Version 1.1

integriti

INTEGRATED SOLUTIONS

DRAFT

INTEGRITI SOFTWARE INSTALLATION MANUAL

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

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. The purchaser assumes all responsibility in the 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.

Integriti Software Installation Manual

Table of Contents

Company Statement

Inner Range Pty Ltd is proud of the reputation it has gained in the provision of high quality electronic security products. Exhaustive factory and field testing ensure that enhanced system programming features and additional hardware components operate as expected prior to their release to our customers. Extensive function testing is carried out on every Inner Range security product prior to it leaving the factory. It is our intention to completely satisfy the requirements of our customers. To that end, Inner Range Pty Ltd stands behind its products with confidence.

Software Maintenance Agreement

Protect your Integriti software investment with an optional Inner Range software maintenance agreement

For a modest annual fee you will receive:

- Telephone and e-mail customer support by our Integriti help desk.
- Free software upgrade releases of Integriti for the software modules for which you are licensed.

Get the most from your Integriti security management software!

Complete and return the Application form contained in your Integriti pack or download the form from: http://www.innerrange.com/downloads/MaintenanceAgreement.pdf

Did you know that Inner Range operates customer training courses throughout Australia, New Zealand, Europe and other areas?

Details of our Integriti system administration courses are listed on our training website at http://www.onlinetraining.innerrange.com/

Enrol on-line or contact Inner Range on +61 3 9780 4300 or via email to: admin@innerrange.com

Product Highlights

Connectivity

- Simplified controller connectivity (only requires a single TCP port).
    - Improved NAT traversal, far less firewall configuration required.
- Simple automatic discovery of controllers on local network.
- Integriti is a true multi-controller, multi-workstation system.
- Supports paths with automatic switching to redundant paths on link failure.
- Clustered architecture: Support for multiple servers for scalability or high availability.

Editing

- Changes to module programming take effect immediately, without a LAN secure.
- Unlimited number of granular permissions and credentials per user.
- Dynamic update of all data. All changes are instantly reflected on other operator workstations, no need to refresh screens if someone else changes something.
- Programming structures, inputs and outputs for LAN modules are created automatically when they are connected to the LAN.
- Fully customizable user interface, allows any editor to be customized to suit customer needs.
- Multi-select edit. Set the properties of multiple records in a single operation, no need to manually apply the change to each record.
- Cross reference: Graphically visualize the relationships between all entities in the system.
- Live LAN status of modules, zones and auxiliaries are displayed.
- Dynamically filter and sort by any field on any entity.
- Dynamically filter and sort by current state (inputs in alarm, doors that are unlocked, etc…).
- Selectively show or hide items based on:
    - Name.
    - LAN status (secured, missing, unexpected, not installed).
    - Programming status (blank, programmed, queued for upload/download).
- Logical groupings: allow entities to be arranged and grouped with infinite flexibility.
- Support for multiple sites, with unlimited sub-sites.
- Window / docking panel placement customisation including layout saving and retrieval per operator.
- Single-click hyper-linking between forms.
- Automatic detection of edits made at any Terminal.
- User editing provides the following features:
    - Users can be exported.
    - Multiple users can be selected for blanking records or exporting.

Reports

- Comprehensive audit trail.
- Any filtered data grid can be exported right from within the system designer.
- 3NF normalized database, can be easily queried and reported on.

Management

- Full support for offline editing.
- Comprehensive operator permissions system providing infinite flexibility.
- Hierarchical operator permissions allowing separate sites to be administered both individually and globally.
- Full support for multi-site and multi-tenancy.

Control

- Remotely control areas, area lists, auxiliaries, auxiliary lists, doors, door lists, floors, floor lists, named actions and zone inputs.
- Per-user permissions are enforced for remote control from the software.

Integriti – Before you start

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

Supported operating systems[1]:

- Windows Vista SP2
- Windows 7 SP1
- Windows Server 2008

Minimum system requirements

All machine specifications must include the following:

- A screen resolution of 1024x768 or higher. A 22” WSXGA+ monitor at 1680x1050 is recommended.
- A DVD R/W drive or higher.
- The Integriti software management suite requires both a keyboard and pointing device to operate.

Client workstation specifications:

- 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.

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

- 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.

[1] Windows XP is not officially supported, however Integriti has been known to work on windows XP SP 3 or newer.

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

- 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.

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

- 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.

Server hardware recommendations

The minimum system requirements outlined in the section above are

Integriti specifications

Approximate disk usage:

~100MB	- Integriti software management suite
550MB – 10GB	- SQL Express 2008[2]

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
1576	- TCP	
4711	- TCP	Controller ↔ Controller server communications

By default, Integriti uses the Microsoft SQL 2008 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. To ease the CPU load on both the SQL database and Integriti server, these can be located on separate computers.

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

[2] 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.

Installing Integriti

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

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

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 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.

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).

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 Panel 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)

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.

There are three registration methods available:

Register online.

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.

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 provided QR code. 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.

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.

Register using another computer or by contacting your distributer.

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

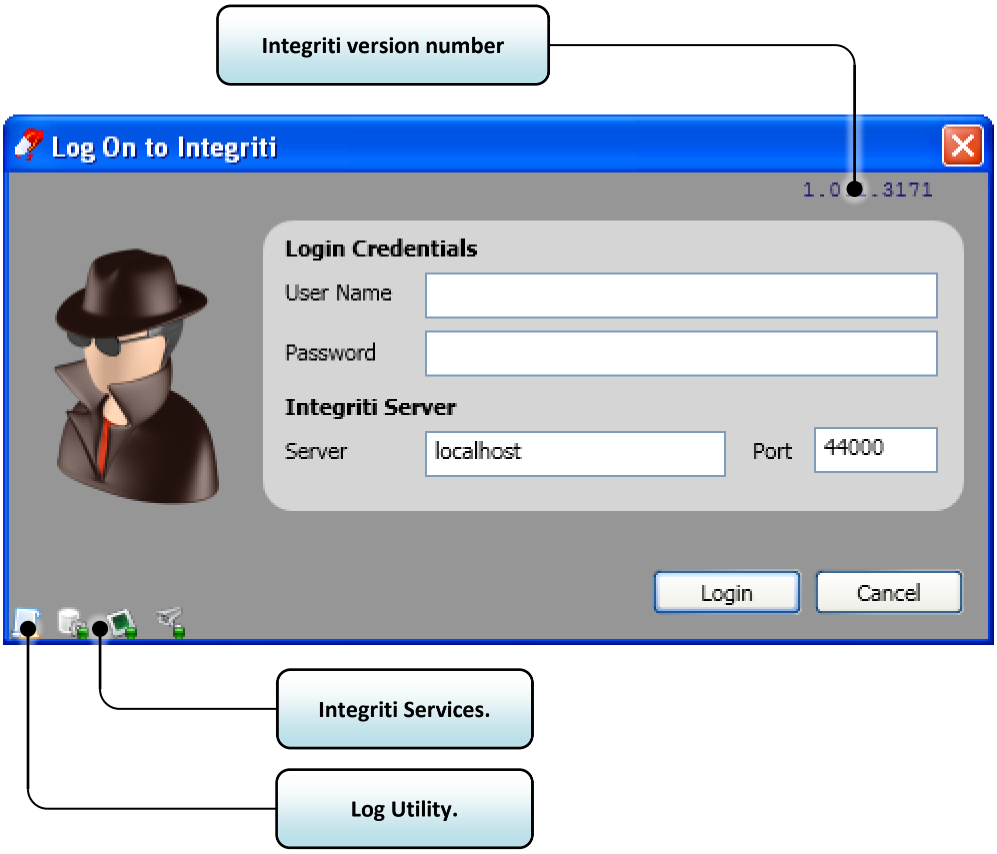
Integriti basics

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.

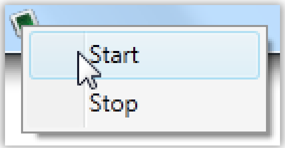
The default Integriti operator login is a user name of 'Installer' with the default password of 'installer'. It is strongly recommended that you remove this operator or change the password as soon as possible.



Make sure the Integriti services are running before you attempt to log in.

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.



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 CCTV server				

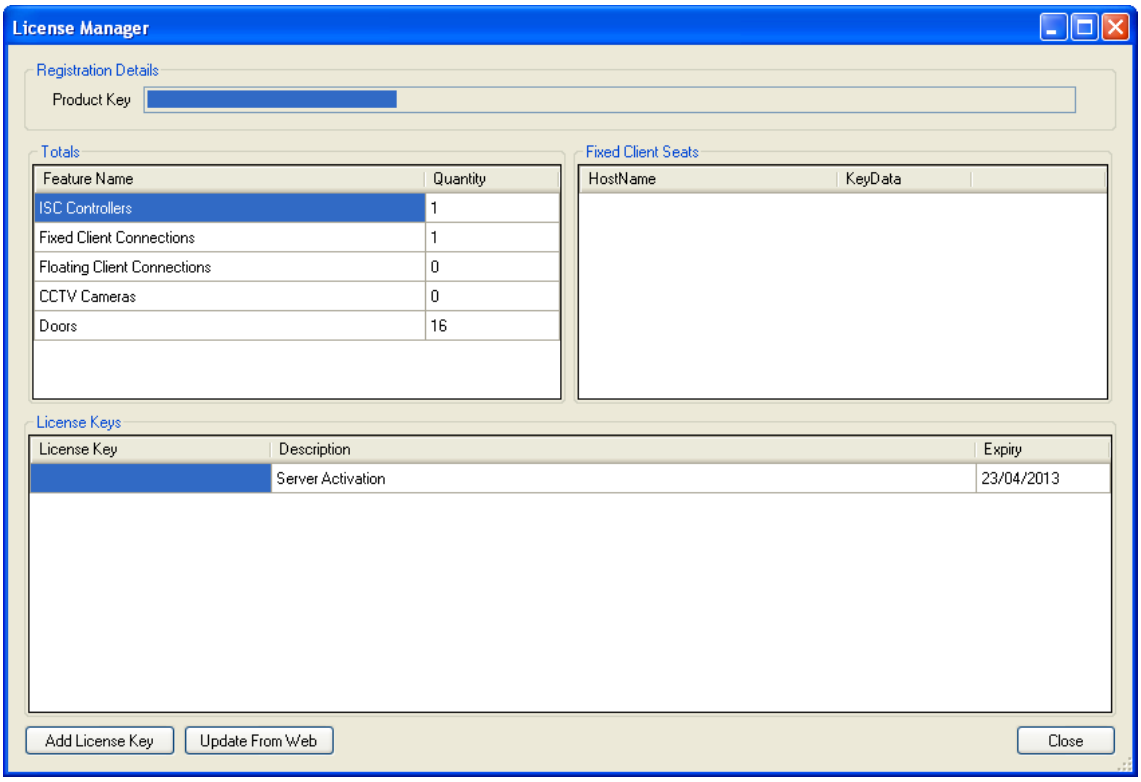
Log Utility

The log utility is used for diagnostic / fault finding purposes. You can access the log utility by double-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.

License Management

After logging in, you might want to check that your licenses are up to date within your license manager.

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



License Manager

Registration Details

Product Key [redacted]

Totals

Feature Name	Quantity
ISC Controllers	1
Fixed Client Connections	1
Floating Client Connections	0
CCTV Cameras	0
Doors	16

Fixed Client Seats

HostName	KeyData

License Keys

License Key	Description	Expiry
[redacted]	Server Activation	23/04/2013

Figure 1

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 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.

Adding Integriti controllers to Integriti

Once Integriti is installed and running, the next thing you will need to do is enrol Integriti controllers. Integriti controllers can be added (enrolled) to Integriti using one of two methods.

Automatic controller discovery (Method 1)

The simplest method of adding controllers to Integriti is by using the 'Auto Discover new Controllers…' feature.

To access this feature, click on the Home tab followed by the Discover Controllers button (***Figure 2***).

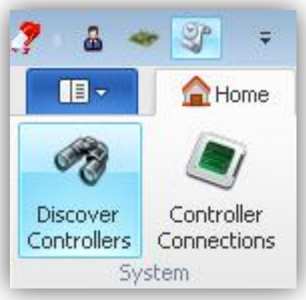
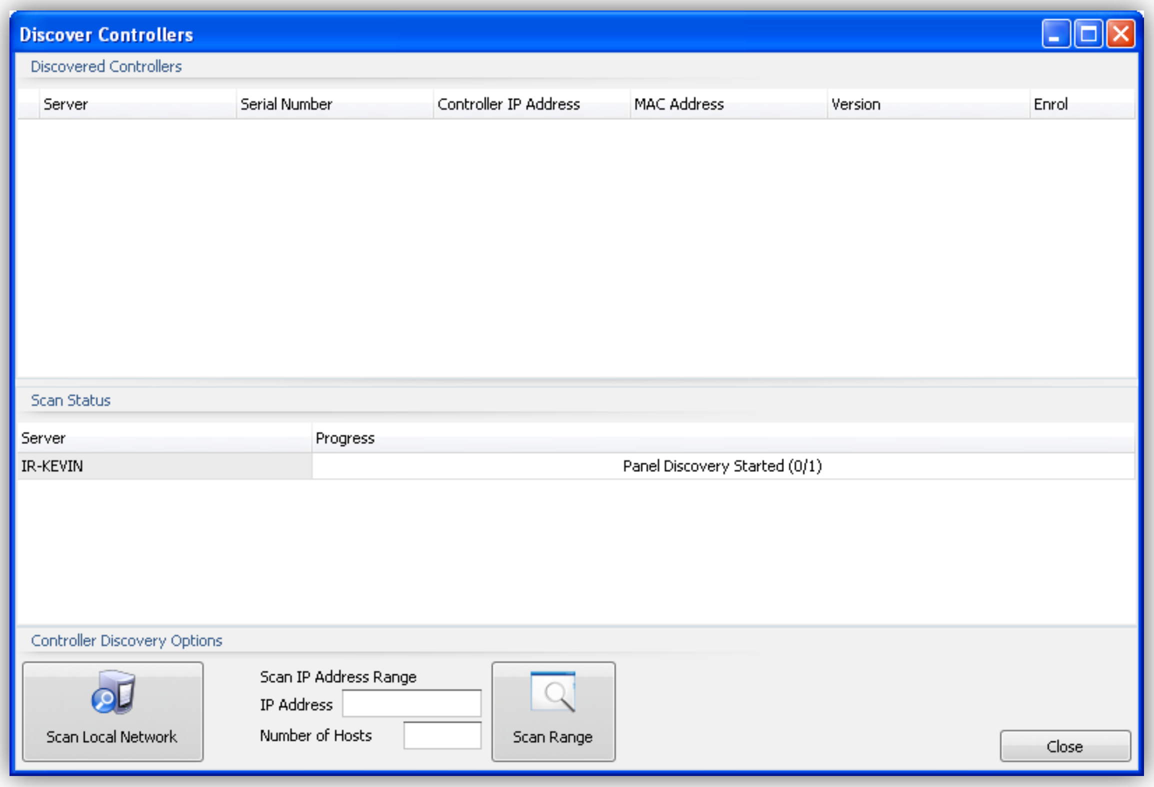


Figure 2

The 'Discover Controllers' dialog will appear and automatic controller discovery will begin (*Figure 3*).



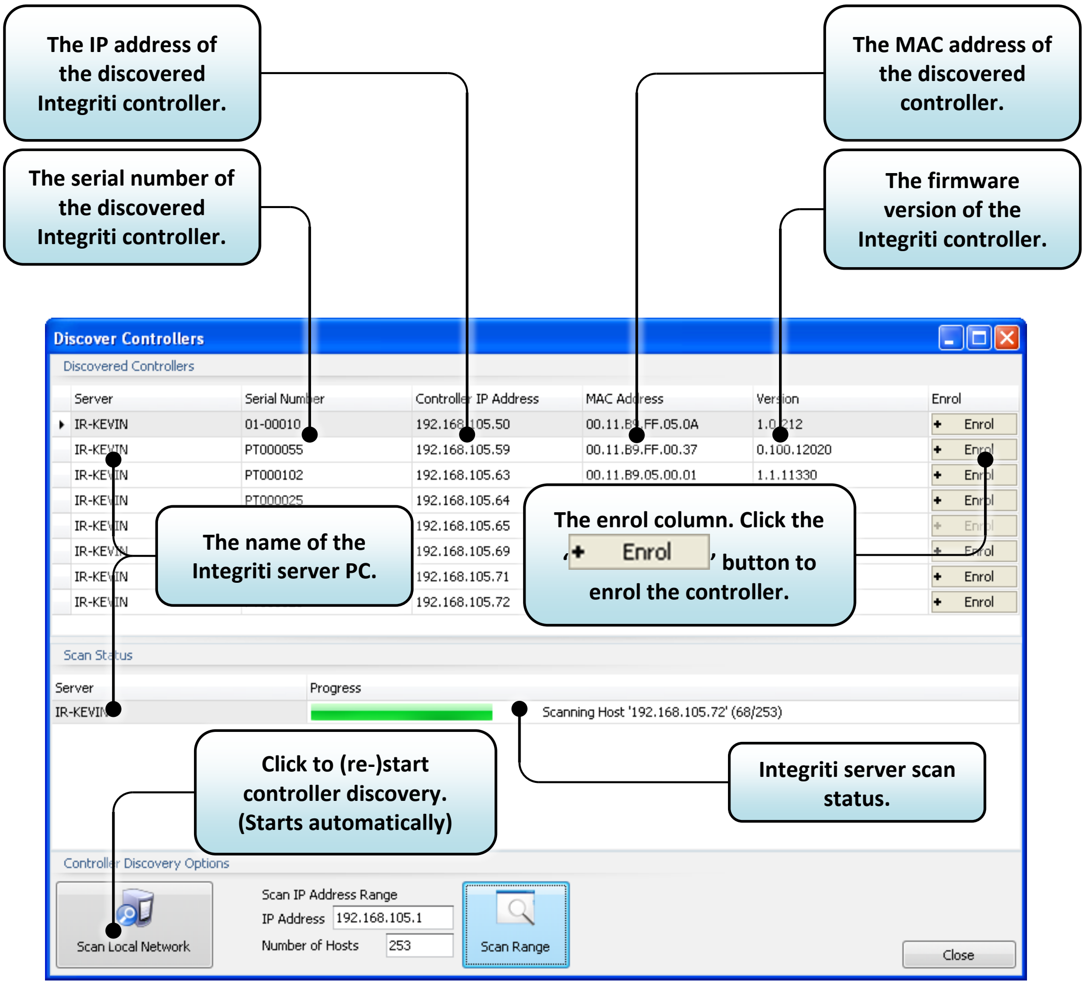
Server	Serial Number	Controller IP Address	MAC Address	Version	Enrol

Server	Progress
IR-KEVIN	Panel Discovery Started (0/1)

Figure 3

When the automatic controller discovery has completed the Integriti controllers will be listed in the upper section (Discovered Controllers) of the dialog window (*Figure 4*).

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



The IP address of the discovered Integriti controller.

The serial number of the discovered Integriti controller.

The MAC address of the discovered controller.

The firmware version of the Integriti controller.

The name of the Integriti server PC.

The enrol column. Click the '+ Enrol' button to enrol the controller.

Click to (re-)start controller discovery. (Starts automatically)

Integriti server scan status.

Discover Controllers

Discovered Controllers

Server	Serial Number	Controller IP Address	MAC Address	Version	Enrol
IR-KEVIN	01-00010	192.168.105.50	00.11.B9.FF.05.0A	1.0.212	+ Enrol
IR-KEVIN	PT000055	192.168.105.59	00.11.B9.FF.00.37	0.100.12020	+ Enrol
IR-KEVIN	PT000102	192.168.105.63	00.11.B9.05.00.01	1.1.11330	+ Enrol
IR-KEVIN	PT000025	192.168.105.64			+ Enrol
IR-KEVIN		192.168.105.65			+ Enrol
IR-KEVIN		192.168.105.69			+ Enrol
IR-KEVIN		192.168.105.71			+ Enrol
IR-KEVIN		192.168.105.72			+ Enrol

Scan Status

Server	Progress	
IR-KEVIN	🟩	Scanning Host '192.168.105.72' (68/253)

Controller Discovery Options

Scan IP Address Range

IP Address: 192.168.105.1

Number of Hosts: 253

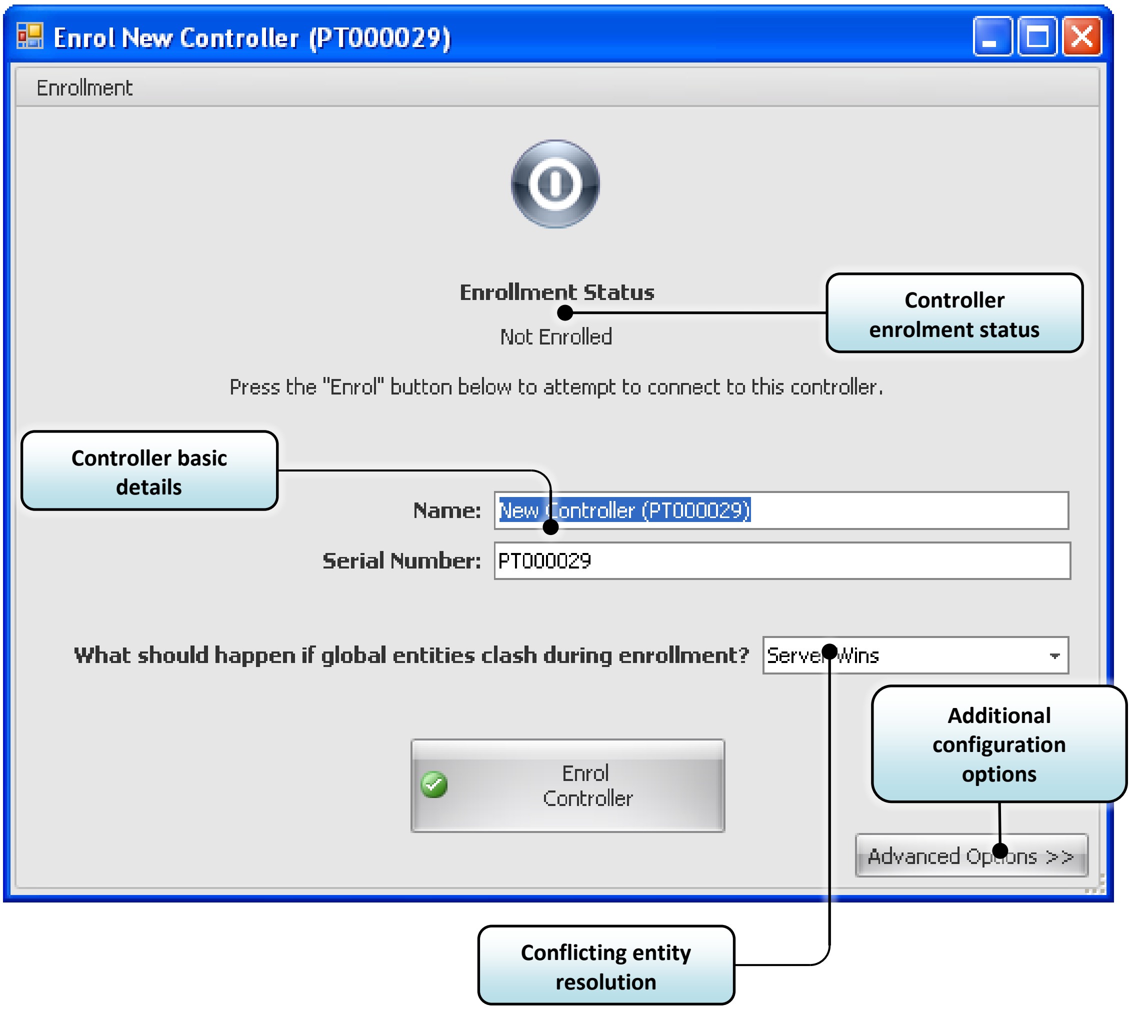
Figure 4

You can enrol controllers as soon as they appear in the ‘Discovered Controllers’ list. Simply click the ✚ Enrol button to open the ‘Enrol New Controller’ form (*Figure 5*).

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

> *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.*

> *Discovered controllers with a greyed out enrol button (* ✚ Enrol *) are controllers that have already been enrolled.*



Enrol New Controller (PT000029)

Enrollment

Enrollment Status

Not Enrolled

Press the "Enrol" button below to attempt to connect to this controller.

Name: New Controller (PT000029)

Serial Number: PT000029

What should happen if global entities clash during enrollment? ServerWins

Controller enrolment status
Controller basic details
Enrol Controller
Additional configuration options
Advanced Options >>
Conflicting entity resolution

Figure 5

After clicking the + Enrol button, there are only two items that require your attention before starting the enrolment process. First, give your controller a name that appropriately describes its purpose or location. Next, you will need to decide how the conflicting entity resolution is handled. When an entity within the controller does not match the corresponding entity in the Integriti server, one of the two options will occur:

- If 'Server Wins' is selected, the entity on the controller is replaced with the corresponding entity on the server.
- If 'Controller Wins' is selected, the entity on the Integriti server is replaced with the corresponding entity on the controller.

> *If you are unsure about what option you should select, leave the default (recommended) setting- 'Server Wins'.*

When you are ready to enrol the controller, click the ✓ Enrol Controller button.

Manual controller enrolment (Method 2)

To manually enrol a controller, use the following procedure:

1. Click on the Controller Connections button under the Home tab.
2. The Controller panel should appear.
3. Click ⊕ Add New to open a dialog window for the creation of the new controller.
4. Give the Integriti controller a name and add any necessary details in the notes field.
5. Click on the Connection Details tab.
6. Enter the serial number of the Integriti controller in the serial number field.

Connectivity

7. Change connection mode to Auto.

Synchronisation

8. Check Enable Data Synchronisation.
9. Change Global Data Sync Options to Deny Controller Edits.
10. Click the 💾 button and close the dialog.
11. Right-click the newly created controller in the Hardware panel and select ⚡ Connect (Manual) … .
12. The Connect to Controller dialog should appear.
13. Enter the IP address of the controller in the Controller IP Address field and click Connect.
14. An icon (⚡) should appear to the right of the controller in the Hardware panel indicating that the server is synchronising with the Integriti controller.

To determine the IP address of the Integriti controller, use the following procedure:

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.

> *Please refer to the Integriti controller installation manual for information on programming via the terminal.*

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 6*).

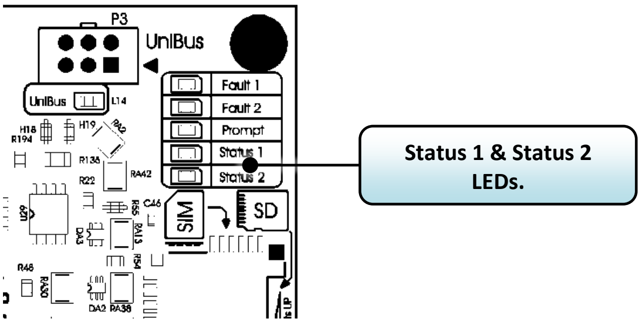


Figure 6

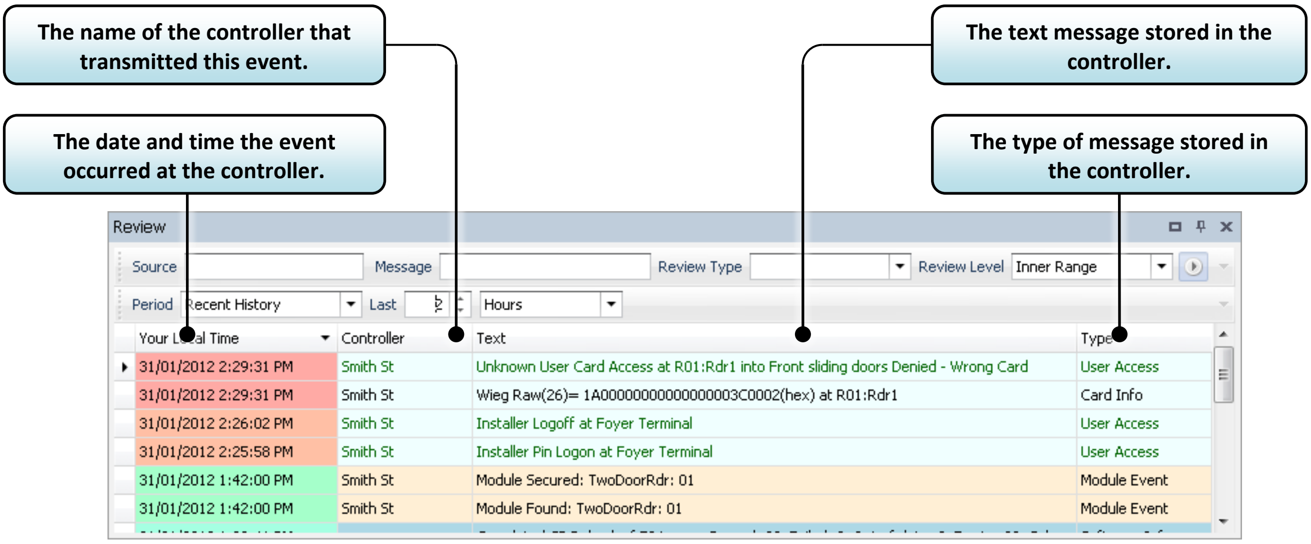
3. Log in to the terminal by pressing: **[0]**, **[1]**, **[Ok]**
4. Go in to controller information by pressing: **[Menu]**, **[1]**, **[9]**
5. Press **[▼]** once to display the controller serial number.
6. Press **[▼]** once more to display the controller MAC address.
7. Press **[▼]** two more times 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)

User Interface

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

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 take place and action them as required.



The name of the controller that transmitted this event.

The text message stored in the controller.

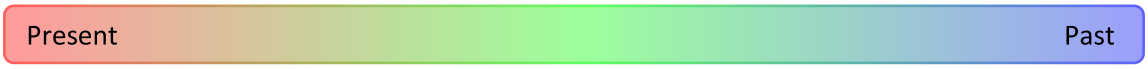
The date and time the event occurred at the controller.

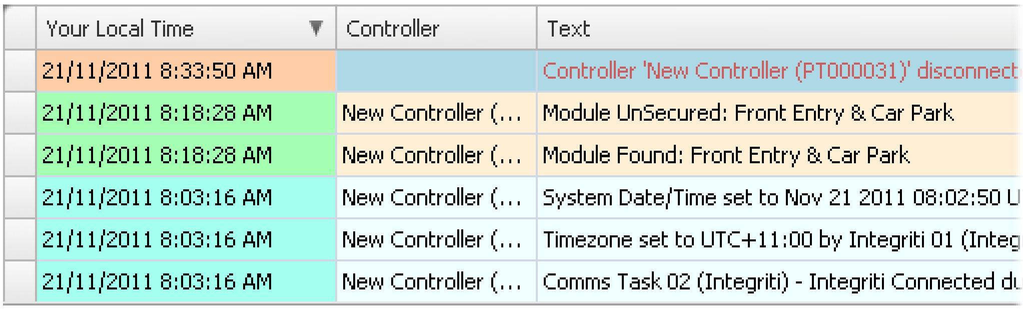
The type of message stored in the controller.

Your Local Time	Controller	Text	Type
31/01/2012 2:29:31 PM	Smith St	Unknown User Card Access at R01:Rdr1 into Front sliding doors Denied - Wrong Card	User Access
31/01/2012 2:29:31 PM	Smith St	Wieg Raw(26)= 1A000000000000003C0002(hex) at R01:Rdr1	Card Info
31/01/2012 2:26:02 PM	Smith St	Installer Logoff at Foyer Terminal	User Access
31/01/2012 2:25:58 PM	Smith St	Installer Pin Logon at Foyer Terminal	User Access
31/01/2012 1:42:00 PM	Smith St	Module Secured: TwoDoorRdr: 01	Module Event
31/01/2012 1:42:00 PM	Smith St	Module Found: TwoDoorRdr: 01	Module Event

Figure 7

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.

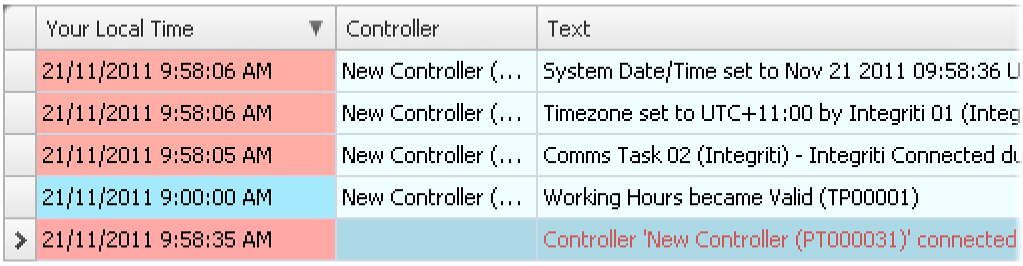




	Your Local Time ▼	Controller	Text
	21/11/2011 8:33:50 AM		Controller 'New Controller (PT000031)' disconnect
	21/11/2011 8:18:28 AM	New Controller (...	Module UnSecured: Front Entry & Car Park
	21/11/2011 8:18:28 AM	New Controller (...	Module Found: Front Entry & Car Park
	21/11/2011 8:03:16 AM	New Controller (...	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 8

The single greatest advantage of this feature is the ability to notice how review events are grouped without reading individual timestamps. ***Figure 8*** 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 9

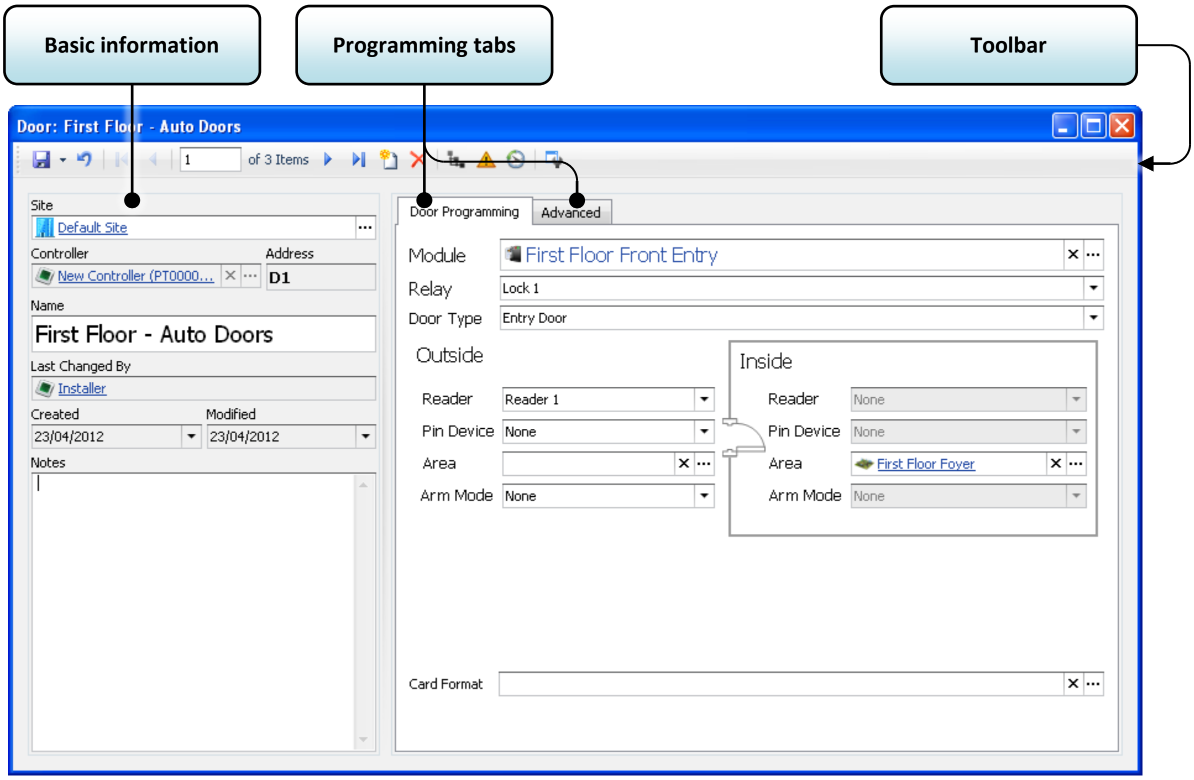
In the example above an older event has been placed in between newer events. This scenario can occur when communications to one or many controllers has been (re-)established. Review filtering and organisation occurs at the time the filter is applied.

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.

Dialog windows

Most programming windows will look like the following example…



Door: First Floor - Auto Doors

Site: Default Site

Controller: New Controller (PT0000…

Address: D1

Name: First Floor - Auto Doors

Last Changed By: Installer

Created: 23/04/2012

Modified: 23/04/2012

Notes:

Module: First Floor Front Entry

Relay: Lock 1

Door Type: Entry Door

Outside

Reader: Reader 1

Pin Device: None

Area:

Arm Mode: None

Inside

Reader: None

Pin Device: None

Area: First Floor Foyer

Arm Mode: None

Card Format:

Figure 10

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

The right side of the programming window contains a number of programming tabs (usually two). The first tab (eg ‘Door Programming’) 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 (Eg inputs to an area).

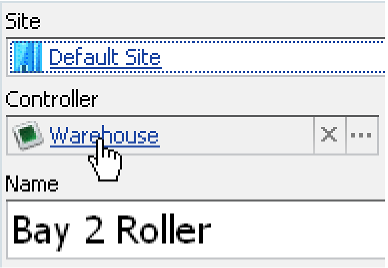
Toolbar

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**	
	Audit	Open a new window displaying the entire history of changes made to this record.
	Customize Layout	Change the layout of the dialog window.

Hyperlinks

Integriti has the added convenience of hyperlinks. Hyperlinks are blue text labels that let 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.

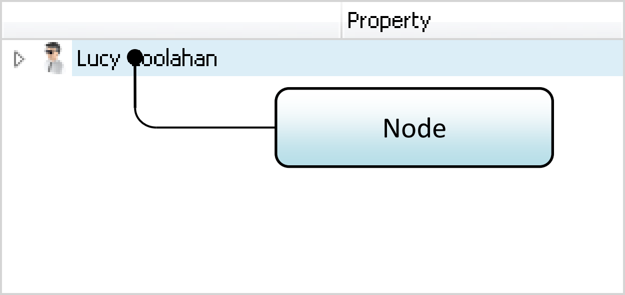


Site
Default Site
Controller
Warehouse
Name
Bay 2 Roller

Figure 11

Cross references

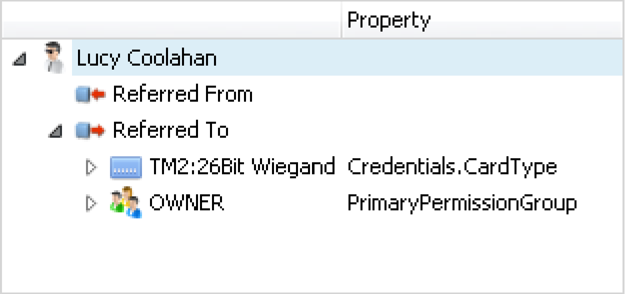
Cross references can be used to quickly discover what entities the current entity is referenced to or referenced from. Click the button to display the cross references for the entity.



	Property
Lucy Coolahan	

Figure 12

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



	Property
Lucy Coolahan	
Referred From	
Referred To	
TM2:26Bit Wiegand	Credentials.CardType
OWNER	PrimaryPermissionGroup

Figure 13

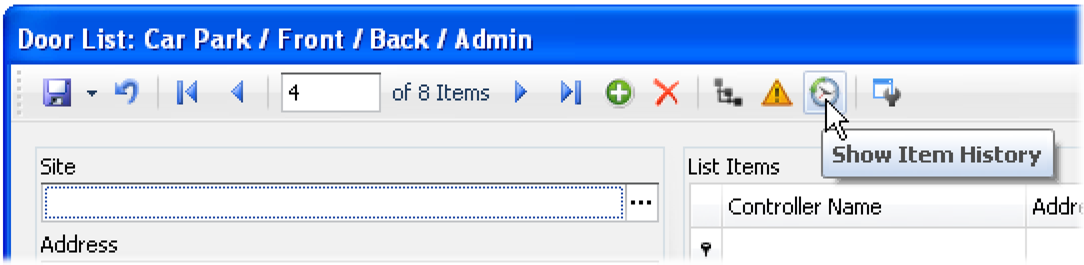
In *Figure 13* we can see that the user 'Lucy Coolahan' has been expanded out. There are two other entities that this node refers to – a credential and permission group.

Audit Trail

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

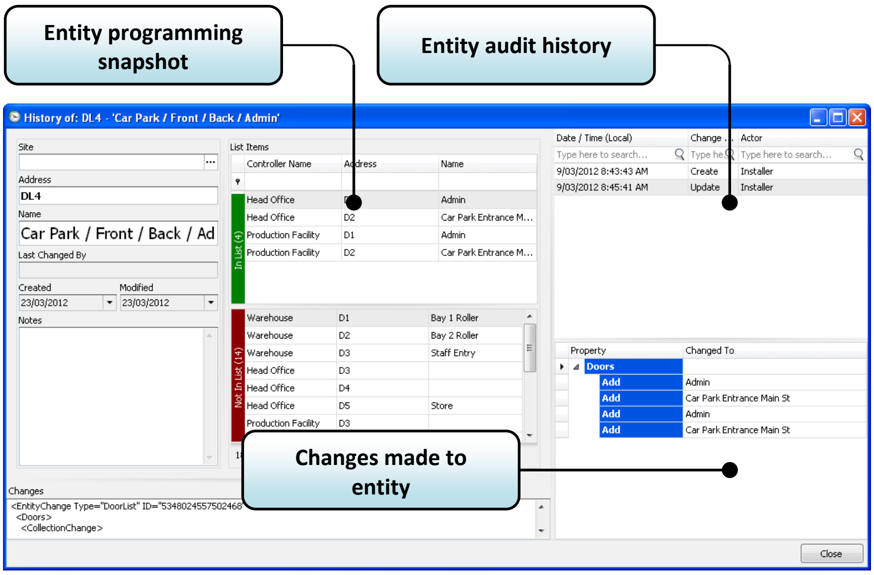
Take advantage of the audit feature. If you've made a programming error, use audit to help review the changes you made.

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



Door List: Car Park / Front / Back / Admin

Figure 14



History of: DL4 - 'Car Park / Front / Back / Admin'

Site:

Address: DL4

Name: Car Park / Front / Back / Ad

Last Changed By:

Created: 23/03/2012

Modified: 23/03/2012

Notes:

List Items

	Controller Name	Address	Name
In List (4)	Head Office	D[illegible]	Admin
	Head Office	D2	Car Park Entrance M...
	Production Facility	D1	Admin
	Production Facility	D2	Car Park Entrance M...
Not In List (14)	Warehouse	D1	Bay 1 Roller
	Warehouse	D2	Bay 2 Roller
	Warehouse	D3	Staff Entry
	Head Office	D3	
	Head Office	D4	
	Head Office	D5	Store
	Production Facility	D3	

Changes

```
<EntityChange Type="DoorList" ID="5348024557502468
 <Doors>
  <CollectionChange>
```

Date / Time (Local)	Change ...	Actor
9/03/2012 8:43:43 AM	Create	Installer
9/03/2012 8:45:41 AM	Update	Installer

Property	Changed To
Doors	
Add	Admin
Add	Car Park Entrance Main St
Add	Admin
Add	Car Park Entrance Main St

Figure 15

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.

Customizing layouts

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.

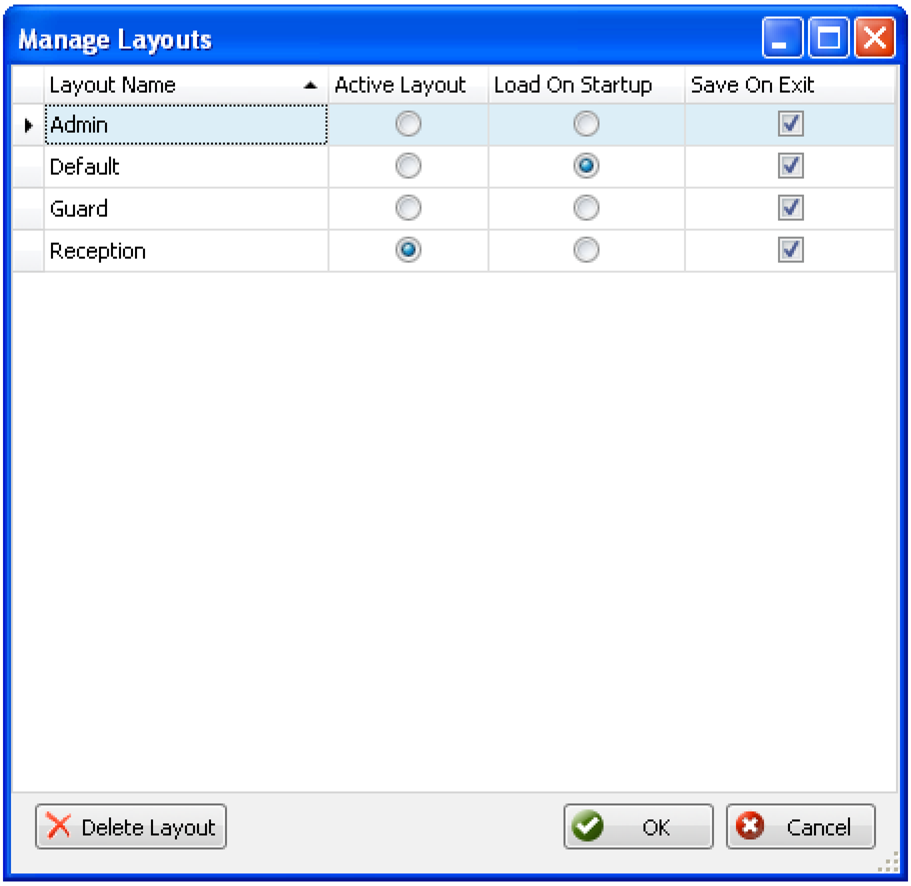
Additional layout configuration settings are found under the Window tab.

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

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.

Click on the Manage button to open the layout manager.



Layout Name	Active Layout	Load On Startup	Save On Exit
Admin	○	○	☑
Default	○	●	☑
Guard	○	○	☑
Reception	●	○	☑

Figure 16

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.

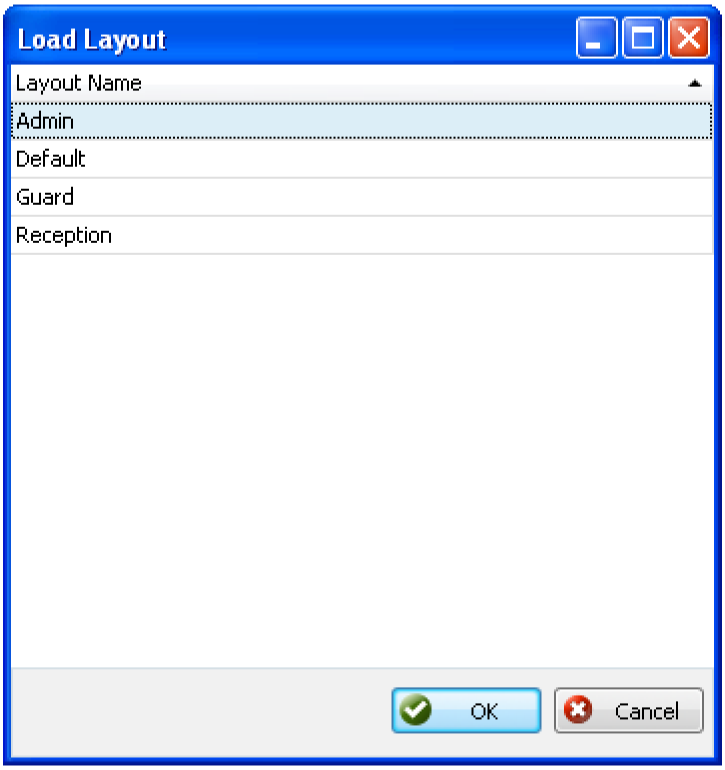
The active layout can be changed at any time by opening the layout manager and clicking on the radio button in the 'Active Layout' column to the right of the desired layout.

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 Save button will save the current layout to the layout that is currently active.

Clicking Save As… 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.

Click on the Load button to load a specific layout.



Layout Name
Admin
Default
Guard
Reception

Figure 17

Click on the desired layout followed by OK.

Editor layout sets

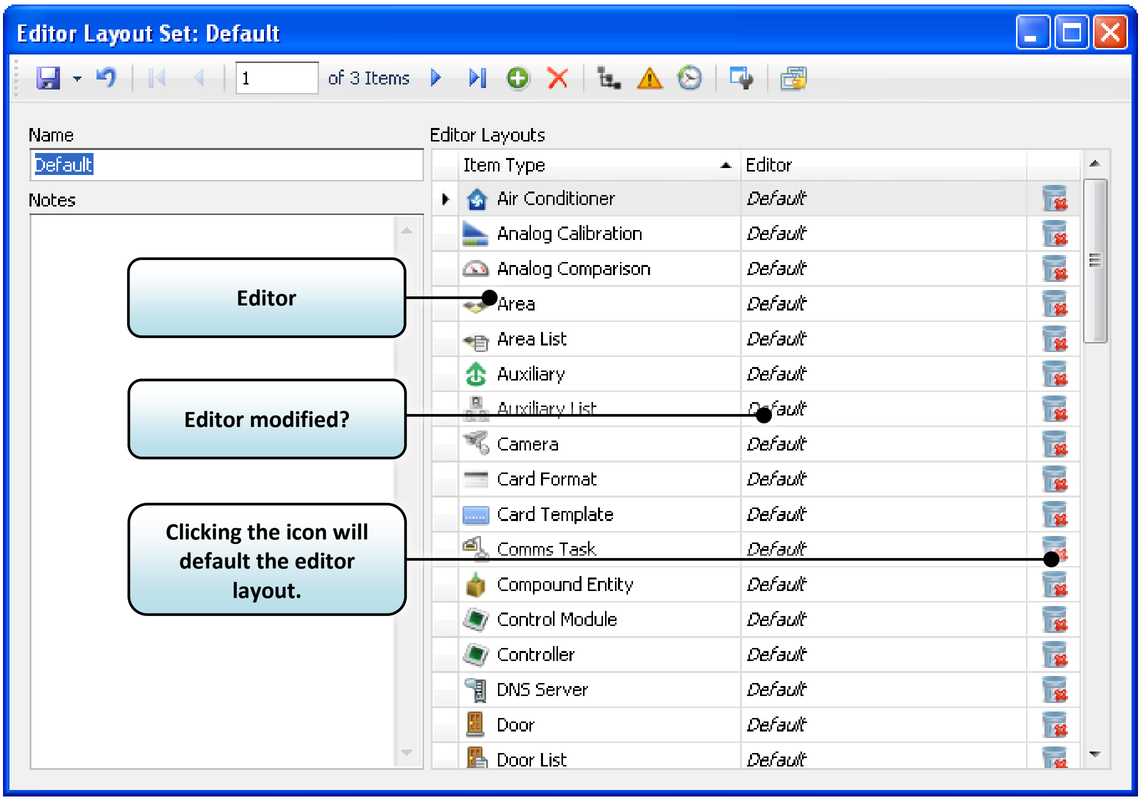
Click on the Editor Layouts button under the Window tab to open the editor layouts panel.

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 Add New to create a new one.



Editor Layout Set: Default

1 of 3 Items

Name: Default

Notes

Editor Layouts

Item Type	Editor
Air Conditioner	*Default*
Analog Calibration	*Default*
Analog Comparison	*Default*
Area	*Default*
Area List	*Default*
Auxiliary	*Default*
Auxiliary List	*Default*
Camera	*Default*
Card Format	*Default*
Card Template	*Default*
Comms Task	*Default*
Compound Entity	*Default*
Control Module	*Default*
Controller	*Default*
DNS Server	*Default*
Door	*Default*
Door List	*Default*

Editor

Editor modified?

Clicking the icon will default the editor layout.

Figure 18

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.

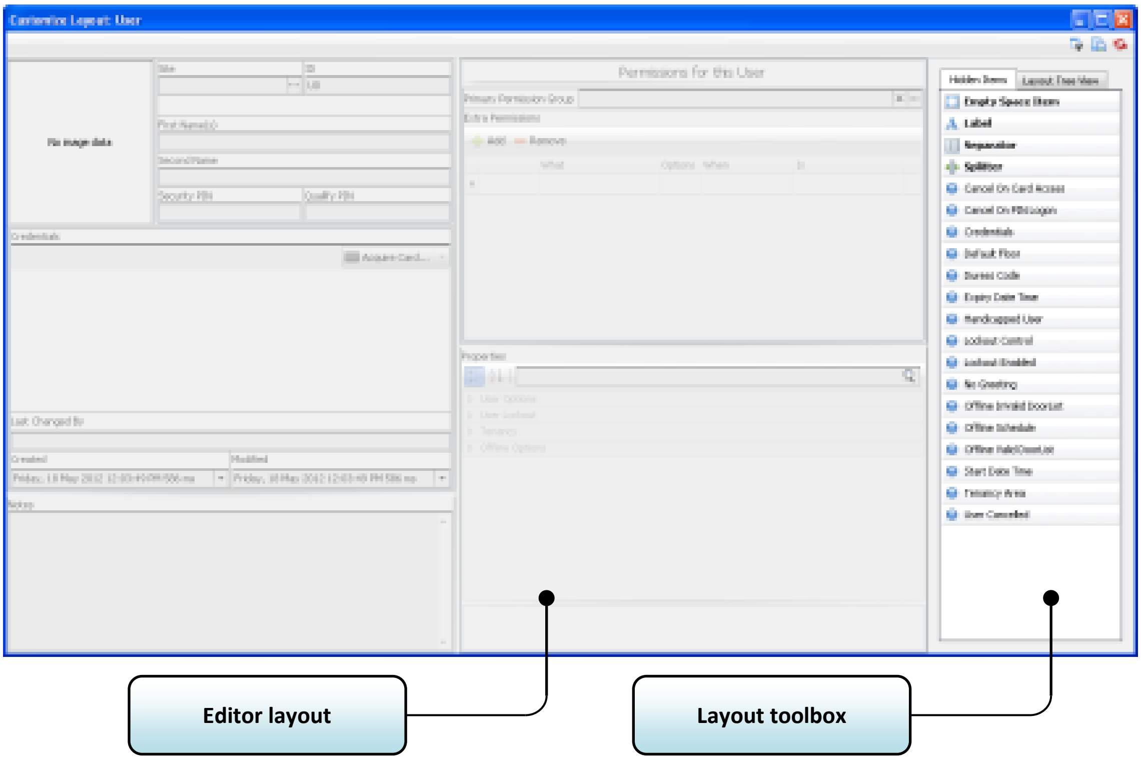


Figure 19

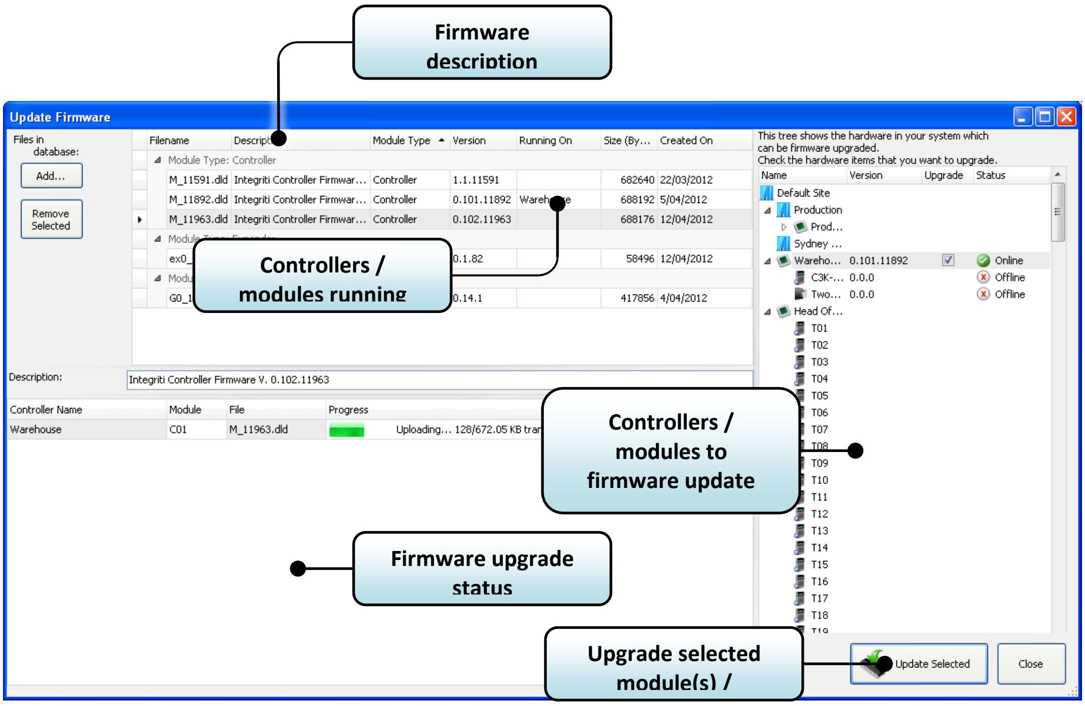
Please refer to the document titled ‘Interface Elements for Integriti’ for more information on how to use the layout manager.

	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)

Maintaining Firmware

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

Click Firmware Update to open the update manager (*Figure 20*).



Files in database:

	Filename	Description	Module Type	Version	Running On	Size (By...	Created On
	Module Type: Controller						
	M_11591.dld	Integriti Controller Firmwar...	Controller	1.1.11591		682640	22/03/2012
	M_11892.dld	Integriti Controller Firmwar...	Controller	0.101.11892	Warehouse	688192	5/04/2012
▸	M_11963.dld	Integriti Controller Firmwar...	Controller	0.102.11963		688176	12/04/2012
	Modul						
	ex0_			0.1.82		58496	12/04/2012
	Modu						
	G0_1			0.14.1		417856	4/04/2012

Description: Integriti Controller Firmware V. 0.102.11963

Controller Name	Module	File	Progress
Warehouse	C01	M_11963.dld	🟩 Uploading... 128/672.05 KB tran

This tree shows the hardware in your system which can be firmware upgraded.
Check the hardware items that you want to upgrade.

Name	Version	Upgrade	Status
Default Site			
Production			
Prod...			
Sydney ...			
Wareho...	0.101.11892	☑	Online
C3K-...	0.0.0		Offline
Two...	0.0.0		Offline
Head Of...			
T01			
T02			
T03			
T04			
T05			
T06			
T07			
T08			
T09			
T10			
T11			
T12			
T13			
T14			
T15			
T16			
T17			
T18			
T19			

Figure 20

The available firmware list 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 a description in the box underneath the firmware list.

If the selected firmware is running on a module it will be displayed in the "Running On" list.

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

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.

Upgrading module(s)/controller(s) firmware

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

.

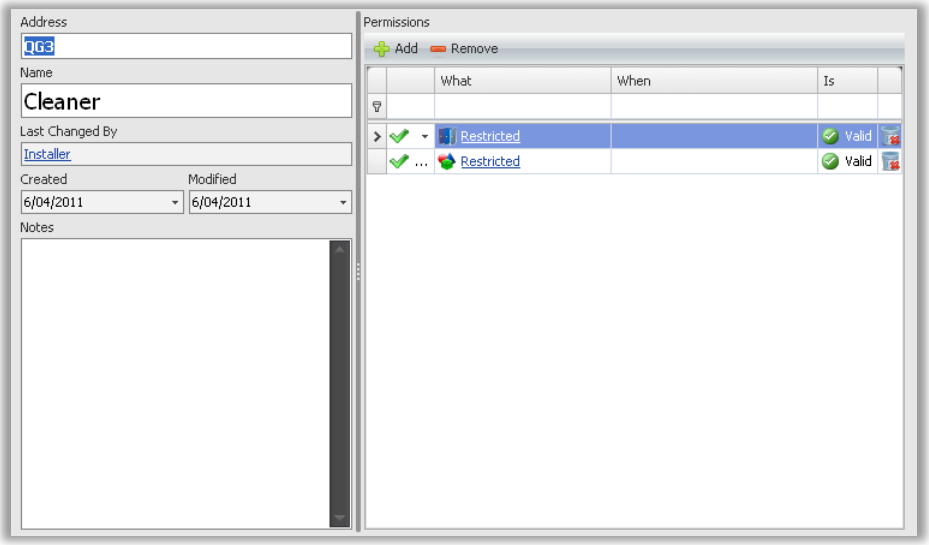
The time it takes to upgrade the firmware of a particular module or controller will vary depending on connectivity to the Integriti server. Please allow up to 30 minutes for the upgrade process to complete.

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

Programming Guide

The purpose of this programming guide is to step you through common programming scenarios. For terminal specific programming detail please refer to the "Integriti Control Module Installation Manual".

Permission Groups



Address: QG3

Name: Cleaner

Last Changed By: Installer

Created: 6/04/2011

Modified: 6/04/2011

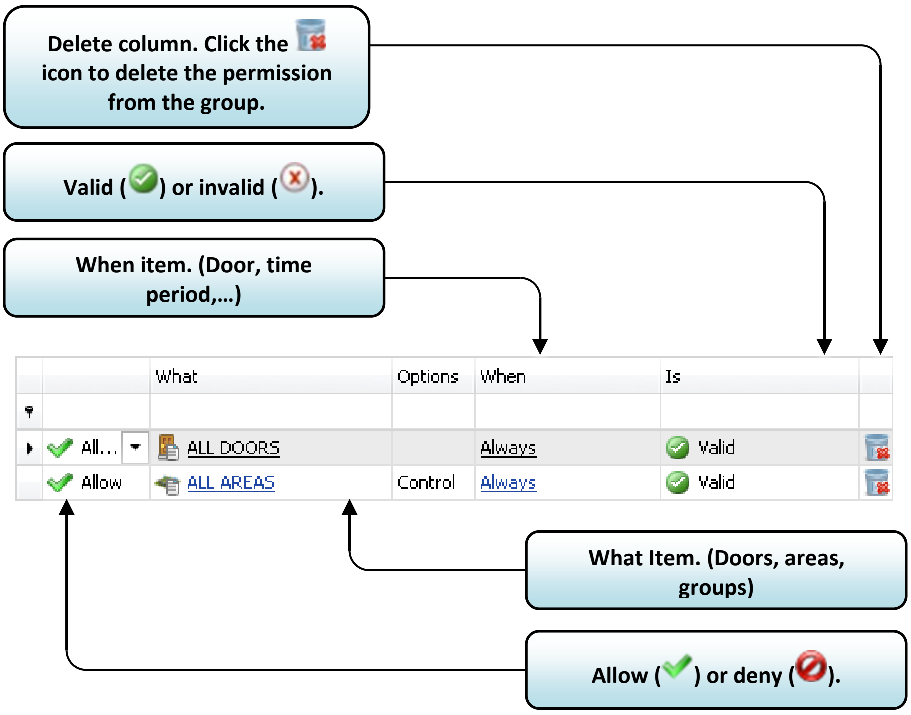
Notes

Permissions

What	When	Is
Restricted		Valid
Restricted		Valid

The Permission Group dialog

System wide permission groups now exist to make user programming easier. A permission group can contain a list of areas, area lists, doors, door lists, menu groups and permission groups from all of the accessible controllers within Integriti.



Delete column. Click the icon to delete the permission from the group.

Valid (✓) or invalid (✗).

When item. (Door, time period,…)

		What	Options	When	Is	
▸	✓ All… ▾	ALL DOORS		Always	✓ Valid	
	✓ Allow	ALL AREAS	Control	Always	✓ Valid	

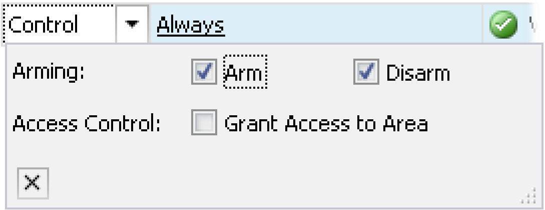
What Item. (Doors, areas, groups)

Allow (✓) or deny (⊘).

Two permissions within a permission group

To create a permission group, use the following procedure:

1. Click on the Home tab followed by the Permission Groups button.
2. Click the Add New icon in the permission groups Panel.
3. The permission group programming dialog should appear.
4. Give the permission group a name and add any necessary details in the notes field.
5. Click the Add button to add a new permission to the group.
6. Select the desired door, door list, area, area list or group and click the ✓ OK button.
7. 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,…
9. Depending on the entity selected in the "What" column, the "Options" column may have a drop-down selection available. ***Figure 21*** is an example of the area control options.



Control ▾ Always ✓

Arming: ☑ Arm ☑ Disarm

Access Control: □ Grant Access to Area

☒

Figure 21

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 needs to be valid or invalid.
12. The last column is a button to allow you to remove the individual permission.
13. Click the 💾 button and close the dialog.

Credentials

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.

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 a controller.

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. Users use these PIN codes 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.

Creating a new user:

1. Click on the Home tab followed by the Users button.
2. Click the Add New icon in the Users Panel.
3. The User Programming dialog should appear.
4. Give the User a First Name, Last Name and add any necessary details in the Notes field.
5. Users have two PIN codes. The Qualify PIN is used for access control purposes where a Card & PIN qualification is required. This number can be duplicated across the system.
   The purpose of the Security PIN is to log in to the terminal.

Primary Permission Group

6. Click ... and select the primary permission group for the user.

Extra Permissions

7. Click Add and select one or many items from the item selection dialog.

Properties

User Options

Property	Description
Cancel On Card Access	Tick this to automatically cancel the user the next time an access control event occurs (such as opening a door).
Cancel On PIN Logon	Tick this to automatically cancel the user on their next PIN access.
Handicapped User	Tick this to set the users access times to the Handicapped Unlocked time specified for each door.
Duress Code	This user will be treated as a duress user. If this user does anything on the system (arm / disarm / open a door…) a configurable duress action can be triggered.
User Cancelled	This user has been cancelled. This user will no longer function but will generate events if they attempt to do anything on the system.
No Greeting	Greetings will not be displayed when a user logs on to a terminal.

User Lockout

Property	Description
`Lockout Enabled`	This user is locked out when the Control Module option 'Enable Lockout' is set.
`Lockout Control`	This user can allow locked out users permission to logon with a pin entry

Tenancy

Property	Description
`Tenancy Area`	Area to be optionally armed/disarmed on door access and reader arming.

Offline Options

Property	Description
`Offline Valid DoorList`	Doorlist to be used for this user when access module offline and Offline Schedule is valid.
`Offline InValid DoorList`	Doorlist to be used for this user when access module offline and Offline Schedule is invalid.
`Offline Schedule`	Schedule to control Offline doorlists when access module offline.

8. Click the 💾 button and close the dialog.

Credentials

Users can have multiple credentials associated with them. A credential can be one of a number of things including but not limited to a swipe card, proximity card or wireless fob.

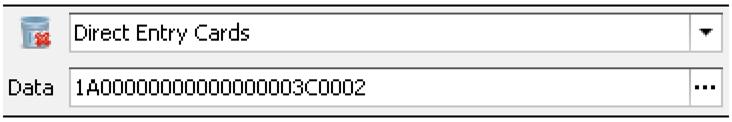
To add a new credential to a user:

- Click on the [Acquire Card… ▾] button to select a card for the user from a reader/wireless receiver on site.

– or –

- Click on the [Acquire Card… ▾] dropdown button to select [Acquire Card…], [Access Card] or [Wireless Fob].

  Clicking the 'Access Card' button will add a new credential record to the user:



Direct Entry Cards ▾

Data 1A00000000000000003C0002 …

Removing a credential from a user is as simple as clicking on the 🗑 button to the left of the credential. Click the 💾 ▾ button to commit these changes.

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:

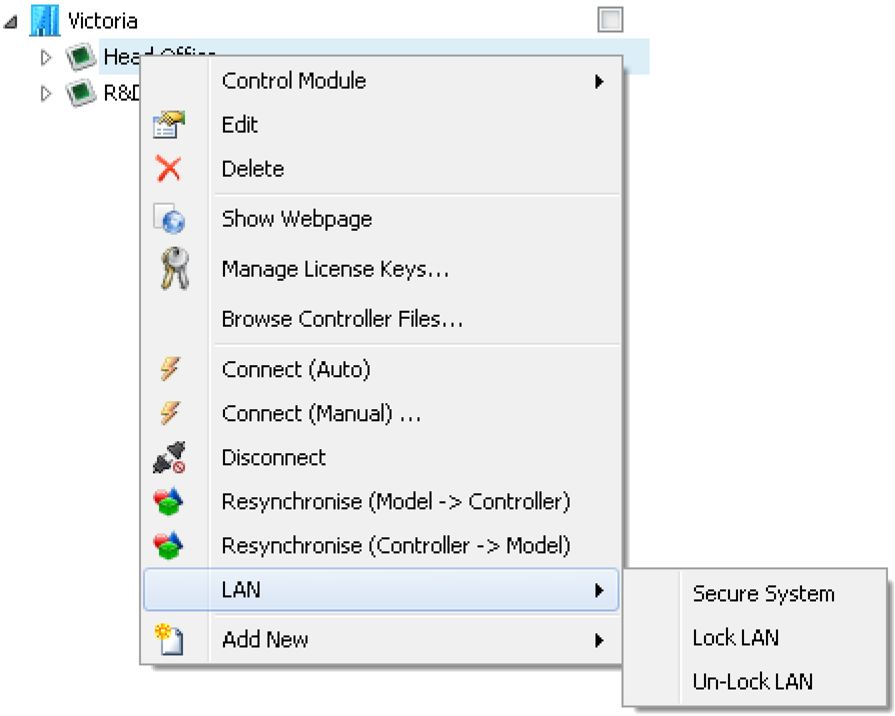


Figure 22

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 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.

Un-Lock LAN

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

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.

Removing Modules

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

Intrusion Programming

Inputs

To configure an input:

1. Click on the Home, Intruder, Automation or Hardware tab followed by the Inputs button.
2. Click the Add New icon in the input Panel.
3. Give the input a Name and add any necessary details in the Notes field.

Inputs on the Integriti system can be one of the following types. The type selected for the input will determine its characteristics - multi-state, analogue or counting:

- Normal
- Analogue
- Count up
- Count down
- Previous Input Count Up
- Previous Input Count Down

Alarm Action

This optional field allows for the configuration of an action that will occur at the time the input is considered as being in an alarm state.

Options

Property	Description
`Summary Zone`	This zone will include in the overall system input summary.
`Ignore Physical Input`	Ignore the physical state of the input so as the state of this input can be manipulated by automation functions such as Actions.
`Swap Alarm and Seal`	The Seal and Alarm conditions of this input will be reversed. This allows the convenient use of normally open devices.
`No test on exit`	The system will not check that this zone is sealed when arming an area to which it is assigned.
`Auto-Isolate on exit`	Auto-isolate will be allowed on the input if the input is unsealed when an Area to which it is assigned is being turned On.
`Zone Self Test Enabled`	Zone self-testing will be performed on this input.
`No Review`	Activity on this input will not be saved to review.
`Isolate All Only`	Only a user with the "Isolate All" permission can isolate this input.

Reporting

Property	Description
`SIA Type`	Sets the SIA reporting type that will be used for reports from this input.
`Contact ID Message`	Sets the Contact ID Point ID that will be used for reports from this input.

Analog & Counting

Property	Description	Usage
Calibration ID	Digital-analog calibration parameters	
Units for Analogue Input	Units that the analogue value of this input, if applicable, is calibrated in.	• Signed Integer • Unsigned Integer • Milli Kelvin • Mill volts • Watt-Hours • Percent • Decikelvin
Analog / Count Log Frequency	Frequency with which to write Analog / Count values to review (1 second increments)	h:mm:ss
Analog Hysteresis	Sensitivity to changes in analog values to initiate transmission	

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.

Process groups are found under the Intruder and System tab.

Click on the Process Groups button to display the process groups panel.

States to Process – States for this PG

Select input one or many states that will be processed by this Process Group.

Processing

Property	Description
Entry Zone	Inputs assigned to this process group will have entry delay on selected states.
Exit Zone	Inputs assigned to this process group will have exit delay on selected states.
Primary Zone	Inputs assigned to this process group can start an entry timer.
Pulse Zone	Inputs assigned to this process group will use the pulse count logic.
One Pulse	Inputs assigned to this process group will can only accumulate one pulse per input.
No 24 Hour if Armed	Inputs assigned to this process group will not process 24hr states if area is armed.
Process 24 Hour	Inputs assigned to this process group will process 'alarm' states as 24hr states.

Areas

To view programmed areas, click on the Intruder tab followed by the Areas button.

Click the Add New icon in the areas Panel to create a new area. Give the new Area a name and add any necessary details in the notes field.

Adding inputs to an area.

1. Open up an area for programming (or create a new area).
2. Click on the Inputs tab followed by Add.
3. Select one or many inputs followed by OK.

Properties

Reporting

Property	Description
Report Openings	Report Openings for this area.
Report Closings	Report Closings for this area.
Close At Exit Start	Report the closing event to the monitoring station at the beginning of the exit delay (instead of the end).
Report Openings After Alarm	Only Report Openings for this area if an alarm report has occurred since closing.
Report 24 Hour Open Close	Report Openings or Closings if the 24hr part of area in armed or disarmed.
Exclude from General Open / Close	Do not include this area as part of a general area open close.
Client Code (Hex)	Enter the client code for this area in hex as an alternative to the CT client code.
Client Code (Dec)	Enter the client code for this area in decimal as an alternative to the CT client code.

Entry / Exit

Property	Description
Entry Delay	The length of the entry delay
Exit Delay	The length of the exit delay

Process Alarm Actions

Property	Description
Process Action 1	If checked in the process group this action will assert if an alarm occurs in the area, and disassert when the area turns off
Process Action 2	If checked in the process group this action will assert if an alarm occurs in the area, and disassert when the area turns off
Process Action 3	If checked in the process group this action will assert if an alarm occurs in the area, and disassert when the area turns off
Process Action 4	If checked in the process group this action will assert if an alarm occurs in the area, and disassert when the area turns off
Process Action 5	If checked in the process group this action will assert if an alarm occurs in the area, and disassert when the area turns off
Process Action 6	If checked in the process group this action will assert if an alarm occurs in the area, and disassert when the area turns off
Process Action 7	If checked in the process group this action will assert if an alarm occurs in the area, and disassert when the area turns off
Process Action 8	If checked in the process group this action will assert if an alarm occurs in the area, and disassert when the area turns off

Sirens

Property	Description
Siren Modules	Sirens on these modules will be sounded on relevant alarms in this Area
Siren Time	Siren on time in h:mm:ss
Holdoff Time	Time to delay siren in h:mm:ss
Siren Pulse Mode	

Internal Siren	No Siren, Instant Siren, Siren on 2nd hit or Siren on backup.
External Siren	
Maximum Siren Triggers	A number. Total number of activations per arm cycle.
Siren Action	The action the system will invoke when zone self-test begins

User Counting

Property	Description
Count Action	The action the system will invoke when the Area Count is reached
Trigger Count Hi	Assert Count Action if reach or go above this value
Trigger Count Lo	DeAssert Count Action if reach or go below this value

Actions

Configurable actions for areas are Close, Entry, Exit, Zone Test, Warning, Isolate and Unseal. Please refer to the section titled actions for information on programming.

General

Property	Description
Test for Users when arming	Warn if any users are considered to still be in areas that are about to be armed.
Sub Area	Sub area for this area that will be armed/disarmed along with this area.
Defer Area	This area can be defer armed by the appropiate user.
Defer Time	Time that area will remain off after being deferred armed.
Max Pulse Count	Maximum pulse count for pulse count style inputs.
Pulse Time	Maximum time that pulse counts are accumulated before pulse count is reset.
Test Time	Maximum time that area can be walktested for.
Arm Self Test	Number of times an area is armed before Zone Self Test is

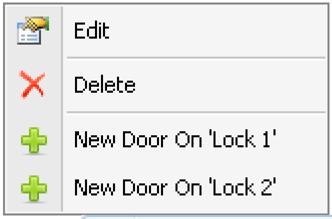
Count	initiated. When left at 0, no zone self test this area.
Re Arm Time	After this time of input inactivity the area will re-arm When left at 0, the area will never re-arm automatically
Re-Arm Qualifier	This entity must be valid for area rearm to occur.
Invert Re-Arm Qualifier	
Battery test on area arm	A short battery test will occur on all batteries in the system as area is armed.

Door Programming

Basic Door Programming

Basic door programming consists of a Door, a Reader Module and an Auxiliary. This procedure will step you through the creation of a door.

1. If required, add a new reader module to your Integriti LAN.
2. Right-click the reader module that the door is to be associated with.



3. Select New Door On 'Lock 1' to create a new door entry.

Time Periods

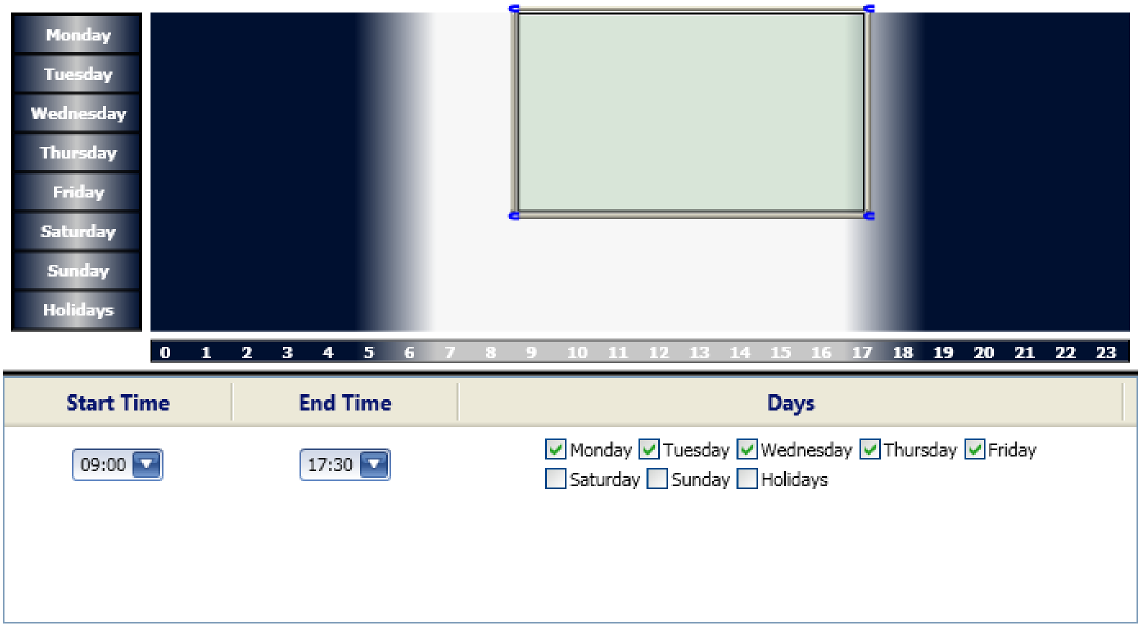
Time periods are most commonly used as the "when" in permissions, but can also be used in named actions.

Time periods are created by clicking and dragging schedule periods on the schedule pane or by manually adding a schedule period by clicking the Add Schedule Period 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. Click on the Home or System tab followed by the Time Periods button.
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 and drag a region (a schedule period) on the schedule pane as many times as required to create the desired time period.
   – or –
   Click the Add Schedule Period button and change the parameters of the newly created schedule period.
5. Click on the Holidays tab followed by Add to add holidays to the Time Period.
6. Click the 💾 button and close the dialog.



Start Time	End Time	Days
09:00	17:30	☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☐ Saturday ☐ Sunday ☐ Holidays

Schedules

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. Click on the Home or System tab followed by the Schedules button.
2. Click the Add New button in the schedules panel.
3. Give the Schedule a Name and add any necessary details in the Notes field.
4. If GMT time is used, tick the GMT 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.

Holidays

To create a new Holiday:

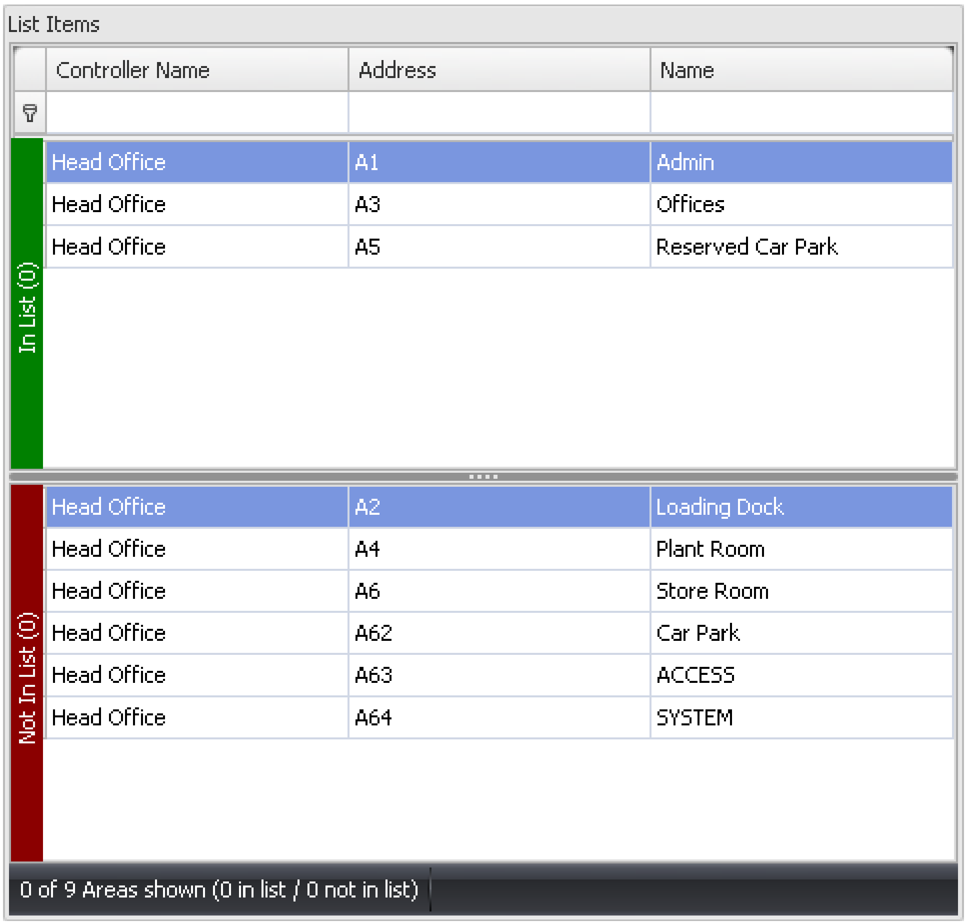
1. Click on the Home or System tab followed by the Holidays button.
2. Click the Add New button in the holidays Panel.
3. Give the Holiday a Name and add any necessary details in the Notes field.
4. Change the start time and date to that of the holiday.
5. Change the end time and date to that of the 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 GMT time is used, tick the GMT check box.
8. Click the 💾 button and close the dialog.

Area Lists & Door Lists

Area / Door lists are a simple collection of areas / doors. These lists can be used in place of associating individual areas or doors to individual users.

To create an area or door list:

1. Click on the Home tab followed by Area Lists or Door Lists.
2. Click the Add New button in the Area lists / Door lists panel.
3. The list properties window will appear with the usual basic options on the left side. Fill in the Name and Notes as necessary.
4. The right-hand side of the window is divided in two sections. The top (green) section contains a list of all of the items associated with this Door / Area list. Double-click items in the upper or lower sections to move them in or out of the list:



List Items

In List (0)

Controller Name	Address	Name
Head Office	A1	Admin
Head Office	A3	Offices
Head Office	A5	Reserved Car Park

Not In List (0)

Controller Name	Address	Name
Head Office	A2	Loading Dock
Head Office	A4	Plant Room
Head Office	A6	Store Room
Head Office	A62	Car Park
Head Office	A63	ACCESS
Head Office	A64	SYSTEM

0 of 9 Areas shown (0 in list / 0 not in list)

5. Click the 💾 button and close the window.

Menu Group

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

To create a Menu Group:

1. Click on the Intruder or Access Control tab followed by Menu Groups.
2. Click the Add New button in the Menu Group panel.
3. The properties window will appear with the usual basic options on the left side.
4. Fill in the configurable menu group properties:

Property	Description
Area	Allows access to arm and / or disarm areas.
Info	Allows access to the controller review and other panel information such as firmware revision and the currently configured IP address.
Access	Allows access to user programming.
Isolate	Allows access to isolate (and sticky isolate) inputs.
Testing	Allows access to walk testing.
Time	Allows access to configure the time and date of the controller. Additionally, you can configure time periods, schedules, holidays and custom LCD messages.
Misc	Allows access to United Kingdom programming.
Installer	Allows access to the installer programming menus.
Service	Allows access to the service menus.
Control	Allows access to control various items such as Doors, Lifts and PActions. Additionally this menu will allows access to adjust counters and user counts.
Lists	Allows access to configure lists.
Groups	Allows access to configure groups.

`Edit Input Count`	Allows access to adjust input counters.
`Edit User Count`	Allows access to adjust user counters.
`RF Remote`	Allows access to the RF Remotes menu. **[Menu], [2], [7]**.
`Full Test Suite Allowed`	Allows access to all of the testing menu items (inputs, auxiliaries, sirens, batteries, etc…).

Sub Menu Items

Provided there are no restrictions on the terminal itself, the following sub menu items are accessible if enabled.

Property	Description
`User Codes`	Allows access to modify user codes.
`User Groups`	Allows access to modify user groups.
`Review`	Allows access to the controller review history.
`Date / Time`	Allows access to modify the current controller time and date.
`Time Periods`	Allows access to modify time periods.
`Schedules`	Allows access to modify the schedules.
`Holidays`	Allows access to modify the holidays.
`LCD Messages`	Allows access to modify the custom LCD messages.
`Card Formats`	Allows access to modify the controllers supported card formats.
`Card Templates`	Allows access to modify the card templates.

Area Control Permissions

Provided there are no restrictions on the terminal itself, the following sub menu items are accessible if enabled.

Property	Description
Initiate Defer	A user with this MG will initiate a deferred area off if turning off a deferred area.
Isolate On Exit	User allowed to isolate unsealed inputs during exit delay.
24 Hour Off	User allowed to turn off 24hr part of an area.
Default List	User will jump to area list control on terminal logon.
Isolate All	User allowed to isolate any input.
Sticky Isolate	User allowed to sticky isolate an input.

Access Control

Provided there are no restrictions on the terminal itself, the following sub menu items are accessible if enabled.

Property	Description
Outside Area Off on Egress	Outside Area will turn off on a door egress.
User Area Off on Egress	User Tenancy Area will turn off on door egress.
Inside Area Off on Ingress	Inside Area will turn off on a door ingress.
User Area Off on Ingress	User Tenancy Area will turn off on a door ingress.
Dual User Provider	This user can provide a credential to validate another user.
Dual User Override	This user can override the need for a 2nd user to validate.
Anti-Passback Override	This user can override an antipassback violation.
Dual Credential Override	This user can override the need for a 2nd credential.

Advanced Options - Action Groups

The user will be permitted to control all of the actions contained within the selected Permitted Action Group.

Optional Action grouping as to what action groups can be controlled by this user.

Remote Access Permissions

Property	Description
`Arm Area`	A user with this operator group will be able to arm areas permitted to this user remotely.
`Disarm Area`	A user with this operator group will be able to disarm areas permitted to this user remotely.
`Arm 24 Hour`	A user with this operator group will be able to arm 24 hour areas permitted to this user remotely.
`Disarm 24 Hour`	A user with this operator group will be able to disarm 24 hour areas permitted to this user remotely.
`Isolate`	A user with this operator group will be able to isolate inputs permitted to this user remotely.
`Control Aux`	A user with this operator group will be able to control auxiliaries permitted to this user remotely.
`Lock Door`	A user with this operator group will be able to lock doors permitted to this user remotely.
`Unlock Door`	A user with this operator group will be able to unlock doors permitted to this user remotely.
`Siren`	A user with this operator group will be able to control sirens permitted to this user remotely.
`CommsTask Control`	A user with this operator group will be able to control communication tasks permitted to this user remotely.
`Adjust Count`	A user with this operator group will be able to adjust count values remotely.

Review

Property	Description
`Review Level`	This sets the level of verbosity for inspecting review.
`Review Classification`	This further filters displayed review based on type of review event.

Message Acknowledge

Property	Description
`Ack Message`	This user is allowed to acknowledge messages for their 'off' areas only.
`Ack All Messages`	This user is allowed to acknowledge messages for all areas.
`Auto Siren Off`	Turn off sirens automatically on terminal logon if sirens sounding in a users 'off' area.

LCD Terminal

To open the LCD terminal panel, click on the Intruder, Access Control or Hardware tab followed by LCD Terminal.

General

Property	Description
Associated Area	Optionally select an area to be associated with this terminal.
No Keypad Beep	No beep feedback when keys pushed.
Entry Display	Show countdown for entry timer for associated area
Entry Beep	Beep during entry timer for associated area
Exit Display	Show countdown for exit timer in associated area
Exit Beep	Beep during exit timer for associated area
LED Mode	Default led operation for this terminal

Advanced Options

Action Groups 1 – 16
Optionally select which alarm categories will be displayed

Logged Off Display

Property	Description
Idle Display	Select display when terminal is logged off
Display Alarm Messages	Select whether terminal will display area alarm messages
Alarm Message Categories	Optionally select which alarm categories will be displayed
Display Status Messages	Select whether terminal will display custom LCD messages
Display LCD Messages	Select whether terminal will display area alarm messages
Display Input Levels	Select whether terminal will display input level messages
Display Single Message	Select whether terminal will display a single lcdmsg for the associated area
Display Area Arm Warning	Only accepted 'Area about to turn on' or LCD Message 1 broadcasts

Logged Off Keys

Property	Description
Up/Down Arrow Mode	Select what the up/down arrow keys will do when logged off
Allow Quick Alarm Review	Select whether quick review will work when logged off using the '1' key
Allow User Actions	Select whether user actions will work when logged off
Allow AirCon Control	Select whether AirCon Control will work when logged off
Allow Show Info	Select whether AirCon Control will work when logged off
Allow Logged off panic	Select whether panic sequence will work when logged off

Access Control

Property	Description
`Door`	Optionally select a door for access at this terminal
`Access Only`	Set this option to only allow access control at this terminal
`No Lock`	Set this option if there is no lock hardware for this door
`Tongue Sense`	Set this option to enable tongue sense logic for both doors
`Zone 2 Rex`	LCD Terminal Zone 2 functions as a REX Button
`Zone 2 Opposite Side`	LCD Terminal Zone 2 REX / REN button is on the opposite side of the door to this terminal
`Reader`	Reader programming

Security

Property	Description
`Lockout Attempts`	Select maximum invalid pin attempts at this terminal before lockout
`Lockout Time`	Select time terminal will remain locked out if lockout Attempts reached
`Attempt Timeout`	Select time after an illegal pin that lockout count will be reset

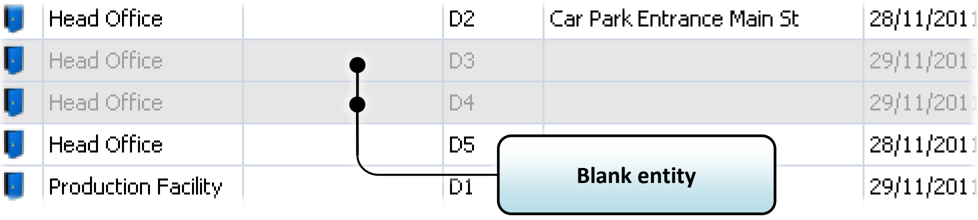
LAN Module

Property	Description
`LAN Poll Time`	
`Battery Test Time`	

Blank Entities

Blank entities are references to entities that no longer exist. Entities can become 'blank' as a result of reference changes. For instance a door record could become a blank entity record if the door was removed from the controller and the reader module still has a reference to it.

Usually this will only occur if the change was made on the controller while it was disconnected from the Integriti management software.



	Head Office		D2	Car Park Entrance Main St	28/11/201
	Head Office		D3		29/11/201
	Head Office		D4		29/11/201
	Head Office		D5		28/11/201
	Production Facility		D1		29/11/201

Figure 23

Actions

A powerful and flexible control mechanism called 'Actions' has been added to the Integriti. Actions can be triggered on a state change of a particular entity.

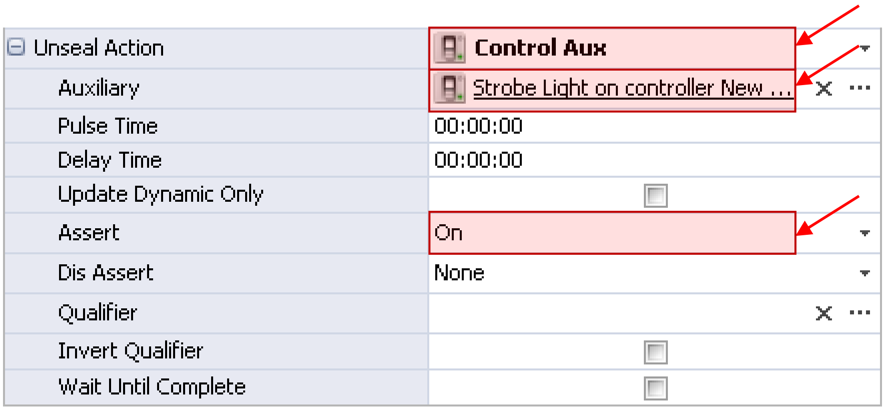
For a description of the various entities state names, please refer to the appendices.

Assert and Dis-assert have been used to indicate the state change of any particular thing within the Integriti panel. Assert examples would include things such as a door opening or an area turning on. Dis-assert examples would include things such as an input changing to a sealed state or an auxiliary turning off.

For example:

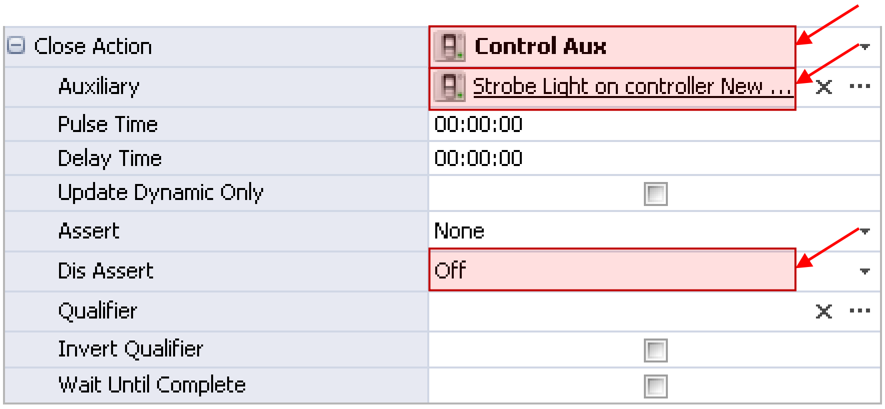
During an arm cycle you might want any input going in to alarm to turn the strobe light on. When the system is disarmed, the strobe light is to turn off.

To do this you could configure the unseal action of the area the input is associated with to turn the strobe light on (Assert) – (*Figure 24*). Additionally you would set the close action for the area disarming to turn the strobe light off (Dis-assert) – (*Figure 25*).



⊟ Unseal Action	**Control Aux**
Auxiliary	Strobe Light on controller New ...
Pulse Time	00:00:00
Delay Time	00:00:00
Update Dynamic Only	☐
Assert	On
Dis Assert	None
Qualifier	
Invert Qualifier	☐
Wait Until Complete	☐

Figure 24



⊟ Close Action	**Control Aux**
Auxiliary	Strobe Light on controller New ...
Pulse Time	00:00:00
Delay Time	00:00:00
Update Dynamic Only	☐
Assert	None
Dis Assert	Off
Qualifier	
Invert Qualifier	☐
Wait Until Complete	☐

Figure 25

Action types

There are currently 22 different types of actions available. The action selected will determine what configurable options are available.

Attributes common to all action types…

Property	Description
When Asserted… & When Disasserted…	Assert and Disassert options can be configured as none, On, Off or Toggle.
Qualifier	The action will require the qualifier to be Asserted in order for the action to operate.
Invert Qualifier	The action will require the designated qualifier to be DisAsserted in order for the action to operate.

Control Area and Control Area List

Property	Description	Usage
Area **Area List**	The Area or Area List that is to be controlled by this action.	• Select an Area • Select an Area List

Control Aux and Control Aux List

Property	Description	Usage
Auxiliary **Auxiliary List**	The Auxiliary or Auxiliary List that is to be controlled by this action.	• Select an Auxiliary • Select an Auxiliary List
On Time	On time in hours minutes and seconds.	• h:mm:ss
Off Time	Off time in hours minutes and seconds.	• h:mm:ss
Delay On	If checked, the On Time will be used as a delay on time.	
Delay Off	If checked, the Off Time will be used as a delay off time.	
Update Dynamic Only	If checked, this means change the internal state, but DO NOT actually change the real state of the output.	

Control Door and Control Door List

Property	Description	Usage
Door Door List	The Door or Door List that is to be controlled by this action.	• Select a Door • Select a Door List
Unlock Time	The time the Door / Door List is to be unlocked for. If left at 0 then the unlock time will be equal to the value configured in each door.	

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

Property	Description	Usage
Floor Floor List Lift Car Lift Car List	The Floor, Floor List, Lift Car or Lift Car List that is to be controlled by this action.	• Select a Floor • Select a Floor List • Select a Lift Car • Select a Lift Car List

Trigger Input

Property	Description	Usage
Target	The Area or Area List that is to be controlled by this action.	- Select an Area - Select an Area List
Input state	Select the state the target input should be changed to.	Select one of the following: - None - InAlarm - Masked - Oriented - Faulty - Range - TamperLow - TamperHigh - Tamper - ZstFail - LowBattery - CryptFailure - PollFailure - State12 - Soaking - SoakFailure - Isolated - Number
Update state	If this item is checked, the target input will maintain the selected input state until either another action or the physical input changes the state once more.	

Set Area User is in

Property	Description
User	The user to move to another area.
Area	The area to move the user to.
Don't update area user counts	If checked, the area user counts will not be updated in both areas.

Set Area User Count

Property	Description
`Target`	The Area / Area List to adjust the count of.
`User Count`	The new user count.

Set Input Counters

Property	Description
`Target`	The Input to adjust the count of.
`Count`	The new input count.

Control Siren

Property	Description	Usage
LAN Module	The Control Module / Expander to control.	
Time	The time the siren will be active for.	h:mm:ss
Siren Tone		Select one of the following: • None • Bell • Sweep • Fire • Evacuation • Chirp: One Pulse • Chirp: Two Pulses • Chirp: Harp • Chirp: Packman • Chirp: Gong
Sound Internal Siren	If checked, the internal siren will be affected by this action.	
Sound External Siren	If checked, the external siren will be affected by this action.	
Override Priority		

Set Timer Variable

Property	Description	Usage
`Timer`	The timer to adjust.	
`Time`		d:h:mm:ss.s

Set Variable

Property	Description	Usage
`Target`	The variable to adjust.	
`Units`	Units is used to define the unit type of the selected variable.	Select one of the following: • Signed Integer • Unsigned Integer • Milli Kelvin • Mill volts • Watt-Hours • Percent • Decikelvin
`Value`	A value defined by units (above).	

Control Air-conditioning

Property	Description	Usage
`Air Conditioner`	The air-conditioner to control.	
`Mode`		Select one of the following: • Off • Heat • Cool • Ventilate • Heat pump
`Delay Time`	The delay time between activations of the air-conditioning unit.	d:h:mm:ss
`Running Time`	The total running time of the air-conditioning unit.	d:h:mm:ss

Run Macro

Property	Description
`Target`	The macro to run.

Isolate

Property	Description
`Target`	The input to isolate.
`Sticky isolate`	If checked, the target input will remain isolated after the associated area(s) are disarmed.

Comms Task Control

Property	Description	Usage
`Target`	The communications task to control.	
`Input state`		Select one of the following: ● Normal ● Restart ● Update All

General Variables

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 on the Automation tab followed by (x) General Variables.
2. Click the Add New button in the Menu Group panel.
3. The properties window will appear with the usual basic options on the left side.
4. The only property that can be set is the optional test value.

The test value is used to determine how the general variable will return 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.

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 done through the Integriti system management software.

Macro characteristics

All macros are implicitly looped –

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

Macros can start automatically –

A macro can be configured to automatically start on panel 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.

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.

To add a new statements to macros

1. Open the macro for editing.
2. Click the Add button.

To remove a statements from macros

1. Open the macro for editing.
2. Click on the statement you want to remove followed by the Remove button.

To relocate statements within macros

1. Open the macro for editing.
2. Click the statement you want moved followed by the Move Up or Move Down button.

Running macros from the Integriti management software

1. Click in the Automation tab followed by Macros.
2. Right-click the macro in the automation the macro panel and select ‘Start’. (***Figure 26***)

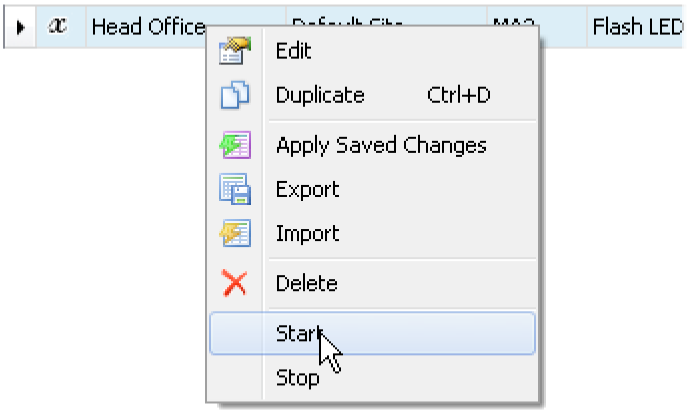


Figure 26

Running macros on controller start-up

1. Click in the Automation tab followed by Macros.
2. Double-click the macro.
3. Tick ‘Run at Controller Startup’.
4. Save (💾) the macro and close the dialog.

Creating a new macro

1. Click in the Automation tab followed by Macros.
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.
5. Save (💾) the macro and close the dialog.

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.
Do an Action if…	Perform the defined action if the condition defined is met.
Goto <label> if…	Go to a label defined elsewhere within the macro.
Pause for Time…	Suspend further execution of the macro for x time.
Define a Label	A placeholder within a macro that execution can carry over to.
Set Entity To Expression…	
Wait for Condition…	Further execution is suspended until the defined condition is met.
Execute Modified Action…	
End Current Macro	Terminates the macro.

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

“D05 && D03” = 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”

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

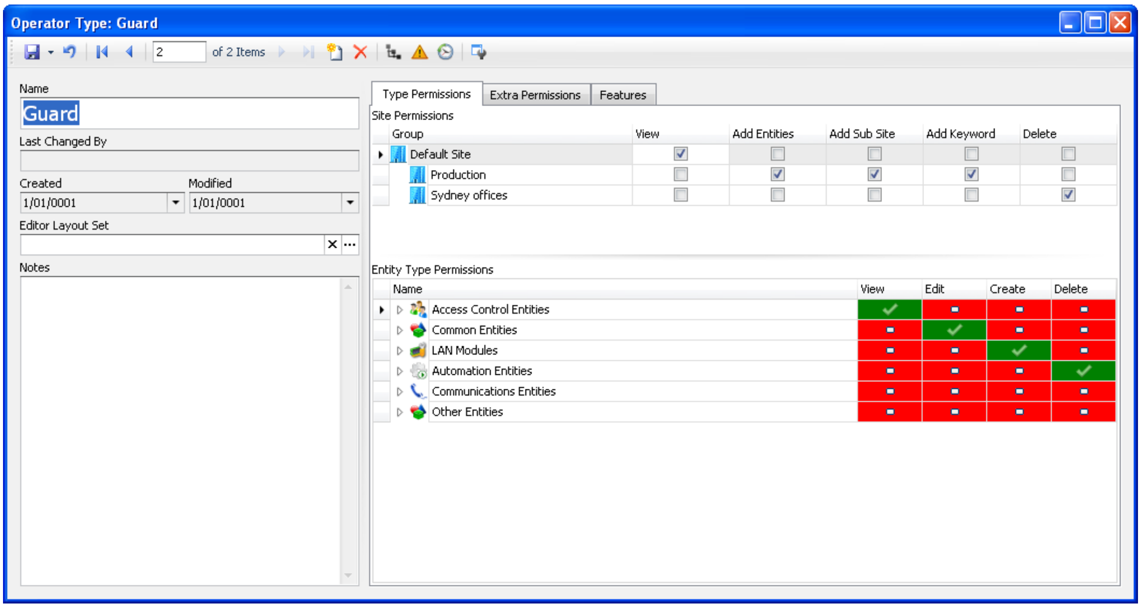
&&	Logical AND	2	Boolean	Boolean
||	Logical OR	2	Boolean	Boolean

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…

Operator Type

Integriti operator types can be configured by clicking on Operator Types under the Administration tab.



Operator Type: Guard

2 of 2 Items

Name: Guard

Last Changed By:

Created: 1/01/0001

Modified: 1/01/0001

Editor Layout Set:

Notes:

Type Permissions | Extra Permissions | Features

Site Permissions

Group	View	Add Entities	Add Sub Site	Add Keyword	Delete
Default Site	☑	□	□	□	□
Production	□	☑	☑	☑	□
Sydney offices	□	□	□	□	☑

Entity Type Permissions

Name	View	Edit	Create	Delete
Access Control Entities	✓	▬	▬	▬
Common Entities	▬	✓	▬	▬
LAN Modules	▬	▬	✓	▬
Automation Entities	▬	▬	▬	✓
Communications Entities	▬	▬	▬	▬
Other Entities	▬	▬	▬	▬

Figure 27

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.

Type Permissions

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

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 operator type can see the site.
Add Entities	Operators with this operator type can add entities to this site.
Add sub site	Operators with this operator type can create sub sites.
Add keyword	Operators can add keywords.
Delete	Operators with this permission can delete this site and / or items under it.

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.

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

Name	Arguments	
🟥□	Use the inherited permission.	**Inherited permission is Deny**
🟥✗	Override the inherited permission Deny.	
🟥✓	Override the inherited permission Allow.	
🟩□	Use the inherited permission.	**Inherited permission is Allow**
🟩✗	Override the inherited permission Deny.	
🟩✓	Override the inherited permission Allow.	

A blank / empty box indicates that the entities for this group are mixed.

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.

Administration

- Ticking the Edit Operators option allows the operator to modify existing operators.

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

Controllers

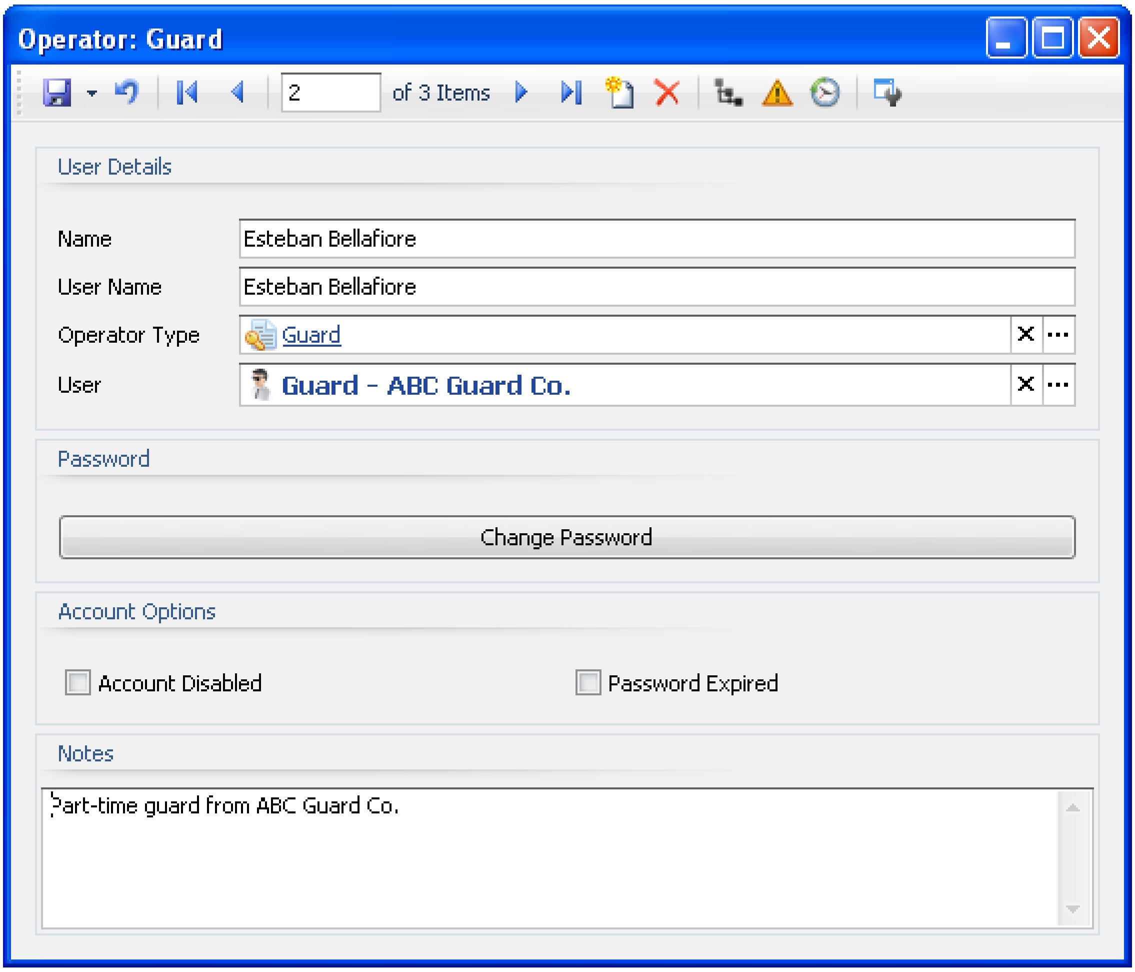
- Ticking Send Actions allows the operator access to control controller items.
- Ticking Enrol Controllers gives the operator permission to enrol additional controllers.
- Ticking Upgrade Controller Firmware gives the operator permission to upgrade controller firmware.
- Ticking View Controller Data gives the operator permission to access version / hardware information.

Layout

- Tick Modify Editor Layouts to give operators permission to modify editor layouts.
- Tick Change Dock Layouts to give operators permission to change dock layouts.

Operator

Integriti operators can be configured by clicking on Operators under the Administration tab.



Operator: Guard

User Details

Name	Esteban Bellafiore
User Name	Esteban Bellafiore
Operator Type	Guard
User	Guard - ABC Guard Co.

Password

Account Options

□ Account Disabled □ Password Expired

Notes

Part-time guard from ABC Guard Co.

Figure 28

Operators consist of a few basic details:

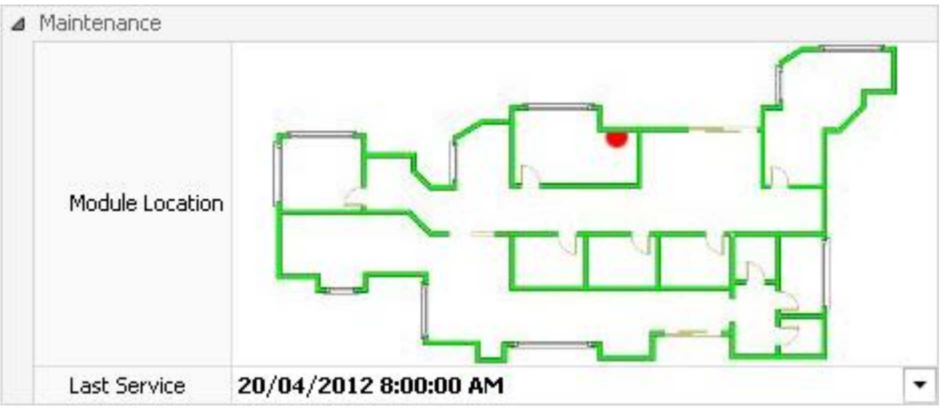
Field	Description
Name	The actual name of the operator.
User Name	The name the operator enters when logging in to the Integriti client.
Operator Type	Configuration settings and permissions given to the operator.
User	Optionally, the operator can be associated with an Integriti controller user.
Password	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.
Notes	Optional space for placing notes on the operator.

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 30*)
- Users – Credit for goods and services available at a facility. (*Figure 30*)
- Powered modules – Date & Time the last service / battery change. (*Figure 29*)
- All modules – Photo / map of physical location of modules. (*Figure 29*)
- Air conditioner – A drop down editable list of the last mechanic to service the air conditioning.



Maintenance

Module Location

Last Service 20/04/2012 8:00:00 AM

Figure 29

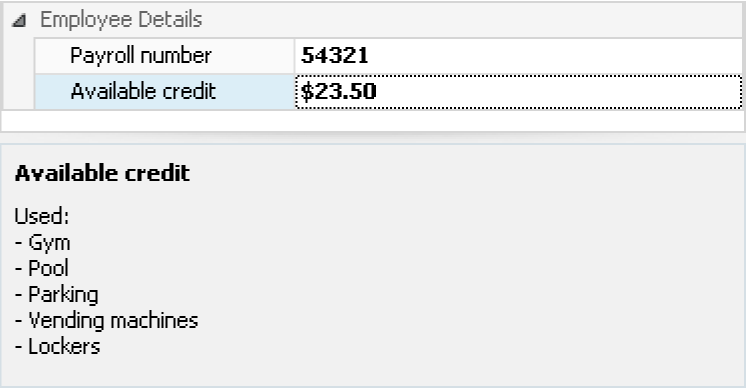
Custom fields can be configured by clicking on Custom Fields under the Administration tab.

To create a new custom field:

1. Click Add New 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 Add 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.



Employee Details

Payroll number	54321
Available credit	$23.50

Available credit

Used:
- Gym
- Pool
- Parking
- Vending machines
- Lockers

Figure 30

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.

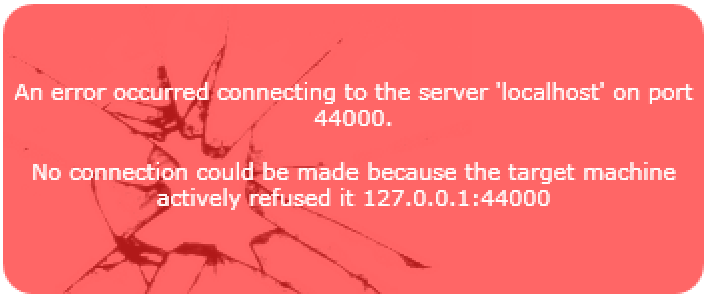
Field Type	Description
Text	A simple text field with up to 8000 characters.
Notes	A multiline text box with up to 8000 characters.
Integer	A number ranging from -2,147,483,648 to 2,147,483,647.
Decimal	A number with 15-16 decimal places ranging from -1.79769313486232E+308 to 1.79769313486232E+308.
Currency	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.

Login errors

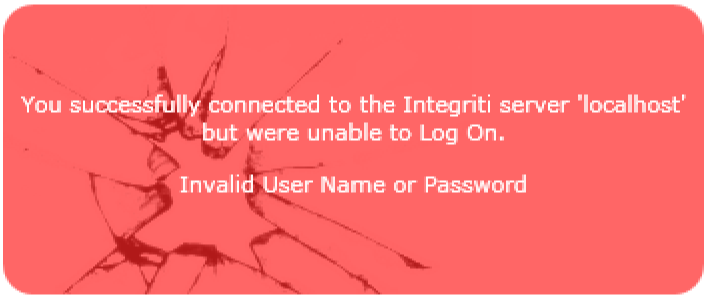
The two most common login errors are:



An error occurred connecting to the server 'localhost' on port 44000.

No connection could be made because the target machine actively refused it 127.0.0.1:44000

Ensure the Integriti Application Server service is running.



You successfully connected to the Integriti server 'localhost' but were unable to Log On.

Invalid User Name or Password

Ensure you have the correct Operator username and password.

For all other error dialogs, please contact your local support department.

Video integration

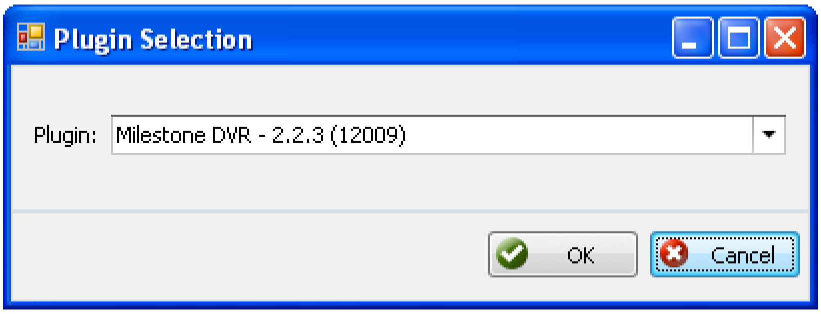
The Integriti software management suite can be used with Insight DVR plugins. Installing and using these plugins requires a slight change to the install procedure.

To install Insight Professional DVR plugins in Integriti:

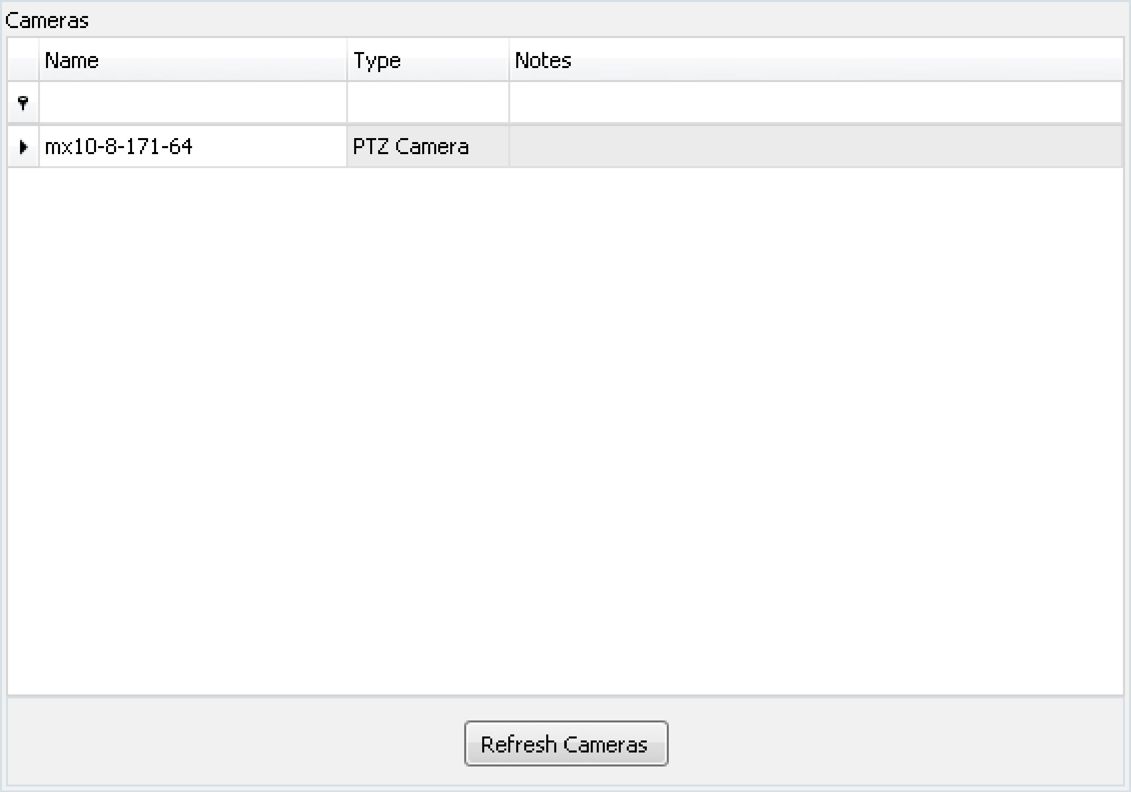
- Run the Insight DVR plugin installer and continue through until you get to the “Select Destination Location” dialog.
- Change the destination folder from the default to your Integriti installation folder.
- Complete the installation.

> *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.*

Enabling video integration within Integriti:

1. Click on the Hardware tab followed by Enrol CCTV Recorder.
2. Select the DVR plugin from the list in the new dialog that appears and click ✓ OK.
3. 

Plugin: Milestone DVR - 2.2.3 (12009)
4. 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.
5. Click ✓ Enrol CCTV Device to enrol the DVR.

6. 

Cameras

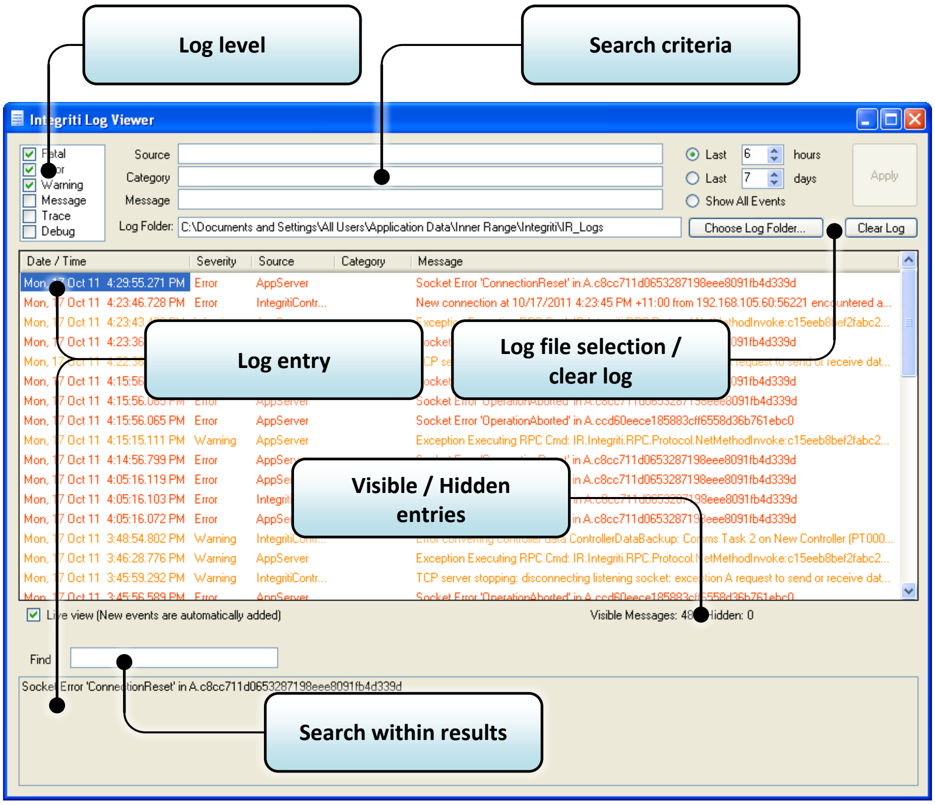
Name	Type	Notes
mx10-8-171-64	PTZ Camera	

Appendices

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



Integriti Log Viewer

☑ Fatal
☑ Error
☑ Warning
☐ Message
☐ Trace
☐ Debug

Source:
Category:
Message:
Log Folder: C:\Documents and Settings\All Users\Application Data\Inner Range\Integriti\IR_Logs

● Last 6 hours
○ Last 7 days
○ Show All Events

Date / Time	Severity	Source	Category	Message
Mon, 17 Oct 11 4:29:55.271 PM	Error	AppServer		Socket Error 'ConnectionReset' in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:23:46.728 PM	Error	IntegritiContr...		New connection at 10/17/2011 4:23:45 PM +11:00 from 192.168.105.60:56221 encountered a...
Mon, 17 Oct 11 4:23:43				Excepti… thodInvoke:c15eeb8bef2fabc2...
Mon, 17 Oct 11 4:23:36				ocket… 091fb4d339d
Mon, 17				CP se… request to send or receive dat...
Mon, 17 Oct 11 4:15:56				ocket… 091fb4d339d
Mon, 17 Oct 11 4:15:56.065 PM	Error	AppServer		Socket Error 'OperationAborted' in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:15:56.065 PM	Error	AppServer		Socket Error 'OperationAborted' in A.ccd60eece185883cff6558d36b761ebc0
Mon, 17 Oct 11 4:15:15.111 PM	Warning	AppServer		Exception Executing RPC Cmd: IR.Integriti.RPC.Protocol.NetMethodInvoke:c15eeb8bef2fabc2...
Mon, 17 Oct 11 4:14:56.799 PM	Error	AppServ		in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:05:16.119 PM	Error	AppSe		in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:05:16.103 PM	Error	Integrit		in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:05:16.072 PM	Error	AppSe		in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 3:48:54.802 PM	Warning	IntegritiContr...		Error converting controller data ControllerDataBackup: Comms Task 2 on New Controller (PT000...
Mon, 17 Oct 11 3:46:28.776 PM	Warning	AppServer		Exception Executing RPC Cmd: IR.Integriti.RPC.Protocol.NetMethodInvoke:c15eeb8bef2fabc2...
Mon, 17 Oct 11 3:45:59.292 PM	Warning	IntegritiContr...		TCP server stopping: disconnecting listening socket: exception A request to send or receive dat...
Mon, 17 Oct 11 3:45:56.589 PM	Error	AppServer		Socket Error 'OperationAborted' in A.ccd60eece185883cff6558d36b761ebc0

☑ Live view (New events are automatically added)

Visible Messages: 48 Hidden: 0

Find:

Socket Error 'ConnectionReset' in A.c8cc711d0653287198eee8091fb4d339d

Figure 31

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.

We recommend only ticking the Message, Trace and Debug options if you have been instructed to do so by the Inner Range technical support team.

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:

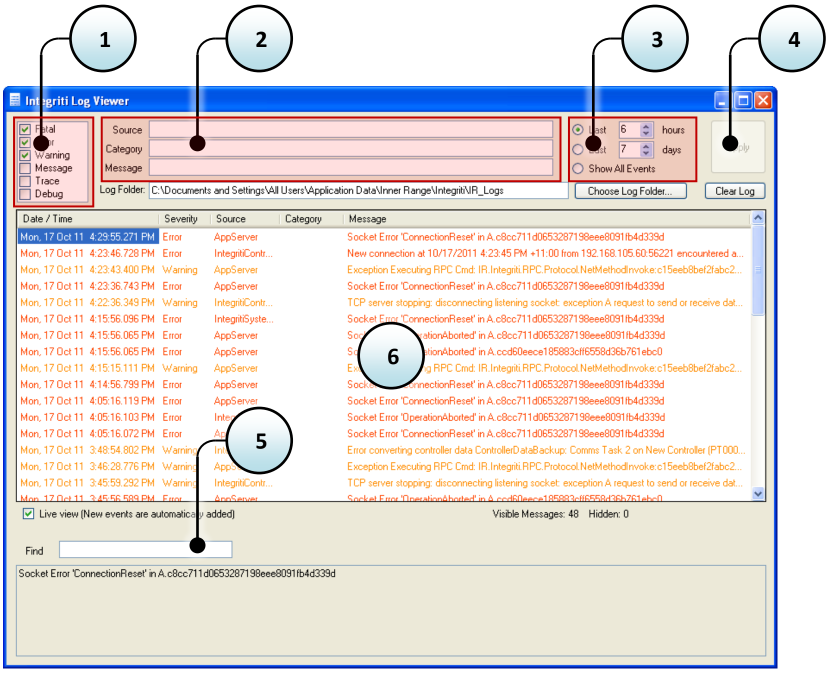
; A semicolon can be used to separate search terms (logic OR).

- 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`".



Integriti Log Viewer

☑ Fatal
☑ Error
☑ Warning
□ Message
□ Trace
□ Debug

Source
Category
Message

● Last 6 hours
○ Last 7 days
○ Show All Events

Apply

Log Folder: C:\Documents and Settings\All Users\Application Data\Inner Range\Integriti\IR_Logs

Choose Log Folder... Clear Log

Date / Time	Severity	Source	Category	Message
Mon, 17 Oct 11 4:29:55.271 PM	Error	AppServer		Socket Error 'ConnectionReset' in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:23:46.728 PM	Error	IntegritiContr...		New connection at 10/17/2011 4:23:45 PM +11:00 from 192.168.105.60:56221 encountered a...
Mon, 17 Oct 11 4:23:43.400 PM	Warning	AppServer		Exception Executing RPC Cmd: IR.Integriti.RPC.Protocol.NetMethodInvoke:c15eeb8bef2fabc2...
Mon, 17 Oct 11 4:23:36.743 PM	Error	AppServer		Socket Error 'ConnectionReset' in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:22:36.349 PM	Warning	IntegritiContr...		TCP server stopping: disconnecting listening socket: exception A request to send or receive dat...
Mon, 17 Oct 11 4:15:56.096 PM	Error	IntegritiSyste...		Socket Error 'ConnectionReset' in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:15:56.065 PM	Error	AppServer		Soc[illegible]rationAborted' in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:15:56.065 PM	Error	AppServer		So[illegible]ationAborted' in A.ccd60eece185883cff6558d36b761ebc0
Mon, 17 Oct 11 4:15:15.111 PM	Warning	AppServer		Ex[illegible]g RPC Cmd: IR.Integriti.RPC.Protocol.NetMethodInvoke:c15eeb8bef2fabc2...
Mon, 17 Oct 11 4:14:56.799 PM	Error	AppServer		Socke[illegible]onnectionReset' in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:05:16.119 PM	Error	AppServer		Socket Error 'ConnectionReset' in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:05:16.103 PM	Error	Inte[illegible]		Socket Error 'OperationAborted' in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 4:05:16.072 PM	Error	Ap[illegible]		Socket Error 'ConnectionReset' in A.c8cc711d0653287198eee8091fb4d339d
Mon, 17 Oct 11 3:48:54.802 PM	Warning	Int[illegible]		Error converting controller data ControllerDataBackup: Comms Task 2 on New Controller (PT000...
Mon, 17 Oct 11 3:46:28.776 PM	Warning	AppS[illegible]		Exception Executing RPC Cmd: IR.Integriti.RPC.Protocol.NetMethodInvoke:c15eeb8bef2fabc2...
Mon, 17 Oct 11 3:45:59.292 PM	Warning	IntegritiContr...		TCP server stopping: disconnecting listening socket: exception A request to send or receive dat...
Mon, 17 Oct 11 3:45:56.589 PM	Error	AppServer		Socket Error 'OperationAborted' in A.ccd60eece185883cff6558d36b761ebc0

☑ Live view (New events are automatically added)

Visible Messages: 48 Hidden: 0

Find

Socket Error 'ConnectionReset' in A.c8cc711d0653287198eee8091fb4d339d

Figure 32

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.

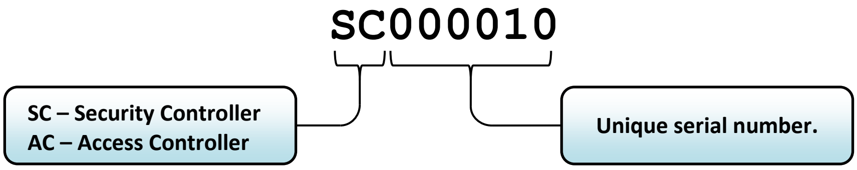
Example usage

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 32***)
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.

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:



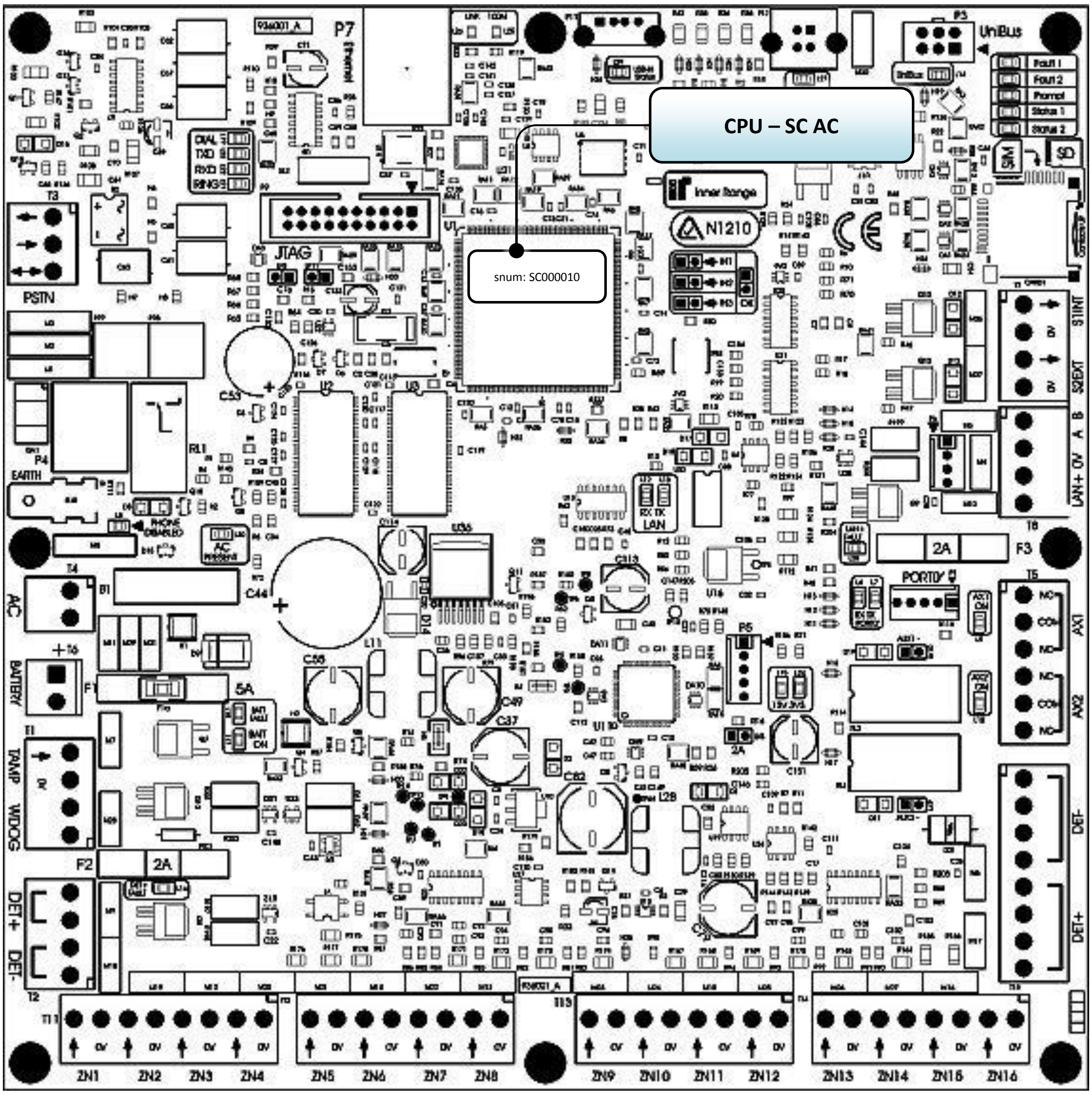


Figure 33

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.

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 & tongue & reed both 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
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*
Predefined Actions	*n/a*	Always
Pre-set text types	*n/a*	Always
Process Group	*n/a*	Always
Process ID	*n/a*	Always
Qpair 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

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

This page has been intentionally left blank