INTEGRITI
USER GUIDE

www.innerrange.com

inner range

Intelligent Security Solutions

TABLE OF CONTENTS

TABLE OF CONTENTS

INTEGRITI SOFTWARE

SOFTWARE APPLICATIONS

The Integriti software suite includes two applications:

- Integriti System Designer for system programming and configuration.

- Integriti GateKeeper for everyday control and monitoring.

INTEGRITI SYSTEM DESIGNER

Integriti System Designer is commonly used to configure and administer your site; this application contains setting and options that if changed can affect the overall functionality of the site. In most cases System Designer is used by your Installer to commission the system or to perform maintenance. Your site administrator may need access to Integriti System Designer to make programming changes.
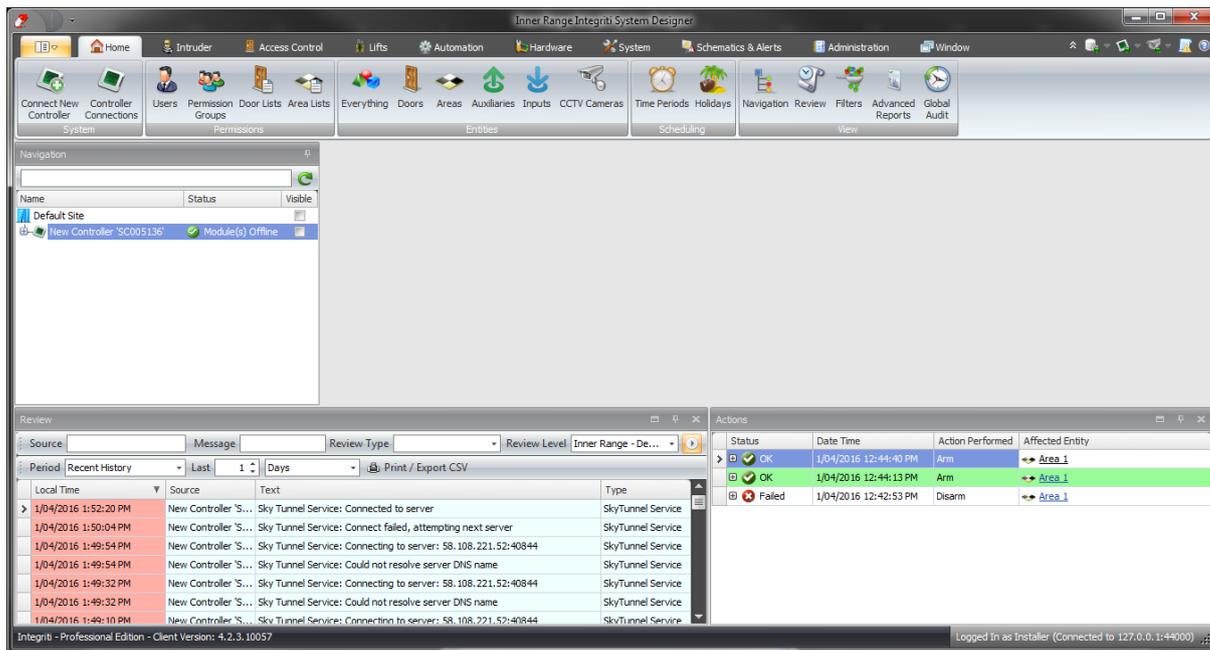
INTEGRITI GATEKEEPER

Integriti GateKeeper provides you with a simplified version of System Designer, which only shows items commonly used to monitor your site. GateKeeper does not allow you to access options that if changed would affect the overall security of the site. GateKeeper is commonly used to monitor and change the state of areas or doors and programme users.
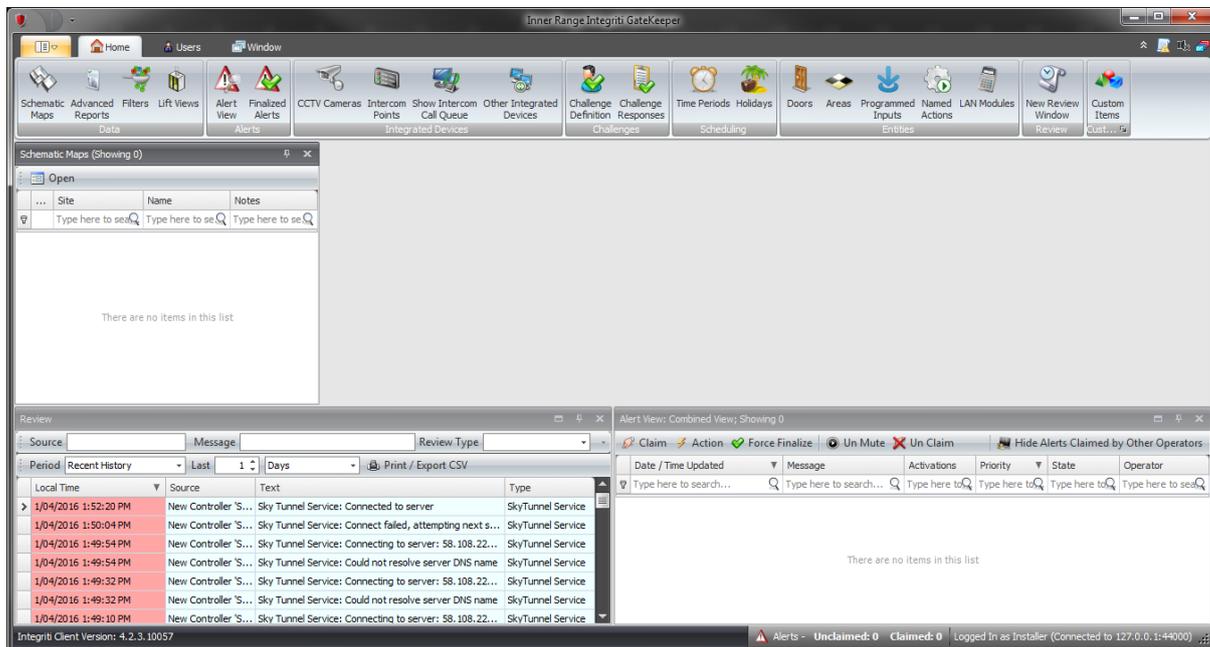
LOGIN WINDOW

To launch System Designer or GateKeeper, navigate to the **Start Menu > All Programs > Inner Range** folder and click the applications icon. Once an application is launched a login window will appear, this window is identical for System Designer and GateKeeper. To log into the application, enter your operator name and password then click the **Login** button.

The **Login** window contains the following options:

1. The **Software Version** number identifies which version of the software you have installed.

2. The default method for logging into System Designer and GateKeeper is **Use These Login Credentials.** This method allows you to login by entering your user name and password. If your software has been configured to use the **Current Windows User** option, you can login without needing to enter a user name and password. This login option is configured by your installer and requires additional licenses.

3. Enter your **User Name** in this field.

4. Enter your **Password** in this field.

5. Do not change the **Integriti Server** settings unless instructed to do so by your Installer.

6. The **Server Icons** show the status of the servers that are required for the software to operate.

INTEGRITI SERVERS

The Integriti servers are required for System Designer and GateKeeper to run, connect to controllers and CCTV systems.

Before you login to System Designer or GateKeeper make sure the Integriti servers are started, this is indicated by a green dot. If they have not started, right-click the **Servers Icon** and click **Start**.

If the integriti servers are not visible you may be on a client workstation or the application was not launched with administrator privileges.

The table below shows all the possible states for the Integriti servers.

	Stopped	Stopping	Starting	Started
Integriti Application Server				
Integriti Controller Server				
Integriti Integration Server				

SOFTWARE NAVIGATION

USER INTERFACE

The default layout for System Designer and GateKeeper share common elements. Below is a breakdown of the System Designer interface.

Quick Access Tool-bar   **Ribbon**   **Workspace**

Review Panel   **Navigation Panel**   **Actions Panel**

RIBBON

The Ribbon is designed to help you quickly find the items you need to programme or monitor the system. Items are organized into logical groups, which are collected under tabs. Each tab relates to a type of function, such as Intruder or Access Control tabs.

Tabs

The tabs arrange all the items by category. The **Home Tab** has the most commonly used items.

Groups

Each tab is divided into smaller groups based on their function

Icons

Each icon relates to a specific system item that can be programmed or monitored.

Quick Access Toolbar

The Quick Access Toolbar provides a location that you can save commonly used items so that they can be opened without navigating through the ribbon. Right-click on any icon and select the **Add to Quick Access Toolbar** option to display the item in the Quick Access Toolbar.

REVIEW PANEL

The **Review** panel is located at the bottom left of the Integriti System Designer window by default. Review is a historical log of the events that have occurred on the security controller or within the software.
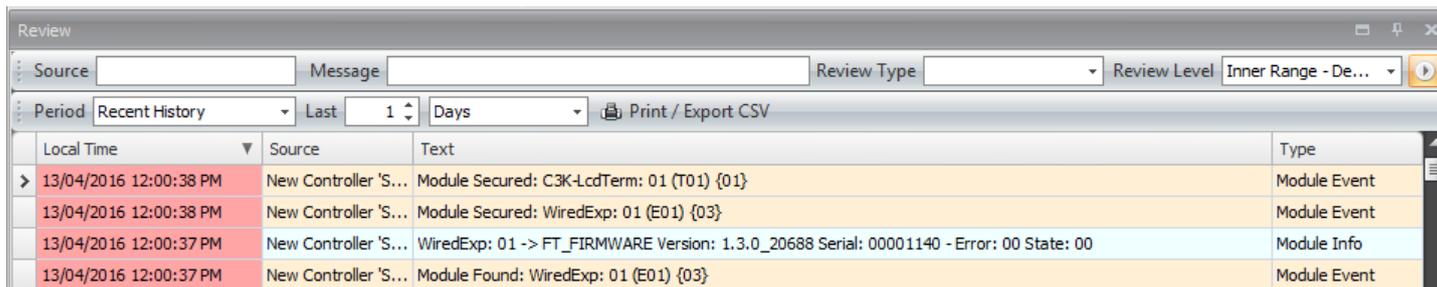
ACTIONS PANEL

The **Actions** panel displays actions that are performed by an operator from the software. The action list will display if the action was successful or failed.
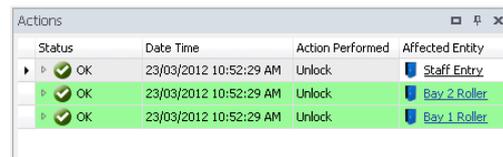
NAVIGATION PANEL

The **Navigation** panel displays the sites, sub-sites, controllers and hardware modules on the system. This display can be used to view the state of controllers and modules or to trigger commands such as connecting or disconnecting a controller.
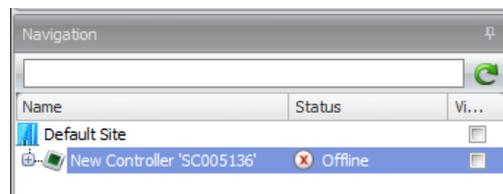
EDITOR WINDOW

When an item such as a user, area or door is edited, all the options and properties appear in an Editor Window. There are some common elements between editor windows for different items.

Tool Bar

Most of the toolbar icons appear on every editor window.

Properties / Options

The main part of the editor window displays all the properties for the item you are editing.

Context-based Help

The help displayed will change based on the selected property or option.
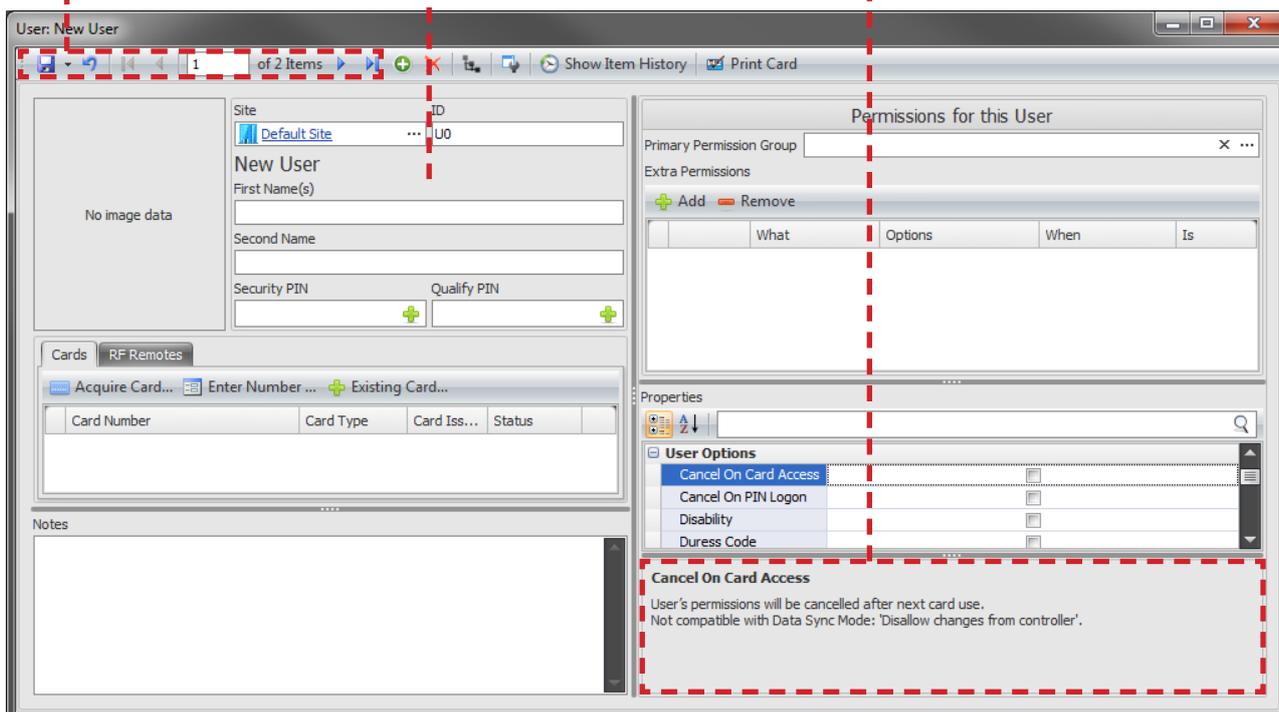
EDITOR WINDOW TOOL BAR

The toolbar contains the following buttons:

1. The **Save** button will save the item that is currently displayed in the editor window.

2. The **Undo** button will revert the last change since the editor window was opened.

3. The **First Item** button will move backwards to the first item in the list.

4. The **Previous Item** button will move backwards one item.

5. The **Item Number** field displays what number that current item is in the series. You can type in a number to jump to a particular item.

6. The **Next Item** button will move forward one item.

7. The **Last Item** button will move forward to the last item in the list.

8. The **Create New** button will make a new blank item.

9. The **Delete** button will remove the currently selected item.

10. The **Show Cross References** button will open a window that shows the other system items that relate to the currently displayed item.

11. The **Show Item History** will open a window that shows the entire history of the item.

12. The **Item Specific Commands** will change based on the item you have open.

You can toggle the automatic save feature by clicking the **Save** button drop-down and selecting the **Auto Save** option. The **Save** icon will change to a green icon when the automatic save feature is active. When you make a programming change to an item and close the window or navigate to the next item, your changes will automatically be saved.
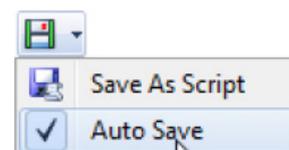
USER PROGRAMMING

CREATING A USER

A user is any person that will interact with the Integriti system via a keypad or card reader. The **User Editor** window allows you to assign the user a PIN number, access card, user permissions or even a photo.

To create a new user from System Designer, navigate to the **Home** tab then click the **Users** icon, this will open the **Users List**. Click the **Add** button to open the User Editor window containing a blank user record.

To create a new user from GateKeeper, navigate to the **Users** tab then click the **Users** icon, this will open the **Users List**. Click the **Add** button to open the **User Editor** window containing a blank user record.

USER EDITOR WINDOW

The top left section of the **User Editor** window contains the basic user information.
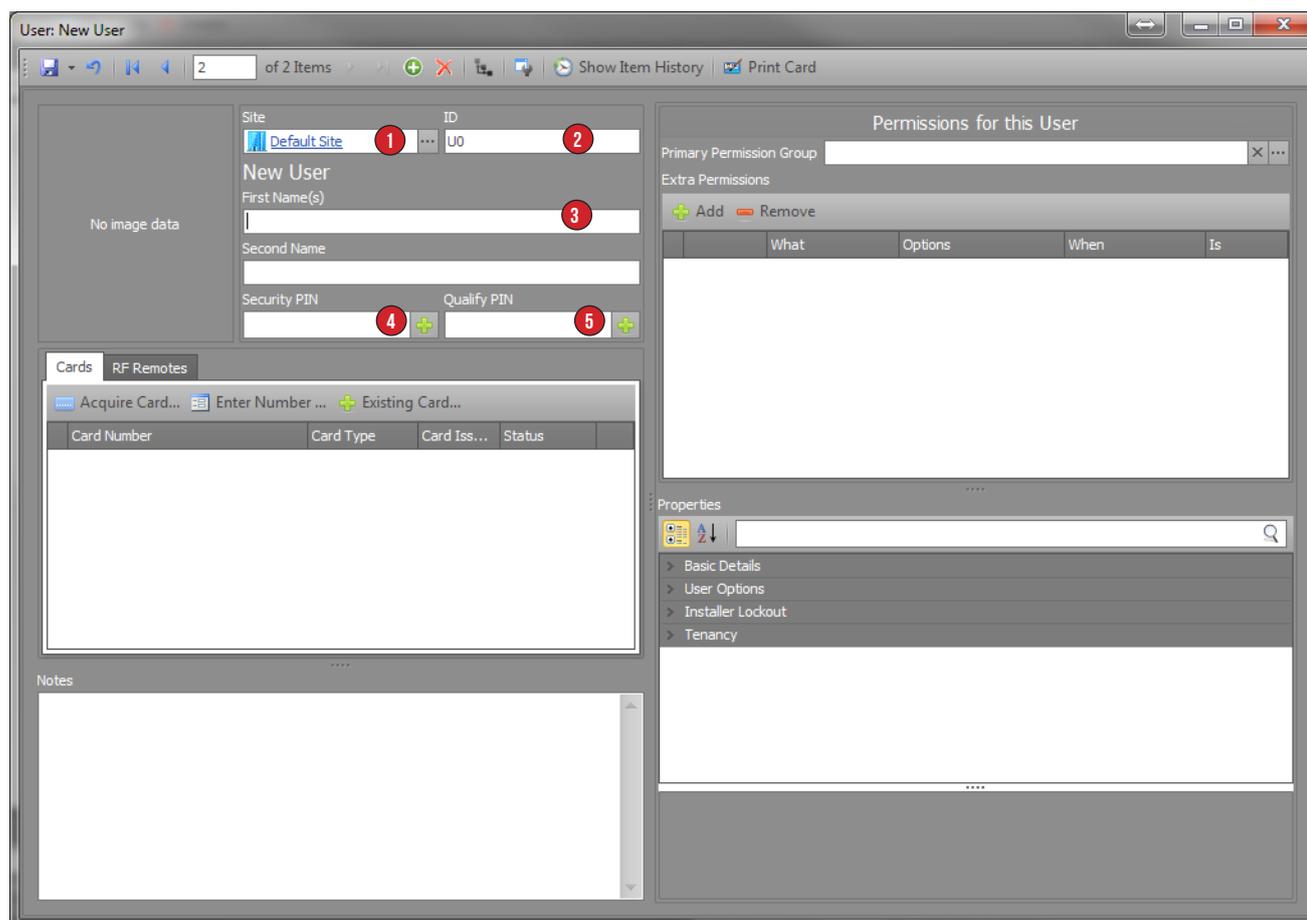
1. The **Site** field is used to associate a user with a site or sub-site, this will not have any impact on the user. The user will only be visible in the software if the operator logged in has permission to view users from that sub-site.

2. The **ID** field is a unique number that you can use to identify the users. Each time you add a new user, the user will be given the next available number. The ID field is just a number that has no effect on the user.

3. The **First & Second Name** fields are where you enter the user's first and last name.

4. The **Security PIN** is required for a user to interact with the Integriti system via a keypad. If the user needs to be able to arm or disarm areas from the keypad, you will need to assign the user a security PIN and a menu group. There is no minimum or maximum length for a Security PIN by default; however your system may have been configured to have a fixed PIN code length. If you enter a Security PIN that is either too long or too short the following error will occur.

5. The **Qualify PIN** can be used instead of the **Security PIN** when entering a door that requires the user to enter a PIN to unlock. The qualify PIN is used so that the PIN number that is used for keypad access can be different to the PIN number used for door access. Please check with your installer if you are unsure if you need to use the qualify PIN.

Warnings : 1 outstanding			⊣ ✕
Time	Affected Controller	Description	
4/12/2015 3:06:39 PM	New Controller 'SC002604'	Data Write Error (RET_PIN_LENGTH_ERROR - User 3)	

⚠ Warnings : 1 outstanding
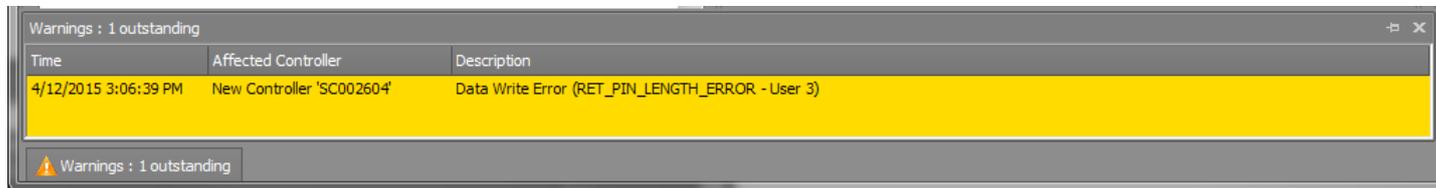
INTRODUCTION TO PERMISSIONS

It is important to understand how user permissions are structured before assigning permissions to a user. A permission is an item that you assign to a user to allow or deny that user the ability to interact with the item. Permissions include doors, areas, floors, lift cars and menu groups. In most cases more than one door or area is assigned to a user. It is recommended that you use a list of items such as area lists, door lists or floor lists when assigning permissions for many of the same item.

PERMISSION GROUPS

A permission group is a collection of permissions that can be assigned to one or more users. Many organizations have an internal structure where users share similar roles, for example, Warehouse Staff. It is easier to assign a single permission group to all of the Warehouse Staff rather than adding individual areas, doors or menu groups to each user. In most cases, the permission groups will closely match the roles within the company. Permission groups make it easier for you to add a single door to a group of users as it only requires the change to be made to a permission group and it will affect all users assigned that permission group.

CREATING A PERMISSION GROUP

Permission groups can only be created or edited from System Designer. To create a new permission group, navigate to the **Home** tab and click the **Permission Group** icon. Click the **Add New** button to open the **Permission Group Editor** window.
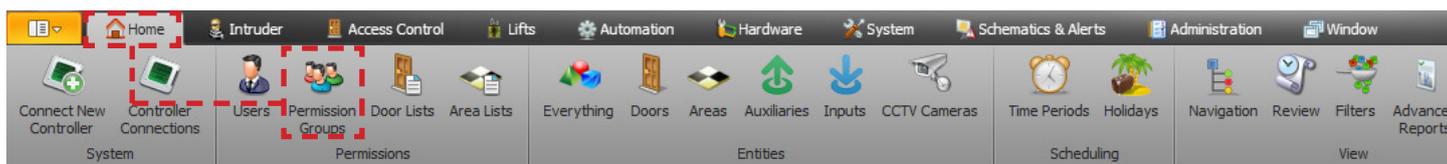
PERMISSION GROUP EDITOR WINDOW

The **Permission Group Editor window** only contains a **Name** field and it is primarily used to add or remove permissions. To add a permission to a permission group click the **Add** button.
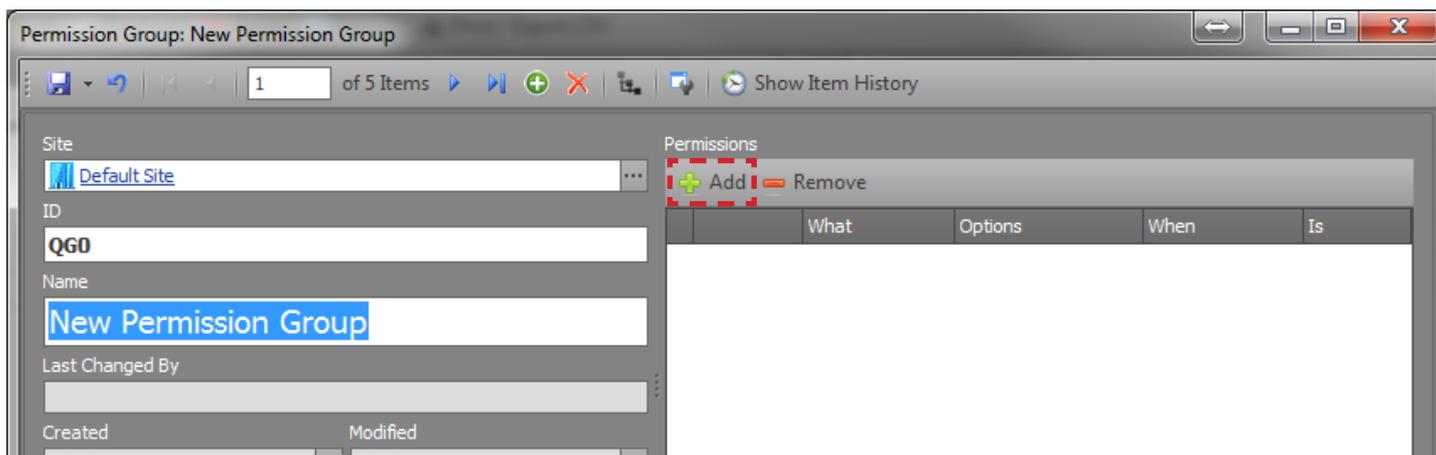
The **Search for What** window will open, this window has two sections:
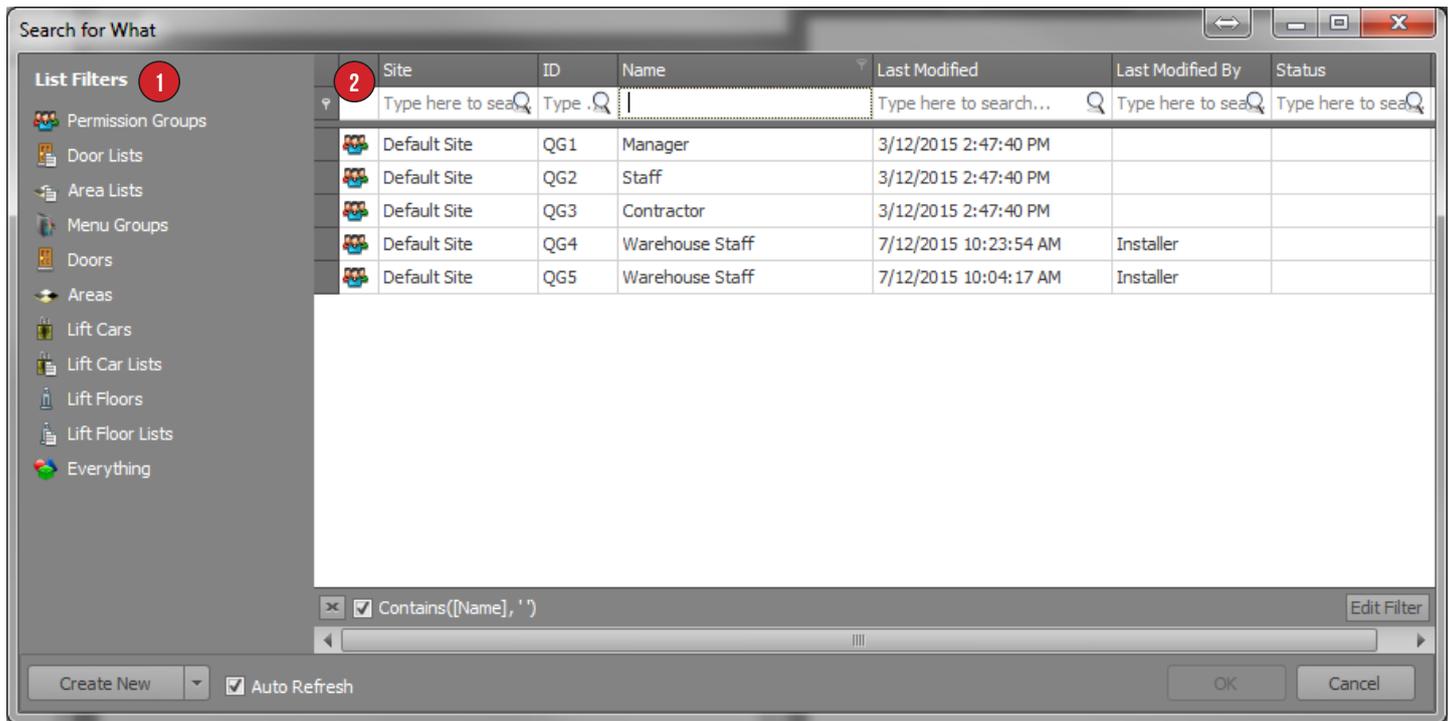
1. The **List Filter** allows you to filter all the available items that can be assigned to a user as a permission based on the item type.

2. The **Filtered Item** list allows you to choose one or more items to assign to the user. To select more than one item at a time, hold down the **CTRL** button and click multiple items.

PERMISSION STRUCTURE

Once you have selected an item from the **Search for What** window click the **OK** button to add it to the permission group. The item is then displayed in the **Permission Group** editor window and has the following options:
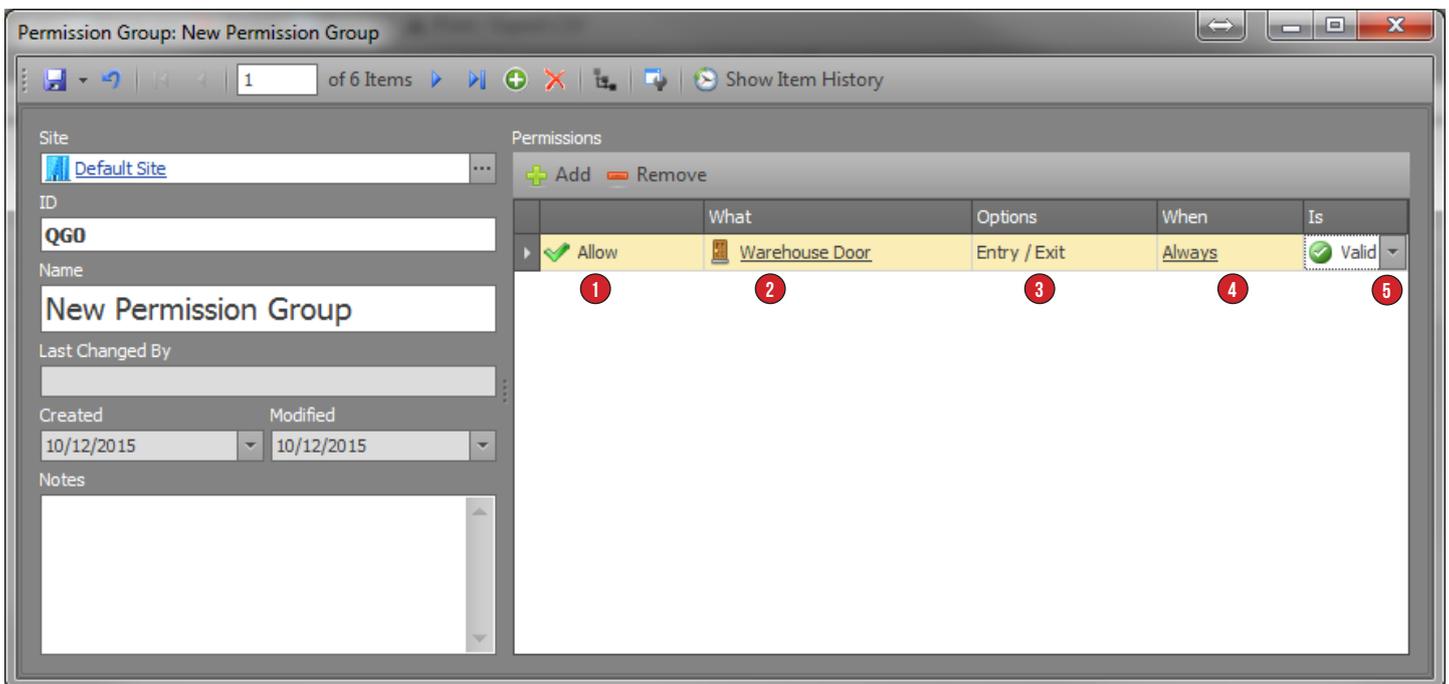
1 : ALLOW OR DENY

This column determines if the permission is allowing or denying access to the item. Please note that if you deny an item that has already been allowed within the permission group, the deny will override the allow.
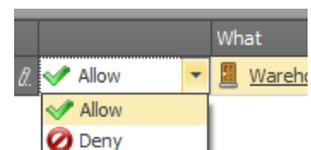
2 : WHAT

The **What** column is used to determine which item the permission refers to. Clicking the ellipsis, (button with three dots) will open the **Search for What** window allowing you to select a different item.

3 : OPTIONS

The **Options** column is used to determine how the user can interact with the assigned item. This allows you to assign a user permissions only to arm a particular area and not disarm it. Alternatively, you can assign the user permissions to only enter or exit a door.
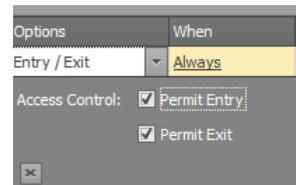
4 : WHEN

The **When** column is used to provide conditional permission to an item. This is most commonly used to assign a user with permission to an item but restrict its access to certain times of the day. For example, you may have a user that is only allowed to access a door during working hours. This can be achieved by adding the Working Hours time period to the **When** column.

5 : IS

The **Is** column is used to reverse the condition that is used in the **When** column. If you only wanted a user to have access to a door after working hours you could put the Working Hours time period time in the **When** column and set the **IS** column to invalid. This is easier than creating a new time period called Non-Working Hours.

ASSIGNING USER PERMISSIONS

The **Permissions for this User** window is divided into two sections, the Primary Permission Group and the Extra Permissions. It is important to understand the structure of permissions before assigning permissions to a user
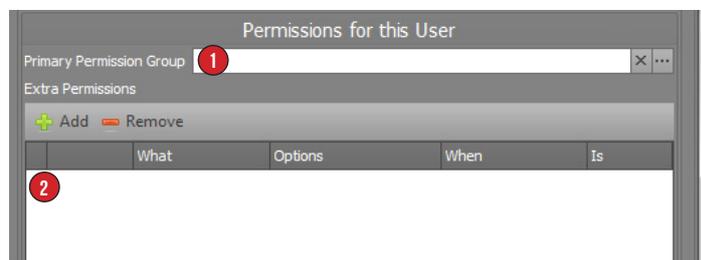
1 : PRIMARY PERMISSION GROUP

The **Primary Permission Group** option is where a user's permissions are usually assigned. This field only allows you to assign a single permission group, in most cases a user will be assigned a primary permission group based on their role in the company.

2 : EXTRA PERMISSIONS

The **Extra Permissions** section lets you allow or deny permissions for items independent of the primary permission group. This feature is commonly used to reduce the number of permission groups within the Integriti system.

If two users have similar roles, for example Warehouse Staff and Warehouse Manager, they can both be assigned the same primary permission group. You would then add extra permissions for the additional doors and areas that the Warehouse Manager needs.

The extra permissions use the same **What & When** structure as in the permission group programming.

USER PROPERTIES

There are many settings found in the **Properties** section of the **User Editor** window, most of these options are rarely used and should not be edited unless instructed to do so by your installer.

Below are three more commonly used options:

1 : USER CANCELED

If flagged, the user's permissions will be disabled. The user will not be able to interact with the Integriti system via a keypad or an access control door.

2 : START DATE TIME

The **Start Date Time** option prevents the user from interacting with the Integriti system until the date and time specified.

3 : EXPIRY DATE TIME

The **Expiry Date Time** option prevents the user from interacting with the Integriti system past the date and time specified.

The **Start Date Time** and the **Expiry Date Time** can be used separately or combined. For example, a visitor that attends a site for a set duration of time between two dates. The **Start Date Time** will ensure that visitor will not be able to access the site early and the **Expiry Date Time** will ensure that the card can not be used past the end of the visit.
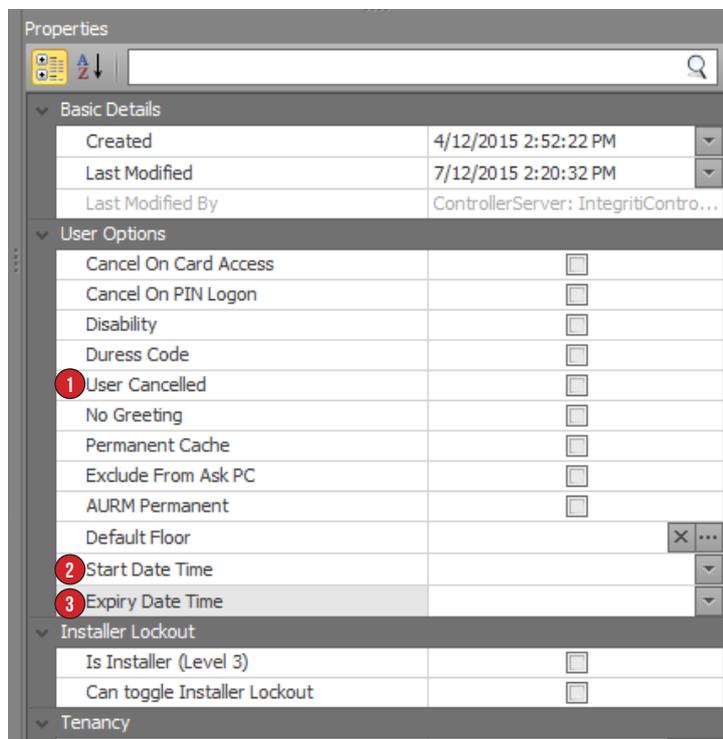
ASSIGNING CARDS TO USERS

Once a user has been created and programmed, the next step is to assign them a card. There are numerous card formats and card types in Integriti, therefore, there is more than one way for you to assign a card to a user.

The following methods for assigning cards will depend on the types of cards you currently use on-site. Check with your installer to confirm which method is correct for you.

DIRECT ENTRY

Direct Entry is a method of using the raw information that is read from a card by a reader. Integriti does not interpret the raw information. **Direct Entry** cards can not be preprogrammed in Integriti as every card needs to be badged to read its information.

To assign a direct entry card to a user, click the **Acquire Card** button found in the **Cards** section of the **User Editor** window. The **Acquire Card** window provides you three methods to acquire a card.
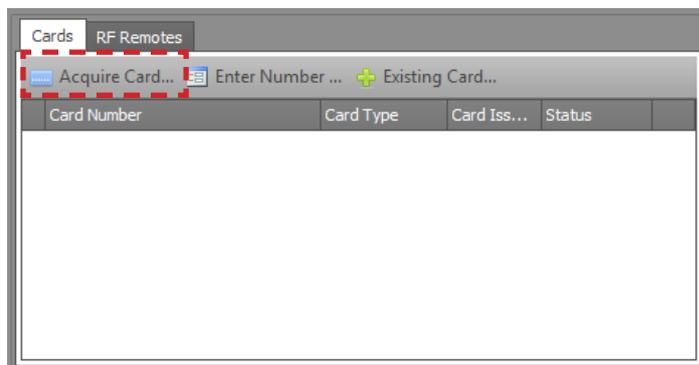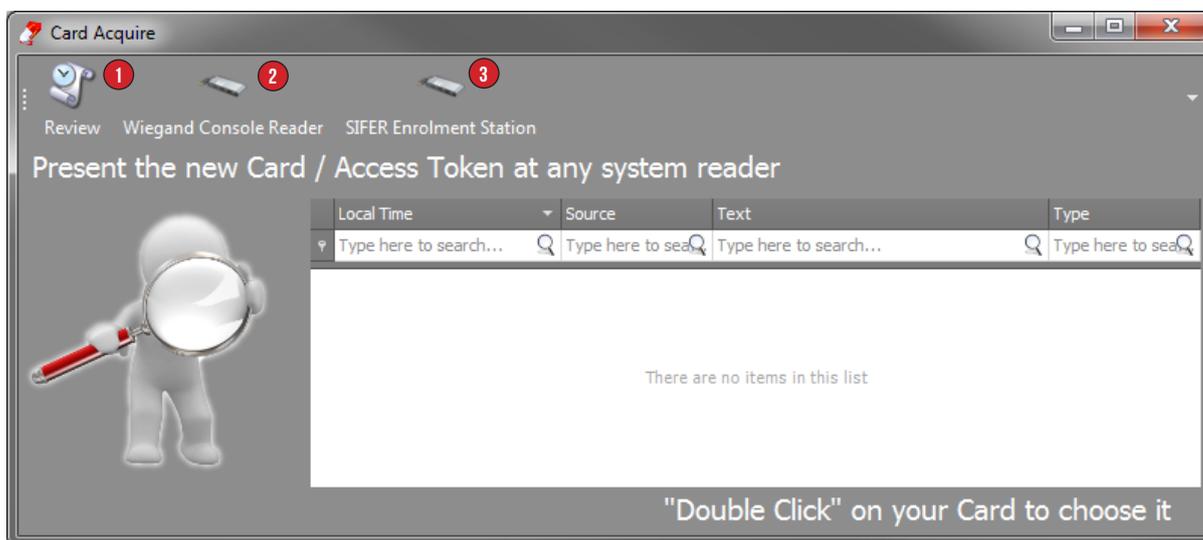
1. **Review:** Selecting this option will scan for review messages of card badges at any reader on the site. Simply badge the card you want to assign to a user at a reader, once it appears in the list double click it to assign it to the user.

2. **Wiegand Console Reader:** If many direct entry cards are going to be assigned, it may be easier to use a Wiegand Console Reader method. The Wiegand Console Reader method uses the enrollment station that attaches to the PC via a serial port. To assign a card to a user, badge a card at the enrollment station and double-click the most recent card information.

3. **SIFER Enrollment Station:** If SIFER Cards and readers are being used, the SIFER enrollment station can be attached to a PC via a USB port to make the enrollment of many SIFER cards easier.

Once the card has been double clicked the card will appear in the **Cards** section of the user programming.
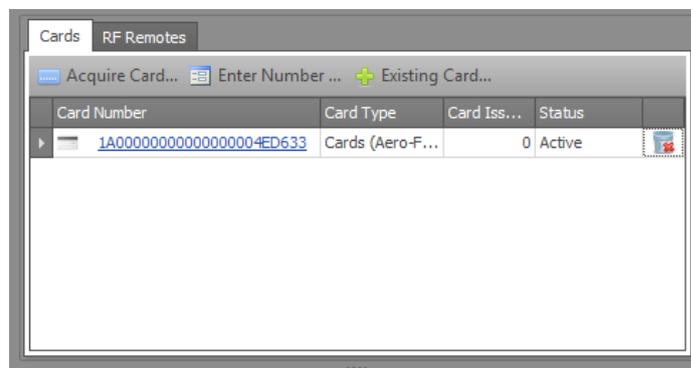
SITE CODED CARDS

Site Coded cards unlike Direct Entry cards can be pre-programmed on the Integriti System and do not require you to badge the card to assign it to a user. In some cases, the number will be printed on the card itself.

If your system has been configured by your installer for site code, you will be able to enter the card number rather than badging the card to assign it to a user.

To assign a Site Coded card to a user, click the **Enter Number** button in the **Cards** section, this will open the **Manual Card Entry** window.
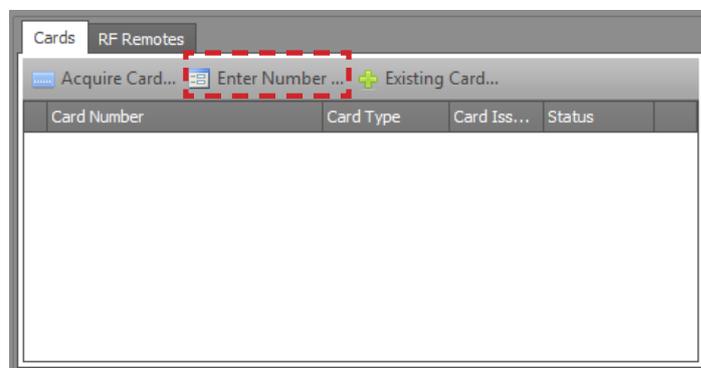
The **Manual Card Entry** window contains two fields that are required to assign a card to a user.

1. The **Card Template** is used to define what type of card you are assigning. In some cases there may be more than one template, this usually occurs when a combination of new and old cards are being used on a site.

2. The **Card Number** field is were you enter the unique card number. In some cases the number will be printed on the card, if it is not printed you may need to badge a card at a reader to view the card details.
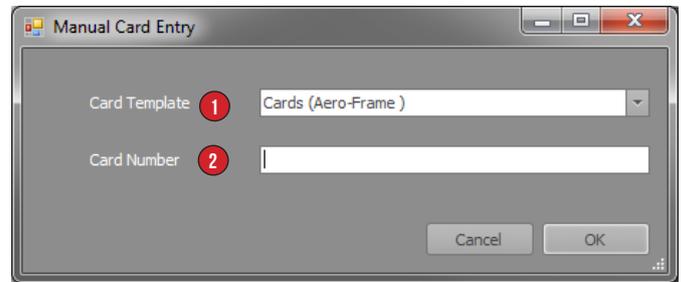
Below is a review message that contains the card information. The card number is 00027417.

Local Time	Source	Text
16/09/2015 1:11:07 PM	Auto-Discovered...	Unknown User Card Access at <R02:Rdr01> out of Door 000 Denied - Wrong Card
16/09/2015 1:11:07 PM	Auto-Discovered...	Wiegand Site (26): Site =00000039(dec) Card = 00027417(dec) Issue = 00000(dec) at <R02:Rdr01>

EXISTING CARD

When users that have cards assigned to them are deleted from the Integriti System, the card remains behind with an unallocated status.

This unallocated card can be assigned to a new user.
To assign an existing card to a user, click the **Existing Card** button in the **Cards** section.

This will open the **Find Entity** window that displays all the unallocated cards. Select a card from the **Available Cards** list and click the **OK** button to assign it to the user.
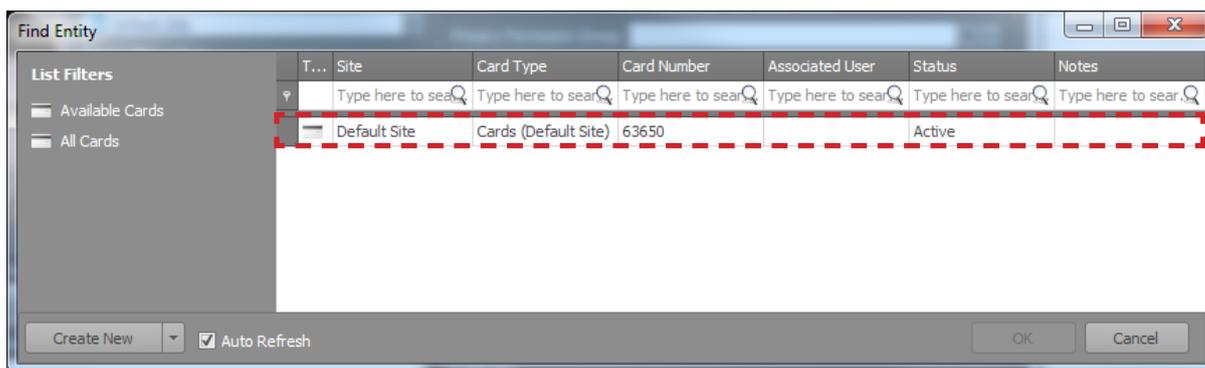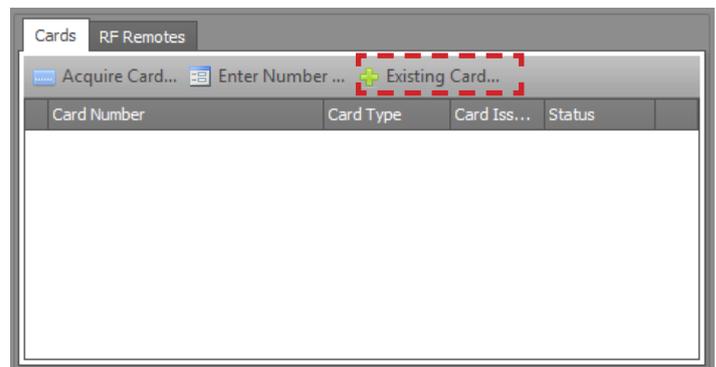
DOOR LISTS

INTRODUCTION TO DOOR LISTS

A door list is a collection of doors that can be used for user permissions, door control or automation. When assigning multiple doors to a user, it is easier to assign a single door list.

An operator can lock or unlock a door list, instead of having to control doors one at a time. The Integriti controller can be configured to automatically lock or unlock a door list.

THE DOOR LISTS MENU

To program a door list, navigate to the **Home** tab and click the **Door Lists** icon.
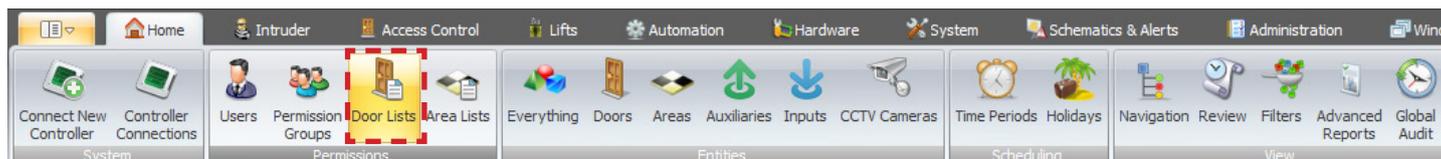
The **Door Lists** menu will open; this list contains all the currently programmed door lists.
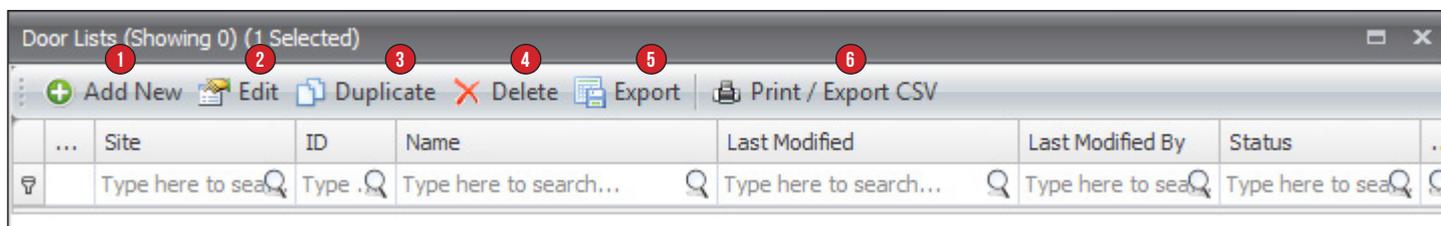
1. The **Add New** button will create a new blank door list.

2. The **Edit** button will open the selected door list for programming changes.

3. The **Duplicate** button will create a new door list that is identical to the selected door list.

4. The **Delete** button will delete the selected door list(s).

5. The **Export** button saves the selected door list(s) as an IR-Entities file.

6. The **Print/Export CSV** button provides a printable version of the contents of the Door Lists window.

CREATING A NEW DOOR LIST

Click the **Add New** button to open the **Door Lists Editor** window.
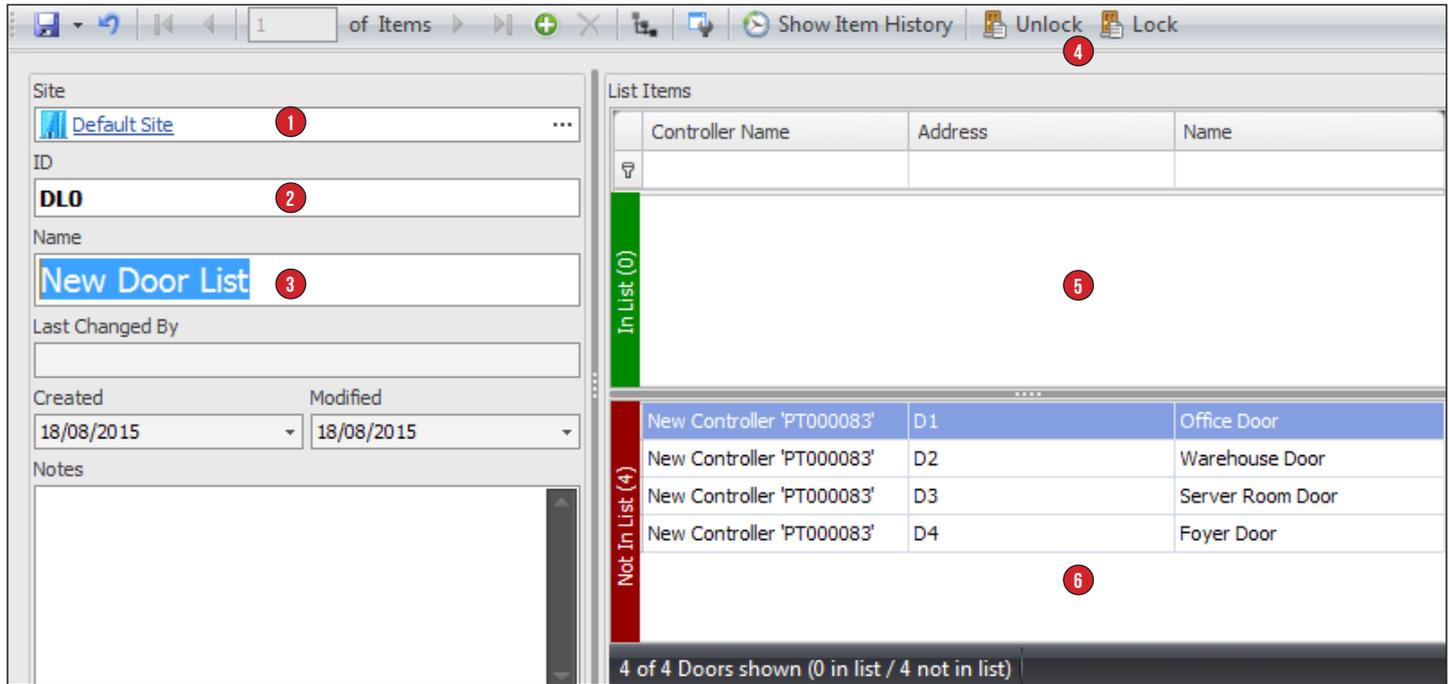
1. The **Site** field determines which site this door list will be associated with.

2. The **ID** field displays the unique identification code for each door list, this ID cannot be changed.

3. The **Name** field is where a name can be assigned to the door list.

4. The **Unlock** and **Lock** buttons will control all of the doors assigned to the door list.

5. The **In List** section displays all doors that are assigned to the door list.

6. The **Not In List** section displays all of the doors that are not assigned to the door list.

ADDING/REMOVING A DOOR FROM A DOOR LIST

ADDING A DOOR

1. Select one or more doors from the **Not In List** section.

2. Click the **Add** button to add the door(s) to the door list.

3. The door will move from the **Not In List** section to the **In list** Section.
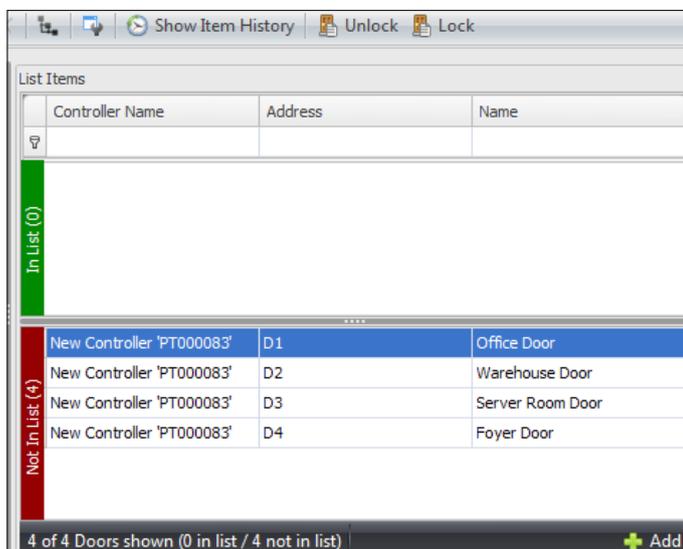
REMOVING A DOOR

1. Select one or more doors from the **In List** section .

2. Click the **Remove** button to remove the door(s) from the door list.

3. The door will move from the **In List** section to the **Not In list** Section.
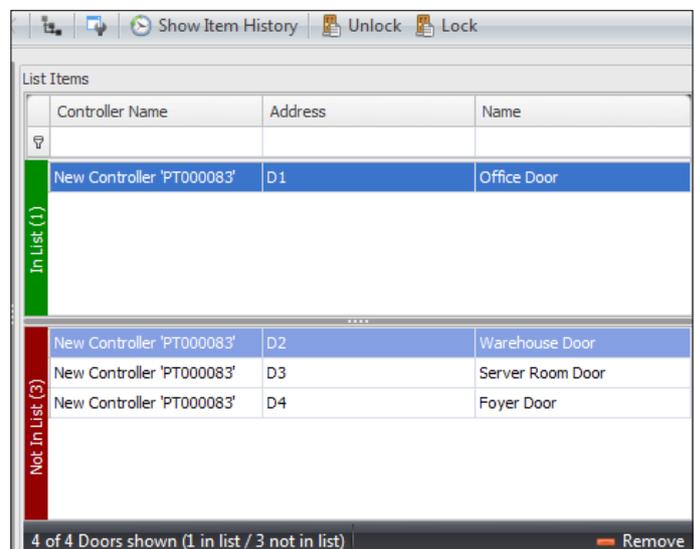
AREA LISTS

INTRODUCTION TO AREA LISTS

An area list is a collection of areas that can be used for user permissions, area control or automation. When assigning multiple areas to a user, it is easier to assign a single area list.

An operator can arm or disarm an area list instead of having to control areas one at a time. The Integriti controller can be configured to automatically arm or disarm an area list.

THE AREA LISTS MENU

To program an area list, navigate to the **Home** tab and click the **Area Lists** icon.
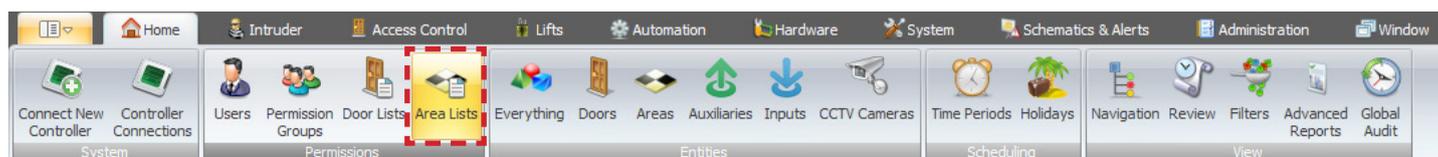
The **Area Lists** menu will open; this list contains all the currently programmed area lists.
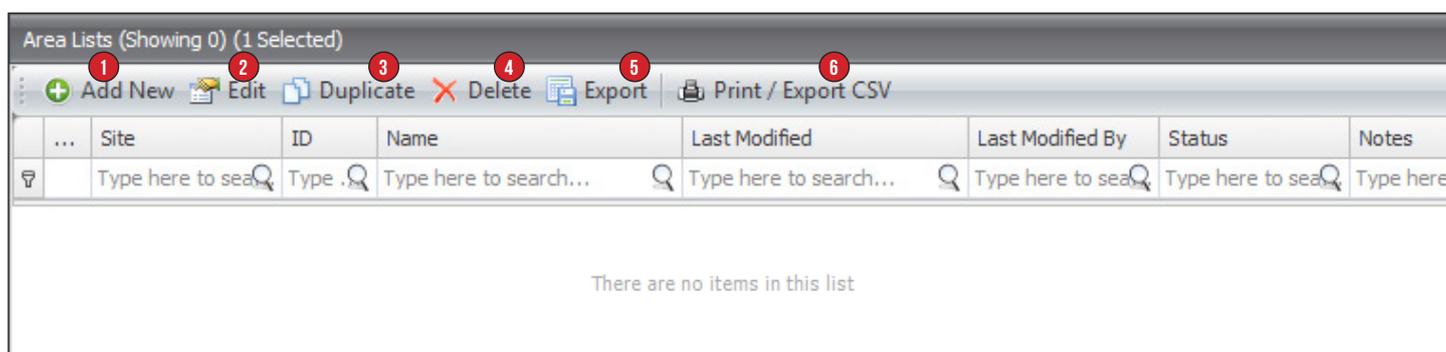
1. The **Add New** button will create a new blank area list.

2. The **Edit** button will open the selected area list for programming changes.

3. The **Duplicate** button will create a new area list that is identical to the selected area list.

4. The **Delete** button will delete the selected area list(s).

5. The **Export** button saves the selected area list(s) as an IR-Entities file.

6. The **Print/Export CSV** button provides a printable version of the contents of the **Area Lists** window.

CREATING A NEW AREA LIST

Clicking the **Add New** button will open the **Area Lists Editor** window.
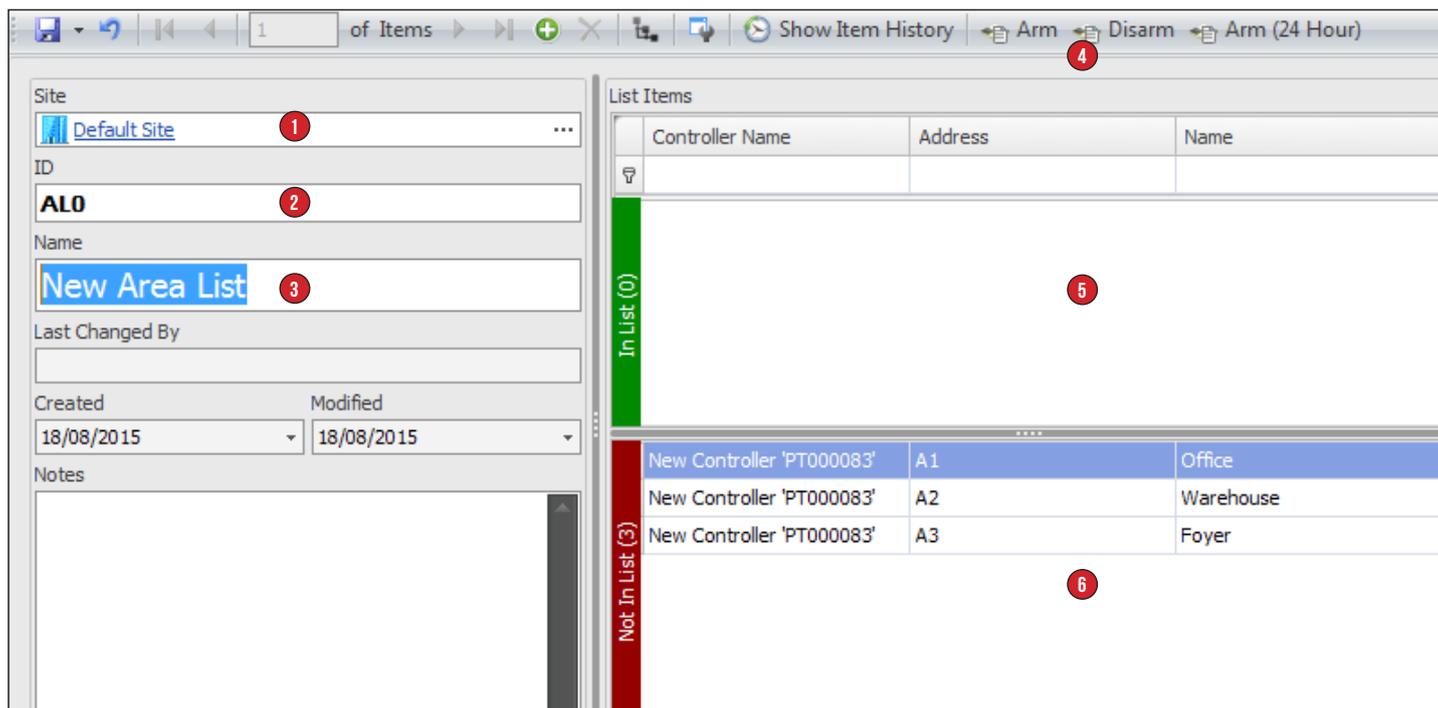
1. The **Site** field determines which site this area list will be associated with.

2. The **ID** field displays the unique identification code for each area list - this cannot be changed.

3. The **Name** field is where a name can be assigned to the area list.

4. The **Arm** and **Disarm** buttons will control all the areas assigned to the area list.

5. The **In List** section displays all the areas that are assigned to the areas list.

6. The **Not In List** section displays all the areas that are not assigned to the area list.

ADDING/REMOVING AN AREA FROM AN AREA LIST

ADDING AN AREA

1. Select one or more areas from the **Not In List** section.

2. Click the **Add** button to add the area(s) to the area list.

3. The area will move from the **Not In List** section to the **In list** Section.
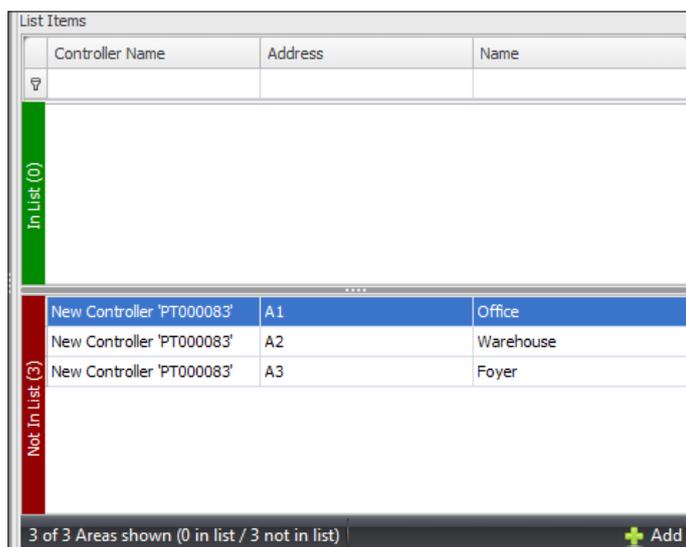
REMOVING AN AREA

1. Select one or more areas from the **In List** section .

2. Click the **Remove** button to remove the area(s) to the area list.

3. The door will move from the **In List** section to the **Not In list** section.
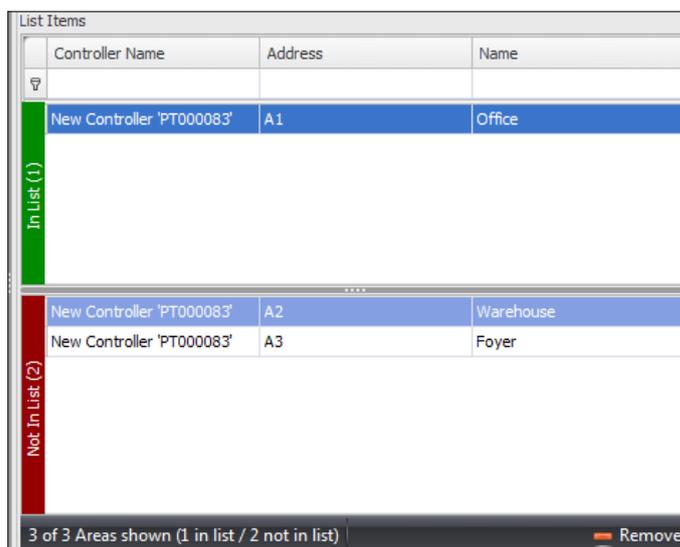
ALERTS

INTRODUCTION TO ALERTS

An alert is a notification that draws an operator's attention to an event or alarm.

For example, when a duress panic/duress button is pressed by a user it will require a guard to respond in person. Without an alert the event may be completely missed or actioned too late.

Alerts are viewed and actioned from Integriti GateKeeper. The alert will remain in the software until it is finalized by an operator.

USING AN ALERT

Alerts are usually configured by your installer, as an end user you will interact with alerts from an **Alert View** window. An alert view is a collection of different types of alerts, in some cases the alerts that you are able to see and respond to may differ from other operators.

Alert views are only visible in Integriti GateKeeper and are part of the default layout. If the alert views are not visible, navigate to the **Home** tab and then click the **Alert Views** icon.

ALERT CREATION

When the event that triggers an alert occurs, the alert is created and appears in the **Alert View** window. The appearance of the alert is determined by how it is configured. Alerts can be configured to have different foreground and background colors, this allows the you to easily identify the type of event that has occurred.

READING ALERT INFORMATION

The **Alert** window has multiple columns that contain information to help you identify the alert priority, what triggered the alert and when the alert was generated. These columns can be used to filter the currently displayed alerts.

1 : DATE / TIME UPDATED

This displays the most recent occurrence of the event that triggered the alarm.

This field can be searched by a specific date or a range of dates, such as last hour.

By selecting the **Show All** check-box, it will display all un-finalized alerts.

2 : MESSAGE

This provides a summary of the event(s) that have occurred to trigger the alert.

Date / Time Updated ▼	Message	Activations	Priority ▼	State	Operator
⌕ Type here to search...	Type here to search...	Type here to	Type here to	Type here to	Type here to sea
> 12/08/2015 9:35:27 AM +10:00	Alarm Activated on Office PIR by Office	1	Priority 1	Unclaimed	

The **Message** field is a basic text-based filter that you can use to filter the displayed alerts by typing the name of an item, for example: office.

Message	▼
office	

This would filter the alerts to only display the ones that contain the word office in the **Message** field.

3 : ACTIVATIONS

Alerts can be grouped by the input, area or review message that created them. The Activations column provides a count of how many times the event has occurred, rather than having individual alerts for each event.

Date / Time Updated ▼	Message	Activations	Priority ▼	State	Operator
⌕ Type here to search...	Type here to search...	Type here to	Type here to	Type here to	Type here to sea
> 12/08/2015 9:35:27 AM +10:00	Alarm Activated on Office PIR by Office	1	Priority 1	Unclaimed	

Activations	▼
	4

This column can also be filtered by entering a number into the search field.

4 : PRIORITY

An alert can be configured to have a priority; you can use this priority to determine which event to action first. The priority scale is from 1 (high) to 16 (low).

Date / Time Updated ▼	Message	Activations	Priority ▼	State	Operator
⌕ Type here to search...	Type here to search...	Type here to	Type here to	Type here to	Type here to sea
> 12/08/2015 9:35:27 AM +10:00	Alarm Activated on Office PIR by Office	1	Priority 1	Unclaimed	

The **Priority** column can be filtered by selecting one or more of the check boxes.

You can view all alerts by checking the **(Select All)** check box.

☐ (Select All)
☐ Priority 1
☐ Priority 2
☐ Priority 3

OK   Cancel

5 : STATE

The state of an alert will either be Unclaimed, Claimed or Finalized; this allows you to identify which alert to action in order to avoid two operators dealing with the same alert.

Date / Time Updated ▼	Message	Activations	Priority ▼	State	Operator
⌕ Type here to search...	Type here to search...	Type here to	Type here to	Type here to	Type here to sea
> 12/08/2015 9:35:27 AM +10:00	Alarm Activated on Office PIR by Office	1	Priority 1	Unclaimed	

The **State** column can be searched by selecting one or more of the check boxes.

You can view all alerts by checking the **(Select All)** check box.

☐ (Select All)
☐ Unclaimed
☐ Claimed
☐ Finalized

OK   Cancel

6 : OPERATOR

Once an alert has been claimed by an operator, the operator's name will appear in the Operator column.

Date / Time Updated ▼	Message	Activations	Priority ▼	State	Operator
⌕ Type here to search...	Type here to search...	Type here to	Type here to	Type here to	Type here to sea
> 12/08/2015 9:35:27 AM +10:00	Alarm Activated on Office PIR by Office	1	Priority 1	Unclaimed	

Operator	▼
David	

The **Operator** column has a basic text-based search field; you can filter the alerts by typing the name of an operator, for example, David.

CLAIMING ALERTS

Integriti GateKeeper can have multiple operators logged in who can view and action alerts at the same time. Claiming alerts is a way to identify who is dealing with an alert, this prevents two operators both actioning on the same alert.

Alert View: Combined View; Showing 1

Claim Action Force Finalize Un Mute Un Claim   Hide Alerts Claimed by Other Operators
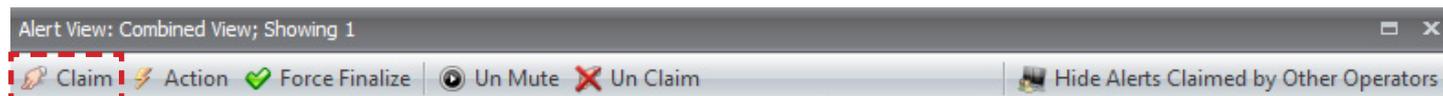
CLAIMING ALERTS   Claim
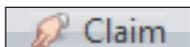
The **Claim** button is used to assign the alert to yourself; this will change the state from unclaimed to claimed.

Additionally your operator name will appear in the **Operator** column in the alert view. Once claimed, only that operator can action and finalize the alert.

UNCLAIMING ALERTS   Un Claim

Once an alert is claimed, the **Claim** button will change to an **Un Claim** button

If you have claimed an alert and needed another operator to action it, you can unclaim the alert by clicking the **Unclaim** button in the alert view.

Note: Claiming an alert will only work if each operator logs in with a unique operator name.

ACTIONING ALERTS

Once an alert has been claimed, the next step is to action it. The **Action** button opens the **Finalize Response** window.

Alert View: Combined View; Showing 1

Claim Action Force Finalize Un Mute Un Claim   Hide Alerts Claimed by Other Operators
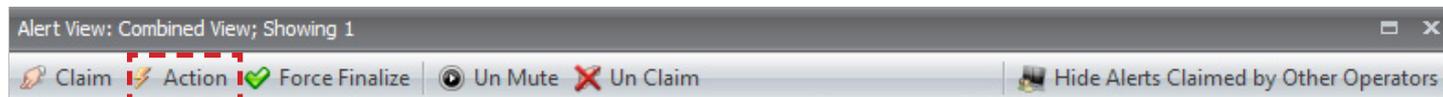
The **Finalize Response** window is used to enter a summary of how you responded to the alert and the alerts outcome.

Finalize Response

False alarm on Duress point.

Mute   Un-Claim   Finalize
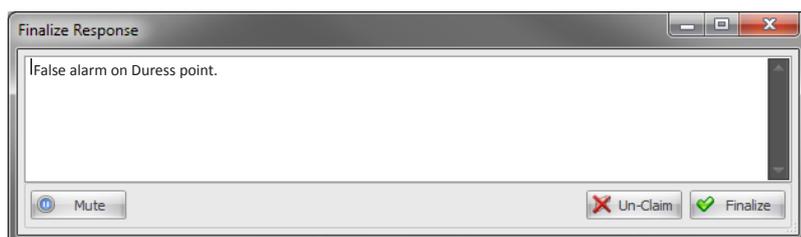
FINALIZING ALERTS

The last step in actioning an alert is to finalize the alert; this removes the alert from the alert view permanently. Finalized alerts are viewable by clicking the **Finalized Alerts** icon in the **Home** tab.

Alert View: Combined View; Showing 1

Claim Action Force Finalize Un Mute Un Claim   Hide Alerts Claimed by Other Operators
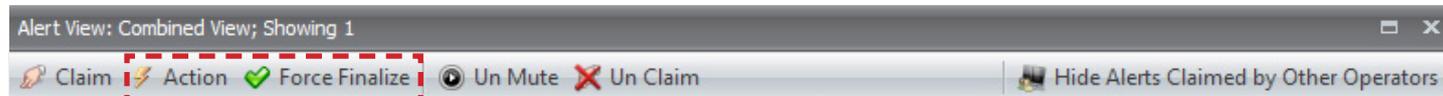
There are two methods for finalizing an alert:

FINALIZE

You can click the **Finalize** button on the **Finalize Response** window when actioning an alert

Finalize Response

False alarm on Duress point.

Mute   Un-Claim   Finalize

FORCE FINALIZE

Force Finalize allows more than one alert to be finalized by an operator, this is used to clear multiple alerts at once.

To force finalize select one or more alerts from the alert view and click the **Force Finalize** button.

The Finalize Response window will open allowing you to submit a response for all the selected alerts.

THE ALERT LIFESPAN

Alerts can be configured to perform actions at specific stages of its lifespan.

These actions may occur when the alert is created, claimed or finalized.

The most common alert action draws the attention of an operator to the workstation when the alert is first created. This can be done by performing one of the following actions:

PLAYING A SOUND

The alert can control a workstation and play an audio file such as a siren sound.

The alert may be configured to play the sound continuously, the sound can be muted by clicking the **Mute** button in the **Finalize Response** window when actioning an alert.

DISPLAYING A SCHEMATIC MAP

The alert can control a workstation and launch a schematic map.

This is commonly used to show the operator a map relating to the alarm.

DISPLAYING CCTV FOOTAGE

The alert can control a workstation and launch CCTV footage.

This is commonly used to show the operator live footage from a camera relating to the Alarm.
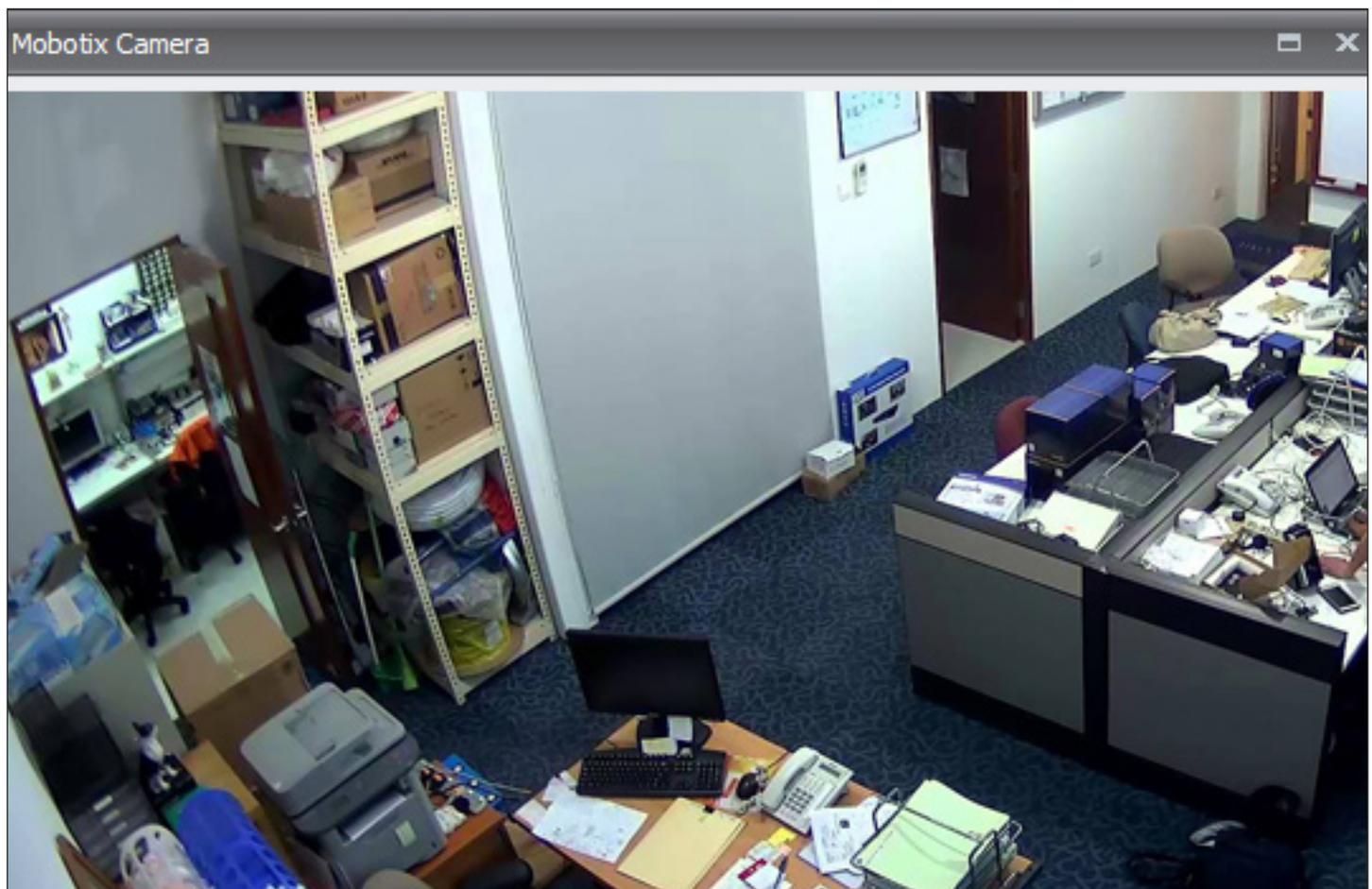
SCHEMATIC MAPS

INTRODUCTION TO SCHEMATIC MAPS

Schematic maps are a graphical representation of your site; they allow you to control and view the state of areas, doors, inputs, auxiliaries and many more items.

A schematic map may be as simple as a single map containing a floor plan with a couple of icons representing detectors or as complex as multiple maps that are navigated for more detailed views.

Schematic maps are usually created and configured by the installer.

OPENING SCHEMATIC MAPS

Schematic maps are usually viewed from Integriti GateKeeper, the **Schematic Maps** item list is a part of the default layout.

To open a Schematic map select a map from the **Schematic Maps Item** list and click the **Open** button. You can also open a schematic map by double-clicking on it.
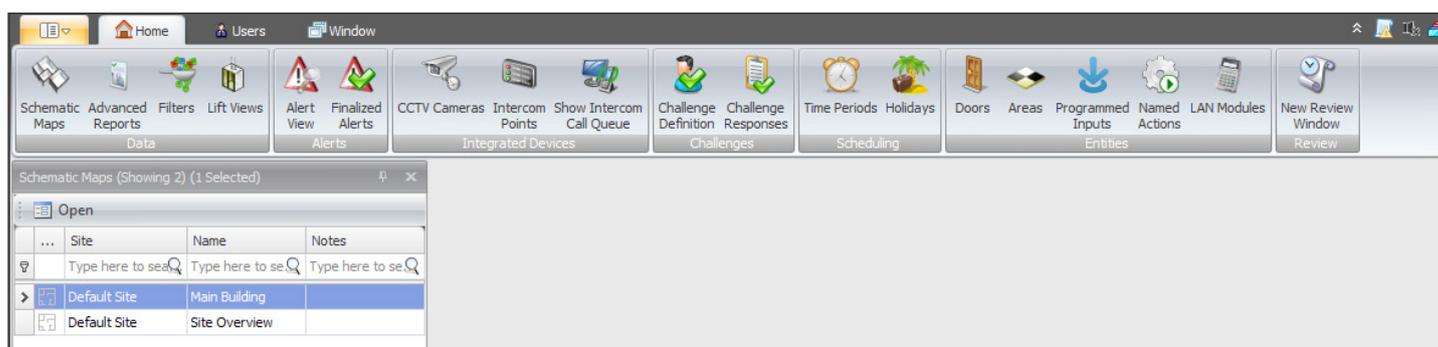
If the **Schematic Map Item** list is not visible, click the **Schematic Map** icon in the **Home** tab.

TOOLBAR & NAVIGATION

The schematic map window is made up of three sections:
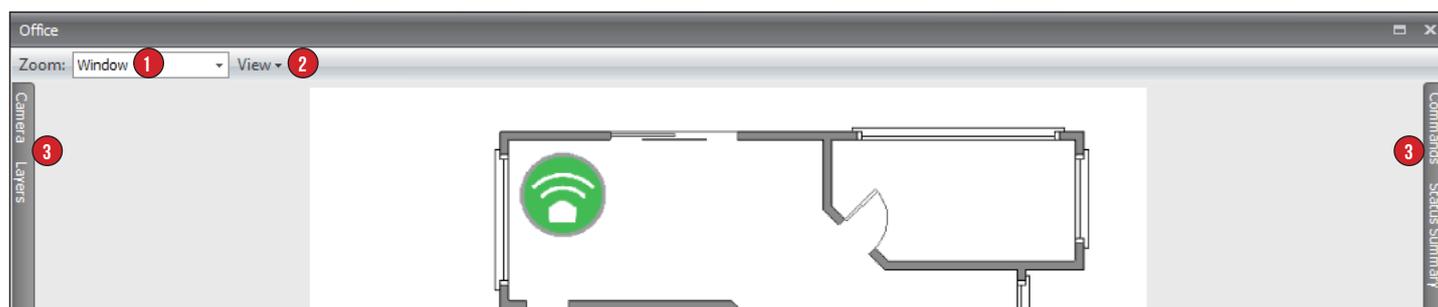
1 : ZOOM

The **Zoom** option allows you to set a zoom percentage, this determines how close or far away you are from the displayed map.

The **Window** option will fit the map in the current window, if the window is resized, the map will resize.
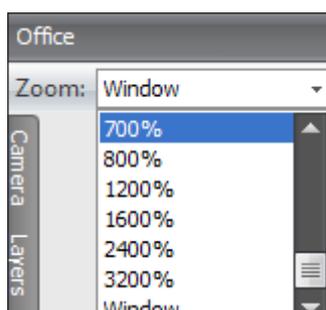
2 : VIEW

The **View** menu toggles the visibility of the **Camera**, **Layers**, **Commands** and **Status Summary** windows.
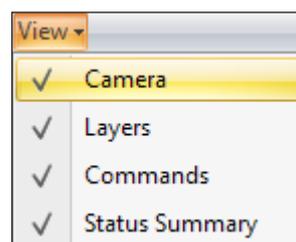
DOCKED WINDOWS

The four docked windows are used to interact with the map, see the status of entities, toggle the visibility of layers and view CCTV footage.

The purpose of these docked windows are explained later in this guide. By default the **Commands** and **Status Summary** windows are visible and the **Layers** and **Camera** windows are hidden.

To dock or auto-hide a window, click on the **Drawing Pin** icon.

Dock Panel:

Auto-Hide:

If set to Auto-Hide, the window will collapse once the operator selects a different window or an item on the map.
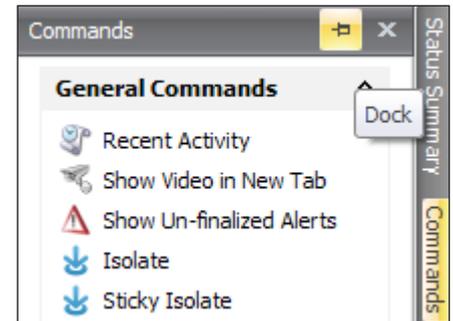
MAP ELEMENTS

Elements are shapes, icons, text or images that are placed on a schematic map. These elements can be static or dynamic.

Static elements are used for design or labeling purposes. For example, a label displaying the name of a map would not need to change, so this would be a static element.

Dynamic elements are used to display the state of item within the Integriti system. For example, an icon representing a particular door will change as the doors state changes from locked to unlocked.

Dynamic elements have an associated or linked item that can be configured when the map is created or edited.

ELEMENT TYPES

There are four element types that you may have on your schematic maps:

- Shapes
- Icons
- Labels
- Images

SHAPES

Shapes are used when the associated entity cannot be represented by an icon, for example, a perimeter fence or a large area.

In addition to this, shapes are commonly used for design elements such as map legends or buttons.

There are five different shapes in schematic maps, they all differ in appearance but have some common features. All shapes have interior and exterior colors. However, the interior color of lines and multi-segment lines are not visible. The **Line Size** setting determines the thickness of the outline.

All shapes have an Opacity setting which determines their level of transparency. These settings are configured when creating or editing the schematic maps.

1. **Rectangle**
   The rectangle is used as a representation of an area, button or border.

2. **Ellipse**
   The ellipse is used as a button.

3. **Line**
   The line is used as a representation of a fence line or as a border.

4. **Multi-Segment Line**
   The multi-segment line is used as a representation of a complex fence line or an area without an internal color.

5. **Freeform**
   The freeform shape is used as a representation of a complex area.

ICONS

Icons provide a simple, dynamic and flexible means of representing system items.

A schematic map can contain hundreds of icons and can still be easily understood as the icons change in appearance as the associated items change state.

A map will never have an icon that is not linked to an entity, but in some cases the map legend may contain what appears to be an icon. The legend only uses the image that is contained within the icon for a particular state.

It would not be appropriate for the key to change state.

LABELS

Labels are elements that display text on a schematic map.

When configured as a static element, the text appearance and contents will not change - this is commonly used for map legends.

The label element can be configured as a dynamic element - doing so will cause its appearance and contents to change based on the state of the entity it is associated with. E.g.: A temperature sensor's label could display 'Server Room Temp: 18.5 degrees C'.

IMAGES

Images can only be used as static elements; they are generally used for design purposes, such as adding a company logo to the map.

ELEMENT STATUS

When an element is linked to an entity, it will change in appearance based on the entity's state.

Each entity in the system has a set of rules that determine its appearance depending on whether it is displayed as a shape, icon or label.

The most commonly found entities on a map are doors, areas, inputs and outputs. In most cases, areas will be displayed as a shape due to the fact that an area does not have a single point location that an icon can represent.

Below are the states for the most commonly used elements:

DOORS

State	Icon	Description
Door Locked		The door is currently locked.
Unlocked		The door is currently unlocked.
Forced		The door is currently locked and has been forcefully opened.
DOTL		The door was unlocked, opened then relocked, but has not been closed for a long time. This state requires numerous other settings to work, not all doors will show DOTL.
Timed Unlocked		The door has been unlocked for a set period of time.
Has Alarms		The door is referenced in an alert; see the alerts section for more details.

INPUTS

State	Icon	Description
Sealed		The PIR detector does not sense movement.
Alarm		The PIR detector senses movement.
Isolated		The PIR detector has been isolated to ignore the alarm and tamper states.
Tamper		The cover of the PIR detector has been removed or someone has tampered with the cabling.

OUTPUTS

State	Icon	Description
On		The auxiliary is on.
Off		The auxiliary is off.

AREAS

State	Shape Option 1	Shape Option 1	Description
Disarmed			The area is currently disarmed.
Armed			The area is currently armed.
Alarm			The area is referenced in an alert.
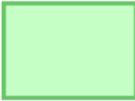
STATUS SUMMARY

The **Status Summary** window provides a summary of the item linked to the map element. This summary includes the type, name and the current status:

Status Summary ✕
Type: Input
Name: Office PIR
Summary: Sealed

Status Summary ✕
Type: Area
Name: Office
Summary: Disarmed
Extended: 1

Status Summary ✕
Type: Auxiliary
Name: Office Lights
Summary: Off

Status Summary ✕
Type: Door
Name: Office Door
Summary: Locked
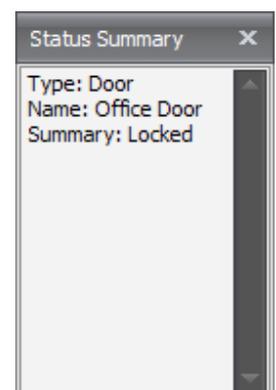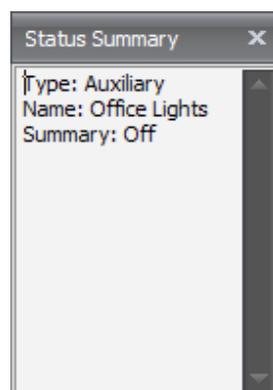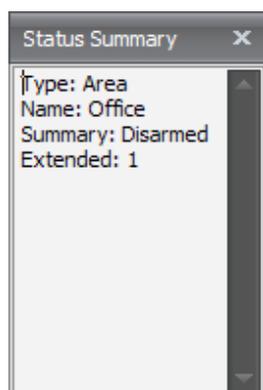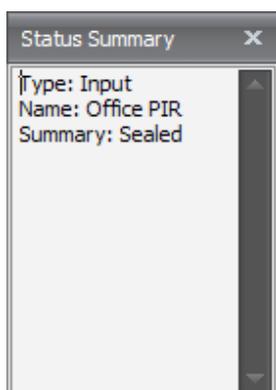
COMMANDS

Each element on a map that is linked to a door, area, input or auxiliary is accompanied with a list of commands.

These commands include viewing review, showing videos and controlling the item. The control commands will change based on the type of item you have selected.

The commands are accessed in one of two ways:

1. Clicking an element on the map will display the commands in the **Commands** window if it is visible. If the Commands window is not visible, click the **View** button and select the **Commands** option.

2. Right click an element on the map to display the **Commands** menu.
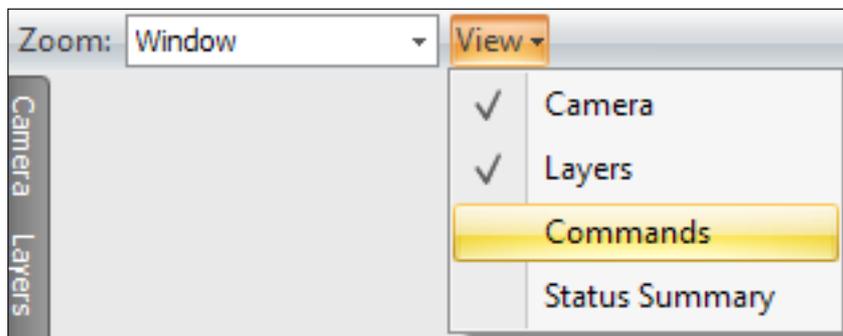
More than one element can be selected by holding the **CTRL** button and clicking the elements you wish to select.

If all of the selected elements are linked to the same type of entity (i.e. areas), the commands will apply to all the selected areas.

There will also be an individual area command that will appear under the areas name (right).

If more than one element is selected and they are not linked to the same entity type (i.e. a door and an area), the commands window will display a drop down menu for each of the selected elements (below).
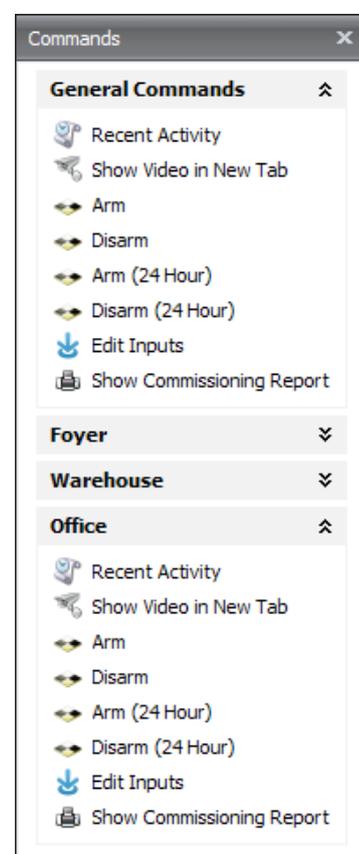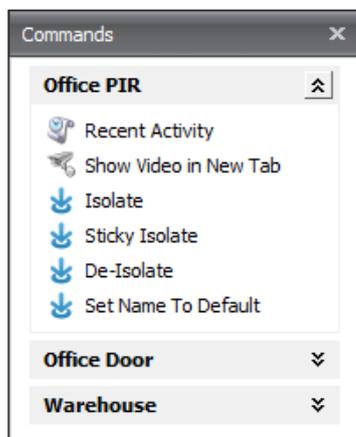
GENERIC COMMANDS

There are three commands that appear for most items that are displayed on schematic maps.

Recent Activity
This displays all review messages that relate to the selected entity for the last hour. This allows you to easily see the recent activity for an area or door.

Show Video in New Tab
If you have the CCTV Integration license, you can launch CCTV footage from cameras that are associated to items on your map. The video will open in a new tab and the schematic map will remain open in the background.

Show Un-Finalized Alerts
If alerts have been configured on your system for the items displayed on your map, clicking this option will display the alerts that are still outstanding for the selected item.

Area Commands	Descriptions
Arm	This will arm the selected area or areas.
Disarm	This will disarm the selected area or areas.
Arm (24 Hour)	This will arm the 24 hour part of the selected area or areas.
Disarm (24 Hour)	This will disarm the 24 hour part of the selected area or areas.

Area Commands	Descriptions
Isolate	This ignores state changes for the input until the area is re-armed.
Sticky Isolate	This ignores state changes for the input until de-isolated.
De-Isolate	This reverses the isolate & sticky isolate command.

Area Commands	Descriptions
Unlock	This unlocks the door indefinitely.
Unlock (Timed)...	This unlocks the door for the specified amount of time, at the end of the time the door will relock.
Lock	This locks the door.
Door-User Activity Report	This generates a review report of all users that have accessed the door in the last day.
Door-User Reference Report	This generates a report that contains all the users that have permission to access the door.

Area Commands	Descriptions
On	This turns the auxiliary on indefinitely.
On (Timed)...	This turns the auxiliary on for the specified amount of time, at the end of the time the auxiliary will turn off.
Off	This turns the auxiliary off.
Set Analogue Value ...	Not commonly used.

CAMERA

If you are licensed for CCTV integration and have a CCTV system enrolled, you can view video footage from within the **Schematic Map** window.

Cameras can be placed on a schematic map as an icon; the icon provides you with the following commands:

- Invoke Command
- Show Video in New Tab
- Show Video in Side Panel

Show Video in Side Panel
This will display live footage from the camera in the Camera tab. If any other camera icon is clicked, the window will automatically change to the selected camera.
If the camera window is not visible in the **Schematic Map** window, click the **View** button and select **Cameras**.
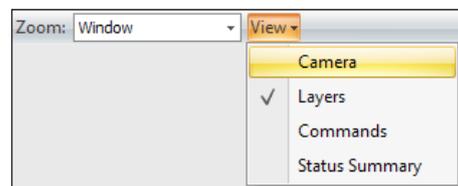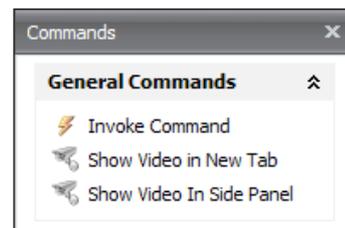
LAYERS

Schematic maps can be configured to contain layers. Layers are a way to group and stack elements on a map. A layer can be made visible or hidden by selecting the **Visibility** check-box.

On a busy schematic map with a large number of icons/shapes, you can hide layers to simplify the map and shift the operators focus on more important items.

You can restrict the layers an operator can view and therefore add or remove map items and commands for an operator. For example, a map can have an administrator layer that has controls and buttons that most operators can not see.

MAP LINKS

If you have more than one schematic map, you may want to navigate from one map to another rather than opening a map from the **Maps** item list.

Some schematic maps are setup so that each map is zooming in or out from the previous map, navigation can be simplified by having a button that returns you to the home/site map.

Map links are a shape, icon, label or image that allow you to navigate between schematic maps.
The following commands are available for map links:

View in New Tab
Opens the linked map in a new tab and the original map remains in the background.

Jump to Map
Opens the linked map in the current tab and replaces the original map.
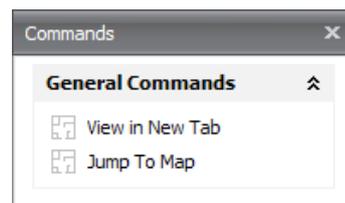
ADDITIONAL MAP FUNCTIONALITY

Depending on how your schematic maps have been setup, the following features may be available to you:

ADDITIONAL COMMANDS

Additional commands can be used to add extra control options to an element on a schematic map.

For example, an image of a large red button could have an additional command to lock down the entire site.

In the Commands window, additional commands will appear at the bottom of the default commands for the linked item.

By default, an additional command will be displayed as a cog icon.
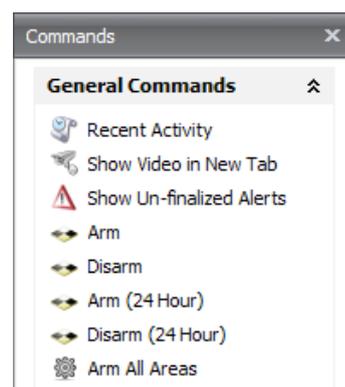
SINGLE CLICK ACTIONS

Single click actions trigger an item action or additional command with a single mouse click; this is useful if the map is displayed on a touchscreen. The default commands are still available by right-clicking the element.

ACTIONS AND COMMANDS REQUIRE VALIDATION

The **Action and Commands Require Validation** option is used to verify that the operator wants to perform the command they clicked.

When the operator attempts to perform a command that is using this feature, the system will prompt them with a confirmation window.

This feature can be applied to only certain elements on a schematic map.
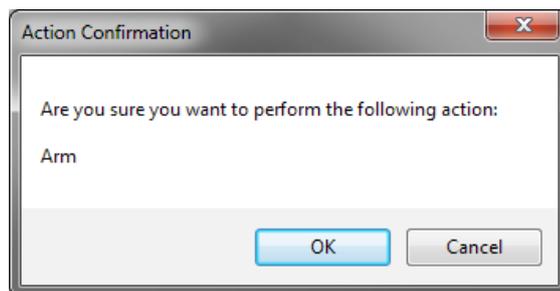
NAVIGATION PANEL

INTRODUCTION TO THE NAVIGATION PANEL

The **Navigation** panel is an ordered list of all the sites, sub-sites, controllers and LAN modules. This panel is only visible in System Designer

The **Navigation** panel allows you to easily find a module, identify its state and make programming changes.

Initially, the Navigation view only contains the default site, as additional sites and controllers are added, the navigation tree will expand.
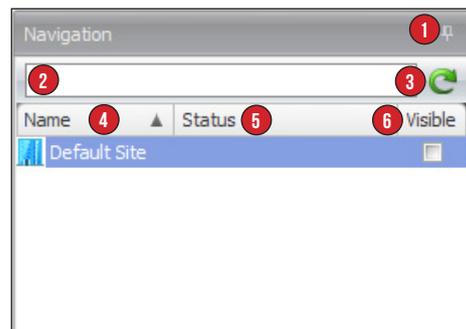
NAVIGATION PANEL BREAKDOWN

1. The **Docking PIN** determines if the navigation bar automatically hides when not in use.

2. The **Search** field filters the items within the **Navigation** panel to entered text

3. The **Refresh** button will refresh the **Navigation** panel if there has been a change made that is not being displayed.

4. The **Name** column contains the names of the site, keywords, controllers and LAN modules.

   All entities in the Navigation panel can be sorted by name in ascending or descending order by clicking on the column heading.

5. The **Status** column displays the state of the Integriti control module, LAN modules and Unibus expanders. This is explained further in the next section.

6. The **Visible** check-box will filter item list to the selected site, controller or module.

   This makes finding an item that relates to a particular site, controller or module much easier.

MODULE STATUS

The **Navigation** panel will display the following status:

Module online

Controller online with modules offline

Controller syncing

Module offline

Controller offline
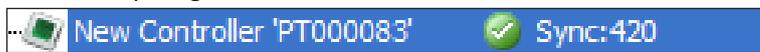
Controller with warnings
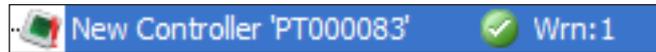
SITE OPTIONS

Right clicking on a site will present you with the following options:

1. The **Site Properties** option opens a menu containing basic site details, CCTV playback buffer and PIN requirements.

2. The **Rename** option allows you to rename the site.

3. The **Export** option will create an IR.Entities file containing all the programming relating to this site. This includes all sub-sites, keywords and controllers.

   This export will not contain software related entities such as operators and operator types.

4. The **Run Site Setup Wizard** option launches the site setup wizard allowing you to configure access cards. This allows you to specify a card template, card format and site code for the site. Any changes will be applied site-wide. In addition to this, the site setup wizard will prompt you to enroll a controller, change the installer password and setup regular backups.

5. The **Add New** menu allows additional sites, controllers and CCTV devices to be added to the **Navigation** panel.
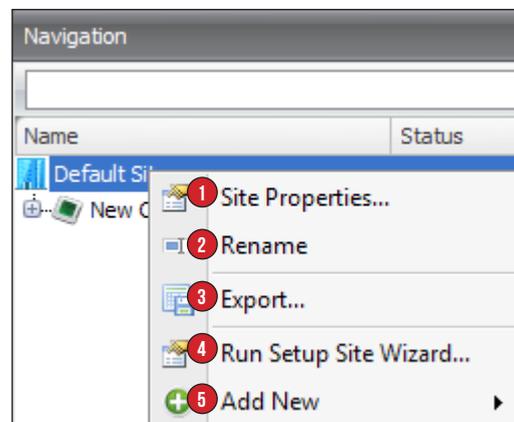
SITE PROPERTIES MENU

The Site Properties menu contains the following settings:

1. The **Site Name** field is used to set the name for the site.

2. The **Default Card Format** field lets you define the card format that will automatically be selected when assigning new cards to users.

3. The **Default Card Template** field lets you define the card template that will automatically be selected when assigning new cards to users.

4. The **Notes** field is used to record any notes for the site.

5. The **Basic Details** section lets you assign contact information for the site including a contact's name, phone number, email and address.

6. The **Automatic Card Expiry** field sets the number of days that a card, when assigned, will remain valid for before automatically expiring. If this value is set to zero, access cards will not automatically expire.

7. The **CCTV Review Playback Buffer** determines how much footage prior to an event is displayed when viewing old footage.

   For example: if this option is set to 10 seconds the footage will start 10 seconds before the event.
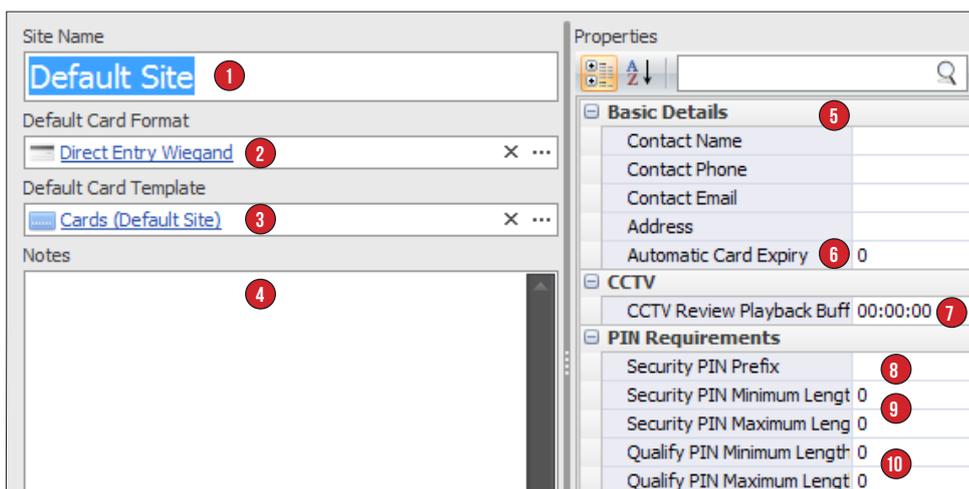
8. The **Security PIN Prefix** is used to add a prefix to the start of the security PIN for all users on the site.

9. The **Security PIN Minimum Length** and **Security PIN Maximum Length** fields are used to restrict the length of users security PIN to a specific number of digits.

10. The **Qualify PIN Minimum Length** and **Qualify PIN Maximum Length** fields are used to restrict the length of users qualify PIN to a specific number of digits.

ADD NEW OPTIONS

The **Add New** menu allows additional sites, controllers and CCTV devices to be added to the **Navigation** panel.

The options available are:
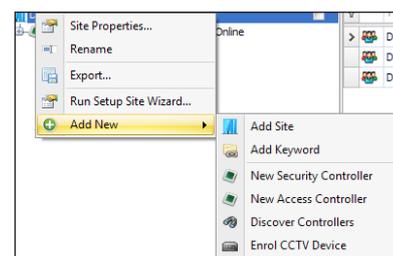
ADD SITE

The **Add Site** option will create a new unnamed sub-site.

1. Once named, the sub site will be located in the hierarchal view below the default site.

2. If a sub site is added to an existing sub site, it will appear nested within the first.
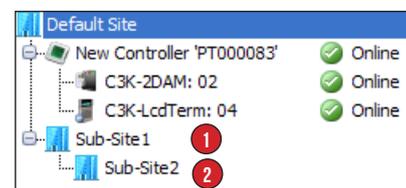
ADD KEYWORD

This option creates a keyword that is located in the selected site.

NEW SECURITY CONTROLLER

This option opens the **Controller Editor** window where a new Integriti Security Controller (ISC) can be programmed.

NEW ACCESS CONTROLLER

This option opens the **Controller Editor** window where a new Integriti Access Controller (IAC) can be programmed.

DISCOVER CONTROLLERS

This option opens the **Discover Controllers** window and will automatically start scanning the local network for controllers.

ENROLL CCTV DEVICE

This option launches the **Plug-in Selection** window where the CCTV system can be selected and then configured.
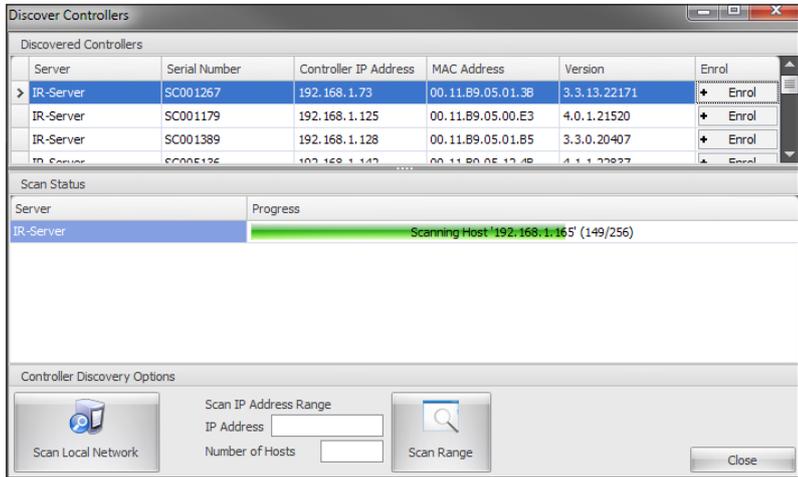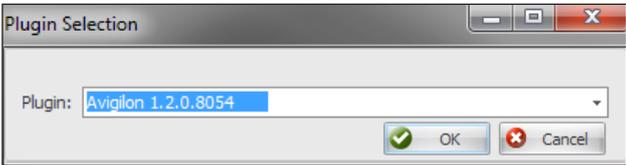
SUB-SITE OPTIONS

The right-click options for a sub-site are identical to a normal site with one exception:

DELETING SUB-SITES

The Delete option will remove the sub-site from the Navigation panel. Since the sub-site may reference a number of other entities within the software, you may find it hard to delete a sub-site.

To solve this you can move entities that reference the sub-site to another site or sub-site.

CONTROLLER OPTIONS

Right clicking a controller will present you with the following options:

1. The **Edit** option will open the **Controller Editor** window allowing you to make programming changes to the controller options.

2. The **Edit in Dashboard** option will open the **Controller** dashboard, which simplifies the programming of the controller. The dashboard also provides the status panel entities such as macros, comms tasks and UniBus devices.

3. The **Delete** command will remove the controller and all of the items on the controller. This will not delete global items such as door lists, area lists or users.

4. The **Export** command will create an IR.Entities file containing all of the Items contained within the panel. This does not contain any global items such as door lists, area lists or users.

5. The **Manage License Keys** command will open the **License Keys for Controller** window that displays the controller serial number, SMART card serial number and the licenses held on the SMART card.

6. The **Browse Controller Files** command will open the file browser for the selected controller. The primary purpose of this window is to upload, rename or delete files located on the controllers Serial Flash, SD Card or a USB Flash Drive.
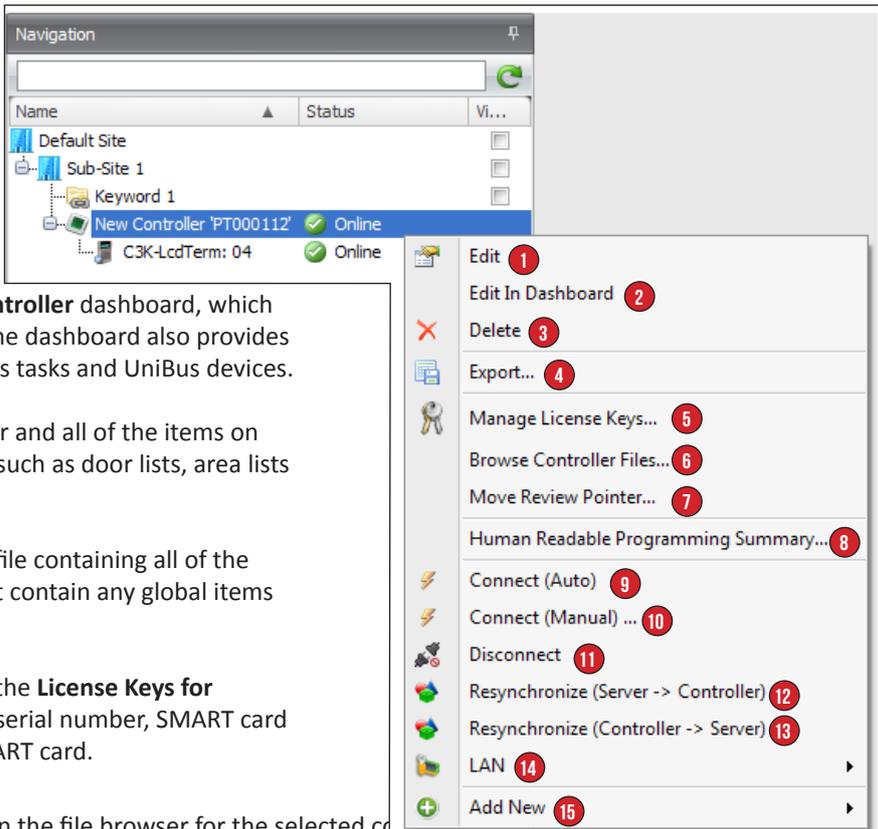
A common use for the **Browse Controller Files** command is to clear the previous versions of firmware stored on the serial flash. If the serial flash storage on the controller is full, no additional files can be copied to this location. This stops any future firmware updates.

In addition to file management, you can use this window to test, install or install and default the controller firmware.

7. The **Move Review Pointer** command will synchronize the specified number of review events on the controller.

This is commonly used if there is a synchronize issue where some review messages are generated by the panel, but do not appear in the software.

The review pointer can be moved back to a certain time or number of events.

8. The **Human Readable Programming Summary** command will generate a full programming summary of your Integriti controller. This will include the inputs, areas, doors etc.

Once generated, the programming summary can be saved or printed.

9. The **Connect (Auto)** command reconnects the panel with the last used connection method.

10. The **Connect (Manual)** command launches the **Connect to Controller** window allowing you to choose the connection method.

11. The **Disconnect** command disconnects the controller from the Integriti software, this includes USB connections.

12. The **Resynchronize (Server -> Controller)** command resynchronizes the current programming held within the Integriti software with the Integriti controller.

13. The **Resynchronize (Controller - > Server)** command resynchronizes the current programming held within the Integriti controller with the Integriti software.

14. The **LAN** menu provides multiple LAN related commands for the currently selected controller.

15. The **Add New** menu allows you to add additional modules to the Integriti controller without having the physical module.

This can be used to create and program a new module before physically connecting it.

Once the module is selected, it will appear in the **Navigation** panel and all related items (such as inputs, auxiliaries etc.) will be created.
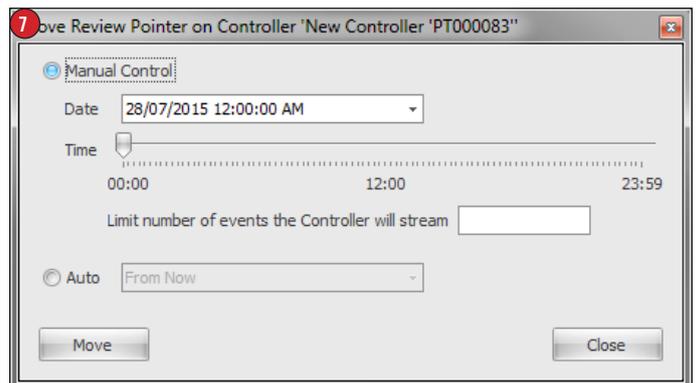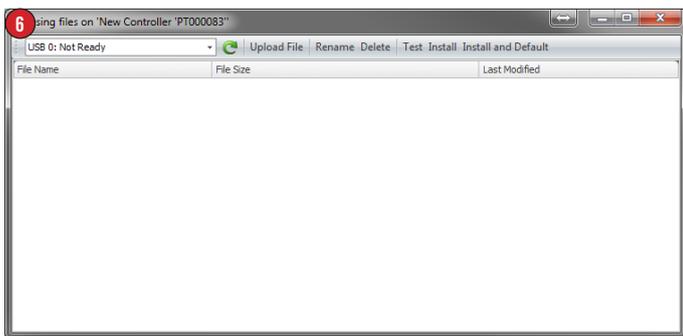
MANAGE LICENSE KEYS MENU

The Manage License Keys menu contains the following:

1. The **Controller Serial Number** and **Smart Card Serial Number** are both displayed in this menu.

2. The **License Key** column contains the unique key associated with each license.

3. The **Description** column provides additional information relating to the licenses.

4. The **Expiry** column displays the expiry information for the licenses.

5. The **Add License Key** button is used to input new license keys.
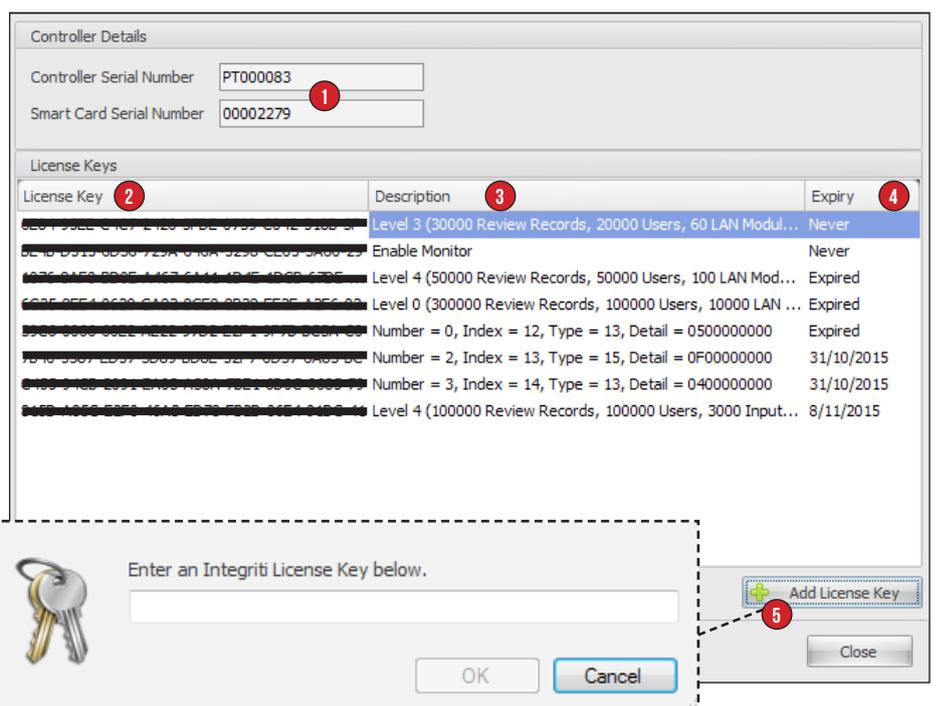
LAN OPTIONS

The **Add New** menu allows additional sites, controllers and CCTV devices to be added to the **Navigation** panel.

The options available are:

LAN	▶	Secure System	1
Add New	▶	Lock LAN	2
		Un-Lock LAN	3
		Hard Reset Controller	4
		Lock out Installer	5
		Reinstate Installer	6
		Beeper On	7
		Beeper Off	8
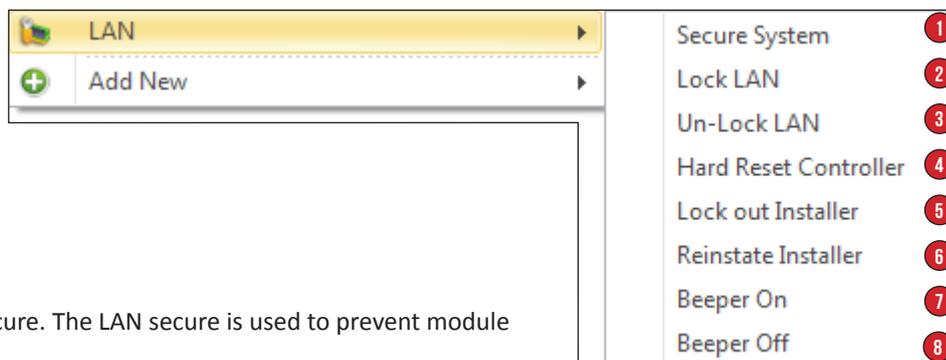
1 : SECURE SYSTEM

This command performs a controller LAN secure. The LAN secure is used to prevent module substitution on the Integriti controller.

The **System Secure** command is the same as the LAN secure function accessible through the LCD terminal (menu 7 - 8 - 1 then 9) for the controller.

2 : LOCK LAN

The **Lock LAN** command prevents any newly attached module from connecting to the Integriti controller.

Modules that are not present at the time the LAN was locked will be ignored by the controller.

To add new modules to the controller, the LAN will need to be unlocked.

3 : UNLOCK LAN

The **Unlock LAN** command removes the LAN lock and will allow new modules to be added to the Integriti controller.

4 : HARD RESET CONTROLLER

The **Hard Reset Controller** command will perform a reset of the selected controller. This function is similar to physically power cycling the controller to reset it.

5 : LOCKOUT INSTALLER

This command is used to stop the installer logging onto a keypad, this is only used in the UK.

6 : REINSTATE INSTALLER

This command is used to allow the installer to log onto a keypad, this is only used in the UK.

7 : BEEPER ON

This command is used to start a beeping noise that can be used to find the control module.

The Integriti Security Controller is not fitted with a beeper, this command will work on an Integriti Access Controller.

8 : BEEPER OFF

This will turn the controllers beeper off.

LAN MODULE OPTIONS

Most of the options in the right-click menu for a LAN module are the same as the right-click options for the Integriti controller.

Some of the options that are unique to certain modules are:

ENABLE ON LAN

This command reverses the **Disable on LAN** command and restores the module functionality.

DISABLE ON LAN

This command allows you to disable the LAN module, this will cause the Integriti controller to ignore the module and the module itself will become unresponsive.

If you disable an Integriti module, the **Enable on LAN** command will restore the modules functionality. However if you disable a older Concept module, the module will need to power cycle the module.

NEW DOOR ON 'LOCK 1/LOCK 2'

This command is available for Access Control modules and keypads. Selecting this command will open the **Door Editor** window, allowing the programming of the door on the selected module, using the selected lock.
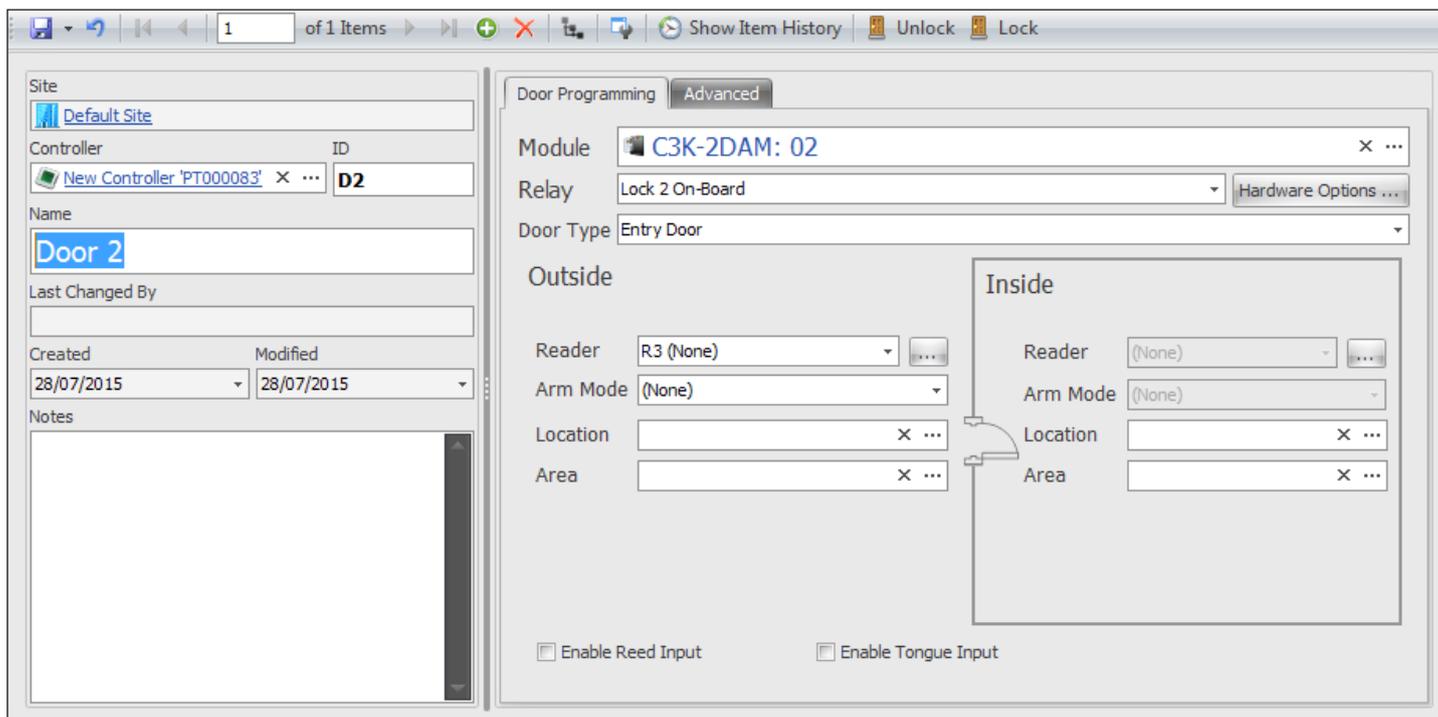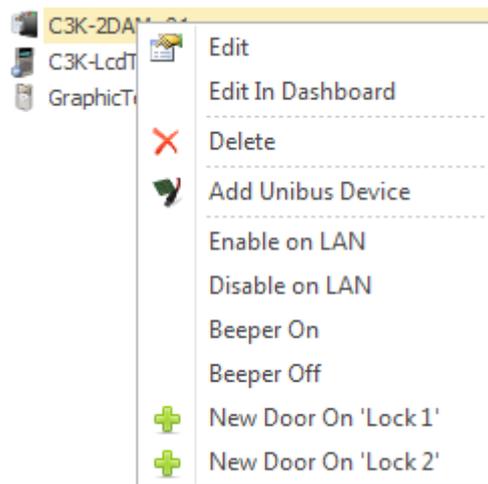
USER COMMANDS (GATEKEEPER)

INTRODUCTION TO USER COMMANDS

Right-clicking a user in GateKeeper will display the following user commands.

1. The **Edit** command will open the **User Editor** window allowing you to make programming changes for the selected user.

2. The **Duplicate** command creates a copy of the currently selected user in the **User Editor** window. This can be used to streamline programming by duplicating similar users and making some minor changes. Be careful not to leave the card number or security PIN the same, as this will cause a credential clash.

3. The **Delete** command will permanently remove the user from the system. You will be presented with a conformation dialogue after clicking the **Delete** command.

4. The **Recent Activity** command provides a filtered review report containing all of the events that relate to the selected user or users for the last one hour. From this window, the duration of the report can be changed and the report can be printed or exported.

5. The **Show Video in New Tab** command will open a new window containing live footage of the associated camera or cameras. This will only work if the selected user is associated to a CCTV camera.

6. The **Show Un-finalized Alerts** command will open a window containing any un-finalized alerts relating to the selected user.

7. The **User-Door Activity Report** command provides a filtered review report containing all of the access events that relate to the selected user or users for the last one hour. This does not contain any review for the lock state or card data. From this window, the duration of report can be changed and the report can be printed or exported.

8. The **User Activity Report** command provides a filtered review report containing all the events that relate to the selected user or users for the last one hour. From this window, the duration of report can be changed and the report can be printed or exported.

9. The **User Reference Report** command provides a report containing all the items that the selected user or users have permission to access; this includes areas, area lists, doors, door lists, permissions groups, menu groups etc.

10. The **Print Card** command uses the **Photo ID** license and allows you to print photo ID cards for users. Clicking the **Print Card** command will open the **Card Print Preview** window.

USER COMMANDS (SYSTEM DESIGNER)

INTRODUCTION TO USER COMMANDS

Right-clicking a user in System Designer will display the following user commands.
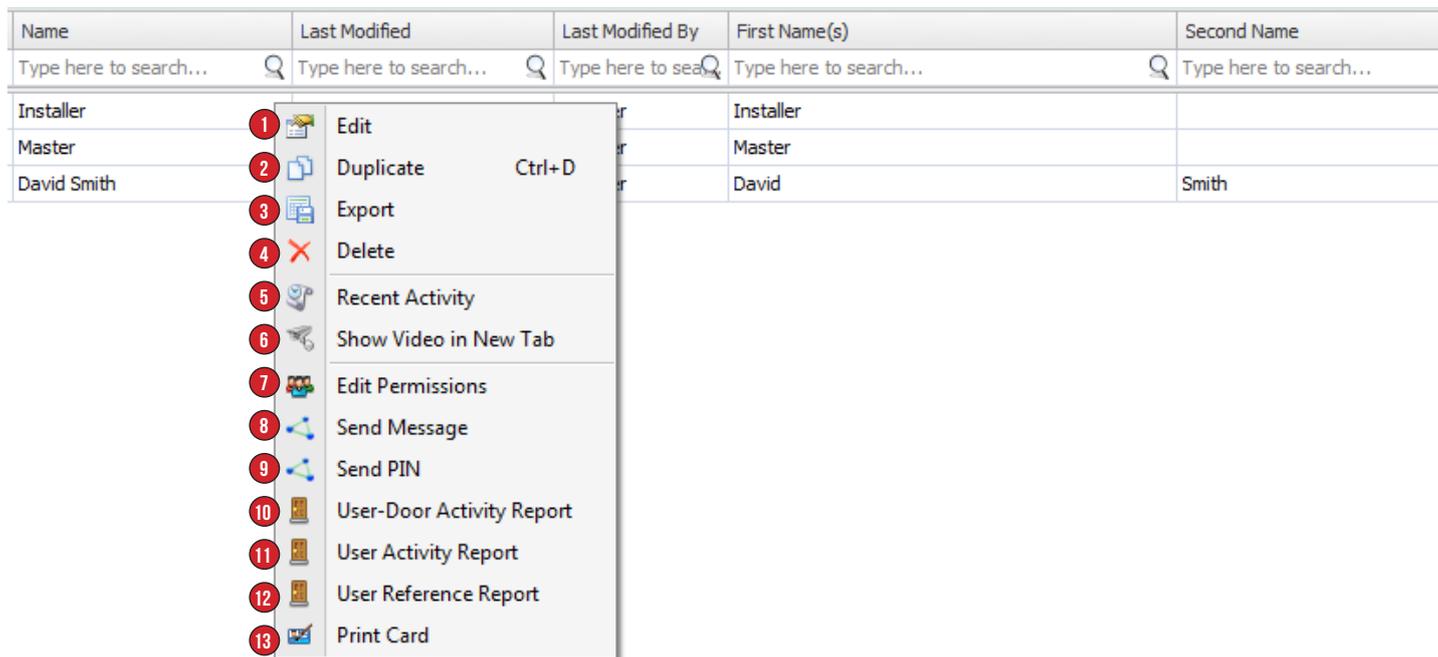
Name	Last Modified	Last Modified By	First Name(s)	Second Name
Type here to search...	Type here to search...	Type here to sea	Type here to search...	Type here to search...
Installer		r	Installer	
Master		r	Master	
David Smith		r	David	Smith

Menu:
1. Edit
2. Duplicate   Ctrl+D
3. Export
4. Delete
5. Recent Activity
6. Show Video in New Tab
7. Edit Permissions
8. Send Message
9. Send PIN
10. User-Door Activity Report
11. User Activity Report
12. User Reference Report
13. Print Card

1. The **Edit** command will open the **User Editor** window allowing you to make programming changes for the selected user.

2. The **Duplicate** command creates a copy of the currently selected user in the **User Editor** window. This can be used to streamline programming by duplicating similar users and making some minor changes. Be careful not to leave the card number or security PIN the same, as this will cause a credential clash.

3. The **Export** button will export the selected user(s) as an IR-entities file.

4. The **Delete** command will permanently remove the user from the system. You will be presented with a conformation dialogue after clicking the **Delete** command.

5. The **Recent Activity** command provides a filtered review report containing all of the events that relate to the selected user or users for the last one hour. From this window, the duration of the report can be changed and the report can be printed or exported.

6. The **Show Video in New Tab** command will open a new window containing live footage of the associated camera or cameras. This will only work if the selected user is associated to a CCTV camera.

7. The **Edit Permissions** option will open the **User Permissions** window, allowing the primary permission group and the extra permissions to be edited without the **User Editor** window being opened. This is used to change the permissions for multiple users at the same time.

8. The **Send Message** command will send an SMS, email or pager message to the selected user or users. This functionality requires the **Communicator** license.

9. The **Send PIN** command will send the security PIN number to the selected user or users. The PIN can be sent as an email or SMS and requires the **Communicator** license.

10. The **User-Door Activity Report** command provides a filtered review report containing all of the access events that relate to the selected user or users for the last one hour. This does not contain any review for the lock state or card data. From this window, the duration of report can be changed and the report can be printed or exported.

11. The **User Activity Report** command provides a filtered review report containing all the events that relate to the selected user or users for the last one hour. From this window, the duration of report can be changed and the report can be printed or exported.

12. The **User Reference Report** command provides a report containing all the items that the selected user or users have permission to access; this includes areas, area lists, doors, door lists, permissions groups, menu groups etc.

13. The **Print Card** command uses the **Photo ID** license and allows you to print photo ID cards for users. Clicking the **Print Card** command will open the **Card Print Preview** window.

CCTV

INTRODUCTION TO CCTV INTEGRATION

The CCTV Integration allows some of the functionality of a third party camera system to be incorporated into the Integriti Software. This allows an operator to view live and historical CCTV camera footage and even control PTZ cameras.

The setup and configuration of the CCTV Integration is usually done by a Certified Technician.

VIEWING CCTV FOOTAGE FROM A CAMERA

To view the live footage from a CCTV camera in GateKeeper, select the Home tab and click on the CCTC Cameras icon.
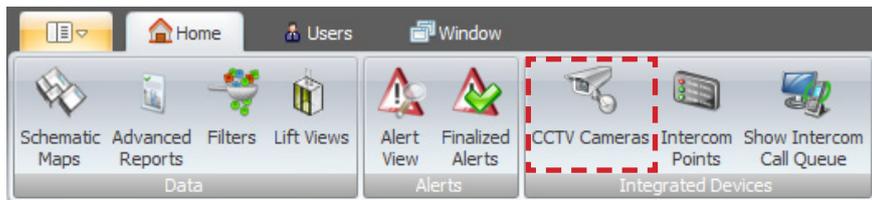
This will launch the CCTV Cameras list that contains all of the cameras that can be viewed by the operator.
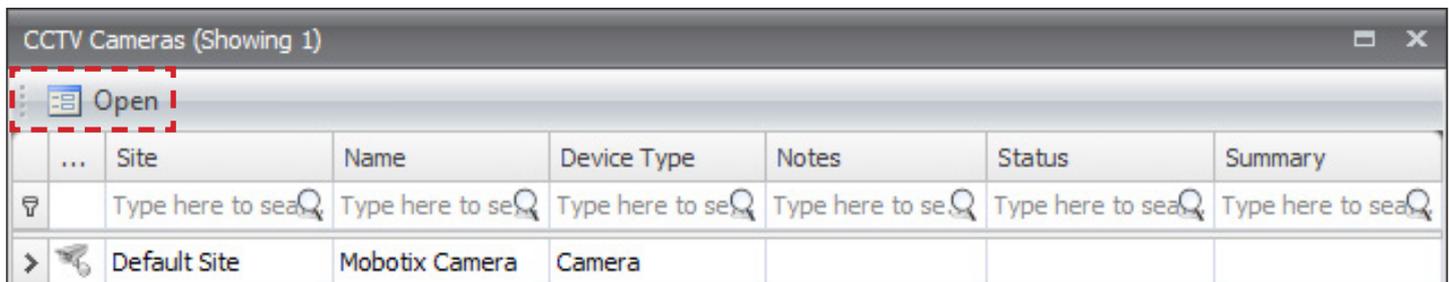
To view the live footage from a camera, select the Camera and click the **Open** button or double-click on the camera.

A new window will open containing the live footage.
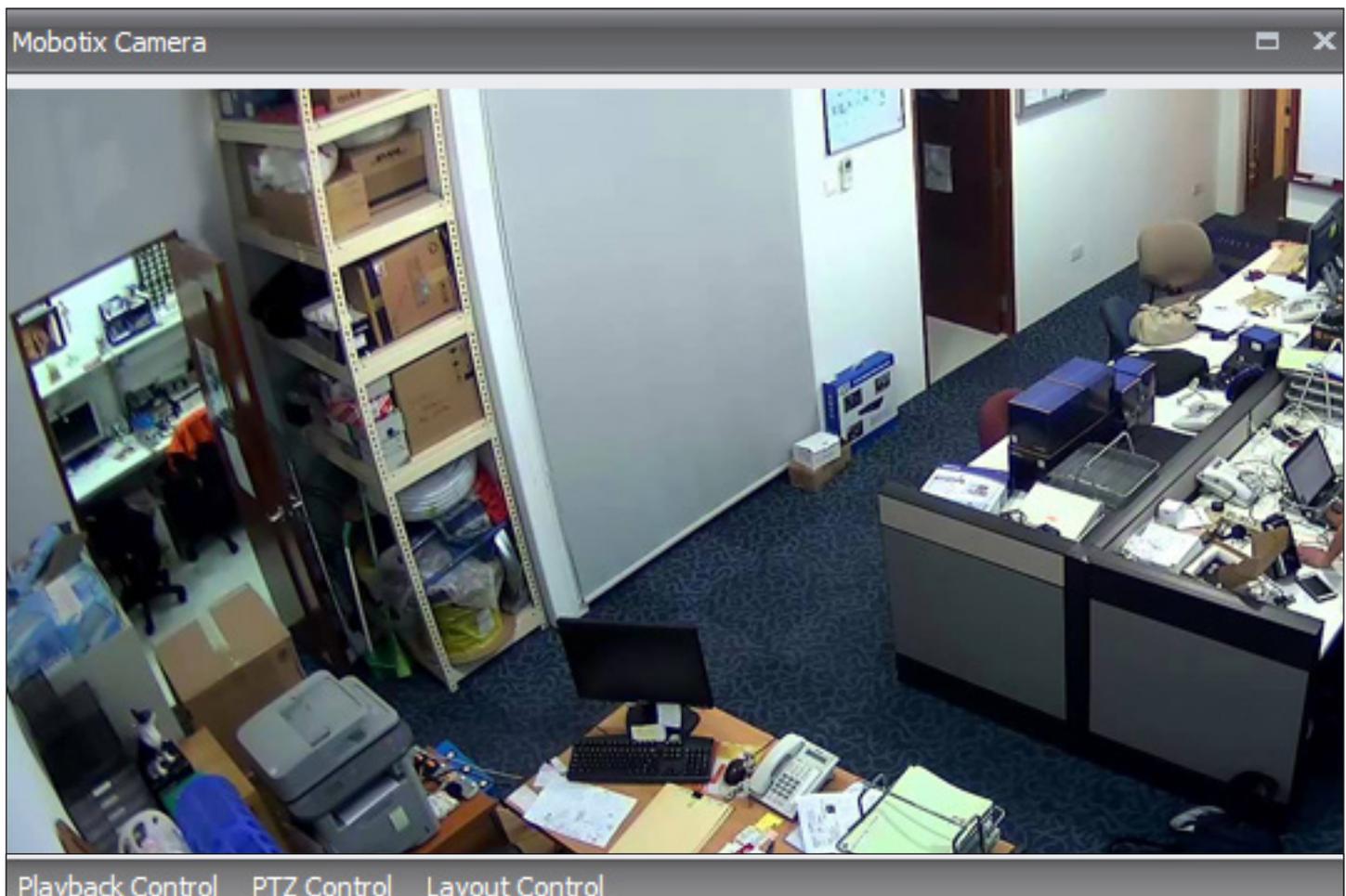
VIEWING HISTORICAL FOOTAGE

In some cases, the CCTV cameras are associated to areas, doors, inputs or outputs in your system. You can view historical footage from the camera by finding the event you would like to see in the **Review** window.

Once you have found the event, right-click the Review Record and select the **Show CCTV Footage** option.
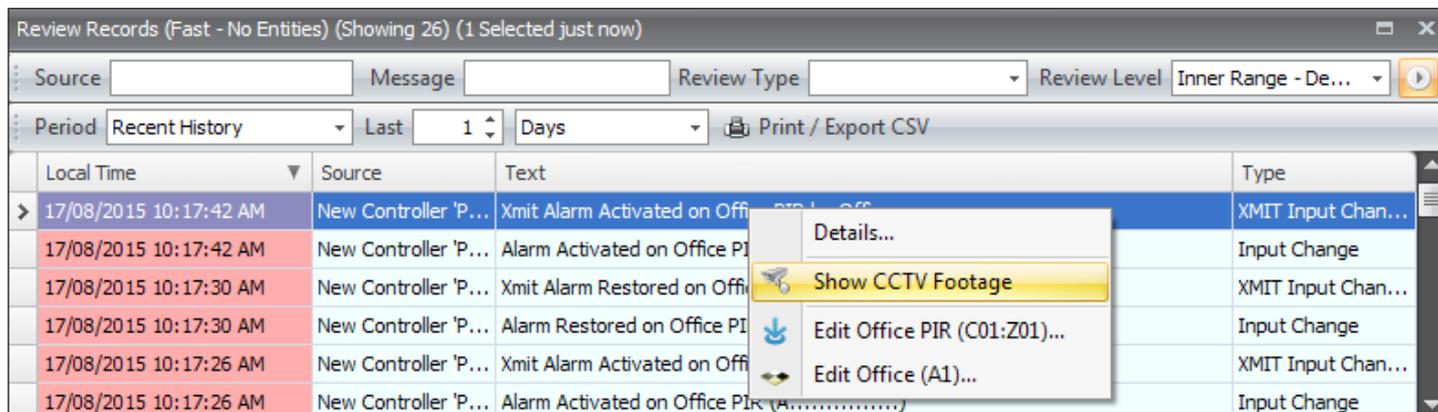
A new window will open containing the historical footage that matches the date and time that the event occurred.

This will only work if there is footage available to view, this may be restricted by the storage space available to the CCTV system.

AUTOMATIC CCTV POP-UPS

If configured, live CCTV footage can pop-up in the Integriti GateKeeper software, this pop-up is based on a particular event. This is commonly used when live footage is required to be seen by an operator for an event such as a duress or panic button being pressed. This functionality requires that either alerts or scheduled tasks are configured.

CONTROLLING THE PLAYBACK OF FOOTAGE

Once you open the camera window, the footage can be controlled with the playback controls, found in the **Playback Control** tab.

DATE & TIME SELECTOR

The **Date & Time** field is used to retrieve footage from a certain time by entering the date and time of the event.
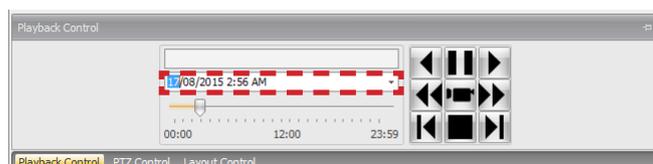
Alternatively the **Date & Time** drop down is used to select the date using a calendar preview.
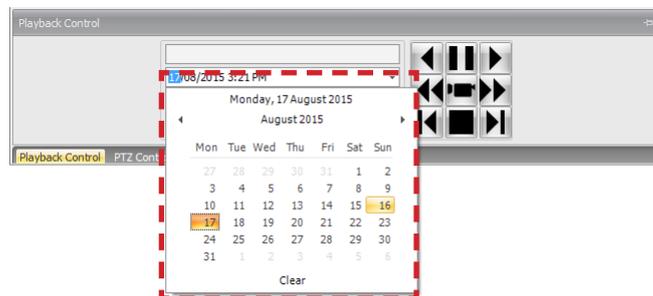
Once the date has been set, the time can be set using the **Time** slider.

Drag the slider to the nearest time to the time the event occurred. The time slider is in a 24-hour format.
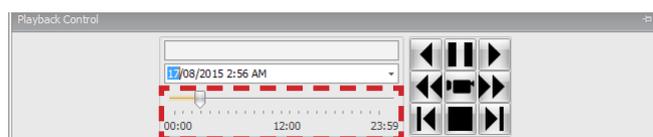
As the time slider is changed, the date and time selector will update.

This is the start time that is used when using the other playback controls.
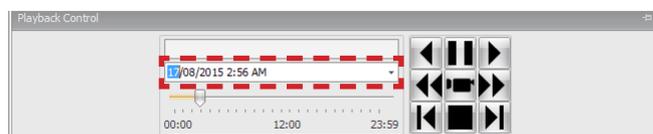
PLAYBACK BUTTONS

The playback buttons allow you to easily play, rewind, fast-play and pause CCTV footage.

The controls below will differ from one CCTV system to another.
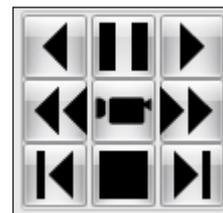
PLAY

This button plays the footage forward at normal speed.

FAST FORWARD

This button plays the footage forward at high speed; each click increases the speed of playback.

REWIND

This button plays the footage backwards at normal speed.

FAST REWIND

This button plays the footage backwards at high speed; each click increases the speed of playback.

PAUSE

This button will pause the footage on the current frame.

LIVE VIEW

This button display live footage from the CCTV camera.

STEP FORWARD

This button advances the footage one frame at a time.

STOP

This will stop the current footage stream.

STEP BACKWARD

This button rewinds the footage one frame at a time.

CONTROLLING A PTZ CAMERA

If you have a PTZ (Pan, Tilt and Zoom) CCTV camera you can control the PTZ functionality via Integriti GateKeeper or System Designer.

Select the **PTZ Control** tab to view the PTZ controls, some of these commands may not work based on your camera's capabilities.
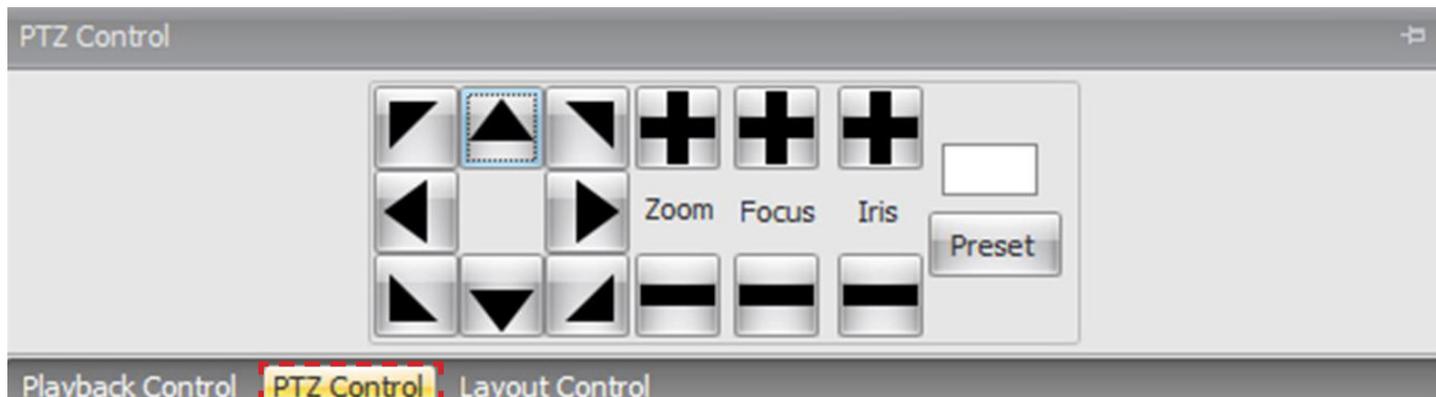
PLAYBACK BUTTONS

The directional arrows are responsible for the pan and tilt of the camera. Single-clicking an arrow will move the camera in the direction you clicked.

If the arrow is clicked and held down, the camera will move until the button is released.
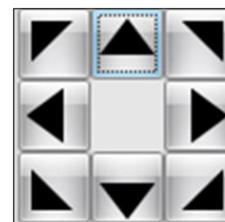
ZOOM

The zoom buttons control the amount that the camera is zoomed in or out.

The "+" button increases the amount of zoom and the "– "button decreases the amount of zoom.
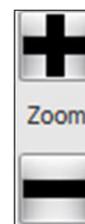
FOCUS

The focus buttons control the area that the camera is focused on, this may be used to bring a foreground object into focus.

The "+" and "–" buttons shift the focal area forward or backward.

IRIS

The iris control will result in more or less light entering the camera through the lenses. This is used to increase or decrease the brightness of the camera footage.

The "+" button increases the amount of light reaching the camera and the "–" button decreases it.
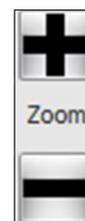
PRESET

If the CCTV camera has been configured to use preset locations, you can trigger the camera to move to a preset by using the preset field.

Once a preset number has been entered, clicking on the Preset button will result in the camera moving to that particular preset location.

VIEWING MULTIPLE CAMERAS

In some cases an area, door, input or auxiliary may be associated to more than one camera, when viewing historical footage the **Camera** window will contain more than one camera.

The number of cameras viewed at once can be changed by using the **Layout Control** tab found in the **Camera** window, this will work for historical and live footage.

The layout of the camera window can be set to: 1x1, 2x2, 3x3 or 4x4.

1 X 1
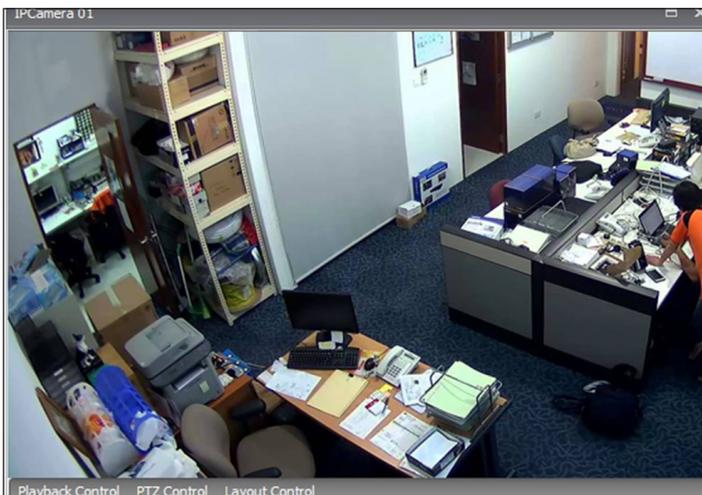
2 X 2
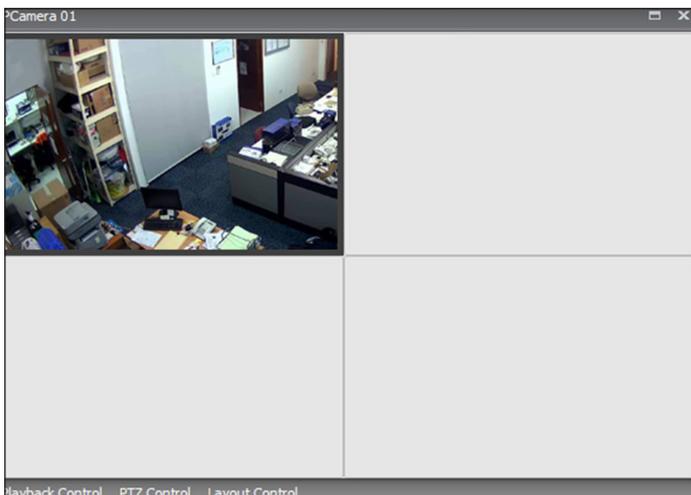
3 X 3
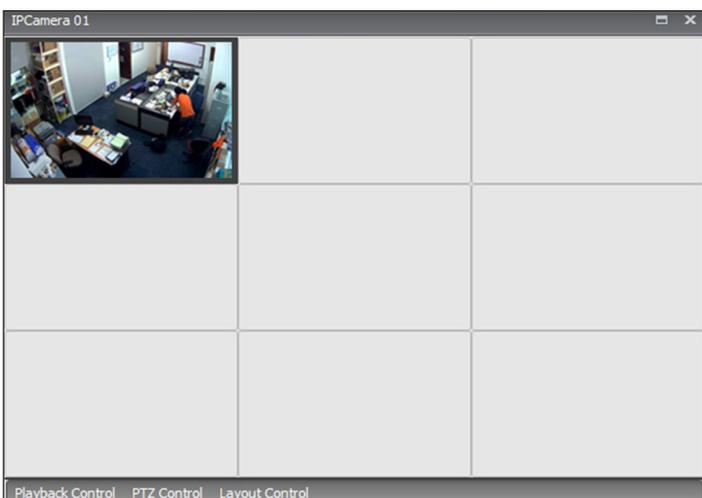
4 X 4
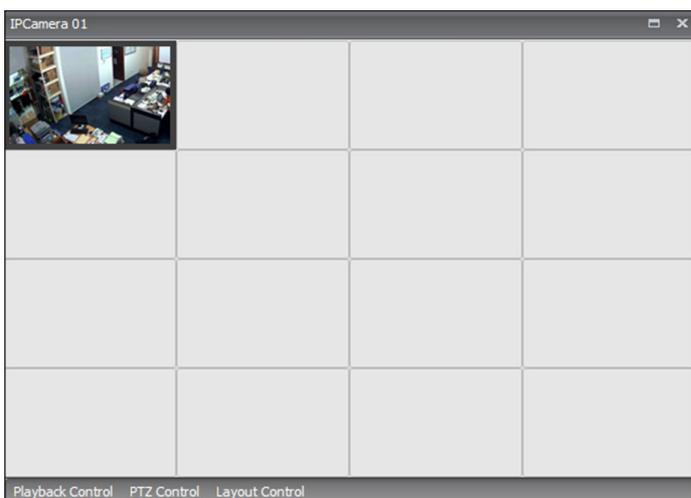
Once you have selected a camera layout, drag additional cameras onto the **Camera** window to be displayed. Closing the **Camera** window will reset the layout.

OPERATORS

INTRODUCTION TO OPERATORS

Operators are the users who login to the Integriti System Designer or GateKeeper software.

Most programming changes to the Integriti system are audited, this audit includes the operator that made the change. It is recommended that each user logging into the software has a unique operator name and password.

To view, edit, create or delete operators navigate to the **Administration** tab and click the **Operators** icon.

OPERATOR EDITOR WINDOW

The **Operator Editor** window is broken down into five sections:
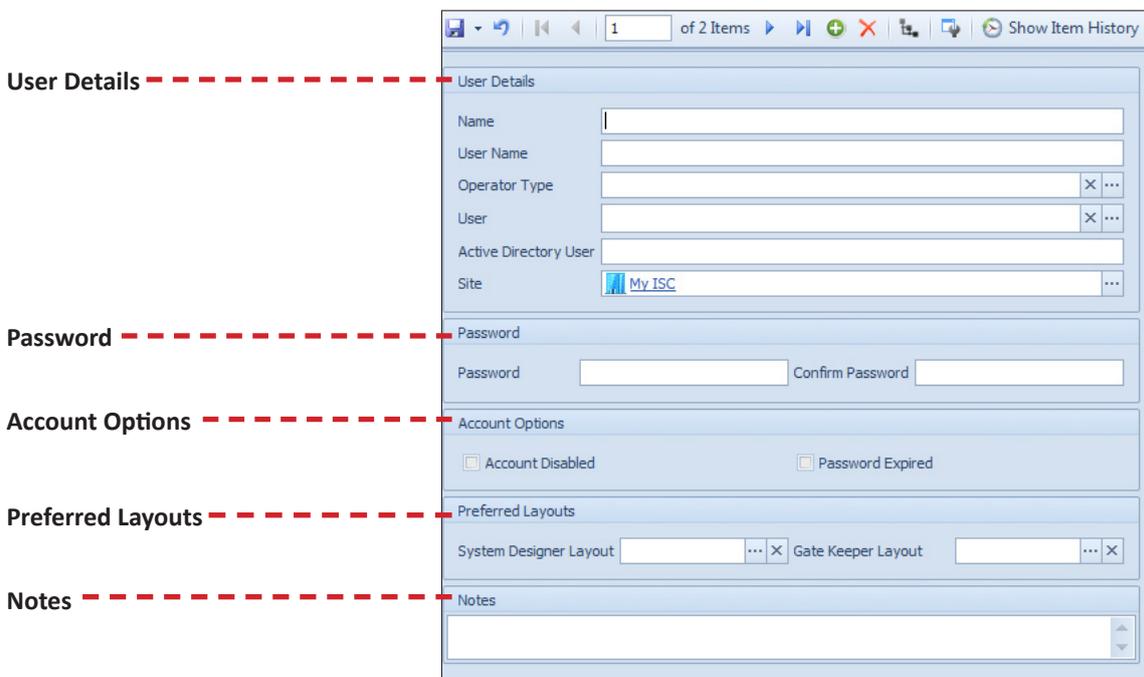
USER DETAILS

1. The **Name** field is used to identify the operator.

2. The **User Name** field is used by the operator to log-in to the Integriti Professional or GateKeeper software.

3. The **Operator Type** determines the permissions/access levels that the operator has.

4. The **User** field allows a user in the controller to be assigned to the operator. The operator will only be able to control items as assigned to the user.

5. **Active Directory User** allow users to login to the Integriti software using their window credentials. Active Directory is a licensed feature

6. The **Site** field sets the default site for any entities that the operator creates (areas, doors, etc.)
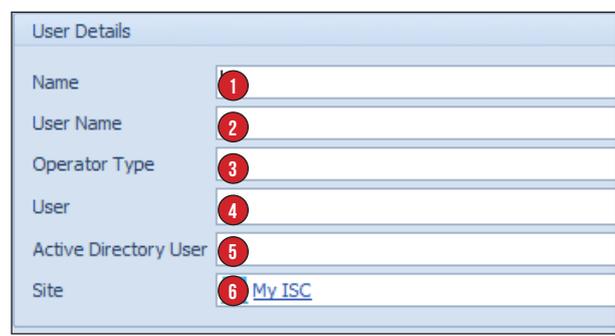
PASSWORD

1. The **Password** and **Confirm Password** fields are used in conjunction with the User Name field to allow operators to log into the Integriti Professional or Integriti GateKeeper software.

ACCOUNT OPTIONS

1. Enabling the **Account Disabled** option will disable the operator and prevent them from logging in.
2. Enabling the **Password Expired** option will force the operator to change their password the next time they log in.

PREFERRED LAYOUTS

The Preferred Layouts are used to define the default layout for the operator when they first log in.

1. The **System Designer Layout** field defines the default layout for the Integriti Professional software.

2. The **GateKeeper Layout** field defines the default layout for the Integriti GateKeeper software.

ASSIGNING USERS TO OPERATORS

The user section allows a user in the system to be assigned to the operator, the operator will only be able to control the items that are assigned to the users permissions. When user is assigned to an operator and the operator controls an item such as a door, the system will generate a review message that contains the user. Below are examples of an operator unlocking a door from the software with and without a user assigned.

WITHOUT AN ASSIGNED USER

| 8/07/2015 4:29:01 PM | SAMSUNG INC | Front Door Unlocked by Comms Task 01 (Integriti CT) (Integriti) (remote) (D022) |

The message describes the event correctly, however there is no information regarding the individual responsible for remotely unlocking the door.

WITH AN ASSIGNED USER

| '07/2015 4:32:26 PM | SAMSUNG INC | Front Door Unlocked by Rob Steed (Integriti) (remote) (D022) |

The review message now contains both the event and the user responsible. For tracking and auditing purposes, it's recommended that all operators who control system entities, such as areas, doors, lift cars etc have an associated user.

If the operator attempts to control an item that their assigned a user does not have permission to control, the following review message will be generated:

| 9/07/2015 8:56:28 AM | SAMSUNG INC | Area Action by Rob Steed (Integriti) (remote) failed in queue 4 because Not Allowed |

ACTIVE DIRECTORY USERS

If **Active Directory Operator** authentication is enabled it will allow users to sign on with their currently logged-on windows account or with the provided Active Directory credentials. This can provide a single sign on (SSO) type functionality to the Integriti software. An Active Directory Operator License is required.

There are two methods that can be used to link Active Directory users to Integriti Operators:

Via Operators
Individual operator records can be manually linked to a domain account.

Via Operator Types
Active Directory Groups can be linked to Integriti Operator Types. Operators are created and controlled by domain administrators.

OPERATOR TYPES

INTRODUCTION TO OPERATORS TYPE

Operator Types determine what items and features an operator can access within the Integriti System Designer or GateKeeper software. The relationship between an operator and the operator type is similar to the relationship between the user and a permission group.

To create, edit or delete an operator type navigate to the **Administration** tab and click the **Operator Types** icon.

CREATING AN OPERATOR TYPE

It is quicker to duplicate an operator type such as **Master** and edit it rather than adding a new operator type and starting from scratch.

Right-click an operator type and select **Duplicate**, this will create an unnamed copy. The **Operator Type** window contains the following items:
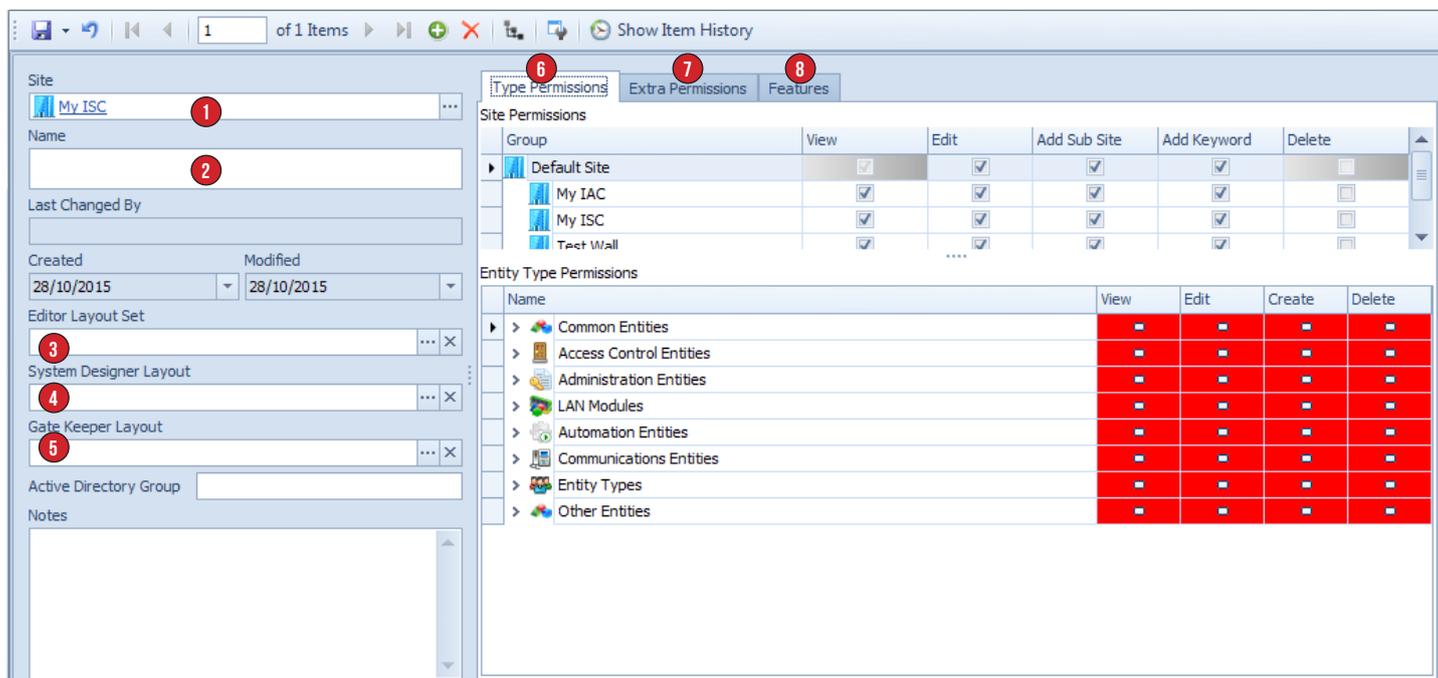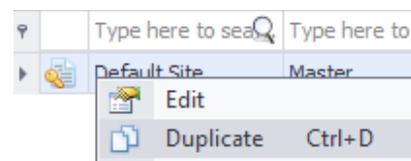
1. The **Site** field is used to identify which site the operator type belongs to.

2. The **Name** field is used to identify the purpose and contents of the operator type. i.e. Security Guard

3. The **Editor Layout Set** determines the appearance of the editor window for each item. This editor layout will load for any operator assigned this operator type. If left empty the default editor layout is used.

4. The **System Designer Layout** determines the appearance of the System Designer software. This layout will load for any operator assigned this operator type. If left empty the default System Designer layout is used.

5. The **GateKeeper Layout** determines the appearance of the GateKeeper software. This layout will load for any operator assigned this operator type. If left empty the default System Designer layout is used.

6. The **Type Permissions** tab determine the groups of items an operator can view, edit, create or delete. Permissions for items can be assigned separately for sites and sub-sites.

7. The **Extra Permissions** tab allows you to set permissions for individual items such as specific door or a specific user.

8. The **Features** tab determine the additional functionality the operator will have in the System Designer or GateKeeper software.

THE TYPE PERMISSIONS TAB

SITE PERMISSIONS

Site Permissions					
Group	View ①	Edit ②	Add Sub Site ③	Add Keyword ④	Delete ⑤
▶ Site A	☑	☑	☑	☑	☐
Site B	☑	☑	☑	☑	☐

1. Enabling the **View** option allows the Operator to see the site in the **Navigation** panel. The **View** option can not be disabled for the default/top site.

2. Enabling the **Edit** option allows the operator to edit the properties of the site such as the site name.

3. Enabling the **Add Sub Site** option allows the operator to add sub-sites to the selected site.

4. Enabling the **Add Key Word** option allows the operator to add a keyword the site.

5. Enabling the **Delete** option allows the Operator to delete the site. The **Delete** option can not be enabled on the default/top site.

ENTITY TYPE PERMISSIONS

Entity Type Permissions				
Name	View ①	Edit ②	Create ③	Delete ④
▶ > 🔧 Common Entities	✓	▪	▪	▪
> 🚪 Access Control Entities	▪	▪	▪	▪
> 📄 Administration Entities	✗	▪	▪	▪
> 🖧 LAN Modules	▪	▪	▪	▪
> ⚙ Automation Entities	▪	▪	▪	▪
> 📠 Communications Entities	▪	▪	▪	▪
> 👥 Entity Types	▪	▪	▪	▪
> 🔧 Other Entities	▪	▪	▪	▪

1. The **View** check-box allows the operator to view the item for the currently selected site.

2. The **Edit** check-box allows the operator to edit the item for the currently selected site.

3. The **Create** check-box allows the operator to create the item for the currently selected site.

4. The **Delete** check-box allows the operator to delete the item for the currently selected site.

You will notice there is 4 selectable options to choose from:

Allow

Inherit Allow (this inherits permissions from the parent site)

Deny

Inherit Deny (this inherits permissions from the parent site)

EXTRA PERMISSIONS TAB

	Type Permissions	Extra Permissions	Features					

	Deny	Entity	View	Edit	Delete	Change Per...
⚲	▣		▣	▣	▣	▣

The **Type Permissions** tab provides an operator permission to view, edit, create or delete an entire group of items. This means that if an operator is provided the permission to edit users there is no restriction on which users they can edit.

The **Extra Permission** tab is used to add and remove permissions for single items. For example, you may have an operator that has permission to edit users, however you want to stop them from editing the **Installer** user. To do this, add an extra permission that denies the edit permission for the **Installer** user.

The example below demonstrates how to restrict an operator from viewing a single user:

1. In the **Type Permissions** tab the **Common Entities > User** options to view, edit and create users are enabled. This allow the operator to view and edit all users.

Name	View	Edit	Create	Delete ▲
▼ 🎡 Common Entities				✗
👤 User	✔	✔	✔	✗

2. In the **Extra Permissions** tab the **Installer** user is added and the **Deny** and **View** options are enabled to stop the operator viewing the Installer user.

	Type Permissions	Extra Permissions	Features

	Deny	Entity	View
⚲	▣		▣
⌶	☑	👤 Installer	☑

The example below demonstrates how to increase an operators permissions using extra permissions.

1. In the **Type Permissions** tab the **Common Entities > User** option only allow the operator to view users. The operator can open and view users however changes will not be saved.

Entity Type Permissions			
Name	View	Edit	Create
▼ 🎡 Common Entities		✗	✗
👤 User	✔	✗	✗

2. In the **Extra Permissions** tab two users are added and the **View** and **Edit** options are enabled. This allows the operator to edit just these two users.

	Type Permissions	Extra Permissions	Features

	Deny	Entity	View	Edit
⚲	▣		▣	▣
	☐	👤 Steve Jones	☑	☑
▶	☐	👤 Tom Smith	☑	☑

FEATURES TAB

The **Features** tab allows you to enable access to specific features within the System Designer and GateKeeper software.

These features are broken up into seven sub-categories:

1. Administration
2. Review
3. Controllers

4. Licensing
5. Layout
6. Integration

7. Software Modules

ADMINISTRATION

The **Import Data** option allows operators to access the **Import Data** feature from the **Administration** tab.

The **Can Administer Servers** option allows operators to view servers, workstations and client connections from the **Administration** tab.

The **View Audit** option allows operators to view a historical log of all programming changes to system items.

The **Reveal PINs** option allows an operator to view other users PINs.

The **Send PINs** option allows an operator send a PINs to users via e-mail or SMS, this feature is used when a user forgets their PIN. A license is required to send SMS or emails from the Integriti software.

The **Force Finalize Alerts** option allows an operators to finalize (close) one or more alerts without writing a response.
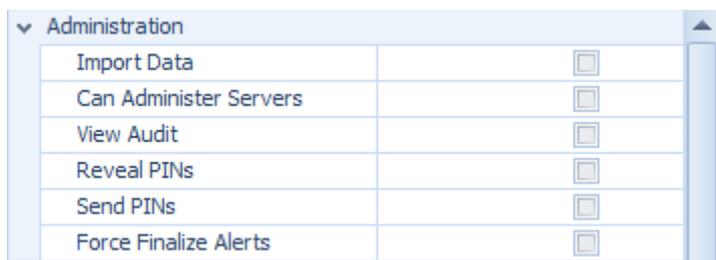
REVIEW OPTIONS

The **View Review** option allows operators to see review.
The **Highest Review Level** determines the highest level of review that the operators will have permission to view.
The review levels are:

1. Everyone
2. User - Essential
3. User – Standard

4. User – Detailed
5. Installer – Detailed
6. Inner Range - Debug

CONTROLLERS OPTIONS

The **Send Actions** option allows operators to control items such as areas, doors or outputs from the System Designer or GateKeeper software.

The **Enroll Controllers** option allows operators to add new controllers to the site from the System Designer software.

The **Upgrade Controller Firmware** allows the operator to upgrade the firmware of the Integriti controller and hardware modules.

View Controller Data allows operators to view controller related information and data such as hardware licenses.

The **Lock/Unlock LAN** option allows operators to perform a LAN lock on integriti controllers, once the LAN is locked no modules can be added to the system until the operator unlocks the LAN. This option should only be enabled for the Installer or site administrator.

The **Remote Hard Reset Controller option** allows operators to reset on a controller via the Integriti software. A hard reset will disable all security and access control for about a minute. This option should only be enabled for the Installer or site administrator.

The **Disable/Enable LAN Modules** option allows operators to disconnect or connect a LAN modules to the Integriti controller. Disabling a LAN module may result in doors, inputs or automation not working correctly. This option should only be enabled for the Installer or site administrator.

The **Can Allow Keypad Edit** option allows operators to change the data synchronization mode for a controller; this can be used to enable or disable programming changes from a keypad. This option should only be enabled for the Installer or site administrator.

The **See Blank Entities** option allows operators to see a list of all blank entities currently present in the system.

LICENSING

The **Can Manage Licenses** option allows operators to add software and hardware licenses to the Integriti System Designer software. To add licenses click the **Administration** tab and select **License Manager**.

LAYOUT

The **Can Move Dock Windows** option allows operators to change the location of windows for the Integriti System Designer and GateKeeper software.

The **Can Switch Dock Layouts** option allows operators to load System Designer or GateKeeper layouts.

The **Can Use Personal Layouts** option allows operators to keep the changes they make to a layout after exiting the software. Their personal layout will automatically be loaded when they next login to the software

INTEGRATION

The Enroll Integration Device option allows operators to enroll new third party devices such as CCTV recorders or intercom systems.

SOFTWARE MODULES

The **System Designer** option allows the operator to log into the System Designer software. This option can be disabled to provide the operator with access to only GateKeeper.

The **GateKeeper** option allows the operator to log into the GateKeeper software. This option can be disabled to provide the operator with access to only System Designer.

The **Client Timeout Mode** is used to automatically log an operator out of the Integriti software. The mode can be set to auto log-out after no system activity, this mode uses the time specified in the **Inactivity Timeout Time.**

The **Inactivity Timeout Time** determines how long the operator needs to be inactive before the system automatically logs them out.

CUSTOM FIELDS

INTRODUCTION TO CUSTOM FIELDS

Custom fields allow you to add fields to almost any programmable item in the Integriti Software. These custom fields allow you to capture or display extra information that is otherwise not present in the default Integriti menus. For example: a users date of birth or driver's license number.

To access the Custom Fields menu, you must navigate to the **Administration** tab and select **Custom Fields**
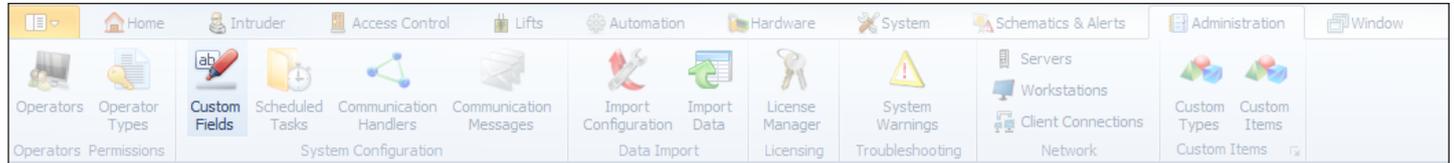
CREATING A CUSTOM FIELD

When creating a custom field, you will be presented with the following menu:

1. The **Key Name** field allows you to create a database name for this custom field. This is particularly useful if you are going to use this custom field in a report. It is a recommended standard that all custom field key names contain the cf_ prefix.

2. When creating a custom field you have the option of selecting an **Item Type**. This will determine where the field will appear.

3. **Field Type** setting allows you to define the type of data that the custom field will contain. These field types ensure that operators are capturing the data in the correct format.

FIELD TYPES

Field Types allow you to define the type of data that the custom field will contain. These field types ensure that operators are capturing the data in the correct format. Below is a list of available field types:

Text	A simple text field up to 8000 Characters.
Notes	A multi-line 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
Currency	A monetary value
Date and Time	A combination of the following 2 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 ticked
Editable Drop Box	A drop down list of selectable items, you may enter custom text
Drop Down Box	A drop down list of selectable items
Email Address	An Email address field
Telephone Number	A Telephone number field (no spaces required)

DEFAULT VALUE

If you specify a Default value then this will be displayed in the field unless changed by the operator.

MANDATORY

If the Mandatory check box is enabled an operator will not be able to save the changes to an item without entering the custom field.

CUSTOM FIELD EXAMPLE

A commonly used custom field is a users email address. The **Email Address** field can be used to send the user emails containing their PIN number or alert messages.

Creating email custom field:

1. Name the custom field.
2. Select **Email Address** from the **Field Type** option.
3. If the field has to be entered by an operator flag the **Mandatory** field.
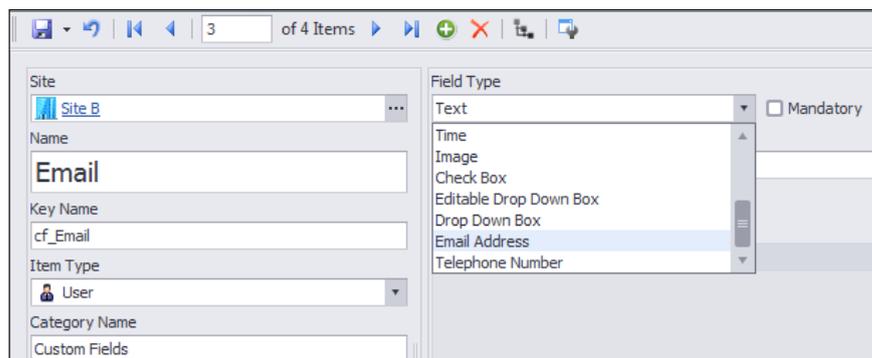
The **Email** custom field bellow will appear in the **User Editor** window

BUILT IN REPORTS

INTRODUCTION TO BUILT IN REPORTS

You can run basic user or door reports from the Integriti Software. These reports can identify what doors a user can access or which users have accessed a door in the last 24 hours.

RUNNING A USER BUILT IN REPORT

Select one or more users and right click to view the user options. The following user reports are available:

USER DOOR ACTIVITY REPORT

This report displays review events for each time the selected user or users accessed a door in the period specified. This includes door access events where the user is granted access or denied.

USER ACTIVITY REPORT

This report displays all the review events that relate to the selected user or users in the period specified. This includes door access events, keypad login and logout.

USER REFERENCE REPORT

This report displays the permissions assigned to the selected user or users.

RUNNING A DOOR BUILT IN REPORT

Select one or more doors and right-click to view the door options. The following user reports are available:

DOOR USER ACTIVITY REPORT

This report displays review events for each time a user accesses the selected door in the period specified. This includes door access events where the user is granted access or denied.

DOOR USER REFERENCE REPORT

The report displays the users with permission to access the selected door or doors.

BUILT IN REPORTS WINDOW

Once you select a report; the report window will open. Below is an example of the User-Door Activity Report:

1. The **Period** filter sets the range of dates and times that the report includes. You can select either a date range or number of days.

2. The **Local Time** column shows the date that the event occurred.

3. The **Source** column displays the controller that generated the review message.

4. The **Text** column displays the logged information for the event that occurred.

5. The **Type** column displays the category of the review event.

6. The **Print/Export** button will print or save the contents of the report to a PDF or CSV file.

REVIEW

INTRODUCTION TO REVIEW

Review is a historical log of the events that occur in the Integriti System. These events can be created by the Integriti controllers, the Integriti application or even third party devices such as CCTV systems.

Review is commonly used to find historical evidence of an event, such as finding out which users accessed a particular door on a particular date. Review can also be used to generate advanced reports such as **Time on Site** reports for payroll.

The **Review** window below appears in System Designer and GateKeeper by default.

Local Time		Source		Text		Type	
29/10/2015 11:30:36 AM		New Controller 'S...		Installer Security Pin code changed by Installer (C3K-LcdTerm: 01)		Pin Changed	
29/10/2015 11:30:28 AM		New Controller 'S...		Installer Pin Logon at C3K-LcdTerm: 01		User Access	
29/10/2015 11:29:24 AM		New Controller 'S...		Installer Logoff at C3K-LcdTerm: 01		User Access	
29/10/2015 11:29:04 AM		New Controller 'S...		Installer Pin Logon at C3K-LcdTerm: 01		User Access	
29/10/2015 11:29:02 AM		New Controller 'S...		Installer Logoff at C3K-LcdTerm: 01		User Access	
29/10/2015 11:29:01 AM		New Controller 'S...		Installer Access at C3K-LcdTerm: 01 (Door not defined) Denied - No Location		User Access	
29/10/2015 11:29:01 AM		New Controller 'S...		Installer Pin Logon at C3K-LcdTerm: 01		User Access	

1. The **Local Time** column displays the date and time that the review event was generated.

2. The **Source** column displays the name of the device that generated the review event. Controller based events will display the name of the controller. Alternatively, there may be review events generated by the Integriti application which will have the source AppServer: IntegritiApplicationServer.

3. The **Text** column contains the review message.

4. The **Review Type** column displays the category of the review message. Every review message falls into a single category, this includes User Access, Card Info and Area Change etc.

REVIEW FILTERS

Located at the top of the **Review** window are a series of filter options that will assist you in locating review records of particular interest.

SOURCE

The **Source** text box is used to filter review based on the controller or application that created the event. This is commonly used on sites with many Integriti controllers to filter review to a single panel.

MESSAGE

The **Message** text box is a quick way to filter review if you know part of the message you are searching for. This method of searching review can often return records that may match your entry but aren't exactly what you're looking for.

For more accurate search results, you will need to use a wild-card. A wild-card is a placeholder symbol that represents one or more characters in the message. In Integriti the wild-card symbol is the % character.
Below is an example of how a wild-card is used:

Installer Pin Logon at C3K-LcdTerm: 04

Entering the text **Installer** or **Inst%** will show this review message.

Entering the text **Installer Logon** will not show this review message as the text does not contain the word **PIN**.

A wild-card can be used to replace words between **Installer** and **Logon**; entering **Installer%Logon** will show this review message.

REVIEW TYPE FILTERING

The **Review Type** filter allows you to display review records based on one or more **Review Type** categories. This can be used to display all records of a particular type, for example **User Access** events.
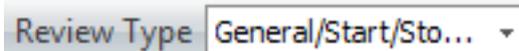
REVIEW LEVEL FILTERING

The **Review Level** filter allows you to filter review record to different levels. The lowest review level is Everyone, this level will show the least number of review events. The highest review level is Inner Range - Debug, this level will display every generated review message.

PLAY / PAUSE REVIEW BUTTON

On sites that generate a large amount of review messages it is difficult to read review messages before they are replaced by new events. The **Play / Pause** button will start and stop new review messages from appearing in the **Review** window. When in the play mode the button will appear highlighted.

PERIOD FILTERING

The **Period** is a time-based filter that filters the review messages based on the date and time setting specified.

The three period filters are:

Live: This option will clear all review events from the review window and only display new events as they are created. If you wish to clear the review window a second time, click the **Refresh Live** button.

Recent History: This filter allows you search historic review based on a last number of weeks, days, hours or minutes. Below is an example of a recent history filter set to one day:

Date Range: This filter allows you to search historic review based on events occurring between to specified dates and times. Below is an example of a **Date Range** filter containing a one hour period of time on a particular day:
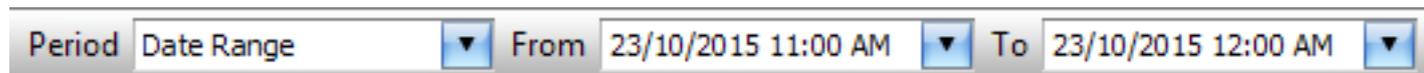
RIGHT CLICK OPTIONS

Right-clicking on a review message will open a list of all the system entities that were involved in generating this review message. Each of the items listed is a hyper-link to the editing screen for that item, this allows you to easily jump to that item to edit it.
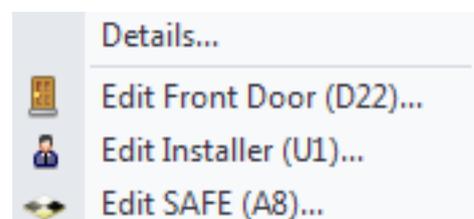
EXPORTING REVIEW

In some cases you may need to provide a copy of the review to someone else in a particular format. Once you have filtered the review records review you can export these review records in the format of your choice. To export review click the **Print Export** button, this will open the **Preview** window.
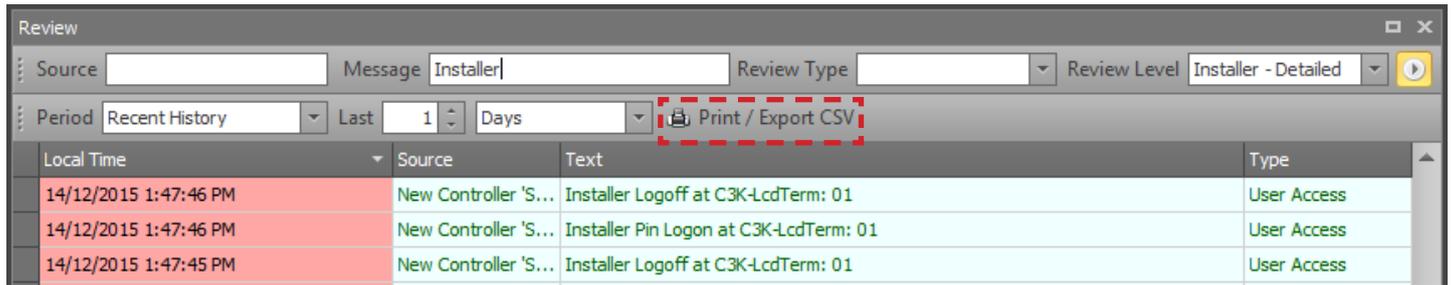
The **Preview** window contains a number of options, the most commonly used ones are:
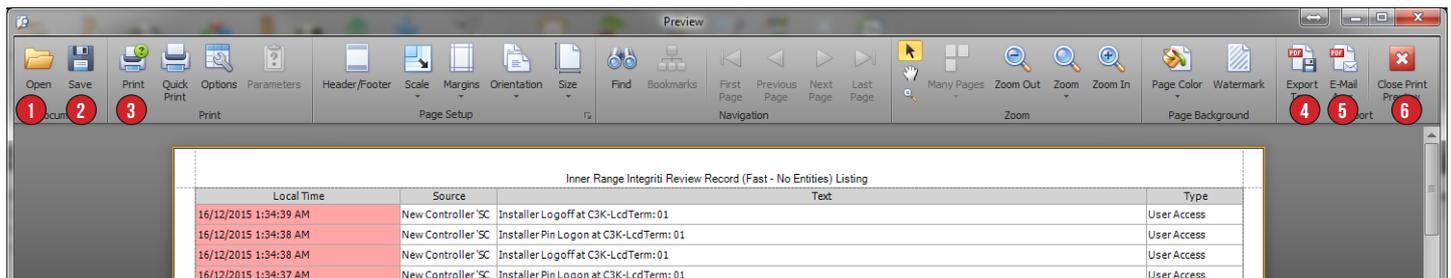
1. The **Open** command is used to open and view a preview that was saved in the native format using the **Save** command.
2. The **Save** command is used to save the contents of the preview window in the native .prnx file. This file can be opened at a later date using the Open command.
3. The **Print** command will open the **Windows Print** window allowing you to select a printer and set the appropriate printing options.
4. The **Export To** command allows you to save the contents of the **Preview** window in the file format of your choice. Commonly used formats are PDF, XLS or CSV. After selecting a format the **Format Options** window will open, these setting are best left as default.
5. The **Email As** command works the same as the **Export To** command, however, once the file is saved it will be attach to a blank email in your default mail client.
6. The **Close Print Preview** button will exit the **Preview** window without saving the contents.