL	Device connected to the system via the LAN to allow user interface via keypad entry and alphanumeric display. e.g. Elite LCD Terminal.
TIME PERIOD	A time period specified in terms of START time, END time, and valid DAY/S of the week. Four such periods can be specified in each Time Period. Time Periods are utilized in many functions such as specifying the valid period of user access, groups and lists, and turning areas and auxiliaries on and/or off automatically.
TWENTY-FOUR HOUR	
USER	Any person allocated a PIN code and/or card who is able to perform operations on the system.
WIEGAND	Data protocol originally developed for sending Wiegand access card data from the Reader head to the host controller and now adopted as an industry standard for access credential Readers including Proximity and Smart Card Readers.
ZONE (or ZONE INPUT)	A physical Input on any Module in an Integriti system. Zone inputs are used for connecting detection devices (PIRs, Door/Window Reeds, Photoelectric beams, etc.), Keyswitches, “Request to Exit” buttons, Smoke detectors, Seismic detectors, etc., etc. Programming of Inputs and Areas will determine how the system will respond (generate an alarm, activate an auxiliary, etc.) when any zone input changes state.
GUI	(Graphical User Interface) A user interface based on graphics (icons and pictures and menus) instead of text; uses a mouse as well as a keyboard as an input device.

C. Identifying the Integriti controller serial number

Each individual controller has its own unique serial number located on the CPU near the centre of the Integriti PCB. Controller serial numbers have the following format:



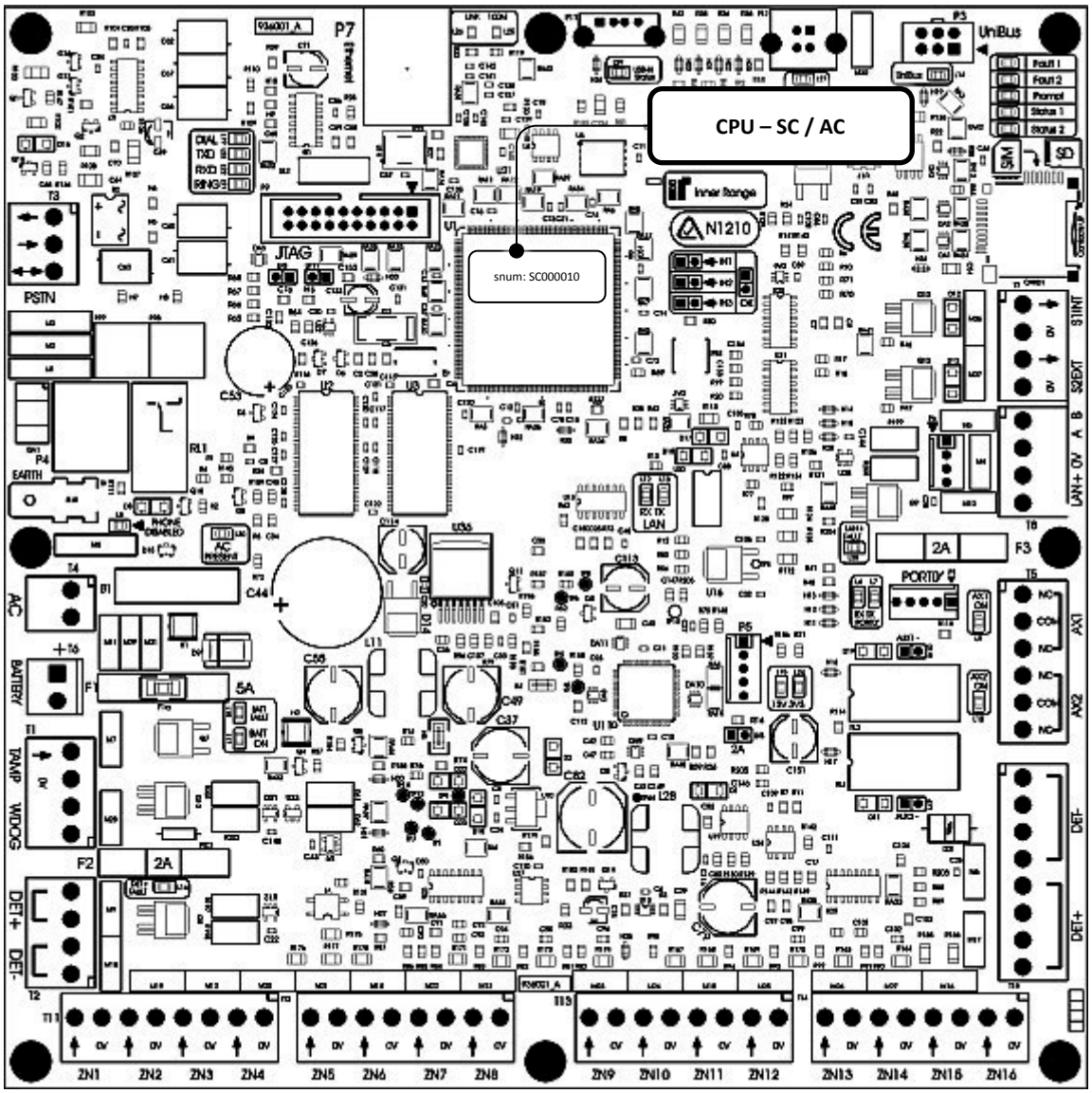


Figure 107

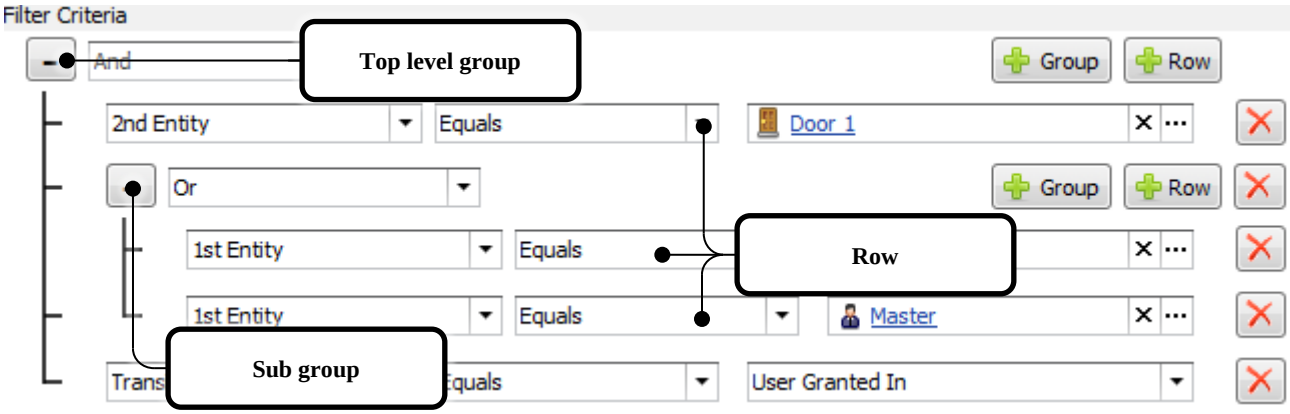
D. Random Number

The Integriti controller has the ability to generate a random number between 1 and 8388607.

To generate a random number, you will need to use a macro to 'Set Entity To Expression…'. If the expression value used is 8388607, the actual value of the entity that is being set will be a random number between 1 and 8388607.

E. Filter Stacks

Filter stacks can be found in a number of locations throughout the Integriti management software. This section describes how to use them.



Use the [-] and [+] buttons to expand and collapse groups.

Click [Group] to add a new sub group to the group.

Click [Row] to add a new row to the group.

Click [✕] to remove the row / group.

A group is a set of conditions combined by the same logical operator. The filter criterion above contains two groups.

Each group has its own operator that defines the logical relationship between the sub rows and groups. Group sub items can use a logical AND or OR.

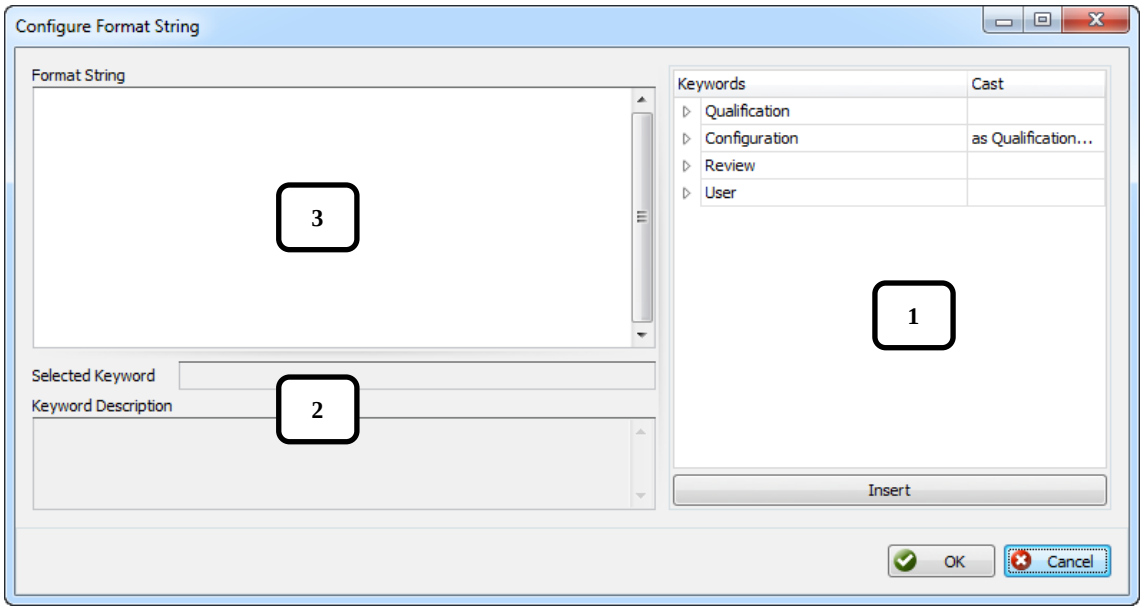
Each row has three properties – criteria, criteria operator and operand value.

F. Action types

Configure Format String

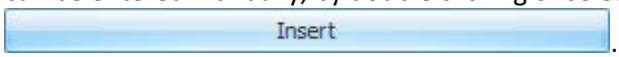
The Configure Format String editor will appear when editing customisable messages that can be sent as part of an action.

Actions such as Log Review or Run External Program have flexible text fields that can contain keywords relevant to the action it is being created for. Click on the ellipsis ... to open the Configure Format String editor.



The keywords **(1)** shown in the Configure Format String editor will differ depending on where the editor was opened from. E.g. 'Log Review' or 'Run External Program'

If a keyword has been selected from the list **(1)** a basic description may appear **(2)**.

The format string field **(3)** allows direct entry of custom text including keywords. Keywords can be entered manually, by double clicking or selecting the item and clicking Insert 

.

Backup Database

This action type will save the database as a .bak file in the specified folder. The default location is '`C:\Program Files\Inner Range\Integriti Pro\Backups`'.

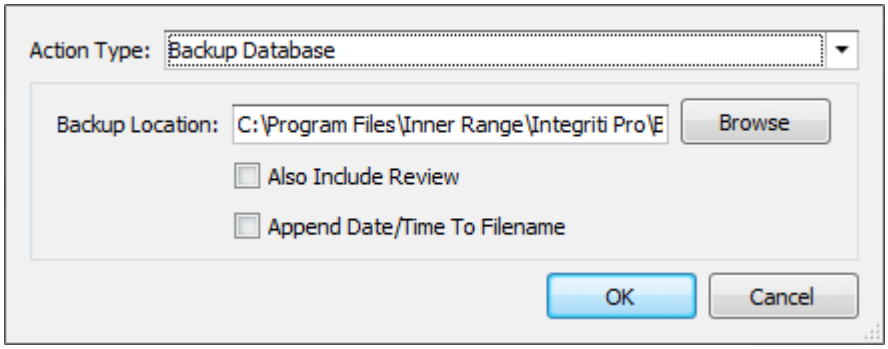


Figure 108

Backup Location

Click the Browse to select a save folder location or you can manually enter a location in the text box provided.

Also Include Review

Ticking this checkbox will cause all review events in the database to be saved in the database backup.

Append Date/Time To Filename

If this option is ticked, databases backed up by this action will have the date and time appended to the filename. Ticking this option is recommended.

An example of a database backup with this option ticked:

```
Integriti Backup 20130130 170613.bak
```

Control Workstation

Control workstation allows remote control of a workstation running the Gate Keeper client application.

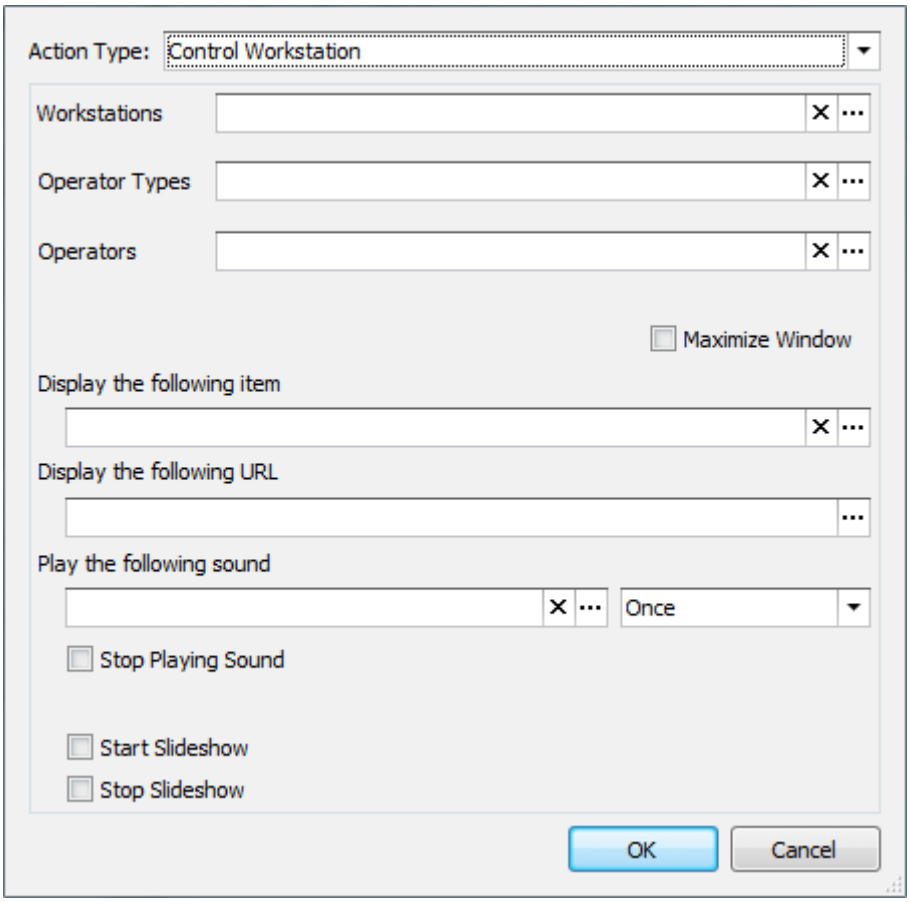


Figure 109

Workstations, Operator Types and Operators are all optional fields. At least one of the three fields must be filled in in order for the action to work. Each of the three fields are bound by AND logic. So for example, if the Workstations and Operators fields were populated, only the specified workstations with the specified operators logged in to them would be controlled by the action.

Ticking the Maximize Window checkbox will cause the Gate Keeper application to maximise from a minimised or floating state. If the Gate Keeper application was not already maximised, the application will be given focus.

Play the following g sound will play the selected .wav audio file on the Gate Keeper client application. The frequency can be set to Once, Twice, Thrice or Continuously.
When playback has been set to 'continuously', the sound can be stopped by another Control workstation action. Use the 'Play the following sound' once option, select 'Stop Playing Sound' or the operator can close the Gate Keeper client.

Select Start or Stop Slideshow to start/stop the pre-configured slideshow. These options have no effect on clients where the slideshow has not been configured.

Please refer to the Gate Keeper documentation for information on configuring slideshows.

Controller Action Types

This section covers items specific to the individual action types within the Integriti controller. For more information on actions please refer to the section titled Named Actions.

The following is a list of all of the available action types:

Control Area & Control Area List

These action types can be used to control an area, set an area defer, control a 24 hour area or cancel an area exit delay.

Control Type	**Normal**	-	Controls the selected area.
	Defer	-	Set/Reset the area defer.
	Twenty-four Hour	-	Controls the 24 hour area.
	Cancel Exit Delay	-	Stops the exit delay and arms the area.
When Asserted…	**Nothing**	-	Don't do anything.
	Arm	-	Arm the area / 24 hour area, Set/Reset the area defer or stop the exit delay.
	Disarm	-	Disarm the area / 24 hour area.
	Toggle	-	Toggle the arm/disarm state of the area / 24 hour area.
When Disasserted…	Can be used to arm, disarm or toggle the selected area or its associated 24 hour area.		

Control Aux & Control Aux List

These action types will control an auxiliary / auxiliary list.

Control Type	**Normal**	-	Normal auxiliary control
	Timed Only	-	
	Leave Timer	-	

When Asserted/
When Disasserted… Can be used to turn on, off or toggle the selected auxiliary.

Delay On/

Delay Off. Ticking these options will change the On/Off Time to a Delay On/Off Time.

Update Dynamic Only

Control Door & Control Door List

These action types will control a door / door list.

Unlock time Time to unlock the door for (up to 18 hours, 12 minutes and 15 seconds.

When Asserted/ When Disasserted… Can be used to turn on, off or toggle the selected auxiliary.

Secure/Unsecure a floor on a lift car, Secure/Unsecure a floor on a lift car list, Secure/Unsecure a floor list on a lift car & Secure/Unsecure a floor list on a lift car list

These action types will secure / unsecure a floor on a lift car / lift car list.

Floor The floor to secure / unsecure.

Lift Car/ Lift Car List The lift car / lift car list to secure / unsecure.

Cancel Button Timer

Floor Time Up to 4 minutes and 15 seconds.

When Asserted/ When Disasserted… Can be used to turn secure, unsecure or toggle the selected lift car / lift car list.

Trigger Input

This action type will control the state of the selected input.

Input State One of the 16 possible input states.

Update State If selected, it will make state change persistent (rather than momentary). The input state can be changed by another action or by the physical input.

When Asserted/ When Disasserted… Can trigger, restore or toggle the state of the selected input.

Set Area User is in

This action type can be used to relocate a user to a specific area.

User The user to .

Area One of the 16 possible input states.

Don't update area user counts One of the 16 possible input states.

When Asserted/ When Disasserted… Can trigger, restore or toggle the state of the selected input.

Set Area User Count

This action type can be used to adjust the user count of the specified area.

Input State One of the 16 possible input states.

Set Input Counters

This action type can adjust the count on the specified input.

Input State One of the 16 possible input states.

Control Siren

This action type will control the state of the selected siren.

Input State One of the 16 possible input states.

Set Timer Variable

This action type can be used to set a timer variable.

Input State One of the 16 possible input states.

Set Variable

This action type can be used to set the value of the specified variable.

Input State One of the 16 possible input states.

Control Airconditioning

This action type will control the specified air-conditioning unit.

Input State One of the 16 possible input states.

Macro Control

This action type will control the specified macro.

Input State One of the 16 possible input states.

Isolate

This action type will control the state of the selected input.

Input State One of the 16 possible input states.

Comms Task Control

This action type will control the specified communications task.

Input State	One of the 16 possible input states.

Grant Amnesty

This action type will grant controller wide amnesty for one transaction per user.

Controller	The controller to grant/deny amnesty.
When Asserted/ When Disasserted…	Can Grant, Deny or toggle controller wide amnesty.

Set Air-Conditioner Temperature

This action type will set the temperature of the specified air conditioning unit.

Air conditioner	The air conditioning unit to control.
Unit	The number of the unit to control.
Zone	The number of the zone to control.
Temperature	The temperature in degrees Celsius to set the air conditioning to.
When Asserted/ When Disasserted…	Can Turn On, Turn Off or toggle the air conditioning unit.

Call Floor

This action type will call a floor on a lift car.
Only the `Floor` and `Lift Car` fields are required. The remaining 'Action To Take` options have no effect.

Floor	The Floor to send the lift car to.
Lift Car	The Lift Car to control. The lift car must be a `Home Floor Caller`.

Escalate Alert

This action will escalate alerts within the specified alert groups. The priority, colour and alert definition can be modified.

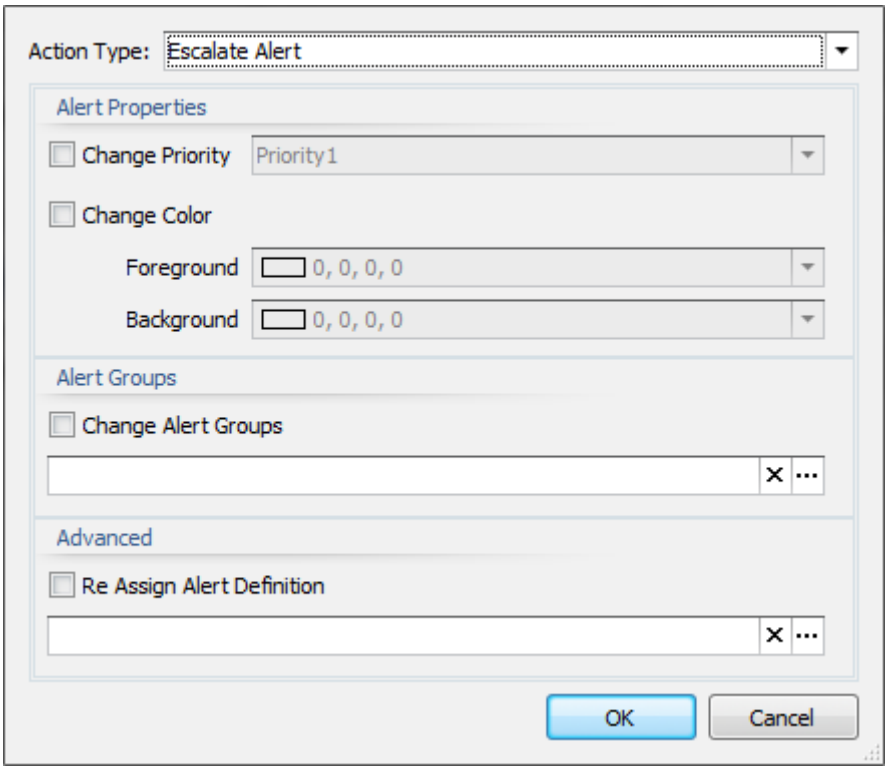


Figure 110

Change Alert Groups

The alert groups that the alerts belong to that are to be modified.

Re Assign Alert Definition

The Alert Definition of the alerts can be changed to the definition selected here.

Change Priority

Changes the priority of the Alert.

Change colour

Changes the foreground and background colours of the alert text seen in the alert viewer.

Log Review

Use Log Review to send custom text to review.

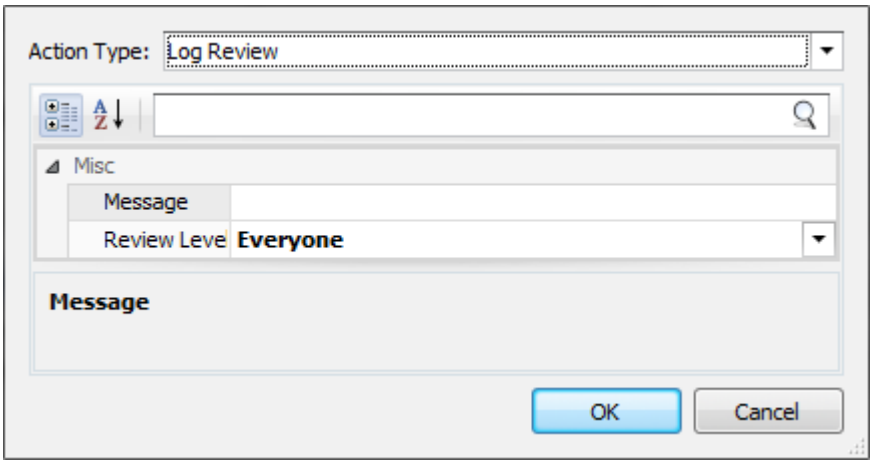


Figure 111

Message

The text to log to review.

Review Level

The review level for the message text.

Parallel Task List

Parallel Task List creates a new task list. All tasks added to this task list will be executed simultaneously.

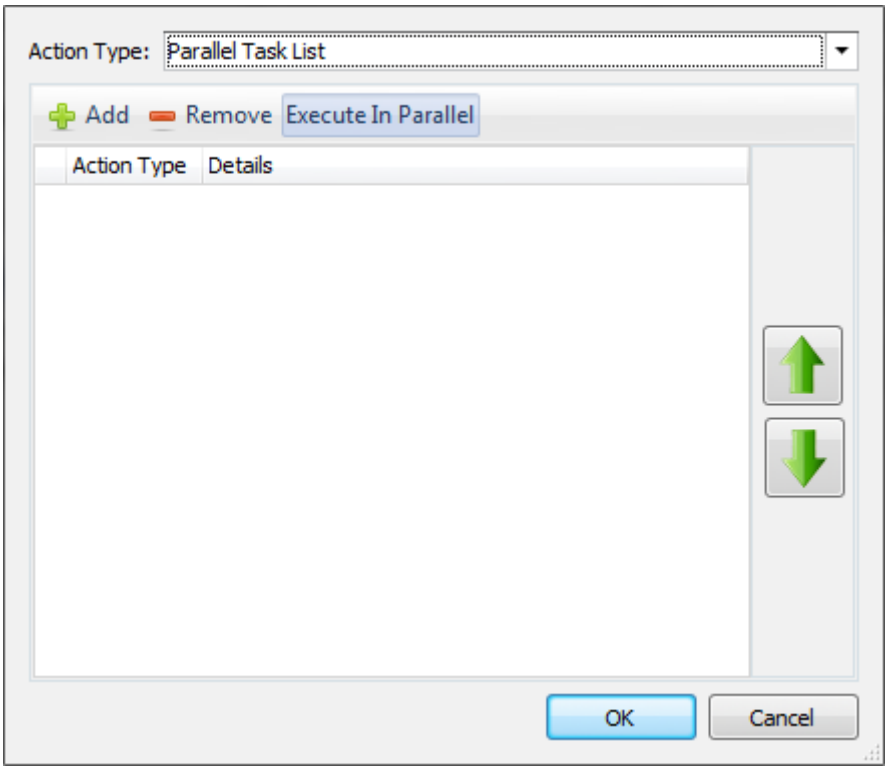


Figure 112

Pause

Pause will suspend execution of the action list for the duration set. This action has no effect in a Parallel Task List.

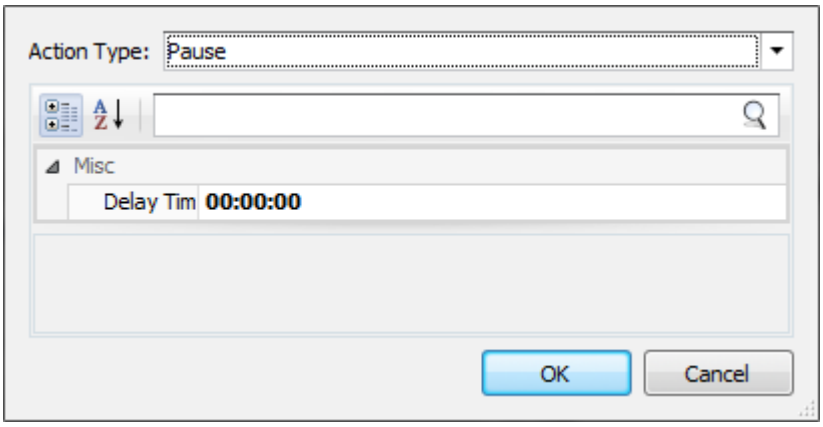


Figure 113

Run External Program

This action can be used to run a 3rd party program.

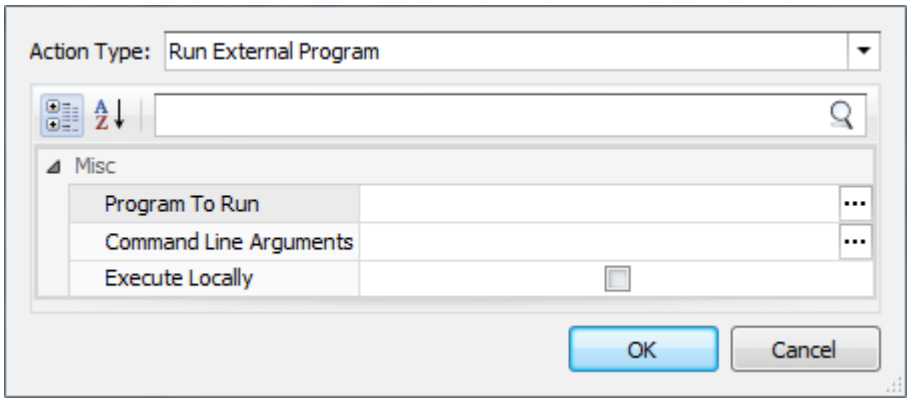


Figure 114

Program To Run

Click on the ellipsis to the right of 'Program To Run' to select the 3rd party application that will be launched.

Command Line Arguments

Optional command Line Arguments can be sent if required. Clicking on the ellipsis for this option will open the Configure Format String editor.

Execute Locally

Ticking the Execute Locally option will result in the application being launched on the client workstation instead of the Integriti server.

Send Communication Message

Use Send Communication Message to send an email or SMS to one or many recipients.

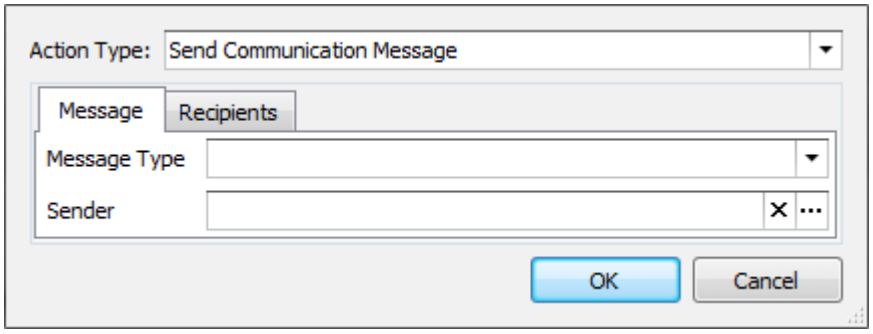


Figure 115

Message

Message Type

Set to SMS or Email. Use None to disable.

Sender

A communications handler must be created for sending of the SMS or Email.

Recipients

Click Add User under the Recipients tab to add users to the list of recipients.

Clicking Add Custom allows entry of a custom number/email/… for the message type selected.

Cleanup Database

This action type will purge review messages, audit history or alerts.

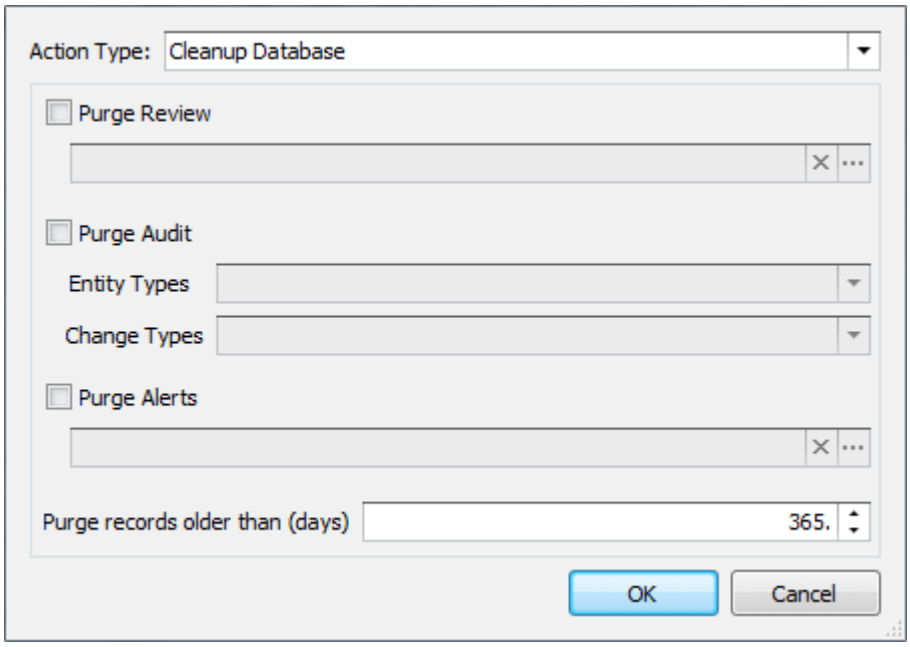


Figure 116

This action cannot be undone. Before using any of the three options, make sure the database has been backed up.

Execute Code

This action type will execute custom C# code.

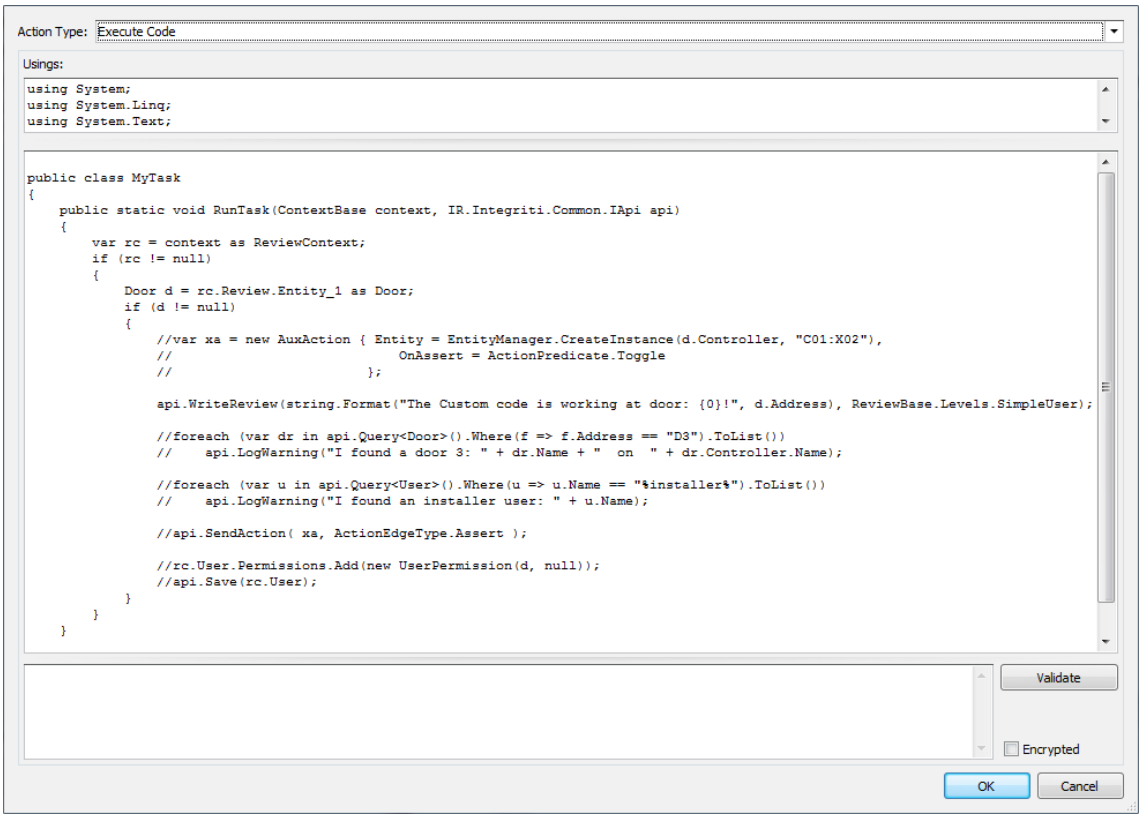


Figure 117

It is assumed that anyone using this option has a clear understanding of the C# programming language. Use of this feature should be carried out under the direction of Inner Range staff.

Sequential Task List

Sequential Task List creates a new task list. All tasks added to this task list will be executed in the order that they appear in the list.

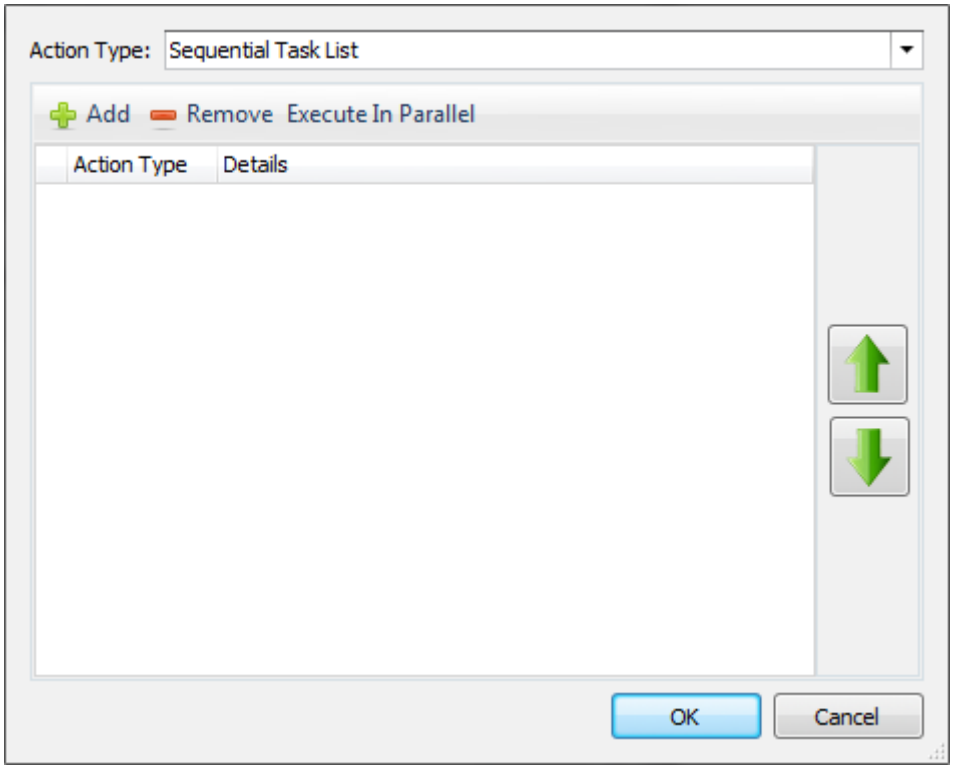


Figure 118

Synchronize Controller Time

Synchronise the time on one or many controllers.

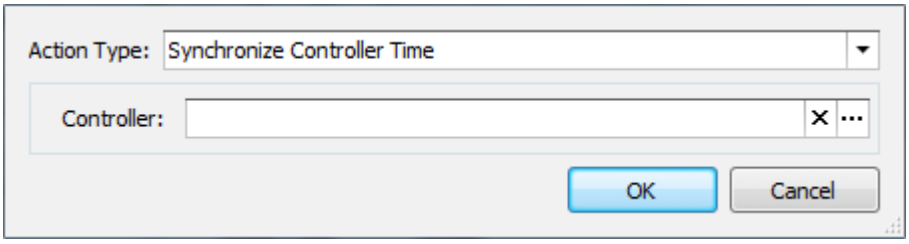


Figure 119

Execute Report

Using Execute Report will run the selected report and send the result to file, a printer or as an email attachment.

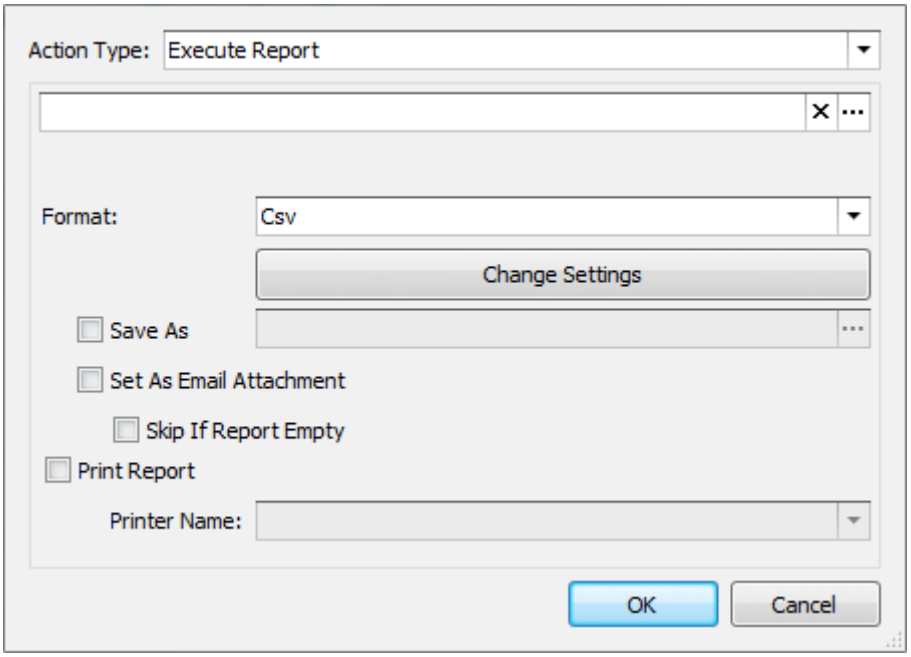
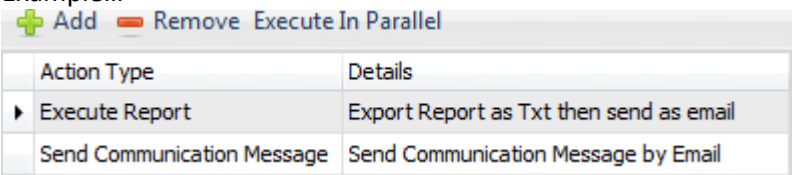


Figure 120

To send the report generated by this action as an email attachment, add the Send Communication Message after this action in a sequential list.

Example…



G. Entity states

Various entities have different valid and invalid states to make more sense of their application. For instance, instead of a door being valid / invalid it is represented as locked / unlocked.

Entity Name	Valid state	Invalid state
24 bit constant	Not zero	Zero
Air conditioning Unit	*n/a*	Always
Area	Area is on	Area is off
Area List	All areas on	One or many areas off
Area Timer eg exit timer	Timer is running	Timer is not running
Aux List	All auxiliaries on	At least one aux off
Auxiliary	Output on	Output off
Button	*n/a*	Always
Card Format	*n/a*	Always
Card Template	*n/a*	Always
Communications Task	Communications task is running	Communications task is not running
Compare	Value is >= threshold1 and <= threshold2	Value is < threshold1 or Value is > threshold2
Compound Entity	If evaluates to TRUE	If evaluates to FALSE
DNS names	*n/a*	Always
Door	Locked, reed & tongue (if present) sealed.	Unlocked or tongue or reed unsealed
Door List	All doors are valid.	One or many doors are invalid
Door Type	*n/a*	Always
EOL	*n/a*	Always

Entity Name	Valid state	Invalid state
FAT file-system file	*n/a*	Always
file/item combination	*n/a*	Always
Floor	Floor secured	One or many floors not secured
Floor List	All floors secure	At least one floor unsecure
Foreign Entities	*n/a*	Always
General Timer (100ms)	Expiry time has elapsed	Expiry time has not yet elapsed
General Variable	Current Value => The Test Value	Current Value < The Test Value
Generic	*n/a*	Always
Holidays	Valid	Invalid
Input	No State Asserted	Any state asserted
Input analogue value	Value is not 0	Value equals 0
Input Counter	Count is not 0	Count is 0
Interlock	Interlocked	Not interlocked
LAN Module	Present on the LAN	Not present on the LAN
LCD message	*n/a*	Always
Lift	Button timer running	Button timer not running
Lift Group	*n/a*	Always
Lift List	*n/a*	Always
Lift Type	*n/a*	Always
Macro procedure	Macro Procedure is running	Macro Procedure is not running
Menu Group	*n/a*	Always
None	Always	*n/a*

Entity Name	Valid state	Invalid state
Named Actions	*n/a*	Always
Pre-set text types	*n/a*	Always
Process Group	*n/a*	Always
Process ID	*n/a*	Always
Permission Group	*n/a*	Always
Qualify Door Type	*n/a*	Always
Qualify Lift Type	*n/a*	Always
Reader	*n/a*	Always
RF Remote Template	*n/a*	Always
Schedule	Valid	Not Valid
Siren module	Internal or external siren(s) are sounding with any tone	Siren(s) are not sounding
Telephone number	*n/a*	Always
Telephone number list	*n/a*	Always
Time Period	Valid	Not Valid
User	User Exists	User does not exist

Table 7

Note that for area lists, door lists, floor lists, compound entities and interlocks if the reverse flag is set then:

Entity Name	Valid state	Invalid state
Area List	All areas off	One or many areas on
Compound Entity	Expression == TRUE	Expression == FALSE
Door List	All doors are invalid	One or many doors are valid
Floor List	All floors unsecure	One or many floors are secure
Interlock	Not interlocked	Interlocked
Auxiliary List	All auxiliaries off	One or many auxiliaries on

Table 8

H. Entity types

All of various entity types are listed in this section.

Modules can have inputs and / or outputs attached to them. The following notation is used to refer to an individual input or output on the module:

C	- Module Designator
01	- Module Address
:	- Separator
X	- Input / Output Designator
	- Input / Output Address

Module Designator	Description
C	Control Module
T	LCD Terminal
K	Touch Terminal
P	LAN Power Supply
G	Graphic Terminal
E	Expander
R	Two Door Reader
I	Four Door Reader
F	Radio Expander
V	Virtual Module

Entity Type	Name
AC*x*	Air Conditioner
AL*x*	Area List
A*xx*	Area
CE*x*	Compound Entity
CF*x*	Card Format
CP*x*	Analog Comparison
CT*x*	Communications Task
C*xx*	Control Module
DL*x*	Door List
DT*x*	Door Type
D*xx*	Door
EL*x*	EOL configuration
E*xx*	Expander Module
FL*x*	Lift Floor List
FT*x*	RF Remote Template
F*xx*	Radio Expander
GT*x*	General Timer
GV*x*	General Variable
G*xx*	Graphic Terminal
HY*x*	Holiday
IA*x*	Analog Calibration
IL*x*	Interlock
LC*x*	Lift Car
LF*x*	Lift Floor

Entity Type	Name
LG*x*	Lift Group
LL*x*	Lift Car List
LT*x*	Lift Type
MA*x*	Macro
MG*x*	Menu Group
NIC*x*	Network Interface
PA*x*	Named Action
PG*x*	Process Group
P*xx*	Power Supply Module
QD*x*	Qualified Door Type
QG*x*	Permission Group
QL*x*	Qualified Lift Type
R*xx*	Reader Module
TL*x*	Telephone Number List
TM*x*	Card Template
TN*x*	Telephone Number
TP*x*	Time Period
T*xx*	Terminal
U*xx*	User
XL*x*	Auxiliary List

Table 9

I. Calibrations

There are two types of calibrated values - scaled and unscaled.
The unscaled value is always an integer and it is determined using the following formula:

$$\frac{Gain \times RawValue}{2^{shift}} + Offset$$

To know what $RawValue$ is you must know something about the underlying hardware of that input.
Examples:

- The $RawValue$ of a standard voltage input on a C3K analog module will be a number between 0-254 directly proportional to 0-5V on the input.
- The temperature sensor on a graphic terminal is an integer which is the decikelvins of the temperature measured.

These inputs can be arranged in a straightforward manner to display what is actually being measured at the input using a calibration.

A number of calibrations have been created for your convenience. These calibration records are for the Graphic Terminal, Concept analogue module and IR-994089 temperature sensor.

Offset

Offset allows us to have values that can go into the negative region have minima above 0, i.e. Degrees Celsius. It is expected that $RawValue$ is an unsigned number.

Gain

Gain is simply an integer that multiplies the $RawValue$.

Shift

Shift is the exponent to the power of 2, so a shift of 3 will divide the $Gain \times RawValue$ product by 8 ($2^3 = 8$).

Let's say we have a module with an analogue input that is measuring 0-10V and it has a 10bit resolution (so its $RawValue$ is 0-1023). We will choose our unscaled calibrated value to be millivolts as we won't gain any more accuracy by going to a smaller integral unit as there are 10000mV in 10V which is much greater than the 1024 possible values we can have. So we

will choose a gain of 10000 as this is our base unit. If we leave shift as 0 we would have a value between 0-10,240,000. We typically make the shift the same number of bits as our ADC so this will become 0-10,000 which is what we want. (Actually this isn't true, we will get:0 $-\left(10000 \times \left(\frac{1023}{1024}\right)\right)$), this inaccuracy can be compensated for in the gain, If you are interested, view the calibration example for an example of how to make a sensor correctly display its full range using a calibration).

It is important to note that for Macros and Compare structures you will need to use the unscaled analogue value for any comparison.

Format / Scale

This way we end up with an integer which is an unscaled calibrated value, which will be representative of the quantity measured, e.g. microvolts, millibar, decikelvin, etc. We need to scale and format it to make it more human readable, using the Format/Scale string. This takes the form of:

```
Kx {S|F}y.x
```

Where x and y are a value from 0 to 9.

The number after K is the number of places to move the decimal point to the left (up to 9), which allows us to display a fractional number. The S or F determines whether we display a sign in front of the displayed value, with S displaying the sign. Note that if the value becomes negative and the format uses 'F' then the negative sign won't be displayed. Also, if the 'S' option is used then positive values will always display a '+' sign in front.

The number before the dot is the number of digits before the decimal place to display. This has to be large enough to display the full number, and will always display leading zeroes on smaller numbers, as the formats are always fixed width currently. The same is true for the number after the dot, which is the number of digits shown after the decimal place. This also is fixed width and will always show trailing zeroes if empty. It is expected that usually the number after the decimal place will equal the number after 'K'.

As an example, if we want to display millivolts as 0-10 volts with no sign we would use the following string: K3 F2.3. To display decikelvin as -99.0 to +99.0 Celcius (assuming offset of -2730 to make 0 the melting point of water) we would use: K1 S2.1.

Display String

The Display String is merely a string that follows the formatted value with a whitespace in between. If the Display String is "C" then the displayed value for our temperature example would be "+22.3 C". If we use "Volts" with the volts example we might get "09.812 Volts".

Minimum & Maximum String

The minimum string and maximum string state what we expect the minimum and maximum values that are di splayed would be. This has no effect on the text of the displayed analogue value but it does affect graphical displays. On the iPhone app if a meter icon is used to display an analogue value. The minimum and maximum deflections on the scale will correspond to the minimum and maximum string values. In future this will also happen on some of the Graphic Terminal icons and some of the presenter elements in Integriti Schematics. The minimum and maximum strings should be the same format as the Format/Scale string, i.e. same sign and number of digits and decimal places, so 0 volts should be “00.000” and 10 volts should be “10.000”.

Calibration Example

This example describes how to make a calibration record for a sensor that has linear output of 4-20mA into Concept 3/4K Analog module (with current mode inputs):

Let us say a sensor measures some value over range $MINvalue$ to $MAXvalue$:

$$MINvalue\ (4mA)\ \rightarrow MAXvalue(20mA)$$

Let us say it measure percentage of relative humidity (RH) from 000.0% to 100.0% as four significant figures, we define $MINinteger$ and $MAXinteger$ as:

$$MINinteger = MINvalue\ \times 10^n$$
$$MAXinteger\ = MAXvalue\ \times 10^n$$

n = number of significant figures required in the output display – max digits in the integer part of $MAXvalue$.

So here $n = 4 - 3 = 1$, so $MINinteger = 0000$ and $MAXinteger = 1000$.

$Range = MAXinteger - MINinteger$, in this case $MAXinteger = 1000$.

$$GAINfloat = \frac{256}{204} \times Range = 1254.902$$

$$OFFSETfloat = MINinteger - \frac{51}{255} \times GAINfloat = -250.98039215686274509803921568627$$

Now we can get the real calibration values:

$Offset = \lceil OFFSETfloat \rceil$ (Rounded up = -250)

$Gain = \lceil GAINfloat \rceil$(Rounded up = 1255)

$Shift = 8$ (Always in this example)

$\frac{Format}{Scale} = Kn\ Sx.n$ where n = n, x = max digits in the integer part of MAX_{value}, y = n

Display String: Anything, perhaps “%RH” for relative humidity.

Minimum String = MIN_{value}

Maximum String = MAX_{value}

J. Default entities

This section contains lists of all of the entities found within a defaulted Integriti database. These entities have been created for your convenience.

Process Groups

ID	Name	Action 1 (Assert)	Action 2 (Assert)	Contact ID Message Type	EN Pin	Entry Zone	Exit Zone	External Siren States	Internal Siren States	Message Category	Message Enable States	No 24 Hour if Armed	Primary Zone	Process 24 Hour	Report Entry	Reporting States	Siren Lockout	Siren Tone	States for this PG
PG1	Intruder/Burglary	A	Tl, Th, T	130	Intruder			A, Tl, Th, T	A, Tl, Th, T	1	A, Tl, Th, T, Z, I					A, Tl, Th, T, I	✓	Sweep	A, T
PG2	Entry-Exit/Delayed Burg	A	Tl, Th, T	130	Intruder	✓	✓	A, Tl, Th, T	A, Tl, Th, T	1	A, Tl, Th, T, Z, I					A, Tl, Th, T, I	✓	Sweep	A, T
PG3	Primary Intruder/Burg	A	Tl, Th, T	130	Intruder	✓	✓	A, Tl, Th, T	A, Tl, Th, T	1	A, Tl, Th, T, Z, I		✓			A, Tl, Th, T, I	✓	Sweep	A, T
PG4	Silent Alarm	A	Tl, Th, T	150						1	A, Tl, Th, T, I					A, Tl, Th, T, I			A, T
PG5	Local Alarm	A	Tl, Th, T	0				A	A	1	A, Tl, Th, T, I						✓	Sweep	A, T
PG6	Local Silent	A	Tl, Th, T	0						1	A, Tl, Th, T, I								A, T
PG7	Fire		Tl, Th, T	110	Fire			A	A	1	A, Tl, Th, T, I					A, Tl, Th, T, I	✓	Evacuation	A, T
PG8	Duress			121	Panic											A, Tl, Th, T, I			
PG9	Panic			123	Panic			A	A	1	A, Tl, Th, T, I					A, Tl, Th, T, I		Bell	A, T
PG10	Emergency			100				A	A	1	A, Tl, Th, T, I					A, Tl, Th, T, I		Evacuation	A, T
PG11	Automation			0															A, T
PG12	Log/Report Only			300										✓		A, Tl, Th, T, I			A, T
PG13	Log Only			0										✓					A, T
PG14	Tamper	A	Tl, Th, T	145	Intruder			A, Tl, Th, T	A, Tl, Th, T	1	A, Tl, Th, T, I	✓			✓	A, Tl, Th, T, I	✓	Sweep	A, T
PG15	LAN Fault	A		333	Intruder			A, Tl, Th, T	A, Tl, Th, T	1	A, Tl, Th, T, I					A, Tl, Th, T, I	✓	Sweep	A, T
PG16	AC Fail	A	Tl, Th, T	301	Power					1	A, Tl, Th, T, I					A, Tl, Th, T, I			A, T
PG17	Battery Problem	A	Tl, Th, T	302	Power					1	A, Tl, Th, T, I					A, Tl, Th, T, I			A, T
PG18	Pwr Supply Fault	A	Tl, Th, T	312						1	A, Tl, Th, T, I					A, Tl, Th, T, I			A, T
PG19	Comms Problem	A	Tl, Th, T	350						1	A, Tl, Th, T								A, T
PG20	RF Tx Fault	A	Tl, Th, T	381						1	A, I					A, I			A, I
PG21	RF Tx Jam	A	Tl, Th, T	344	Primary ATS					1	A, I					A, I			A, I
PG22	Access Alarm			423				A	A	1	A, Tl, Th, T, I					A, Tl, Th, T, I	✓		A, T
PG23	Access Silent			426						1	A, Tl, Th, T, I					A, Tl, Th, T, I			A, T
PG24	Access Local			0						1	A, Tl, Th, T, I								A, T
PG25	Time Report			602							A								A

A - Alarm, Tl - Tamper Low, Th - Tamper High, T - Tamper, I - Isolate, Z - ZST Fail

Analogue Calibrations

ID	Name	Calibrate Calculation	Display String	Effective Gain	Format / Scale	Gain	Maximum String	Minimum String	Offset	Shift
IA1	Raw Value	((1 X RawValue) / 1) + 0	Raw Units	1	K0 F5.0	1	65535	0	0	0
IA2	IR 994089 Temp Sensor	((10 X RawValue) / 2) + 0	C	5	K1 S2.1	10	40	0	0	1
IA3	C3K Alog 0-5 Volts	((5020 X RawValue) / 256) + 0	Volts	19.60938	K3 F1.2	5020	5	0	0	8
IA4	C3K Alog 4-20mA as ma	((20079 X RawValue) / 256) + 0	mA	78.43359	K3 F2.1	20079	20	4	0	8
IA5	C3K Alog 4-20mA as %	((12550 X RawValue) / 256) + -2500	%	49.02344	K2 S3.1	12550	100	0	-2500	8
IA6	GT Light %	((1004 X RawValue) / 256) + 0	%	3.92188	K1 F3.1	1004	100	0	0	8
IA7	GT Temp DegC	((1 X RawValue) / 1) + -2732	C	1	K1 S2.1	1	50	-10	-2732	0
IA8	Unibus Alog 0-10 Volts	((20480 X RawValue) / 8192) + 0	Volts	2.5	K3 F2.2	20480	10.00 Volts	00.00 Volts	0	13
IA9	Unibus Alog 4-20mA as ma	((20480 X RawValue) / 2048) + 0	mA	10	K3 F2.2	20480	20	4	0	11

Card Formats

ID	Name	Card Number Length	Card Number Offset	Card Type	Encoding Method	Issue Number Length	Issue Number Offset	Secure 40 Scheme Type	Site Code Length	Site Code Offset	Total Bits	Wiegand Card Type
CF1	Direct Entry Wiegand	0	0	Wiegand Raw Data	Standard	0	0	Standard	0	0	0	N Bit
CF2	26Bit Wiegand (H10301)	16	9	Wiegand Site Code	Standard	0	0	Standard	8	1	26	N Bit
CF3	Indala 27 Bit - Wiegand	14	13	Wiegand Site Code	Standard	0	0	Standard	13	0	27	N Bit
CF4	Keri 30 Bit Wiegand	16	13	Wiegand Site Code	Standard	0	0	Standard	12	1	30	N Bit
CF5	Ind/Kant KSF 32Bit Wiegand	16	15	Wiegand Site Code	Standard	0	0	Standard	8	7	32	N Bit
CF6	HID 32 Bit Wiegand	18	13	Wiegand Site Code	Standard	0	0	Standard	12	1	32	N Bit
CF7	KASTLE 32Bit Wiegand	16	15	Wiegand Site Code	Standard	0	0	Standard	8	7	32	N Bit
CF8	HID 34Bit Wiegand (H10306)	16	17	Wiegand Site Code	Standard	0	0	Standard	16	1	34	N Bit
CF9	Indala 34Bit Wiegand	16	1	Wiegand Site Code	Standard	0	0	Standard	11	22	34	N Bit
CF10	HIDCorp1000 35Bit (H50360)	20	14	Wiegand Site Code	Standard	0	0	Standard	12	2	35	N Bit
CF11	HID 35 Bit Wiegand	20	10	Wiegand Site Code	Standard	0	0	Standard	8	2	35	N Bit
CF12	Indala 36 Bit Wiegand	16	19	Wiegand Site Code	Standard	0	0	Standard	18	1	36	N Bit
CF13	HID 36Bit Wiegand (Std)	16	19	Wiegand Site Code	Standard	0	0	Standard	18	1	36	N Bit
CF14	HID 36Bit Wieg (S906133A)	16	1	Wiegand Site Code	Standard	4	17	Standard	12	21	36	N Bit
CF15	HID 37Bit No SC (H10302)	35	1	Wiegand Site Code	Standard	0	0	Standard	0	0	37	N Bit
CF16	HID 37Bit SC (H10304)	19	17	Wiegand Site Code	Standard	0	0	Standard	16	1	37	N Bit
CF17	HID iClass 37Bit Wiegand	16	20	Wiegand Site Code	Standard	0	0	Standard	19	1	37	N Bit
CF18	BQT 38Bit Wiegand	19	1	Wiegand Site Code	Standard	0	0	Standard	13	24	38	N Bit
CF19	HID 40Bit Wiegand	16	16	Wiegand Site Code	Standard	0	0	Standard	12	4	40	N Bit
CF20	IR Secure40 Wiegand	0	0	IR Secure40	Standard	0	0	Standard	0	0	0	N Bit
CF21	IRMag Secure	6	16	IR Mag Swipe	Standard	2	22	Standard	10	6	24	N Bit
CF22	C3K Mag Direct	0	0	Hashed Credit Card	Standard	0	0	Standard	0	0	0	N Bit
CF23	Integrity Mag Direct	0	0	Mag Swipe Raw Data	Standard	0	0	Standard	0	0	0	N Bit

K. System Input Process Group Defaults

The table below describes what System Input should be assigned to a system Area with what Process Group.

Process Group	System Input Name
AC Fail	AC fail Ext AC fail Low Volts
Access Alarm	Door DOTL Door*x* DOTL
Access Silent	Door Forced Door*x* Forced
Battery Problem	Batt Test Ext Low Batt Ext Batt Test Low Batt
Comms Problem	Phone Line
Duress	Duress Deadman Rdr*x* Duress
LAN Fault	LAN Comms Unibus
Local Alarm	DET Fuse Ext DET Fuse Ext LAN Fuse Ext Low Volts Invalid Card LAN Fuse Light Level Low Volts Pin Attempts Reset Temperature
Local Silent	DBase Changed Rdr*x* Fault Rdr*x* Invalid
Panic	Panic

Process Group	System Input Name
Pwr Supply Fault	Ext PS Fail PS Fail
RF Tx Fault	Xmit LowBatt XmitPollFail
RF Tx Jam	Xmitter Jam
Tamper	Cab Tamper Door Reed Door Tamper Door Tongue Doorx Fault Ext Sir Tamp Int Sir Tamp Pin Attempts Rdr Tamper
Time Report	Time Report

Table 10

L. Integriti Programming Examples

This portion of the document contains programming examples to help get a better understanding of how to fully utilise the Integriti controller.

Example 1 - Flashing auxiliaries during a time period

This example demonstrates the use of macros in conjunction with a few entities. This example will toggle an auxiliary once every 5 seconds. Every fifth toggle, another auxiliary will turn on for 10 seconds. This macro will only run while a time period is valid.

Entities used:

- 1x General variable
- 1x Macro
- 1x Time period
- 2x Auxiliaries

Entity configuration:

In this example we have created a time period called '`Working Hours`'. This time period has been configured for 09:00 to 17:30 Monday to Friday.

The general variable used has been called 'Example Counter'. The test value for the general variable has been set to 4.

The two auxiliaries (C01:X01 and C01:X02) have been labelled 'Flasher 1' and 'Flasher 2'.

Macro statements:

A total of eight statements are required to achieve this goal:

Macro: **`Example 1`**

#	Statement	Configuration	
1	`Wait for Condition…`	**Expression:**	`TP1`
2	`Do an Action`	**Action:**	`Control Aux`
		Auxiliary:	`C01:X01`
		When Asserted:	`Toggle`
3	`Pause for Time…`	**Expression:**	`50`
4	`Set Entity To Expression…`	**Expression:**	`GV1+1`
		Entity to Set:	`GV1`
5	`Goto <label> if…`	**Expression:**	`!GV1`
		Label:	`SkipOn`
6	`Do an Action`	**Action:**	`Control Aux`
		Auxiliary:	`C01:X02`
		On Time:	`00:00:10`
7	`Set Entity To Expression…`	**Expression:**	`0`
		Entity to Set:	`GV1`
8	`Define a Label`	**Label:**	`SkipOn`

Statement summary for macro: **`Example 1`**

1. Prevent further execution of the macro until the time period (`TP1`) is valid.
   - `TP1` (`Work Hours`) has been configured for 09:00 to 17:30 hours Monday to Friday. If the panel time and day fall within these values then the test of time period `TP1` will return true and remainder of the macro will be executed.
2. This statement toggles the first auxiliary (`Flasher 1`).
   - C01:X01 (Flasher 1) has been to toggle on assert. Every time this statement is executed the state of the auxiliary will be inverted.
3. Pause for `50` x 100ms (5 seconds).
   - The macro will pause for a period of 5 seconds.
4. Add 1 to the general variable (`GV1`).
   - The general variable GV1 is set to a value that is itself plus one.
5. If the test of general variable (`GV1`) does not return true, go to the label '`SkipOn`'.
   - When the general variable (`GV1`) was configured, its test value was set to four. If the general variable is greater than this value, it will return true.
   - The expression '`!GV1`' is a test to see if `GV1` is not returning true (If the value is equal to four or less).
   - If the expression returns true, the following two statements will be skipped.
6. Turn on the second auxiliary (Flasher 2) for 10 seconds.

- If an on time other than zero is specified for an auxiliary action, the target auxiliary will turn off after the time expires.

7. Reset the general variable (GV1) back to `0`.
    - The general variable GV1 is set to zero.
8. This is the label (`SkipOn`) that the macro moves execution to if the general variable (`GV1`) does not return true (GV1 is greater than 4).
9. Return to step 1.

Example 2 - Random bag inspections

During work hours random bag inspections are carried out. Users going through door x will be denied access at random. An input or users with special access can be used to reset the random bag inspection and allow the user to pass through.

Entities used:

- 1x Door
- 1x General variable
- 1x Input
- 1x Named Action
- 1x Reader module
- 1x Time period
- 2x Macros
- 2x Permission Groups
- 2x Users

Entity configuration:

In this example we have configured a door (Door x) as a normal entry door associated with a reader module (Reader x).

We have two users - User '`Employee`' is subject to random bag inspections. The '`Supervisor`' user is not. We will name the two permission groups '`Employees`' and '`Supervisors`' respectively. Each user has its own credential.

We have called the time period '`Working Hours`'. This time period has been configured for 09:00 to 17:30 Monday to Friday.

The general variable '`Random inspection`' is used to determine user access. It is assigned a random number using the first macro 'Random bag' and reset to zero by the other macro 'Reset random bag'.

The named action 'Start random bag' is triggered by 'Door x' but only when working hours are valid. 'Start random bag' will start the macro 'Random bag' every time 'Door x' is opened.

The Input 'Reset bag' is used by the supervisor on duty. Pressing the button attached to the input 'Reset bag' will start the macro 'Reset random bag'.

Macro statements:

Both macros are small (only containing two statements each):

Macro: **`Random bag`**

#	Statement	Configuration	
1	`Set Entity To Expression…`	**Expression:**	`8388607`
		Entity to Set:	`GV2`

2	End Current Macro

Macro: **Reset random bag**

#	Statement	Configuration
1	Set Entity To Expression…	**Expression:** 0 **Entity to Set:** GV2
2	End Current Macro	

Statement summary for macro: Random bag

1. The entity GV2 'Random inspection' is assigned a value of 8388607.
    - The number 8388607 is a magic number. Entities assigned this number are actually given a random number between 1 and 8388067. For more information, please refer to the appendices.
2. Stop the macro.
    - This statement will cause the macro to stop.

Statement summary for macro: Reset random bag

1. The entity GV2 'Random inspection' is assigned a value of 0.
2. Stop the macro.
    - This statement will cause the macro to stop.

M.Licenses

Software and hardware licenses are used to enable specific features within the controller or software management suite.

Integriti licenses are managed online by KeyPoint.

Licenses can be managed from https://license.innerrange.com/

Software licenses

Below is a list of all of the available Integriti licenses.

#	Name	Description
996905UPG	Integriti Express to Pro Upgrade	Users running Integriti Express can upgrade to Integriti Pro using this license key.
996909	Allow RDP Remote Connections	This license allows remote desktop connections.
996910	Software Client License (Fixed)	This license is reserved for a specific client machine. (Can be changed to another computer if needed) Ideal for situations where specific client machines must / should be connected to the Integriti server at all times.
996911	Software Client License (Floating)	This client license adds to a pool of available client connections. Ideal for situations where many machines may connect to the Integriti server for a session but not all simultaneously.
996912	Extra Controller Connection License for Integriti Pro	Licenses the connection of an additional Integriti controller.
996920	CCTV – First 32 Cameras	Permits the connection of up to 32 cameras.
996921	CCTV – Extra 8 Cameras	Permits the connection of additional cameras. The 'CCTV – First 32 Cameras' license (996920) is required.
996922	Integriti Photo ID	Enables printing of Photo IDs.
996923	Integriti Advanced Reports	Enables Integriti advanced reporting.

#	Name	Description
996925	Integriti Advanced Alert - Alarm event & Escalation Manager	Enables more functionality in the Integriti alert handler.
996930	Integriti Communications Module SMS & EMAIL	Enables the SMS and eMail communication handlers.
996940	Integriti Pro – Additional Door License	
996950	XML READ – 3rd Party Interface	Enables 3rd party read functionality. 3rd party software can interrogate the Integriti database.
996951	XML Write – 3rd Party Interface	Enables 3rd party write functionality. 3rd party software can write to the Integriti database.
996952	XML Control – 3rd Party Interface	Enables 3rd party control of Integriti entities.
996955	Integriti DUIM	Enables the dynamic user import module. Automatically imports users for creation, modification or deletion from a 3rd party product.

Table 11

Hardware licenses (Smart card)

There are 5 license levels the Integriti controller can have. The following table describes the controller limitations for each level. Integriti controllers without a smart card will have a license level of '*none*'.

License	Review	Users	Zones	Doors
none	10,000	200	100	16
Level 1	20,000	2,000	200	40
Level 2	30,000	10,000	600	80
Level 3	60,000	65,000	2,000	160
Level 4	100,000	100,000	3,000	240

Table 12

Below is a list of all of the available Integriti controller licenses.

#	Name	Description
996020U01	ISC Smart Card Upgrade BLANK to Level 1	Level 1 license: 20,000 Review events, 2,000 Users, 200 Zones and 40 Doors
996020U12	ISC Smart Card Upgrade Level 1 to Level 2	Level 2 license: 30,000 Review events, 10,000 Users, 600 Zones and 80 Doors
996020U13	ISC Smart Card Upgrade Level 1 to Level 3	Level 3 license: 60,000 Review events, 65,000 Users, 2,000 Zones and 160 Doors
996020U14	ISC Smart Card Upgrade Level 1 to Level 4	Level 4 license: 100,000 Review events, 100,000 Users, 3,000 Zones and 240 Doors
996020U23	ISC Smart Card Upgrade Level 2 to Level 3	Level 3 license: 60,000 Review events, 65,000 Users, 2,000 Zones and 160 Doors
996020U24	ISC Smart Card Upgrade Level 2 to Level 4	Level 4 license: 100,000 Review events, 100,000 Users, 3,000 Zones and 240 Doors
996020U34	ISC Smart Card Upgrade Level 3 to Level 4	Level 4 license: 100,000 Review events, 100,000 Users, 3,000 Zones and 240 Doors
996021	ISC Smart Card 5 User Web Interface License	Enables remote web access to the Integriti controller. Designed to be used in conjunction with the Android or Iphone Integriti app.
996022	ISC Smart Card Automation Interface License	Enables 3rd party interface communication tasks.
996023	ISC Smart Card EMS License (Lift Integration)	Enables high-level lift integration.
996024	ISC Smart Card Global Salto	Enables Salto integration.
996020L1	ISC Smart Card – Level 1	

#	Name	Description
996020L1T	ISC Smart Card Blank Card Version 1	

Table 13