Integriti Programming Reference Manual

V3.3

(Current to V3.3.13)

Additional Reading

Integriti Programming via LCD Terminal-Generic Operations
Provides overviews and descriptions of the following LCD Terminal operations:
- Generic programming operations
- Logged-off operations
- The Information Menu
- The Test Menu
- The Service Menu

NOTE: Programming menus provided on an LCD Terminal are primarily intended for testing and commissioning purposes. Depending on the system settings, changes made via the LCD Terminal may be overwritten by the Integriti software.

Reporting Format Mapping Tables
These tables provide details of the Input mapping schemes for alarm reporting formats such as: Contact ID SIMSII IRfast SIA

Integriti Software Manuals
- Interface Elements for Integriti
- System Configuration Handbook
- A range of guides covering specific Integriti Software features.

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

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

DISCLAIMER

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

Please send any comments on this manual to:
publications@innerrange.com

Integriti Programming Reference.

Table of Contents

Generic Programming Operations

Permission programming (Qualify Pairs)

Permissions allow relevant entities to be paired together to provide a simple and logical, yet flexible and powerful means of defining permissions or qualifying operations.

A Permission consists of a "What" entity (Qualifyee) and an optional "When" entity (Qualifier).

- "What" is an item or a list of items that will be allowed or denied, or that will be processed together in some way. e.g. "What" is typically an entity such as an Area, Area List, Door, Door List, Floor List, Menu Group, Input, User Action, etc.
- "When" is an optional item or list of items that will determine when the permission applies. i.e. Defines when the "What" entity will be used in the processing. e.g. "When" is typically an entity such as a Time Period, Schedule, Area, Input, Comparison, etc. The absence of a "When" entity implies that the permission "Always" applies.

When programming via the Integriti System Designer, Permissions or Qualify Pairs are given different titles depending on where they are applied.
e.g. When applied to User programming, they are called "Extra Permissions" or "Permissions".
See the list below for how Permissions are described when they are applied to other entities.

In short, a Permission or Qualify Pair determines "what" entity is used in that permission or operation, and "when" it is used.

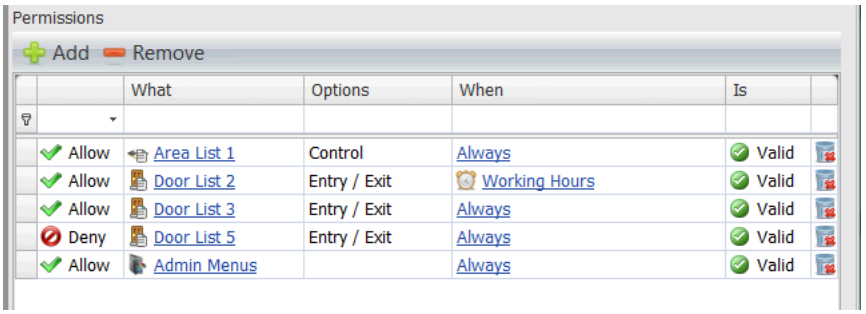
This Number of Permissions:	Can be assigned to:	Where they are referred to as:
8	Users	Extra Permissions
16	Permission Groups	Permissions
6	LCD Terminals	Extra Restrictions
2	Integriti Graphic Terminals	Extra Restrictions
16	Interlock Groups	Interlocked Entities
8	Qualified Door Types	Door Types
8	Qualified Lift Types	Lift Types
3	Lift Cars	Restricted Floors

Entities relevant to each type of Permission listed above are as follows:

Permission Type	Relevant Entities
Users (Extra Permissions)	Permission Groups. Menu Groups. Door Lists. Doors. Area Lists. Areas. Lift Cars. Lift Car Lists. Lift Floors. Lift Floor Lists.
Permission Groups (Permissions)	Permission Groups. Menu Groups. Door Lists. Doors. Area Lists. Areas. Lift Cars. Lift Car Lists. Lift Floors. Lift Floor Lists.
LCD Terminals (Extra Restrictions)	Menu Groups. Door Types. Area Lists. Areas. LCD Messages.
Graphic Terminals (Extra Restrictions)	Menu Groups. Door Types. Area Lists. Areas. LCD Messages.
Interlock Groups (Interlocked Entities)	Door Lists. Doors. Area Lists. Areas. Auxiliaries. Inputs.
Qualified Door Types (Door Types)	Door Types.
Qualified Lift Types (Lift Types)	Lift Types.
Lift Cars (Restricted Floors)	Lift Floor Lists. Lift Floors.

Regardless of which of the above entities the Permissions are assigned to, a dialog box like the one pictured below is displayed.

- The “Allow or Deny”, “What”, “When” and “Is Valid/Invalid” columns are always available, regardless of the entity being programmed.
- The “Options” column is only available in User, Permission Group, LCD Terminal and Graphic Terminal programming, but might not be active, depending on the type of entity selected for the “What” parameter.



Option	Initial Screen / Option	Description
What	Door Door List Area Area List Lift Floor Lift Floor List Lift Car Lift Car List Menu Group Permission Group User Door Type Lift Type Auxiliary Aux List Input LCD Message	Select the entity to be used as the “What” for this Permission. The options listed opposite are the entities most likely to be used in this setting, depending on the type of Permission being programmed. *See table on the previous page.* When you click on the “+ Add” button a search window will open to allow an entity to be selected. The entity types relevant to the Permission being programmed will automatically be displayed in the “List Filters” column on the left-hand side. Other entity types may be accessed via the “Everything” filter, however, this option should be used with extreme caution or on advice from Technical Support and should be tested thoroughly, as you might choose an entity type that is not relevant to the Permission and will not work.
Allow / Deny		Select whether the entity that is to be defined in this Permission, is to be “Allowed” or “Denied” by this Permission. e.g. If a Door List is to be defined and this option is set to “Allow”, then those Doors will be allowed.
Options		Depending on the type of “What” chosen, options for that entity may then be available. Options are provided for Door, Door List, Area or Area List.
	DOOR / DOOR LIST OPTIONS Permit Entry Permit Exit	Entry / Exit Options Access via an Entry Reader is permitted. Access via an Exit Reader is permitted.

	AREA / AREA LIST OPTIONS Arm (On) Disarm (Off) Grant Access to Area.	Area Control Options. On control (Arm) allowed. Off control (Disarm) allowed. Allow a User to gain entry through a Door into an Area that is allowed, regardless of whether the Door is allowed.
When		If the “What” entity selected is not “Always” allowed, you will need to select a “When” entity. e.g. Time Period, Area, etc. Refer to the table in the next option for a list of the entities most likely to be used in this setting.
Is	 Valid / Invalid Valid / Invalid Locked / Unlocked All Locked / Any Unlocked Armed / Disarmed All Armed / Any Disarmed Valid / Invalid Valid / Invalid Valid / Invalid Valid / Invalid Valid / Invalid Valid / Invalid Valid / Invalid Valid / Invalid Valid / Invalid Valid / Invalid Valid / Invalid Valid / Invalid Non-Zero / Zero Running / Not Running Valid / Invalid	If a “When” entity is selected you now need to define how it will qualify the What entity. This is done by choosing the required option from the “Is” column. e.g. If a Time Period is selected and this option is set to “Valid”, then the “What” Entity will only be allowed when the Time Period is Valid. The following table shows the options available for the types of entities that might be used in this option. Time Period / Schedule / Holiday User Qualification Door Door List Area Area List Floor Floor List Lift Car Lift Car List Auxiliary. (Valid = ON. Invalid=OFF) Auxiliary List Zone. (Valid = Sealed. Invalid=Unsealed) User LCD Message Named Action Macro Comparison General Variable General Timer Compound Entity

Action programming.

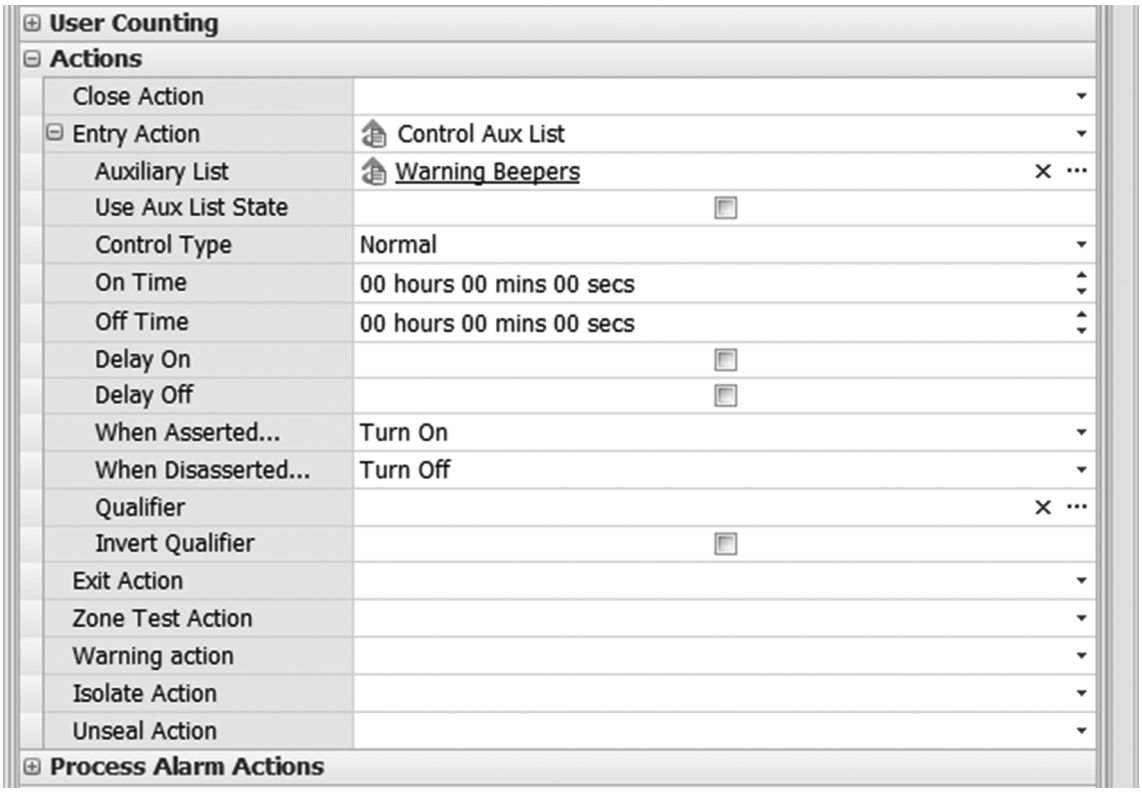
Actions allow an entity to be programmed to provide direct control of another entity.
This eliminates the need to program separate intermediate logic operations to link these entities.

Actions can be programmed for entities such as:

- Zones and System Inputs (Alarm Action)
- Areas
- RF Remote Templates (Button Actions)
- RF Expanders (Feedback Action)
- Communications Tasks (Status Actions and Command-back Action)
- Named Actions
- Macros
- Comparisons

If an Action is not required to operate at all times, a Qualifier may be assigned to determine the conditions under which the Action will be enabled and disabled. e.g. A Time Period, an Area State, etc. may be used to qualify the Action.
Note that Action processing only checks the Qualifying entity on assert, not de-assert.

Regardless of which of the above entities an Action is programmed for, when the required Action option is expanded, a dialog box like the one pictured below is displayed.
This example is the “Entry Action” in Area programming.



Programming is described in the following tables.

- The first table describes the programming options common to all actions.
- The second table describes the programming specific to particular entity types.

Action Type and Qualification settings

Option	Initial Screen / Option	Description
Action Type		Select the Entity type that will be controlled or adjusted by the entity that you are currently programming. e.g. In Zone Input programming, this is the entity that will be controlled by the Alarm/Seal state of this Input.
	None	
	Control Area	Control an Area (On/Off/Defer)
	Control Area List	Control an Area List (On/Off/Defer)
	Control Aux	Control an Auxiliary
	Control Aux List	Control an Auxiliary List
	Control Door	Unlock/Lock a Door
	Control Door List	Unlock/Lock a Door List
	Secure/Unsecure a floor on a lift car	Secure/Unsecure a floor on a lift car
	Secure/Unsecure a floor on a lift car list	Secure/Unsecure a floor on a lift car list
	Secure/Unsecure a floor list on a lift car	Secure/Unsecure a floor list on a lift car
	Secure/Unsec a floor list on a lift car list	Secure/Unsecure a floor list on a lift car list
	Trigger Input	Trigger an Input State
	Set Area User is in	Adjust the location of a nominated User.
	Set Area User Count	Adjust the number of Users currently in an Area.
	Set Input Counters	Adjust the current value of an Input event count.
	Control Siren	Control a Siren
	Set Timer Variable	Trigger a General timer
	Set Variable	Trigger a General Variable
	Control Air-conditioning	Control Air conditioning zones
	Macro Control	Start/Stop a Macro
	Isolate	Isolate a nominated Input
	Comms Task Control	Comms Task operation. E.g. Restart or Update.
	Grant Amnesty	Reset all User Anti-Passback Area records.
	Set Air-conditioner Temperature	Adjust Temperature setting for a nominated Zone in a nominated Air-conditioning Unit.
	Call Floor	Enable the Floor Selection button for a nominated Floor on a nominated Lift Car.
	Set Analogue Auxiliary	Set the value of an Analogue Auxiliary output.
	Set Analogue Auxiliary List	Set the value of the Analogue Auxiliaries in an Auxiliary List.
	Execute Action List	Control an Action List.
	Set Analogue Input	Set the value of an Analogue Input.
	Make XMIT for Area (Area Commissioning Report)	Forces an "XMIT" (reporting) Review entry for one Input, or all Inputs, in a nominated Area as a method of providing a commissioning report to a Central Monitoring Station.
	EN Function	Perform the nominated EN50131 operation.
	Reset Panel	Reset or perform a Memory Default on the nominated Controller (ISC or IAC).
Select the Entity to control.	The terminology specific to each entity type for this option is shown in the next table.	When the Action Type has been selected, the title of the next field will change accordingly and you can select the entity of that type. e.g. If "Control Aux List" is selected, the title of the next field will change to "Auxiliary List" and you can select from the Auxiliary Lists available in the system.

When Asserted / When De-asserted	The terminology for the options in this setting adjusts for the selected entity. The options specific to each entity type are shown in the next table.	The “When Asserted” option specifies the operation that will be performed on the selected entity when the action is asserted. e.g. 1. In Zone Input programming, this is the action that will occur when the Input goes into the “Alarm” state. 2. In the Area Close Action it is the action that will occur when the Area is turned On. The “When De-asserted” option specifies the operation that will be performed on the selected entity type when the action is De-asserted. e.g. 1. In Zone Input programming, this is the action that will occur when the Input goes into the “Seal” state. 2. In the Area Entry Action it is the action that will occur when the Entry Timer expires, or the Area is turned Off.
Qualify settings		Actions may be qualified by the state of another entity. e.g. An action may be programmed to cause a Door to be unlocked when an Area is Disarmed. A Time Period can then be used in the Qualify options for this action to ensure that the action will only occur during normal working hours.
Qualifier		Select the Entity to be used to Qualify the Action. e.g. Time Period, Schedule, Area, Auxiliary, etc. The Action will be allowed if the Qualifier is Valid. e.g. Time Period or Schedule is Valid Area is Off Door is Unlocked. etc.
Invert Qualifier		Enable this option if the Action is required to be allowed when the Qualifier is NOT Valid. e.g. Time Period or Schedule is Invalid Area is On Door is Locked etc.

Action Entity settings

The next settings that will be displayed will depend on the Action Type selected above.

AREA or AREA LIST		
Area or Area List to control.		Select the Area or Area List to be controlled by this Action.
Control Type.	Normal Defer Twenty-four Hour Cancel Exit Delay Arm 1st Stage Arm 2nd Stage	Select the type of control to be performed. Normal Arm/Disarm Start Defer Arming Timer Arm Disarm 24 Hour (Tamper) part of Area Cancel Exit Delay timer and Arm. Trigger 1st Stage Arming. See Note below. Trigger 2nd Stage Arming. See Note below. "Arm 1st Stage" and "Arm 2nd Stage" are only relevant to systems in which "Enable EN50131 processing" has been selected in the Control Module options and for Areas where the 2nd Stage delay has been programmed. *See Control Module, Process Group and Area programming for more details.*
When Asserted / When De-asserted	Nothing Arm Disarm Toggle	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Area or Area List will be Armed. Area or Area List will be Disarmed. Area will change to the opposite state. (NOTE: Not applicable to Area List Control)
AUXILIARY or AUXILIARY LIST		
Auxiliary or Auxiliary List selection.		Select the Auxiliary or Auxiliary List to be controlled by this Action.
Use Aux List State	False (Unchecked) True (Checked)	This option is only used in conjunction with the "Control Aux List" action and the "Toggle" operation. *See "When Asserted/When De-asserted" below.* Every Auxiliary in the Auxiliary List will have its state toggled independently. If <u>any</u> Auxiliary in the list is OFF then <u>all</u> Auxiliaries will be set to ON. If <u>all</u> Auxiliaries in the list are ON then <u>all</u> Auxiliaries in the list will be turned OFF.
Control Type	Normal Timed Only Leave Timer	Select the type of control required for this Auxiliary/Aux List. Auxiliary will be controlled as specified in the Action. If a timer is currently running on the Auxiliary, the timer will be restarted with the new timer value. If a timer is currently running on the Auxiliary, it will not be refreshed.

On Time.		If the Auxiliary action requires an On timer, program the timer value in Hours, Minutes and Seconds. A value of up to 65535 Seconds may be programmed. i.e. 18 Hrs, 12 Mins and 15 Seconds.
Off Time.		If the Auxiliary action requires an Off timer, program the timer value in Hours, Minutes and Seconds. Value setting as above.
Auxiliary Action options	 Delay On Delay Off Update Dynamic Only	If required, select one or more of the required Auxiliary Action options. Delay On instead of Timed On. Delay Off instead of Timed Off. NOT AVAILABLE V3.0 OR LATER. Changes the internal state, but does not change the real state of the output.
When Asserted / When De-asserted	 Nothing Turn On Turn Off Toggle	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Auxiliary or Aux List will be turned On. Auxiliary or Aux List will be turned Off. Auxiliary will change to the opposite state. NOTE: For the Toggle option to work with Auxiliary List control, Controller firmware must be V3.0 or later. *See "Use Aux List State" option above for details of how the Toggle option operates with Auxiliary List Control.*
DOOR or DOOR LIST		
Door or Door List selection.		Select the Door or Door List to be controlled by this Action:
Unlock time		If the Door or Door List is required to Unlock for a specific period of time, program the timer value in Hours, Minutes and Seconds. A value of up to 65535 Seconds may be programmed. i.e. 18 Hrs, 12 Mins and 15 Seconds.
Override Mode	 Normal Override Resume	This option allows an override mode to be selected. No override mode. Override unlock causes the Door to be unlocked regardless of its underlying state. Override locked causes the Door to be locked regardless of its underlying state. The underlying Door state is remembered. Resume Mode means that either edge (lock or unlock) will cancel any override and cause the Door to resume its underlying state.

When Asserted / When De-asserted	 Nothing Lock Unlock Toggle	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Door or Door List will be Locked. Door or Door List will be Unlocked. Door will change to the opposite state. (NOTE: Not applicable to Door List Control)
FLOOR (LIST) and LIFT CAR (LIST)		
Floor or Floor List		Select the Floor or Floor List to be controlled by this Action.
Lift Car or Lift Car List		Select the Lift Car or Lift Car List to be controlled by this Action.
Cancel Action Timer		Select this option if this action is to cancel any Floor selection button timers currently running for this Floor.
Floor Time		If the Floor or Floor List is required in Free Access for a specific period of time, program the timer value in Minutes and Seconds. A value of up to 255 Seconds (4 mins 15 secs) may be programmed.
When Asserted / When De-asserted	 Nothing Secure Unsecure Toggle	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Floor or Floor List for the nominated Lift Car or Lift Car List will be Secured. Floor or Floor List for the nominated Lift Car or Lift Car List will be put into Free Access. Floor for nominated Lift Car will change to the opposite state. (NOTE: Not applicable to Floor List or Lift Car List Control)
TRIGGER INPUT		
Input to trigger		Select the Input to be controlled by this Action. "Trigger Input" normally causes an input to briefly go into the nominated state and then return to its previous state. e.g. The Alarm state is asserted just long enough to cause an alarm to be reported in an Area. An option is also available to allow the input to remain in the nominated state. *See "Update State" below.*

State to trigger		Select the Input state to be triggered.
	Alarm Mask Orientation Fault Range Tamper Low Tamper High Tamper Zone Self-test Failure Low Battery Encryption failure Poll failure Spare Soaking Soak Test Fail Isolate	The "Alarm" state will normally be chosen.
Update State		Selects whether the Action will cause the nominated state selected above to be a momentary or permanent change.
	False (unchecked)	When the action is executed the Input will only have an "edge" generated for the Input and will then return to the previous state.
	True (Checked)	The Input will remain in the selected state after the Action has been executed. i.e. An "edge" is generated for the Input and then the Input is left in the nominated State. **Physical Zone Inputs:** The input will be triggered into the nominated state, but if the physical state of the input changes, the input will revert to that physical state. E.g. If C01:Z01 is triggered into Tamper while it is physically in the seal state, then the physical input goes in alarm, the input state will be updated from Tamper to Alarm. **Non-physical Inputs (e.g. C01:Z33):** Will only leave the nominated state when another Trigger Input action is performed on the Input with a Restore or Toggle operation selected. *See below.* e.g. If C01:Z33 is in the Alarm and Isolate states and a Trigger Input action is performed for a Restore operation on the Alarm state, the input will only remain in the Isolate state.
Operation When Asserted / When De-asserted		"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted.
	Nothing Trigger Restore Toggle	No action. The nominated Input State will be Triggered. The nominated Input State will be Restored. The nominated Input State will change to the opposite state.

SET AREA USER IS IN (User Location)		This action is used to put a User in a particular Area. This will also cause Area User counts to be updated (i.e. Area User count for the Area the User is in will be decremented and Area User count for the Area the User is put in, will be incremented. As a result, one or more Area User count actions may be invoked if required.
User.		Select the User to whom the nominated Area will be assigned.
Area.		Select the Area to be assigned to the User by this Action.
Don't update Area User Counts		Enable this option if you do not want the Area User Count to be incremented/decremented when the User location is altered.
When Asserted / When De-asserted	 Nothing Set	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. The nominated Area will be set as the Area the User is in.
SET AREA USER COUNT (Number of Users in Area)		This action is used to set the number of Users in Area to a number. Area User count action will not be tested.
Area.		Select the Area to be adjusted by this Action.
User Count		Enter the value that the Area Count will be set to when the Action is triggered. The value is programmable from 0-9999999.
When Asserted / When De-asserted	 Nothing Set	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. User Count will be set to the programmed value for the nominated Area.
SET INPUT COUNTERS		
Input.		Select the Input that will have its Count adjusted by this Action.
Count		Enter the Count Value required. The selected Input will have its count adjusted to this value when the Action is triggered.

When Asserted / When De-asserted	 Nothing Set	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Count will be set to the programmed value for the nominated Input.
SIREN CONTROL		
LAN Module		Select the Module on which Sirens will be controlled by this Action. At present, the Integriti Security Controller, Zone Expander Modules and Graphic Terminals can be selected. Note that the Graphic Terminal only supports Siren tones via its built-in speaker and cannot be used to drive a Horn Speaker or Piezo Screamer.
Time		Enter a Siren Time in Hours, Minutes and Seconds. Determines how long the siren will stay active when the Action is triggered. A time of up to 1 Hr, 49 Min and 13 Seconds may be set.

Siren Tone		Select the Siren Tone to be used for Alarms for this Action.
	None	None
	Bell	Bell Chime tone.
	Sweep	Intruder Alarm Sweep tone.
	Fire	Fire tone. Fast alternating tones.
	Evacuation	Evacuation tone. Long sweeps low to high tone.
	Chirp: Arm Fail	Chirp: Fail. Mid frequency tone followed by LOW frequency tone. Intended to indicate that an attempted operation failed. e.g. In V3.3.13 or later this tone will be sounded on Sirens assigned to an Area that fails to arm via a Reader 3-badge or Button arming attempt.
	Chirp: Arm Success	Chirp: Success. Mid frequency tone followed by HIGH frequency tone. Intended to indicate that an attempted operation succeeded.
	Chirp: Beep	Single Beep.
	Chirp: Double Beep	Quick Double Beep at the same pitch.
	Exit Delay	Exit Delay. High pitched short beeps.
	Warning	Warning. Medium pitched long beeps.
		Different siren tones have different priorities so that if more than one Input triggers the same Siren, the highest priority Siren Tone will be sounded. The Siren Tone Priority can be overridden by enabling the "Override Priority" option in the Siren Options below. Priorities are as follows:
	Highest priority	- Evacuation - Fire - Sweep - Bell - Warning (Equal priority with Exit delay) - Exit Delay (Will override Warning tone) - Chirp: Beep - Chirp: Double Beep - Chirp: Arm Success
	Lowest Priority	- Chirp: Arm Fail
Siren Options		Siren options allow you to select which Sirens will be triggered and the Siren tone priority.
	Sound Internal Siren	The Module's Internal Siren output will be triggered.
	Sound External Siren	The Module's External Siren output will be triggered.
	Override Priority	If this option is enabled, and the nominated Siren is already running, the Siren tone selected for this Siren Action will override the Siren tone currently sounding, regardless of the Siren tone priority. If this option is not enabled, then the highest priority Siren tone will sound.

When Asserted / When De-asserted	 Nothing Turn On Turn Off Toggle	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Siren will be turned On. Siren will be turned Off. Siren will change to the opposite state. Note that this option only applies to continuous Siren tones and will have no effect on the "Chirp" Siren tone types.
SET TIMER VARIABLE		
Timer		Select the General Timer that will be adjusted by this Action.
Time		Enter a Timer period in Days, Hours, Minutes and Seconds. A time of up to 49 days may be set.
When Asserted / When De-asserted	 Nothing Set	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. The General Timer period will be set to the programmed value.
SET GENERAL VARIABLE		
General Variable		Select the General Variable that will be controlled by this Action.
Use Entity	 False (Not checked) True (Checked)	Select whether the Value or Entity will be used for this Action. Use the programmed "Value" for this Action. Use the selected "Entity" for this Action.
Value		If "Use Entity" is set to "False", the selected General Variable is set to this value.
Entity		If "Use Entity" is set to "True", select the Entity that will be evaluated to get its value. The selected General Variable is set to whatever numerical value the entity equates to. Entities currently supported in this option are: Input – Input States Input – Input Count Input – Analogue Value Auxiliary – Analogue Value General Variable Value.

When Asserted / When De-asserted	 Nothing Set	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. General Variable will be set to the value of the constant value or entity as selected above.
CONTROL AIR-CONDITIONING		
Air Conditioner		Select the Air Conditioner to be controlled by this Action.
Mode	 Off Heat Cool Ventilate HeatPump Max Mode	Select the Mode of operation to be applied.
Zone Enables		Determines which Air Conditioning Zones to control. Create an 8-bit binary bitmap by using a 1 for the Zones to control. The Most Significant Bit (Left-hand end) represents Zone 1. Convert that binary number to a decimal number between 1 and 255, and enter that decimal number here. e.g. To control Zones 2, 3 and 5 the bitmap will be 01101000 Converting that binary number to decimal gives 104.
Control Options	Enables Only Boost	Not implemented Not implemented
Delay Time		Program the Delay timer. Enter a Timer period in Days, Hours, Minutes and Seconds. A time of up to 45 Days, 12 Hours, 15 Minutes (65,535 Minutes) may be set.
Running Time		Program the Running Time. Enter a Timer period in Days, Hours, Minutes and Seconds. A time of up to 45 Days, 12 Hours, 15 Minutes (65,535 Minutes) may be set.

When Asserted / When De-asserted		"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted.
	Nothing	No action.
	Turn On	Air Conditioner will be turned On. (After the Delay Time, if programmed)
	Turn Off	Air Conditioner will be turned Off. (After the Delay Time, if programmed)
	Toggle	Air Conditioner will change to the opposite state.
MACRO CONTROL		
Macro		Select the Macro to be controlled by this Action.
When Asserted / When De-asserted		"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted.
	Nothing	No action.
	Start	The Macro will be Started.
	Stop	The Macro will be Stopped.
	Toggle	The Macro will be toggled. i.e. Started if currently stopped, or stopped if currently running.
ISOLATE / SOAK TEST AN INPUT		
Input		Select the Input to be Isolated or Soak Tested by this Action. Isolating an Input allows the Input to be temporarily disabled and will prevent the Input from being processed in any way. e.g. It may be necessary to Isolate an Input when a detection device or input wiring is faulty in order to allow an Area to be turned on and/or prevent the faulty device from causing alarms. Soak Testing an Input allows an Input to be temporarily disabled from being processed, while still being monitored for problems. Note that a Soak Test time must also be programmed for each Area in which Soak Testing may be required. The Soak Test timer allows any Inputs that are put into the Soak Test state to be automatically re-instated if no problems are detected during the soak time.
Sticky Isolate		Enable this option if the Input is not to be De-Isolated by Area Off. (Isolated Inputs are normally automatically de-isolated when the Area is turned off, this option prevents auto de-isolate)
Mode		Selects whether the Input is to be Isolated, or put in the Soak Test state.
	Isolate Mode	The Input will be Isolated.
	Soak Mode	The Input will be set to the Soak Test state.

When Asserted / When De-asserted		"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted.
	Nothing Isolate De-isolate Toggle	No action. The Input will be Isolated or set to Soak Test. The Input will be De-isolated or removed from Soak Test. The Input will be changed to the opposite state relevant to the Mode selected above.
COMMS TASK CONTROL		
Comms Task		Select the Comms Task to be controlled by this Action.
State		Select the operation to perform when the Action is triggered.
	Normal	Activate = Start. Deactivate = Stop. Toggle = toggle.
	Restart	Activate = Restart if active or Start if idle. Deactivate and Toggle not used.
	Update All	Activate = Update. Deactivate and Toggle not used. If CT is programmed and running and the programming is the same then skip. If CT is programmed and running and the programming is different, then Restart to implement programming changes. If CT is programmed and stopped then Start. If CT is not programmed but is running then Abort.
When Asserted / When De-asserted		"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted.
	Nothing Activate Deactivate Toggle	No action. Start, Restart or Update according to the "State" selected above. Stop the Comms Task if "Normal" selected above. Toggle the Active/Idle state of the Comms Task if "Normal" selected above.
GRANT AMNESTY		
Select Controller		Select the Controller to provide Anti-passback Amnesty for.

When Asserted / When De-asserted		"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted.
	Nothing Grant Amnesty Deny Amnesty Toggle	No action. Anti-passback Amnesty will be granted for all Users on this Controller. i.e. Location for all Users will be reset to "No Area". No action will take place. Not applicable to Amnesty.
SET AIR-CONDITIONER TEMPERATURE		
Select Air-conditioner		Select the Air-conditioning Unit to control.
Unit		Enter the Air-conditioning Unit number.
Zone		Enter the Zone number to adjust.
Temperature		Enter the temperature that you wish the nominated Zone to be set to.
When Asserted / When De-asserted		"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted.
	Nothing Set Temperature Turn Off Toggle	No action. Set the nominated Air-Conditioner Zone to the programmed temperature. Not applicable to Set AirCon Temperature. Not applicable to Set AirCon Temperature.
CALL FLOOR		The Call Floor action is for a HLI Remote Call Giver InterFace (e.g. Kone). It will tell the lift system to send the nominated Lift Car to its home floor (e.g. Building Lobby) and enable it to go to the destination floor specified.
Floor		Select the Destination Floor.
Lift Car		Select the Lift Car.
Cancel Action Timer		Not relevant to this Action.
Floor Time		Not relevant to this Action.
When Asserted / When De-asserted		"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted.
	Nothing Call	No action. Send the Call Floor command with the nominated Floor and Lift Car parameters to the EMS.

SET ANALOGUE AUXILIARY / AUXILIARY LIST		
Auxiliary/Auxiliary List selection.		Select the Analogue Auxiliary or Auxiliary List to be controlled by this Action.
No Review If Same	True (Checked)	If the analogue value to be set is the same as the current analogue value of the selected Analogue Auxiliary, a Review event will not be logged. Intended for use in applications such as advanced automation (e.g. A Fence monitoring interface) to avoid constant review being generated every time automation updates the state but the state hasn't changed.
Value		The selected Analogue Auxiliary/Auxiliaries will be set to this value.
When Asserted / When De-asserted	 Nothing Set	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. The Analogue Auxiliary will be set to the programmed value.
EXECUTE ACTION LIST		
Action List.		Select the Action List to be controlled by this Action.
When Asserted / When De-asserted	 Nothing Execute Assert Edge Execute Deassert Edge Toggle	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Sends the Assert edge to all actions in the Action List. Sends the Deassert edge to all actions in the Action List. No action.
SET ANALOGUE INPUT		
Input selection.		Select the Input to be controlled by this Action.
Value		The selected Analogue Input will be set to this value.
When Asserted / When De-asserted	 Nothing Set	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. The Analogue Input will be set to the programmed value.

MAKE XMIT FOR AREA (Commissioning Report)		This action forces an "XMIT" (reporting) Review entry to be generated for one Input, or all Inputs, in a nominated Area. The resulting alarm messages can serve as a method of providing a commissioning report to a Central Monitoring Station. If a reporting format such as "IRfast with text" is used, the Monitoring Station will receive an alarm message for the nominated inputs that includes the text description for every input. That text can then be used to populate the Zone/Input list for that client. IMPORTANT NOTES: 1) Ensure that Input names have been programmed for all the Inputs to be reported. 2) Liaise with the Central Monitoring Station before performing this action so that normal alarm response procedures are not invoked when the alarm messages are received.
Area Selection	Area	Select the Area to make XMIT Review entries for.
Input Selection	Input	Optional Input to use. If you only wish to report one specific Input, this option allows that Input to be assigned. The "All Inputs" option below must be Disabled.
Options	All Inputs Do Restore	Forces an XMIT Review message to be generated for all Inputs in the nominated Area. Forces a Restore XMIT Review message to be generated for each Input. This may be of benefit to the Central Monitoring Station to clear the alarms generated by this action in their Automation Software.
Input State Selection	States to Save Alarm Tamper Low Tamper High Tamper Zone Self-Test Fail Battery Isolate	Select the Input State/s to Save to Review. Normally, only the "Alarm" state would be selected for this action. *See Process Group programming for more information on Input states if required.*
When Asserted / When De-asserted	 Nothing Make	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. An XMIT Review message will be generated for the selected Input/s in the nominated Area.
EN FUNCTION		
Controller	Target Controller	Select the Controller on which the action is to be performed.

Function	EN Function None Clear Lockout	Select the EN50131 operation to be performed. No function. Clear the User Lockout state.
Options	Act as Installer	If enabled allows the operation to be performed with Installer permissions.
When Asserted / When De-asserted	 Nothing Activate	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. Perform the nominated operation.
RESET PANEL		
Controller	Target Controller	Select the Controller (ISC or IAC) on which the action is to be performed.
Reset Type	 No Change Default	Select the type of Reset operation to perform. Will Reset the Controller without making any programming changes. Will Reset the Controller and perform a Memory Default. CAUTION. This operation will return the Controller to factory default settings and programming.
When Asserted / When De-asserted	 Nothing Reset	"When Asserted" specifies the operation that will be performed on the selected entity when the action is asserted. "When De-asserted" specifies the operation that will be performed on the selected entity when the action is De-asserted. No action. The nominated Reset operation is performed. When a Reset is performed the Controller will be out of operation for around 30 to 60 seconds. Integriti software and any other devices that communicate with the Controller (e.g. Multipath IP reporting device) will probably report an offline, comms fail or similar condition. These communications paths should automatically be restored after the reset. The Central Monitoring Station should be informed prior to performing a Reset.

Users and Permissions

Entity/Feature	Description
User Codes	Edit User name, credentials, options and permissions.
Permission Groups (User Groups)	Edit User Group name, options and permissions.
Lists	Edit the names and members of Lists. Available Lists are: • Area Lists • Door Lists • Telephone Number Lists • Floor Lists • Lift Car Lists • Auxiliary Lists
Groups	Edit the names, options and permissions of Groups. Available Groups are: • Menu Groups • Process Groups • Interlock Groups
Backup Cards	Not yet implemented.
RF Remotes	Register or De-register an RF Remote, set its status and associate it with an RF Remote Template and a User.
Card Templates	Edit Card Templates. A Card Template is assigned to each User with a card credential to define how their card will be processed.
RF Remote (Fob) Templates	Edit RF Remote Fob Templates. An RF Remote Template is assigned to each RF Remote to define how the Fob will operate.
Apartments	Edit Apartment settings. Apartments allow an Intercom unit to be linked to an access controlled Floor.
User Qualifications	Edit User Qualification settings. User Qualifications allow User Permissions to be qualified by additional parameters such as currency of training qualifications or licences, induction program completion, membership of an organization, credits, etc.

User Codes

Feature	Option	Description
User Codes		Select the User you wish to edit.
User Name		Program a text name for the User. Fields are provided for “First Name(s)” and “Second Name”. e.g. Given name and Surname/Family name. Note that the name stored in the Controller is limited to 32 characters. If the total number of characters in the two name fields exceeds 31 characters, the name stored in the Controller will be truncated and will consist of: - the First Name - a Space - then as many of the Second Name characters that will fit with an arrow (→) symbol in the 2nd last character position to indicate that the name has been truncated.

Security PIN		The Security PIN is the primary PIN code for a User, and is used to logon to Terminals and perform keypad security operations. If a Qualify PIN is not programmed (see below), the Security PIN is also used in the User's Access Control operations. Enter a PIN Code of up to 8 digits. The Security PIN MUST be unique for every User.
Qualify PIN		The Qualify PIN, if programmed, is the PIN Code that will be used in User Access Control operations. i.e. When the Door Credential Mode is "PIN only", "Card & PIN" or "Card OR PIN". If a Qualify PIN is not programmed, the User's Security PIN is used for these operations. The Qualify PIN can never be used to logon to a Terminal. Enter a PIN Code of up to 8 digits. The Qualify PIN does NOT have to be unique for every User.
Cards		There are three methods for assigning a Card to a User. • Acquire Card: The Card to be assigned to the User is presented at a Reader connected to an Integriti Module or a Reader connected to the Management Software PC. • Enter Number: A pre-programmed Card Template is selected and the Card number is entered manually. • Existing Card: The Card can be selected from a list of pre-programmed Cards. <u>Extended User Data.</u> Prior to Controller Firmware V3.2.1, one Card could be assigned to each User. Controller Firmware V3.2.1 or later introduces the "Extended Users" feature. This feature allows up to 6 Cards to be assigned to a User. In addition, the maximum number of: - Permissions increases from 8 to 68 - User Qualifications increases from 8 to 168. NOTES: 1) The memory required to utilize the Extended Users feature is obtained from unused User Records. Therefore, when more than 1 Card and/or 8 Permissions and/or 8 User Qualifications are assigned to a User, the total number of User Records in the Controller is reduced. 2) Extended User Records cannot be programmed or edited via an LCD Terminal.

	Acquire Card	If the User's Card data is assigned via the "Acquire Card" method, select the "Acquire Card" option to open the "Card Acquire" dialogue. Select the source of the Card data: • Review: A Reader connected to an Integriti Module. • Console Reader: A Reader connected to the Management Software PC. If "Console Reader" is selected, choose the PC Com Port that the Reader is connected to. Follow the displayed prompts and instructions to assign the Card to the User. *See the Integriti software manual for more details.*
	Enter Card Number Card Template Card Number	If the User's Card data is assigned via the "Enter Card Number" method, the following two options must be programmed. Select the "Enter Number" option to open the "Manual Card Entry" dialogue. Select the Card Template relevant to this User. Card Templates are programmed separately. The data entered here will depend on the Card Template selected. If the Card Template is a Site Code type, the Card Number may be entered in Decimal. If the Card Template is a type that utilizes raw card data, the User's Card may be entered in this field in HEX format. Up to 32 Hexadecimal characters may be entered.
	Existing Card	The "Existing Card" option allows individual Cards or batches of Cards to be pre-programmed into the system to simplify the process of assigning Cards to Users. *See "Cards" in the chapter "Users and Permissions" for details.* If the User's Card data is assigned via the "Existing Card" method, select the "Existing Card" option to open the "Find Entity" dialogue. Choose a List Filter ("Available Cards" is recommended), then select the required card from the displayed list. *See the Integriti software manual for more details.*

RF Remotes	Remote Template	RF Remotes are programmed separately with details of the ID data, functionality (via an RF Remote Template) and status. An RF Remote is associated with a User. This can be done via the RF Remote programming dialogue or the User programming dialogue. When associating an RF Remote with a User from the User programming dialogue, the two options described below are provided. When an RF Remote has been associated with a User, the Remote Template, Remote Data and current Status is displayed.
	From Review	"From Review" allows the RF Remote to be associated with the User by selecting this option, then pressing a button on the Remote. Note that the person operating the RF Remote button must be within range of an RF Module to use this option. For further details refer to the Integriti software manual.
	Existing Remote	"Existing Remote" allows an RF Remote that has already been programmed, to be selected for this User.
Primary Permission Group (Qualify Group)		Select the Permission Group that defines the operations and permissions relevant to the User being programmed. Permission Groups (Qualify Groups) are programmed separately.
Extra User Permissions		Up to 8 additional User Permissions may be assigned to the User to define operations and permissions for the User. This may not be necessary if all the operations and permissions required for this User have already been defined via the "Primary Permission Group". Extra User Permission Groups can be assigned in addition to, or in place of, the User's Primary Permission Group. e.g. To define the Menu Group, Area List, Door List, User Operations, etc, allowed. Controller Firmware V3.2.1 or later introduces the "Extended Users" feature. This feature allows up to 68 Permissions to be assigned to a User. *See User 'Cards' programming above for details.*
	What When Options	Defines the entity for this User Permission. e.g. Door List, Menu Group, etc. Defines when the entity is valid for this User Permission. e.g. Time Period, Area state, etc. Defines options relevant to the entity. E.g. Control options if the entity is an Area or Area List. Options are not available for all entity types. *See "Permission Programming" for details of how to program this User option.*

User Options		Enable/Disable the general options for this User.
	Cancel on Card access.	User's permissions will be cancelled after next card use.
	Cancel on PIN Logon.	User's permissions will be cancelled after next PIN use. Controller Firmware V3.2.1 recommended if this option is used with a Weatherproof Terminal.
	Disability.	Longer unlock times etc, if programmed, will automatically be invoked to cater for a User with a disability.
	Duress Code.	The Duress System Input will be triggered on the Module where this User PIN and/or Card is used.
	User Cancelled.	User is currently cancelled. No security or access operations will be allowed.
	No Greeting	Greetings will not be displayed for this User when logging on to an LCD Terminal.
	Permanent Cache.	This User will be stored permanently in the Card Cache on Reader Modules for access when the Module is offline.
	Exclude from "Ask PC".	This option allows a User record to be excluded from the Active User Rotation Module (AURM) feature and/or the Operator Challenge feature. AURM. *See the "Enable AURM" option in the Controller General Behaviour options for more details.* OPERATOR CHALLENGE *See the Integriti Software "Guide - Operator Challenge" document for more details.*
	AURM Permanent	If this option is enabled, this User will not be removed from any Controller's local User database by the Active User Rotation Module (AURM) feature. *See "Ask PC" above.*
	Default Floor	Sets the default Floor that will optionally be sent to the Elevator Management System on door access.
	Start Date/Time	If programmed, the "User Cancelled" option will be cleared at the designated Date and Time. i.e. The User will be enabled if they weren't already.
	Expiry Date/Time	If programmed, the "User Cancelled" option will be invoked at the designated Date and Time. i.e. The User will be cancelled if they weren't already.
Lockout Options		Programs options relating to the EN50131 User Lockout feature.
	Lockout Enabled.	Causes this User to be locked out when the Control Module "Enable Lockout" mode is set.
	Lockout control.	Enables this User to allow a "locked out User" permission to logon with a PIN entry.
User Tenancy Area		Area to be optionally armed and/or disarmed on Door access and/or Reader arming, instead of the Area/s assigned to the inside/outside of the Door.

Custom Fields	User Qualification Date or Value.	One or more Custom User data entry fields may be added to support additional system features. User Qualifications is a feature that requires a Custom Field to be added. If the User Qualification is an Expiry Qualification type, a Date field will be added to allow an expiry date to be entered for the Qualification. If the User Qualification is a Credit Qualification type, a value field will be added to allow a decimal credit value to be entered for the Qualification. Note that the text labels for Custom Fields are programmable and will therefore be unique to each system. *See "User Qualifications" for details.*

Permission Groups

Entity/Feature	Option	Description
Permission Groups		Select the User Permission Group you wish to edit.
Name		Program a name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Permissions		Up to 16 Permissions may be assigned to the Permission Group to define operations and permissions for this Group.
Permissions 1 to 16	What When Options	Defines the entity for this User Permission. e.g. Door List, Menu Group, etc. Defines when the entity is valid for this User Permission. e.g. Time Period, Area state, etc. Defines options relevant to the entity. E.g. Control options if the entity is an Area or Area List. Options are not available for all entity types. *See "Permission Programming" for details of how to program this option.*

Lists

Entity/Feature	Option	Description
Lists	Area Lists Door Lists Telephone Number Lists Floor Lists Lift Car Lists Auxiliary Lists	Edit the names and members of Lists. Lists simplify the programming of other entities such as User Permissions, Permission Groups and Actions by providing pre-programmed groups of the same entity.
AREA LISTS		Select the Area List you wish to edit.
	Area List Name.	Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
	Area assignment.	Assign the required Areas to this Area List. Highlight the required Areas in the bottom ("Not In List") field and click on the "Add" button to assign them to the List. Once an Area is in the List it will be displayed in the top ("In List") field.
DOOR LISTS		Door Lists are edited in the same manner as Area Lists described above.
TELEPHONE NUMBER LISTS		Select the Telephone Number List you wish to edit.
	Name	Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
	Assign Telephone Numbers	Assign the required Telephone Numbers to the list. Select from the available Telephone Numbers in the "Not In List" field. The Telephone Numbers are programmed separately.
FLOOR LISTS		Floor Lists are edited in the same manner as Area Lists described above.
LIFT CAR LISTS		Lift Car Lists are edited in the same manner as Area Lists described above.
AUXILIARY LISTS		Select the Auxiliary List you wish to edit.
	Name	Program a text name of up to 32 characters in length.
	Assign Auxiliaries	Assign the required Auxiliaries to the list. Select from the available Auxiliaries in the "Not In List" field. Up to 32 Auxiliaries can be assigned to an Auxiliary List. NOTE: Prior to V3.0, only 16 Auxiliaries can be assigned to an Auxiliary List.

Groups

Entity/Feature	Option	Description
Groups	Menu Groups Process Groups	Edit the names, options and permissions of Groups. Groups simplify the programming of other entities such as Users, Input processing and Modules by providing pre-programmed entities that define permissions and operations.

MENU GROUPS		Select the Menu Group you wish to edit.
Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Menu Permissions	Area Information Access Isolate Testing Time Miscellaneous Installer/Engineer Service Control Lists Groups Edit Input Counters Edit User Counters RF Remote Full Test suite allowed Alter Any PIN	Defines which Menu options are allowed at a User Terminal for Users with this Menu Group.
Sub Menu Permissions 1	User Codes User Groups (Permission Grps) Review Date and Time Time Periods Schedules Holidays LCD Messages Card Formats Card Templates Soak	Defines which Sub-Menu options are allowed at a User Terminal for Users with this Menu Group.

Area Control Permissions.		Define which Area and Zone Isolate operations are allowed.
	Initiate Defer	User will initiate a deferred Area Off operation if turning off an Area defined as a "Defer" Area.
	Isolate on Exit	Unsealed Inputs will automatically be Isolated on Area Arming.
	24 Hour Off	User is allowed to turn off the 24-Hour (Tamper) part of an Area.
	Default List	Terminal display will default to Area List control on User logon. Controller Firmware V3.1.2 or later recommended if the Area List control feature is used.
	Isolate All	User is allowed to Isolate any Input. Not just Inputs in Areas that they have permission for.
	Sticky Isolate	User is allowed to Sticky Isolate an Input. i.e. The Input will not be automatically de-isolated on Area Off.
Access Control Options	Exit (Leaving) options	Access Control Leaving (Exit or Egress) options. Defines Area control operations allowed from Access control Exit Readers.
	Outside Area OFF on Egress (Exit)	Door "Outside" Area will turn Off on egress.
	User Area Off on Egress (Exit)	Door "Tenancy Area" will turn Off on egress.
	Entry options	Define the Access Control Entering (Entry or Ingress) options. Defines Area control operations allowed from Access control Entry Readers.
	Inside Area OFF on Ingress (Entry)	Door "Inside" Area will turn Off on entry.
	User Area Off on Ingress (Entry)	Door "Tenancy Area" will turn Off on entry.
	General User Credential options.	
	Dual User Provider	This User can provide a credential to validate another User when "Dual User" access is required.
	Dual User Override	This User will not require another User to validate when Dual User" access is required.
	Anti-Passback Override	This User can override an Anti-passback restriction.
	Dual Credential Override (e.g. Card + PIN Override)	This User can override the need for a second credential when the Door has options such as "Card + PIN" enabled.
Advanced Options	Named Action Groups	Named Actions (Predefined Actions) can be grouped together in up to 16 Action Groups. This is done in the Named Action programming. This option allows the Action Groups that are allowed for Users with this Menu Group to be defined. Select which of the 16 Action Groups are allowed.

Remote Control Permissions		Define the Remote Control operations allowed for this Menu Group.
	Arm Area	Area Arming allowed
	Disarm Area	Area Disarming allowed
	Arm 24 Hour Part of Area	Arming of 24-Hour (Tamper) part of Area allowed
	Disarm 24 Hour Part of Area	Disarming of 24-Hour (Tamper) part of Area allowed
	Isolate	Isolate allowed
	Control Aux	Auxiliary control allowed
	Lock Door	Lock Door allowed
	Unlock Door	Unlock Door allowed
	Siren control	Siren control allowed
	Comms Task control	Enable/Disable Comms Task control allowed
	Adjust Count	Adjust Counter values allowed
	Secure Allowed	Can Set Lift Floor/s to Secure mode.
	Free Access Allowed	Can Set Lift Floor/s to Free Access mode.
	Installer Access	Can connect to Panel via Integriti CS (Commissioning Software). E.g. via Ethernet, SkyTunnel, iModem (Dialler) or USB.
Review Level		Select the Review Level required for Users with this Menu Group. This option determines the amount of detail that will be included in the Review log.
	Everyone	Lowest level of detail.
	User - Essential	
	User - Standard	
	User - Detailed	
	Installer - Standard	
	Installer - Detailed	
	Inner Range - Debug	Highest level of detail.
		The Review Level settings in the four default Menu Groups will give a guide to how you might select this setting in any additional Menu Groups programmed.

Review Classifications	Input Area User Communications Isolate Module Siren General Timer Auxiliary Door Rtos Area Timer C info Lift Time Period Holiday Schedule Debug Air-conditioning Area Counters Input Counters RF Device Information EN50131 Message Power & Battery Testing Macro Comms Task Analogue I/O	Select the Categories required for Users with this Menu Group. This option determines the types of entities that will be included in the Review log. The Review Classification settings in the four default Menu Groups will give a guide to how you might program these options in any additional Menu Groups programmed.
Message Acknowledge	 Acknowledge message. Acknowledge All Messages. Auto Siren Off. Clear EN pins on logon	Select the Message Acknowledge options required. The User is allowed to acknowledge alarm messages in the Areas that they have permission to turn Off. The User is allowed to acknowledge all alarm messages. Sirens sounding in the Areas that the User has permission to turn Off, will be cancelled on User logon. The User is allowed to clear any EN pin states when they logon. *Do not change the setting of this option unless you understand the implications for EN50131 Alarm processing.*
EN: Message Acknowledge Options	Clear UK Lock Clear EN Alarm Clear EN Fault	The User is allowed to clear a “User Lockout” condition. This option is relevant when the Control Module “Enable Lockout” mode is set. The User is allowed to acknowledge an Alarm condition when EN50131 Alarm processing is enabled. The User is allowed to clear a Fault condition when EN50131 Alarm processing is enabled. *Do not change the setting of these options unless you understand the implications for EN50131 Alarm processing.*
Message Acknowledge options	Clear Annunciate	Not yet implemented. *Do not change the setting of this option unless you understand the implications for EN50131 Alarm processing.*

PROCESS GROUPS		Select the Process Group you wish to edit. Process Groups define how Inputs of the same type are to be processed. A Process Group is assigned to each Zone or System Input when it is placed in an Area. Integriti allows extremely flexible Input processing by allowing a different Process Group to be assigned for each Area that a Zone is in. e.g. The same movement detector can provide Intruder alarm monitoring in one Area, while also providing timed lighting control in another Area.
Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
States to process.	Alarm Tamper Low Tamper High Tamper Zone Self-Test Fail Battery Isolate EOL Input States Alarm Tamper Low Tamper High Tamper Logical Input States Zone Self-Test Fail Battery Isolate	Select the Input States to process. Other Input States will be ignored. A list of the Input States currently available is displayed for selection. Some Input States are physical states determined by the End-Of-Line (EOL) Resistor scheme used in the Input wiring. Most devices support one or more of these physical states; Alarm, Tamper Low, Tamper High and Tamper. Other Input States are logical states determined by system operations and processes or data transfer. Most devices only require the Zone Self-Test Fail and/or Isolate states to be processed. The current Input States that fall under each type are listed opposite. Do not select an Input state for monitoring unless you understand how the relevant EOL scheme or Logical Input State scheme operates for those states.
Processing.	Entry Zone. Exit Zone. Primary Entry Zone. Pulse Count Zone. One Pulse Count only. No 24 Hour if Armed. Process 24 Hour. 2nd Stage Arm EN Ack requires Installer	Inputs will have Entry Delay applied on selected states. Inputs will have Exit Delay applied on selected states. Inputs can start the Entry Timer. Inputs will have Pulse Count logic applied. Inputs can only contribute one pulse per Input to the Pulse Count. 24-Hour Input states will not be processed while Area armed. The EOL "Alarm" states will be processed as 24-Hour states. Inputs are processed the same, regardless of the On/Off state of the Area. When this Zone alarms, and the Area is in 1st Stage Arm, the restore on that Zone will trigger the 2nd Stage Arm. "2nd Stage Arm" is only relevant to systems in which "Enable EN50131 processing" has been selected in the Control Module options and for Areas where the 2nd Stage delay has been programmed. *See Control Module, and Area programming for more details.* Only Installers can acknowledge EN50131 messages.

Messages. (Terminal message options)	States to generate Terminal messages Alarm Tamper Low Tamper High Tamper Zone Self-Test Fail Battery Isolate	Define the Input States to generate Terminal messages. Options are the same as “Input States to process” above. A list of the Input States currently available is displayed for selection. *See “States to Process” above for details.* **NOTE:** Do not edit these options unless you understand how the Input States scheme operates.
	Terminal Message Categories.	Select one or more of the Message Category/s to allow messages from this Process Group to be sent to User Terminals with the corresponding Message Category options enabled. Up to 8 Message Categories may be utilized. e.g. 1) To send all messages to all Terminals simply assign Category 1 in all Process Groups, and Category 1 in all Terminals. 2) To ensure Intruder and Holdup alarm messages are not sent to Terminals in Public access areas, only assign Category 2 to Process Groups for these types of alarms, then enable Category 2 for Terminals in secure Areas, but disable Category 2 for Terminals in public Areas.
Communications Options. (Reporting)	States to report Alarm Tamper Low Tamper High Tamper Zone Self-Test Fail Battery Isolate	Define the Input States to report. Options are the same as “Input States to process” above. A list of the Input States currently available is displayed for selection. *See “States to Process” above for details.* **NOTE:** Do not edit these options unless you understand how the Input States scheme operates.
	Comms Task Groups	Option to allow Input event reporting to be filtered based on the type of Input. Up to 16 separate Comms Task reporting Groups can be established. If one or more Groups are enabled in these options, the Input events will only be reported by Comms Tasks that have: - At least one matching Comms Task Group enabled, Or - No Comms Task Groups enabled. If no groups are enabled in these options, the Input events can be reported by any Comms Task, regardless of how the Comms Task Group options have been set in the Comms Task Programming.
	Reporting options. Report Entry. Report Exit. No Xmit Restore. Delay Report.	Select the required general reporting options. Transmit Alarm events during Entry. Transmit Alarm events during Exit. Don’t report Input state Restores. Delay Reporting of events via Digital Dialler formats by the Comms Task Delayed Report Time.

	Swinger Shutdown Max	Maximum number of reports that can be sent on an Input before the Input is Isolated.
	Swinger Shutdown Input States. Alarm Tamper Low Tamper High Tamper Zone Self-Test Fail Battery Isolate	Define the Input States, that if reported, will be used in the Swinger Shutdown count. Options are the same as “Input States to process” above. A list of the Input States currently available is displayed for selection. *See “States to Process” above for details.* **NOTE:** Do not edit these options unless you understand how the Input States scheme operates.
	Contact ID Message Type (Event Code)	If required, enter a Contact ID Event Code to be used for this Process Group. If left at “0”, the CID Event Code assigned to the individual Input (if programmed), or via the “Report Type” (if programmed below) or the default Contact ID Event Code defined in the selected Contact ID Map, will be used. *See “Alarm Message reporting priorities” below for more information.* An appropriate default Contact ID Event Code is assigned to some of the pre-programmed Process Groups. Note: Process Groups assigned to System Inputs normally have this option set to “0”, as appropriate Event Codes are already defined in the selected Contact ID Map. *See the table “Integriti Default Process Group Contact ID Event Codes and typical applications” at the end of Process Group programming for details.*

	SIA Type	Select the SIA Type for this Process Group if required. Controller Firmware V3.2.1 or later only. If left at "None", the SIA Type assigned to the individual Input (if programmed), or via the "Report Type" (if programmed below) or the default SIA Type defined in the selected SIA Map, will be used. *See "Alarm Message reporting priorities" below for more information.*
	None	The SIA Type will be determined by Input programming, the Process Group Report Type or the default SIA Type.
	ATAR	AC Power Trouble
	BABR	Burglary
	DDDR	Access Denied (e.g. Illegal Card)
	DFDR	Door Forced
	DLDH	Door Open Too Long
	EMEN	Expansion Device Missing (e.g. LAN Comms Fail)
	ESEJ	Expansion Device Tamper (e.g. Seismic Tamper)
	ETER	Expansion Trouble
	FAFR	Fire
	GAGR	Gas
	HAHR	Holdup Alarm (Duress)
	IAIR	Equipment Failure
	JAUX	User Code Tamper (Too many PIN tries)
	KAKR	Heat
	LTLR	Phone Line Fault
	MAMR	Medical Alarm
	NANS	No Activity (e.g. RF Transmitter Fail)
	NCNR	Network Condition (e.g. End-Of-Line Module Tamper)
	NTNR	Network Failure (e.g. End-Of-Line Module Comms Fail)
	PAPR	Panic Alarm
	QAQR	Emergency
	RPUX	Automatic Test (e.g. Periodic Test Report)
	RRUX	Power-up Reset
	RXUX	Manual Test (e.g. Manually triggered Test Report)
	SASR	Sprinkler
	TATR	Tamper Alarm (e.g. Cabinet Tamper)
	UAUR	Untyped Zone Alarm
	UXUX	Undefined
	WAWR	Water
	XQXH	RF Interference
	XTXR	Transmitter Low Battery
	YAYH	Bell Fault (e.g. Siren Tamper/Fault)
	YFUX	Parameter Checksum Fail (Memory or Download fault)
	YIYJ	Over-current Trouble
	YPYQ	Power Supply Trouble
	YTYR	System Battery Trouble (e.g. Low Battery)
	YXUX	Service Request
	ZAZR	Freezer

	Report Type Burglary Emergency (Personal Emerg) Fire Freezer (Refrigeration) Gas Detected General Alarm Heat Holdup (Duress) Medical Panic Sprinkler Tamper Water	Select an appropriate Report Type if required. The Report Type can be used instead of the Contact ID message or SIA Type in the Input or Process Group programming. *See "Alarm Message reporting priorities" below for more information.* When Peer-to-Peer alarm reporting is used, the Report Type must be programmed in every Process Group that is used with Zone Inputs and in which reporting is enabled. (Process Groups that are only used for System Inputs do not require a Report Type to be programmed) The Report Type will determine the Contact ID Message or SIA Type that will be reported for Zone Inputs by the reporting Peer Controller. Using Report Types provides a simpler method of defining the Contact ID message or SIA Type that will be reported, but in doing so, may not provide as much detail. **Contact ID** **SIA** 130 BABR 101 QAQR 110 FAFR 152 ZAZR 151 GAGR 140 UAUR 114 KAKR 121 HAHR 100 MAMR 120 PAPR 113 SASR 145 TATR 154 WAWR
	Alarm Message reporting priorities.	For reporting an Input Alarm, Contact ID Messages and SIA Types can be defined in a number of ways: 1. In Input programming via the Contact ID Message or SIA Type option. 2. In Process Group programming via the Contact ID Message or SIA Type option. 3. In Process Group programming via the "Report Type" option. (Zone Inputs only) 4. The default Message Type defined in the relevant Contact ID or SIA Mapping Table. When more than one of these options is programmed, the priority is as per the order shown in the list. Remember that some default Process Groups already have Contact ID Messages and/or Report Types programmed. Note that the Message Type for Zone Inputs sent to another Controller for reporting via the Peer-To-Peer Reporting feature can only be determined by the Process Group "Report Type".

	EN Pin state. None Fire Panic Intruder Fault Power Jam Battery Mask Soak Primary ATS Secondary ATS Tamper Soaking Spare Spare	Enter the EN Pin state to be used to identify the alarm type from this Process Group. None (Pin 0) Fire (Pin 1) Panic (Pin 2) Intruder (Pin 3) Fault (Pin 4) Power (Pin 5) RF Transmitter Jam (Pin 6) Battery (Pin 7) Mask (Pin 8) Soak Fail (Pin 9) Primary Alarm Transmission System (Pin 10) Secondary Alarm Transmission System (Pin 11) Tamper (Pin 12) Soaking (Pin 13) Spare (Pin 14) Spare (Pin 15)
	4+2 Reporting format Event Code.	Enter the 4+2 Code to be used to identify the alarm type from this Process Group when reporting in 4+2 Dialler format.
Siren Programming	 None Bell Sweep Fire Evacuation Chirp: Arm Fail Chirp: Arm Success Chirp: Beep Chirp: Double Beep Exit Delay Warning Highest priority Lowest Priority	Select the Siren Tone to be used for Alarms for this Process Group. None Bell Chime tone. Intruder Alarm Sweep tone. Fire tone. Fast alternating tones. Evacuation tone. Long sweeps low to high tone. Chirp: Fail. Mid frequency tone followed by LOW frequency tone. Intended to indicate that an attempted operation failed. Chirp: Success. Mid frequency tone followed by HIGH frequency tone. Intended to indicate that an attempted operation succeeded. Single Beep. Quick Double Beep at the same pitch. Exit Delay. High-pitch short beeps. Warning. Medium-pitch long beeps. Different siren tones have different priorities so that if more than one Input triggers the same Siren, the highest priority Siren Tone will be sounded. Priorities are as follows: - Evacuation - Fire - Sweep - Bell - Warning - Exit Delay (Will override Warning tone) - Chirp: Beep - Chirp: Double Beep - Chirp: Arm Success - Chirp: Arm Fail
	External Siren Input states.	Define the Input States to trigger External Sirens. Options are the same as “Input States to process” above.

	Internal Siren Input states.	Define the Input States to trigger Internal Sirens. Options are the same as “Input States to process” above.
	Siren Options Siren Lockout Siren Refresh	Select the Siren control options required. An Input that triggers the Siren/s will be Isolated at the end of the Siren Time. If an Input triggers the Siren/s while the Sirens are already running, the Siren timer will be re-started.
Action Programming	Action Assert Input states.	Define the Input state/s that will trigger the nominated Area Process Action when asserted. Options are the same as “Input States to process” above. Up to 8 Input Process Actions can be programmed.
	Action De-assert Input states.	Define the Input state/s that will cancel the nominated Area Process Action when de-asserted. Options are the same as “Input States to process” above. Up to 8 Input Process Actions can be programmed.

Integriti Default Process Group Contact ID Event Codes and typical applications.

	Default Process Group	CID Event	Input Example
Process Groups 1 to 13 are primarily intended for use with physical Zone Inputs.			
1	Intruder/Burglary	130	Internal intruder detector.
2	Entry-Exit/Burg Delayed	130	Internal intruder detector in Entry-Exit path.
3	Intr/Burg Primary	130	Intruder detector at point of entry.
4	Silent Alarm	150	Plant alarm with off-site reporting.
5	Local Alarm	0	Plant alarm with local audible/visual annunciation only.
6	Local Silent	0	Plant alarm with Terminal message only.
7	Fire	110	Smoke or Heat-rise detector.
8	Duress	121	Duress device, Keypad Duress or Holdup device.
9	Panic	123	Panic device or Terminal Panic.
10	Emergency	100	Evacuation device.
11	Automation	0	Lighting and HVAC control.
12	Log & Report Only	300	Memory Fault.
13	Log Only	0	
Process Groups 14 to 25 are intended for use with System Inputs.			
14	Tamper	0 (145)	Cabinet Tamper Siren Tamper LAN Power Supply Auxiliary Tamper
15	LAN Fault	0 (143)	LAN Comms Fail LAN Unsecured
16	AC Fail	301	AC Fail
17	Battery Problem	0 (302)	Low Battery Battery Test Fail Battery Fail
18	Power Supply Fault	0 (312)	Fuse Fail Low Volts Detector Over-current Battery Over-current Over Volts PS Fail / PS Slave Fail
19	Comms Problem	0 (350)	Unibus Problem Comms Backup Triggered Comms Fail Phone Line
20	RF Transmitter Fault	0 (381)	RF Transmitter Timeout RF Transmitter Low Battery RF Transmitter Poll Fail
21	RF Jam	344	RF Transmitter Jam
22	Access Alarm	0 (423)	Door Forced / Lock Tamper / Reader Tamper
23	Access Silent	0 (426)	DOTL
24	Access Local	0	Too Many Tries / Invalid Card
25	Time Report	0 (602)	Triggers Periodic Test Report

NOTES: Process Group Contact ID (CID) Event Codes.
1) "0" indicates that the default Event Code defined in the relevant Contact ID Mapping table or the Event Code assigned by the Installer in Input Programming will be used.
2) A number in brackets shows the default CID Event Code that was assigned to the Process Group in V1.1 to V2.5 Integriti Controller Firmware.

Cards

Cards can be pre-programmed into the system to simplify User programming.
Once created, Cards can then be associated with Users, either within Card programming, or in User programming via the 'Existing Card' option.
Cards can be added either individually, or in bulk. Both methods are described below.

Entity/Feature	Option	Description
ADD CARD		Select the Card to program.
Name		Program a name of up to 32 characters for this Card. The name may include the Card Number, Template, Site Code and/or Type.
Credential	Card Type Card Number Card Issue Number	Select a Card Template. Card Templates are programmed separately and define the Format and Site Code parameters. Enter the Card Number. Enter the Card Issue Number if available. Card Issue numbers are only implemented rarely. This option may need to be programmed if using Inner Range Magnetic Swipe Card Format in Site Code mode.
	Status Active Inactive – Lost Inactive – Suspended Inactive – Unused	View or set the status for this Card. The Card is active. The Card has been lost. The Card has been temporarily suspended. The Card is unused.
Card Data	Card Data (Hex)	The raw Card Data in hexadecimal format is displayed here. This data is derived from the Card Type, Card Number and Issue Number data and should not be edited manually.
Association	Associated User	The User to be associated with this Card may be selected here. This association can also be assigned in User programming.
Miscellaneous Options	Last Used	The date and time that the Card was last used in this system is displayed here.
ADD BATCH OF CARDS		This feature allows a batch of sequentially numbered Cards to be programmed into the system with an option to automatically associate each Card with a new User.
	Card Template	Select a Card Template. Card Templates are programmed separately and define the Format and Site Code parameters.
	Start at Card Number	Define the Card Number of the first Card in this batch.
	Number of Cards	Define how many Cards are in this batch.
	Also create a User with each Card Assign created Users this Primary Permission Group	Selecting this option will cause a new User to be created for each Card created. When the "Create a User' option is selected, another option is provided to nominate the Primary Permission Group. It may be convenient to add batches of Cards and Users according to their Primary Permission Group requirement. This option is particularly useful if all of the new Users/Cards in the batch require the same permissions.

Card Templates

Entity/Feature	Option	Description
Card Template		Select the Card Template to program. Card Templates enhance User programming by combining the Card Format and Site Code in a single entity.
Name		Program a name of up to 32 characters for this Card Template. The name may include the format and/or Site Code of the cards and/or the tenancy of the Users.
Format	Card Format. Direct Entry Wiegand 26Bit Wiegand (H10301) Indala 27 Bit – Wiegand Keri 30 Bit Wiegand etc…	This screen allows the Card Format to be selected. Card Formats are programmed separately. A wide range of defaults are available covering the majority of common industry Card Formats. *See 2 Door Reader Module programming for the full list of default card formats and their details.*
Site Code		Enter the Site Code for this Template. The Site Code can be entered in Decimal or Hexadecimal format. When the Site Code is entered in one field, the other field will automatically be populated with the equivalent number in the alternate format.
Photo ID		Select a Photo ID Design to go with this Card Template if required. When printing a Card with this Card Template, this Photo ID design will be used as the default. Photo ID Designs are programmed separately.

RF Remotes

Entity/Feature	Option	Description
Name		Program a name of up to 32 characters for this RF Remote. The name may include the User's name and/or the purpose of the Remote.
Credential	Remote Data	Allows an RF Remote ID to be viewed and/or manually entered.
	Remote Template	Assign an appropriate RF Remote Template to this Remote to define the operations. Remote Templates are programmed separately.
	Status Active Inactive – Lost Inactive – Suspended Inactive – Unused	Set or view the current status for this RF Remote.

Association	Associated User	The User to be associated with this RF Remote may be selected here. This association can also be assigned in User programming.
Miscellaneous		The date and time that the Remote was last used in this system is displayed here.

RF Remote Templates

Entity/Feature	Option	Description
Name		Program a name of up to 32 characters for this RF Remote Template. The name may include the main purpose and/or functionality offered by the template.
Button Definitions	Actions	Program the Action for each button to be used. Depending on the Remote Model, up to 4 Button Actions may be programmed. *See Table Below.*
	Areas	Select one or two Areas to be controlled. Depending on the Remote Model, up to 2 Areas or Area Lists may be selected. *See Table Below.* Note: If Area List control is required, Controller Firmware V3.2.1 or later should be used.
	Inputs	Select one or two Inputs to be controlled. Depending on the Remote Model, up to 2 Inputs may be selected. *See Table Below.*
Options	PIN Code options	Paradox REM3 Only.
	Needs 6 Digits	If PIN Code operation is selected in either of the following options, this option forces a requirement for PIN Codes to be 6 digits long.
	Needs PIN for PGMs.	PIN Code is required to control Actions.
	Needs PIN for Area On/Off	PIN Code is required for Area On/Off operations.

RF Remote operations supported

Brand/ Model	Button Actions				Areas		Inputs	
	1	2	3	4	1	2	1	2
Paradox REM1	On	=>			Y			
Paradox REM2	●	●●			Y			
Paradox REM3	PGM1	PGM2	PGM3	PGM4	1 & 7	2 & 8		
Paradox REM15	●	●●			Y			
Visonic MCT-231		●						
Visonic MCT-234	⌂	Unlock	Lock	*				

Apartments

Feature	Option	Description
Apartment		Select the Apartment you wish to edit. Apartments allow an Integriti Floor to be associated with an Intercom Unit and Floor. This feature operates in conjunction with the "Intercom" Comms Task format to provide sophisticated Intercom access control integration.
Name		Program a text name of up to 32 characters in length. The name may include the Apartment number and/or Floor details.
Settings	Floor	Select the Floor to be associated with this Apartment.
	Intercom System Floor	Enter the Intercom system Floor number to be associated with this Apartment.
	Intercom System Unit	Enter the Intercom system Unit number to be associated with this Apartment.

User Qualifications

Integriti User Qualifications are a separately licensed feature that allows Users to be granted or denied Door access based on an Expiring or Credit Qualification.

Expiring Qualifications allow an expiry date to be entered for each User that is subject to the Qualification. This type of Qualification can be used where the User is required to hold a license, membership, training certificate, etc. to gain access, and that qualification must be regularly renewed. e.g. A machinery operator's licence, an annual club membership, safety training certificate, etc.

Credit Qualifications allow a decimal number value to be entered for each User that is subject to the Qualification. This type of Qualification can be used where a User is limited to a specific number of entries through the nominated Door or Door List.

e.g. A User may pay in advance for a specific number of days of parking in a secure car park. Each time the User is granted entry into the car park, their credit value is reduced by 1. If the value reaches 0, the User will be denied access.
Credit Qualifications can use multiple triggers to credit and/or debit from the User's credit value.

Qualifications work by allowing a User access to a particular Door according to the validity of the Qualification and/or whether the User can otherwise access that Door based on their other permissions.

A Qualification controls User access by use of the 'When' characteristic of a Door (or Door List) permission that is assigned to a User or a Permission Group.
i.e. Depending on how the Qualification is to interact with the other permissions, the permission will typically be programmed to:

- "Allow" the Door/Door List when the nominated User Qualification is "Valid".

Or - "Deny" the Door/Door List when the nominated User Qualification is "Invalid".

In addition to being used in the User Door access permission logic, User Qualifications also allow one or more nominated Actions to be triggered to indicate that a User's Qualification is about to expire ("Warning Action") or has expired (Expiry Action).

To implement User Qualifications:

1. Create a Custom Field for each Qualification to be implemented. This is used to add one or more custom fields to User programming for entering the expiry date or credit value for any User Qualifications that the User will be subject to.
2. Create one or more User Qualifications.
3. Assign each User Qualification to the relevant Users and/or Permission Groups.

See the Integriti Software "Guide – User Qualifications" document for more details.

Feature	Option	Description
User Qualification		Select the User Qualification you wish to edit.
Name		Program a text name of up to 32 characters in length. The name may include specifics of the qualification.
Qualification Type		Select the type of Qualification to program.
	Expiring Qualification	Door access may be restricted by an Expiring Qualification and an expiry date is entered for each User subject to that Qualification.
	Credit Qualification	Door access may be restricted by a Credit Qualification and a credit value (decimal number) is entered for each User subject to that Qualification.
Associated Field		Allows a Custom data entry field to be associated with the Qualification for the purpose of entering the expiry date or credit value for each User subject to the Qualification. Custom Fields are programmed separately. One or more relevant Custom Fields must be created before this option can be programmed. *See the Integriti Software "Guide – User Qualifications" document for more details.*

Triggers (Credit Qualification Only)	Filter Stack	One or more Filters can be programmed to define additional triggers for the Credit Qualification. • Credit Qualifications can contain multiple filters, each with their own deductions and filter rules. • Credit triggers can be used to add or remove credits at a specific Door (or Doors). • Deductions can be a negative value if required to add credits. • Expiry occurs when the credit value reaches or falls below 0.
	Enabled	Each trigger filter has its own enable option . Once defined, individual trigger filters may then be Enabled or Disabled as required.
	Change Amount	Enter the decimal value to deduct for this trigger. If the value is to be added, enter a negative number. *See the Integriti Software "Guide – User Qualifications" document for more details.*
Warning Action	Warning Action	One or more Warning Actions may be defined. Warning actions could be used to notify the User or a Supervisor of an approaching expiry (e.g. a license expiry) Only one warning will be generated per User when the warning threshold has been reached. After an Action Type and Entity type is chosen, the additional options relevant to control of that type of entity will be displayed. *For Controller Actions, see Action Programming in "Generic Programming Operations" for more details.* *For Integriti Software Actions, see the System Configuration Handbook appendices section F.*
	Warning Time (Expiring Qualfication Only)	If an Expiring Qualification is being programmed, a warning time may be programmed. The configured Warning Actions will be carried out when the Warning Time reaches the specified period.
	Warning Value (Credit Qualfication Only)	If a Credit Qualification is being programmed, a warning value may be programmed. The configured Warning Actions will be carried out when the Warning value reaches or falls below the specified value.

Expiry Action	Expiry Action	One or more Expiry Actions may be defined. Expiry actions could be used to notify the User or a Supervisor that a Qualification has expired. The Expiry Action will only be triggered once per User when the expiry threshold has been reached. After an Action Type and Entity type is chosen, the additional options relevant to control of that type of entity will be displayed. *For Controller Actions, see Action Programming in "Generic Programming Operations" for more details.* *For Integriti Software Actions, see the System Configuration Handbook appendices section F.*

Times

Entity/Feature	Option	Description
Times		The various Times entities provide all the settings and programming options relating to Time/Date, Time Periods, Schedules and programmable LCD Terminal messages.
Time and Date		Set the current Time and Date.
Time Periods		Edit Time Period name, Time/Day parameters and options.
Schedules		Edit Schedule name, Start/Stop Date & time, Days of week and options.
Holidays		Edit Holiday name, Start/Stop Date & Time and options.
LCD Messages		Edit the LCD message name, control entity and message text.

Time and Date

Entity/Feature	Option	Description
Time and Date		The Controller Time and Date is normally synchronised with the software when a connection between the software and the Controller is established. The Controller Time and Date can also be synchronised periodically by programming a Scheduled Task to define when, and how often, the Date and Time will be synchronised. There is currently no means of manually manipulating the Controller's Real-time Clock from the Software. If the Controller's Real-time Clock needs to be changed to a different time for testing and commissioning purposes, this must be done at an LCD Terminal via MENU, 5, 1. If there is a Scheduled Task programmed to synchronise the Controller time, you may wish to disable it while performing the testing.

Time Periods

Entity/Feature	Option	Description
Time Periods		Select the Time Period you wish to edit.
Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Options	Defined in UTC Time	Program the options for this Time Period. Time Period is defined in Greenwich Mean Time (GMT). i.e. Coordinated Universal Time (UTC).

Start and End times.	Start Time End Time	Program the Start and End time for the Period. Up to 4 separate Periods can be programmed.
Period Days of Week.	Monday Tuesday Wednesday Thursday Friday Saturday Sunday Ignore Holidays	Assign the Days of Week to be used in the Period. The Period will only be Valid on the days specified. Select "Ignore Holidays" if the Time Period will not be made invalid by Holidays. Up to 4 separate Periods can be programmed. Note that it is not necessary to use separate periods to program a Time Period that spans across midnight. The nominated "End Time" on the following day will automatically be included in the period, even though that day is not selected. After programming the Time Period parameters, always check the graphical display of the Time Period at the top of the dialogue box to ensure that the programmed parameters meet the requirements.
Holidays		Assign the Holidays that will be obeyed by this Time Period. Up to 256 Holidays can be defined.

Schedules

Entity/Feature	Option	Description
Schedules		Select the Schedule you wish to edit.
Name		Program a name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Date/Time	Recurrence	Select the recurrence frequency for this Schedule. Selecting a repeat frequency causes the nominated value in the Time/Date setting to be ignored. e.g. If "Daily" is selected then the day part of the date setting will be ignored. This allows the Schedule to repeat in the nominated period within the limits of the other values in the Date/Time setting. e.g. If "Daily" is selected, then the Schedule will repeat at the same time each day in the nominated Month and Year.
	Never Hourly Daily Weekly Monthly Yearly Weekday Of Month	Single shot at the programmed Start/Stop Date & Time. Repeat Hourly. Repeat Daily. Repeat Weekly. Repeat Monthly. Repeat Yearly. Repeat on the same day each month.
	Start Date/Time	Program the Start Date and Time for this Schedule. Enter the current Time and Date in the format; DD/MM/YY – hh:mm Where: DD = Day of month MM = Month YY = Year hh = Hours in 24Hour format mm = minutes

	Stop Date/Time	Program the Stop Date and Time for this Schedule. The format is the same as Start Date/Time above.
	Options UTC Time	Program the options for this Schedule. Schedule is defined in Greenwich Mean Time (GMT). i.e. Coordinated Universal Time (UTC).
Days of Week	Sunday Monday Tuesday Wednesday Thursday Friday Saturday	Program the Days of Week for this Schedule. Options are the same as the Days of Week options in Time Period programming, but without the Holidays option.

Holidays

Entity/Feature	Option	Description
Holidays		Select the Holiday you wish to edit.
Holiday Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Start Date/Time		Program the Start Date and Time for this Holiday. Enter the current Time and Date in the format; DD/MM/YY – hh:mm Where: DD = Day of month MM = Month YY = Year hh = Hours in 24Hour format mm = minutes
End Date/Time and/or Duration		Program the End Date and Time for this Holiday. Use the "Duration" setting and/or the "End Date" field to set the End Date/Time. The End Date/Time format is the same as Start Date/Time above.
Holiday Options	 Recur Annually Use UTC Time	Program the options for this Holiday. Repeat this Holiday Annually. This option is used for holidays that recur on the same date every year. If this option is enabled, the Year value in the Start and Stop settings is ignored. Holiday is defined in Greenwich Mean Time (GMT). i.e. Coordinated Universal Time (UTC).

LCD Messages

Entity/Feature	Option	Description

LCD Messages		Select the LCD Message you wish to edit.
Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Message Text		Program the message text. Up to 160 characters may be entered for the message. Note: In Controller Firmware prior to V3.0.2, messages more than 16 characters in length might not be displayed correctly.
Select Qualifier Entity		Defines the entity that will be used to cause the LCD Message to be valid. e.g. A Time Period, Area Status, Schedule, etc.
Qualifier Options	Invert Qualifier	Inverts the logic of the Message Qualifier. i.e. The message text will be displayed when the Qualifier is Invalid.

Installer

Entity/Feature	Option	Description
Installer		The programming options listed in this section of the manual cover the settings and programming options relating to installation, commissioning and operation of the system.
Inputs		Program/Edit the Input parameters.
Areas		Program/Edit the Area parameters.
Modules		Program/Edit the Module parameters.
	LCD Terminal	Elite LCD Terminal.
	Graphic Terminal	Integriti Graphic Terminal
	Expander	Expander. Integriti Zone Expander Modules and Legacy Concept 3000/4000 Zone Expander Modules including Universal Expanders and Mini Expanders.
	Radio (RF) Expander	Legacy Concept 3000/4000 RF Expander Modules
	Reader Module	Integriti SLAM (2-Door Reader Module) and Legacy Concept 3000/4000 1 Door/2 Door Reader Modules/Weatherproof Terminals.
	Intelligent Reader	Integriti ILAM (Intelligent LAN Access Module) and Legacy Concept 4000 Intelligent 4-Door Controller.
	LAN Power Supply	Legacy Concept 3000/4000 LAN Power Supply Module.
	Control Module	Integriti Controller. ISC or IAC.
	Fob and Zone Registration	RF Expander Remote Fob and Zone Registration Menu
Communications	Integriti Monitor Dialler GSM Automation EMS Securitel Intercom BMS EN32pin SkyTunnel E Modem Peer Reporting	Program/Edit the Communications parameters.
System		Program/Edit the System configuration and system-wide operations.
	Memory	"Default 1" is currently the only Memory configuration supported.
	Auxiliaries	Allows basic Auxiliary parameters to be defined for each Auxiliary.
	EOL Configurations	Allows EOL scheme parameters to be viewed and edited. CAUTION! Do not edit parameters or options in this menu unless you fully understand the ramifications of the changes. Changing settings for an EOL scheme will affect the operation of all Inputs in the System that use that scheme. Selection of the EOL scheme to be used on specific banks of Inputs is done in the "Modules" Menu (MENU, 7, 2) and NOT in this Menu.

Access Control	Entity Types and Groups Door Types Qualified Door Types Lift Types Qualified Lift Types Lift Groups	Allows the various Entity Types and Groups related to Access Control operations to be programmed and edited.
	Access Control Entities Card Formats Doors Lifts Floors	Allows the various Entities related to Access Control operations to be programmed and edited.
Automation	Named Actions Macros Air conditioners Comparisons Compound Entities General Variables General Timers Calibrations Automation Points	Allows the various Entities related to Automation operations to be programmed and edited.

General Controller Programming

Controller – Module Details

Entity/Feature	Option	Description
Inputs	EOL for Zones… (EOL [End-Of-Line] Resistor Scheme for Zone Inputs)	Select the End Of Line Resistor scheme to be used for the Zone Inputs on the Integriti Controller. An EOL scheme can be selected for each block of 8 Zone Inputs: Block 1: Zones 1 to 8 Block 2: Zones 9 to 16 Block 3: Zones 17 to 24 Block 4: Zones 25 to 32
	Concept 3K	Concept 3000 EOL scheme. This is the EOL scheme using 2k2 and 6k8 Resistors that is the default scheme for Integriti and also the Concept 1000 through to Concept 5000 product ranges. Recommended for new installations and when Integriti hardware is replacing existing Concept 1000, 2000, 3000, 4000 or 5000 products.
	8-State	An EOL scheme for factory use only.
	Tecom Compat	EOL scheme using 2x 10k Resistors. Not recommended for new installations. This scheme is provided for compatibility with existing installations where the Detectors/Input devices already have two 10k Resistors fitted.

Locale Settings	Country None Australia Czech Republic Great Britain Hungary Iceland Ireland Netherlands New Zealand Norway Poland Sweden	Select the Country in which the Controller is being installed. This ensures that Controllers comply with local standards. e.g. Operation of the built-in modem complies with local telecommunications standards.

General Behavoir		
	Salto Cache Duration	The period of time for which the Salto Locks will cache valid cards. Program a value in Days.
	Enable AURM	Enables this Controller to be used with the Integriti Software "Active User Rotation Module". The AURM feature allows systems to support numbers of Users far in excess of what the Controller can store locally by dynamically updating the local database from the software database when a credential unknown to the Controller is presented in the system. If a User Credential is presented at a Reader that has the "Ask PC" option enabled, and the Credential is not found in the Integriti Controller database, then the Controller will request a check of the Integriti Software database. If a match is found, and the User record has this option enabled, the User record is downloaded to the Controller which then proceeds with processing the operation. *See Active User Rotation Module in the Integriti Software manual for details.*
	Enable Global Antipassback	Enables the use of Global Antipassback across multiple Controllers by using the "Location" assigned to the Inside and/or Outside of each Door, rather than the Area.
	Enable EN50131 processing.	Configures this Controller to operate in accordance with the EN50131 Alarm processing standard. Enables system-wide functionality pertinent to EN50131 (European standards for Intruder Alarm Systems)
	Override EOL	Overrides the EOL Resistor requirement for the REX (Request to Exit) and REN (Request to Enter) Inputs on all Doors. When enabled, the Normally Open contacts of the switch can be wired directly into the REX and/or REN Inputs with no EOL resistors.
	Force Input Review	Force Input Review. Overrides any Input "No Review" settings forcing all Inputs to log activity to Review.
	PIN +1 Duress	PIN+1 Duress. Enables any security PIN Code to be incremented by 1 to generate a Duress Alarm at a Terminal. e.g. Normal PIN is 1234. Use 1235 for Duress. Normal PIN is 6789. Use 6780 for Duress.
	Save Review to USB	USB Review. Save review data to a USB Drive if one is attached.
	AC Holdoff Time	The AC Fail Holdoff time, is the period of time required to pass before the control module registers an AC fail. This allows for brief AC mains supply outages to occur without triggering an AC Fail Alarm. Enter a value in Hours, Minutes and Seconds. A value of up to 18 Hrs, 12 Mins and 15 Seconds can be entered.

	Warning Time.	Global Area Defer Arming warning time for all deferred arming Areas managed by this Controller. Determines the Warning Time that will be provided prior to an Area Arming when it has a Defer Arm Timer running. The Warning time starts when the Defer timer expires. Therefore, if no User action is taken, the total time that the Area is Timed Off is the Defer time + the Warning Time. Enter a value in Hours, Minutes and Seconds up to a maximum of 1 Hour, 49 Minutes and 13 Seconds.
	Three Badge Wait	Global "Three Badge (3 Swipe) Arming" wait time for all Readers managed by this Controller. This is the maximum time allowed between the first and third presentation of the User credential (e.g. Card) for a Three Badge Arming operation. If this option is not programmed, the default wait time of 5 seconds will be used. This option is available in Controller Firmware V3.3.0 or later.
	Dual Wait Time.	Determines the length of the wait timer for Dual User and Card & PIN operations. Enter a value in Hours, Minutes and Seconds up to a maximum of 18 Hours, 12 Minutes and 15 Seconds.
	Maximum Review Level Everyone User - Essential User - Standard User - Detailed Installer - Standard Installer - Detailed Inner Range - Debug	Sets the Maximum Level of Review that will be saved. Selecting the Review Level determines how much detail is provided in the Review Log. Higher Review Levels will log more events to provide additional detail. Lower levels will allow the Review log to cover a longer period of time, but will provide less detail. NOTE: Do not change the default setting unless you understand the ramifications. Lowest Level of detail. Most detailed Level. Recommended, especially during system installation and commissioning.
	Fixed PIN Code length.	Determines a fixed number of PIN digits for User access codes. Enter a number between 1 and 8. A setting of 4 or less is NOT recommended.
	Maximum Software Connections	This option defines the maximum number of unique Integriti Systems this Controller will allow connections to. The setting will normally be 1 or possibly 2. e.g. One permanent Integriti Pro system management connection with a 2nd connection allowed for temporary connection of Integriti CS by the Installer when necessary.

Connectivity:	Rings to Answer	Set the number of rings before the Controller's Modem will answer the call. If normal answer call operation is required, then the Fax Bypass time below must be set to 0. If Fax Bypass operation is required, then the Fax Bypass time must be programmed.
	Fax Bypass time (mS)	If Fax timed bypass operation is required, this option must be programmed to specify the amount of time during which the Controller will answer incoming calls instantly, after detecting that rings have stopped before the number of "rings to answer" is reached. V3.3.6 or later only. Fax Timed Bypass is enabled by programming this option to a non-zero value. The "Rings to Answer" option must also be programmed. When enabled, then if a call is made to the Controller that stops ringing before the "rings to answer" is exceeded, the Controller will enter a state (for the period of time programmed in this option) where it will answer any phone calls immediately. If "rings to answer" is exceeded the Controller will not answer the line, allowing the Fax machine to answer.
Connectivity: Serial Reader Settings	Serial Channel None Modem Onboard RS485 Reader Port Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) USB Slave USB Master	**IAC ONLY. V3.3.2. or later.** No Modem connection. Not relevant to this option. IAC "RDR RS485" Port. On-board "Port 0" connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4. Port 1 Unibus UART 4, Port 2 Not relevant to this option. Not relevant to this option.
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	

	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	
	Stop Bits 1 Bit 2 Bits	
Lockout Settings	User Lockout	Set this option to lockout all Users with the "Lockout Enabled" option set while any Area is Armed.
Battery Test Settings	Day of Week Sunday Monday Tuesday Wednesday Thursday Friday Saturday	Select the Day of the Week on which the System Battery Test will commence.
	Weeks between Tests	Battery Test frequency. Program the number of Weeks to elapse between each Battery Test. A value between 0 – 255 may be entered. A setting of 0 disables Battery Testing. A setting of 1 to 4 weeks is typical. If the system is being installed to a specific standard, ensure that the Battery Test settings comply with the standard.
	Battery Test Hour	Program the Hour for the Start of the Battery Test. Hours. Enter a value between 0 - 23.
	Battery Test Minute	Program the Minute for the Start of the Battery Test. Minutes. Enter a value between 0 - 59. e.g. To start Battery Testing at 1:15 PM program as follows: Battery Test Hour: 13 Battery Test Minute: 15
Time Report	Hour of the Day	Program the Hour of the Day that the Periodic Test Report will be sent to the Monitoring Station. Note that the Time Report System Input must be assigned to an Area with an appropriate Process Group.

	Day of Week Sunday Monday Tuesday Wednesday Thursday Friday Saturday	Program the Day of the Week that the Periodic Test Report will be sent to the Monitoring Station. One or more days may be selected.
Default Modules	Default RF Reader	Defines the default RF Expander Module that will be used for enrolling Wireless Remotes. e.g. Paradox REM devices or Visonic Remotes.
SkyTunnel	Primary TCP options	Sets up the Primary TCP options for SkyTunnel communications.
	Server IP Address	Enter or view the IP Address of the Integriti Server PC.
	TCP Port	View or enter the Server TCP Port Number. The default Port Number does not normally need to be changed. A different Port number is only required to be entered if the customer has their own dedicated SkyTunnel server.
	DNS Name	Select the required DNS Name from the list. DNS names are programmed separately.
	TCP Mode	Determines whether SkyTunnel will run as a Server, a Client or neither on this Controller.
	Retries	The number of times to retry connecting upon a failed attempt before connection attempts is aborted. Only applicable to the "Client" TCP Mode if selected above.
	Connection Timeout	Not yet implemented.
	Connection Attempt Timeout	Not yet implemented.
	Secondary TCP options	Sets up the Secondary TCP options for SkyTunnel communications. Options are the same as those described for the Primary TCP options above.
	SkyTunnel Password	Allows the SkyTunnel password to be changed.
	SkyTunnel Options Disable SkyTunnel Disable Web via SkyTunnel Disable IRIP via SkyTunnel	 When set, this Controller will never connect via SkyTunnel. Prevent web interface (ie: smartphone app) from connecting via SkyTunnel. Prevent the Integriti software connecting via SkyTunnel.

	SkyTunnel Online Input	An unused Zone Input may be assigned to monitor the "Online" status. The Input will be sealed while the SkyTunnel connection is online and in alarm when offline. Any Zones used for this purpose must have the "Ignore Physical Input" option enabled in Input programming. Note that the Input for monitoring the online status of SkyTunnel Reporting is not programmed here. A separate "Online Input" is provided in the SkyTunnel Reporting Comms Task options.
Access Control Hardware Mapping (IAC Only)	Door Mapping (IAC only)	Door Mapping is used to map the logical Door number on an Integriti Access Controller to the Hardware that is to be used for that Door. There are 8 logical Doors on an Integriti Access Controller (IAC). The Door mapping is programmed by defining the following parameters for each logical Door to be used: - The hardware "Device Type". - The "DIP Switch Setting" on the device (if relevant) - The number of the entity on the device. i.e. Number 1 or 2 if the device supports 2 Readers, or 2 Doors.
	Device Type: Not Present Onboard Hardware Unibus Reader Unibus Door Salto Aperio Serial Reader OSDP	 Not present Onboard Hardware. Unibus Reader (2 Readers). Unibus Door (2 Readers / 2 Doors) Salto RS485. Aperio. Serial Reader. OSDP Reader.
	DIP Switch Setting	Enter a value between 1 and 8.
	Number on Device	Enter a value between 1 and 2.

	Reader Mapping (IAC only)	Reader Mapping is used to map the logical Reader number on an Integriti Access Controller to a hardware Reader Port. There are 16 logical Readers on an Integriti Access Controller. The Reader mapping is programmed by defining the following parameters for each logical Reader to be used: - The hardware "Device Type". - The "DIP Switch Setting" on the device (if relevant) - The number of the entity on the device. i.e. Number 1 or 2 if the device supports 2 Readers, or 2 Doors.
	<u>Device Type:</u> Not Present Onboard Hardware Unibus Reader Unibus Door Salto Aperio Serial Reader OSDP	 Not present Onboard Hardware. Unibus Reader (2 Readers). Unibus Door (2 Readers / 2 Doors) Salto RS485. Aperio. Serial Reader. OSDP Reader.
	<u>DIP Switch Setting</u>	Enter a value between 1 and 8.
	<u>Number on Device</u>	Enter a value between 1 and 2.
Peer-to-Peer Reporting	Controller Firmware V3.2.1 or later required.	When multiple Integriti Controllers are installed on the same site or within the same system, the Peer-to-Peer feature allows those Controllers to share information and data in a number of ways.
	1. Peer-To-Peer Reporting. Reportable events can be sent to another Integriti Controller.	Allows for a nominated Integriti Controller to receive relevant Review messages from one or more other Controllers for reporting to a Central Monitoring Station. *See the Peer-To-Peer Reporting Comms Task format for more information.*
	2. Foreign Entities. The state of an Entity on one Controller can be used in operations on one or more other Controllers.	"Foreign Entities" can be defined to target an Entity on a different Controller. The Foreign Entity can then be selected in programming wherever a general Entity can be assigned. E.g. The 'Optional Trigger' option in a Named Action.
	3. Locations. Enables Global features such as Global Anti-passback.	"Locations" can be defined and then assigned to the Inside and/or Outside of any Doors that are to be included in Global Anti-passback processing. Note that the reliability of Peer-To-Peer operations is dependent on the network over which the Controllers will communicate with each other. The Peer-To-Peer features should only be used when necessary, and the quality of the network connections should be taken into consideration when deciding on their implementation.

	Peer-to-Peer settings.	
	Multicast IP Address	This is the IP address that peer-to-peer messages will be multicast to.
	Port	This is the Port that peer-to-peer messages will be multicast to.
	Encryption Key	All Controllers in the Peer-to-Peer relationship will need to share the same encryption key.
	Time Window (secs)	The number of seconds of difference allowed for timestamps.
	Peer-to-Peer ID	Each Controller connected in a Peer-to-Peer relationship must have a unique ID.
	Peer-to-Peer options.	
	Receive Alarms	Receive Alarms from other Controllers for reporting to a Monitoring Station. If this option is enabled, all Controllers that will send alarms to this Controller must have the appropriate "Report Type" selected in every Process Group that is used with Zone Inputs and in which reporting is enabled. (Process Groups that are only used for System Inputs do not require a Report Type to be programmed)
	Receive State	Receive the state of foreign entities. Foreign Entities are entities on a different Controller. In any Controller where the state of any entity on another Controller needs to be monitored, a "Foreign Entity" must be created for each entity to be monitored.
	Send State	Transmit the state of foreign entities.
	Locations	Allows User Locations to be sent to linked Controllers. This option is required if peer-to-peer is to be used for features such as global anti-passback.
Readers	IAC only.	Parameters are programmed for up to 16 Readers that may be connected to an IAC and its associated UniBus 2 Door/2Reader Boards. *See "Readers" in Reader Module programming for details of the options available.*
Door Access Control	IAC only.	Parameters are programmed for up to 8 Doors that may be connected to an IAC and its associated UniBus 2 Door/2Reader Boards. *See "Access Control" in Reader Module programming for details of the options available.*
Lift Access Control	IAC only.	Up to 8 Lift Cars may be assigned to an IAC and its associated UniBus Boards.
LAN Module Options	Poll Time	Not Relevant to Control Modules.

	Battery Test Time	Enter a Battery Test Time in Hours and Minutes. Determines the duration of battery test time for the main Control Module C01. (Battery test times for other Modules are set within the options for each individual Module) Enter a value in Days, Hours and Minutes. Battery Test times are determined by the Battery capacity, the normal total load (which includes the Module itself, and its peripherals), and the battery charge required to be retained at the end of the test (to allow for AC failure occurring shortly after the end of a battery test). e.g. For a 7.0 AH battery required to deliver 1.2 Amps during an AC Failure, a battery test time of 3 hours would discharge the battery to just under half its capacity. A Value of up to 45 days, 12 Hours and 15 Minutes may be entered.
	Unibus Modules	Lists the Unibus Modules connected to this Controller.
Basic Details	Controller ID	Records the ID for this Control Module.

Controller – Connection Details

Entity/Feature	Option	Description
Module Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
Basic Details	Serial Number	Records the Controller Serial Number.
Connectivity	Connection Mode	
	Auto	The Controller will automatically attempt to connect to the Integriti Software.
	Manual	The connection needs to be manually initiated at the Integriti Software. The Comms Task will not attempt to connect to the server if it is disconnected.
	Disabled	Integriti Software connection to this Controller is disabled. The Controller won't try to connect to the server at all if the Comms Task is programmed.
	Connection Path	Selects the preferred method of connection between the Integriti Controller and the Software.
	TCP	Onboard Ethernet Port
	USB	Onboard "USB-P" Port
	Serial	UniBus UART Serial Port
	IModem	Onboard PSTN Modem
	EModem	External PSTN Modem
	SkyTunnel	SkyTunnel
	Phantom	Not yet implemented.

	Connection Timeout	Program a connection timeout time in milliSeconds. The connection will be closed if the Controller does not sent at least one packet within this time. The default setting of 30000 should be retained unless advised otherwise.
	Connection Poll Time	Program a Poll time in milliSeconds. This is the maximum amount of time between heartbeat messages and must not exceed the Connection Timeout time above. The default setting of 10000 should be retained unless advised otherwise.
	Modem Serial Port	The Computer Serial Port that a PSTN Modem is connected to when a Modem connection is to be available.
	Modem Configuration String	Optional modem configuration string if a special string is required to configure the modem.
	Modem Phone Number	The telephone number for the PSTN Modem
	SkyTunnel Password	The Code used to establish connectivity via SkyTunnel. This can be found via MENU, 8, 0 at an LCD Terminal.
Integriti CS User authentication.		These records are required to establish a remote Integriti CS connection to the Controller. i.e. Via an Ethernet, SkyTunnel or Dialler connection. Note that the nominated User will not be allowed to connect if currently disabled (e.g. expired) or locket out in the Integriti system.
	Username	Enter the User name. This must be a valid User that exists in the Integriti System and has the “Installer Access” option enabled under Remote Access Permissions in their Menu Group. This is typically the Installer, however, another User may be assigned, or a User may be programmed in the system specifically for this purpose. Note that the Username is case-sensitive and must therefore be entered exactly as it is programmed in the system.
	PIN	Enter the “Security PIN” number for the User selected in the Username record. A PIN number of “01” is not allowed unless via a SkyTunnel connection in which case the SkyTunnel password provides additional security.

Synchronisation	Review Synchronisation Mode	Select a Review Synchronisation Mode to determine the point from which Review will be synchronised, and how much Review will be synchronized.
	All Historical Review	Will synchronize Review from the oldest event to the newest event. Note that if the Controller has accumulated a large Review log, this may take some time.
	From Now	Will synchronize Review from the point of time of the connection being established between the Controller and the software.
	Continuous	Will synchronize Review from the last event that the Controller sent in the previous connection session.
	Don't Sync Review	Review will not be synchronized.
	Don't Sync Time Upon Connection	Option to not synchronise the Controller and Server time upon connection.
	Time Zone	Defines the Time Zone of the location that the Controller is installed in.
	Enable Data Synchronisation	Select to allow data synchronisation between the Controller and the Server.
	Data Sync Mode	Determines how conflicting changes are resolved in an entity has been altered while the Controller is offline.
	Merge Changes	Changes from the Controller and the Software will both be accepted.
	Disallow Changes from Controller	Changes to the Controller will not overwrite the data in the Software.
	Prefer Controller Changes	Changes in the Controller will overwrite the data in the Software.
	Prevent State Syncing	Select to prevent the state of anything connected to the Controller from being synchronised.
Version	Protocol Version	Records the Controller's protocol version
	Firmware Version	Records the version of the Firmware currently installed on the Controller.
Smart Card	Smart Card Serial Number	The Serial Number of the Smart Card installed in the Controller.

Input Programming

Entity/Feature	Option	Description
Create/Find Input		Select Input to program
Input Name		Program a text name of up to 32 characters in length. This feature can be used to describe the type, location and/or purpose of the Input.
Input Type		Select Zone Type.
	Normal	Normal Digital EOL Zone Input.
	Analogue	Analogue Zone Input.
	Count Up	Event Counter Input, counting up.
	Count Down	Event Counter Input, counting down.
	Previous Input Count Up	Event Counter Input, contributing an up count to the previous Zone Input ID.
	Previous Input Count Down	Event Counter Input, contributing a down count to the previous Zone Input ID.
Input Actions	Alarm Action	The Alarm Action allows an Input to be programmed to provide direct control of another entity. Once the required Entity is selected, the options relevant to the control of that Entity type will be displayed.
Input Options		Zone Input Options.
	Summary Zone.	This Zone will be included in the overall Input summary.
	Ignore physical Input.	Ignore the physical Zone state. Used when the Zone is only to be triggered by an Action or similar operation. e.g. If an "Online", "Fail" or "Backup" Input is assigned in a Comms Task.
	Swap Alarm and Seal	Swap the Alarm and Seal states. For Normally Open alarm contacts.
	No test on Exit.	The system will not check that this zone is sealed when arming an Area to which it is assigned. E.g. Perimeter Door or Barrier that is used to exit the premises and must remain open until after arming.
	Auto Isolate on exit.	Auto Isolate on arming. Auto-isolate will be allowed on the Input if the Input is unsealed when as Area to which it is assigned is being turned On.
	Zone Self Test enabled.	Zone Self Test enabled. Controller Firmware V3.2.1 recommended if Zone Self Test is enabled.
	No Review.	Activity on this Input will not be saved to Review.
	"Isolate All" only.	Only a User with the "Isolate All" permission can isolate this Input.
	No Xmit Restore	Input Restores will not be reported for this Input.
	Review Each Period	If the Input is processed as an analogue or counter Input, the analogue or counter value will be logged to Review at the nominated "Log Frequency". *See "Analog & Counting" options below.*

SIA Type State		Select the SIA Type if required. It is only necessary to assign a SIA Type to an Input if it requires a different SIA Type to the one defined in its associated Process Group via the "SIA Type" or "Report Type" programming, or the default SIA Type in the SIA Mapping Table. *See "Alarm Message reporting priorities" in Process Group programming for more information.* Controller Firmware V3.2.1 or later only.
	None	The Process Group SIA Type or the default SIA Type will be used.
	ATAR	AC Power Trouble
	BABR	Burglary
	DDDR	Access Denied (e.g. Illegal Card)
	DFDR	Door Forced
	DLDH	Door Open Too Long
	EMEN	Expansion Device Missing (e.g. LAN Comms Fail)
	ESEJ	Expansion Device Tamper (e.g. Seismic Tamper)
	ETER	Expansion Trouble
	FAFR	Fire
	GAGR	Gas
	HAHR	Holdup Alarm (Duress)
	IAIR	Equipment Failure
	JAUX	User Code Tamper (Too many PIN tries)
	KAKR	Heat
	LTLR	Phone Line Fault
	MAMR	Medical Alarm
	NANS	No Activity (e.g. RF Transmitter Fail)
	NCNR	Network Condition (e.g. End-Of-Line Module Tamper)
	NTNR	Network Failure (e.g. End-Of-Line Module Comms Fail)
	PAPR	Panic Alarm
	QAQR	Emergency
	RPUX	Automatic Test (e.g. Periodic Test Report)
	RRUX	Power-up Reset
	RXUX	Manual Test (e.g. Manually triggered Test Report)
	SASR	Sprinkler
	TATR	Tamper Alarm (e.g. Cabinet Tamper)
	UAUR	Untyped Zone Alarm
	UXUX	Undefined
	WAWR	Water
	XQXH	RF Interference
	XTXR	Transmitter Low Battery
	YAYH	Bell Fault (e.g. Siren Tamper/Fault)
	YFUX	Parameter Checksum Fail (Memory or Download fault)
	YIYJ	Over-current Trouble
	YPYQ	Power Supply Trouble
	YTYR	System Battery Trouble (e.g. Low Battery)
	YXUX	Service Request
	ZAZR	Freezer

Contact ID Message Number		Program the Contact ID Event Type to be used when reporting Alarms on this Zone if required. It is only necessary to assign a Contact ID Message to an Input if it requires a different message to the one defined in Process Group programming via the "Contact ID Message" or "Report Type" or the default Message in the Contact ID Mapping Table. *See "Alarm Message reporting priorities" in Process Group programming for more information.* The Event Type is a number between 000 and 999. If left at 000, an appropriate default Contact ID message will be used depending on the Process Group assigned to the Input. *See the Contact ID Tables for details.*
Analogue & Counting	Analogue Calibration	Select the Analogue Input calibration parameters. Predefined Calibrations are programmed separately, and once programmed, can then be assigned to relevant Inputs.
	Count Calibration	Select the Counter Input calibration parameters. Predefined Calibrations are programmed separately, and once programmed, can then be assigned to relevant Inputs.
	Analogue / Count Log Frequency	Program a frequency in Hours, Minutes and Seconds, to determine how often the Analogue or Counter value on this Input is saved to Review. 0 = No logging. The logging frequency can be set to a value between 1 Second (most frequent logging frequency) and 18 Hours (the least frequent).
	Analogue Hysteresis	Sets the sensitivity to changes in analogue values to trigger an Input analogue value update. NOTE: Not used for legacy Concept 3000 Analogue Modules. For Concept 3000 Analogue Modules, this option is set in the relevant Module programming.
Assign the Input to an Area.	Don't forget to assign your Inputs to at least one Area	Assigning Zones and System Inputs to Areas is performed in Area programming.

Area Programming

Entity/Feature	Option	Description
Create/Find Area		Select the Area you wish to edit.
Area Name		Program a text name of up to 32 characters in length. This feature can be used to describe the location and/or function, etc. of the Area.
Reporting Options	Report Openings. Report Closings. Close at Exit Start. Report Openings after Alarm. Report 24 Hour Open/Close. Exclude from General Open/Close	Central Monitoring Station reporting options. Report Opening. Report Closing. Report the closing event at the beginning of the exit delay, instead of at the end. Only report Openings for this Area if an Alarm report has occurred since Closing. Report Open/Close on the 24 Hour (Tamper) part of the Area. Do not include this Area as part of a General Area Open/Close report.
	Client Code	Determines the Account code to be sent when reporting events from this Area. An Account Code (Client Code) may be entered for any Areas where the Account Code needs to be different from the one programmed in the relevant Comms Task. Account Codes are typically provided by the Central Monitoring Station. The number of digits required will depend on the reporting format. Enter a Decimal value between 0 – 65535, or a Hexadecimal value between 0 – FFFF. (Hexadecimal available in Controller Firmware V3.2.1 or later only)
Entry / Exit	Entry Delay Timer	Sets the Entry delay period upon triggering an entry zone. Enter a value in Hours / Minutes / Seconds. Maximum value is 1 hr, 49 min, 13 sec.
	Exit Delay Timer	Sets the Exit delay period on Area arming if required. Enter a value in Hours / Minutes / Seconds. Maximum value is 1 hr, 49 min, 13 sec.
Siren Programming	Siren Modules	Determines what sirens will sound when an Input programmed to activate sirens is triggered. Sirens are selected by selecting one or more of the Modules that support Siren outputs. At present, the Integriti Security Controller, Zone Expander Modules and Graphic Terminals can be assigned. Note that the Graphic Terminal only supports Siren tones via its built-in speaker and cannot be used to drive a Horn Speaker or Piezo Screamer. Up to 8 Siren Modules may be assigned to an Area. Additional Sirens may be assigned via the Siren Action or Area Process Actions if required.

	Siren Time:	Determines the siren activation time for sirens assigned to this Area. Check local regulations for any limits on the length of time that Sirens are allowed to run. Enter a value in Hours, Minutes, Seconds. Maximum value is 1 hr, 49 min, 13 sec.
	Siren Holdoff Time:	Determines the Siren Holdoff time for sirens assigned to this Area. The Siren Holdoff time is the amount of time that Siren activation will be delayed. Enter a value in Hours, Minutes, Seconds. Maximum value is 1 hr, 49 min, 13 sec.
	Internal Siren Mode: No Siren Instant Siren Siren on 2nd Hit Siren on Backup Siren if got confirm pin.	Determines how the Internal Sirens will work if required. No Internal Sirens. Triggered instantly. Triggered on the 2nd hit on any Input programmed to activate Sirens. Only triggered if the Backup Comms Task has been triggered. Only triggered if the confirm pin for this Area is activated to indicate a verified alarm condition.
	External Siren Mode No Siren Instant Siren Siren on 2nd Hit Siren on Backup Siren if got confirm pin.	Determines how the External Sirens will work if required. Options are the same as for Internal Siren Mode above.
	Max Siren Triggers	Determines the number of siren activations that can occur in this area before sirens become disabled. The trigger count applies to one arming cycle. Sirens will automatically be re-enabled when the Area is disarmed.
	Siren Action	You may select another Entity type or additional Siren that will be controlled when the Siren Activates and/or Deactivates. After an entity type is chosen, the additional options relevant to control of that type of entity will be displayed.
User Counting	Count Action	Select Count Action - Select the Entity type that will be controlled when the Counter reaches/exceeds the High Count and/or reaches/drops below the Low Count. After an entity type is chosen, the additional options relevant to control of that type of entity will be displayed.
	User Trigger Count High	Determines the Trigger Count High value for Area User Counting. The Count Action will be asserted if the Count value reaches or goes above this value.
	User Trigger Count Low	Determines the Trigger Count Low value for Area User Counting. The Count Action will be De-asserted if the Count value reaches or goes below this value.

Area State Actions		Programs the Actions that will occur when the corresponding Area state is Asserted and/or De-asserted. After an entity type is chosen, the additional options relevant to control of that type of entity will be displayed. *See Action Programming in "Generic Programming Operations" for more details.*
	Close Action	Select Close Action - Select the Entity type that will be controlled when this Area is Armed / Disarmed
	Entry Action	Select Entry Action - Select the Entity type that will be controlled when this Area's Entry Delay Starts / Ends
	Exit Action	Select Exit Action - Select the Entity type that will be controlled when this Area's Exit Delay Starts / Ends
	Zone Test Action	Select Test Action - Select the Entity type that will be controlled when this Area Starts / Ends Input testing
	Warning Action	Select Warn Action - Select the Entity type that will be controlled when this Area starts / ends the Defer Arming Warning Timer.
	Isolate Action	Select Isolate Action - Select the Entity type that will be controlled when Inputs in this Area are Isolated / De-isolated.
	Unseal Action	Select Unseal Action - Select the Entity type that will be controlled when Inputs in this Area are Unsealed / Sealed
Process Alarm Actions (Area Input Actions)		Programs the Actions that will occur when at least one of the Input states specified in the corresponding Process Group Input Action are Asserted and/or De-asserted. Up to 8 Area Input Actions are available. Select an Entity type that will be controlled by the Area Input Process Action. After an entity type is chosen, the additional options relevant to control of that type of entity will be displayed. For an Area Input Process Action to operate, the corresponding Input Action/s must be enabled in the Process Group. Note that some of the default Process Groups have Action 1 (Typically used for Strobe control) and Action 2 already defined for the Alarm state and Tamper state respectively where relevant.
General Area Options	Test for Users when Arming.	Provides a warning if any Users are considered to still be in the Area when it is about to be armed. This option only applies when the Arming operation is being performed at an LCD Terminal or Colour Graphic Terminal. When an Area is Armed successfully, the number of Users in that Area is set to zero.
	Force Area Pre-Arm Walk Test	If there are any Inputs in the Area that must be tested before the next arming, force a pre-arm walk test when the Area is armed at an LCD or Graphic Terminal.

	Sub Area	Allows a sub Area to be defined. The Sub Area will be controlled by the state of its associated Area. Sub-Area programming allows a one or more Areas to control the state of a common Area. e.g. The common Area (Sub-Area) will disarm when the first Area it is associated with disarms, and will only rearm when all of the Areas it is associated with are armed.
	Defer Area.	Allows this Area to be timed off (deferred) by a User with the appropriate permission settings. Firmware V3.2.2 or later allows Defer Arm of an Area regardless of whether it is currently armed or disarmed. Prior to V3.2.2 firmware, Defer Arm can only be performed on an Area that is currently armed.
	Defer Time	Determines how long this area will remain Off (Disarmed) when turned off and a Defer timer is triggered. i.e. Timed Off. For this feature to operate, the Area must be defined as a Defer Area and the User or Action that performs the Disarm operation must also have the Defer operation enabled. Enter a value in Hours, Minutes, Seconds. Maximum value is 1 hr, 49 min, 13 sec.
	Max Pulse Count	Determines the number of pulse counts required within the pulse count time to generate an alarm. Enter a value of up to 255.
	Pulse Time	Determines the pulse count time to apply to Inputs that are programmed as Pulse Inputs via their Process Group in this Area. The nominated Pulse Count below, must be reached within the programmed Pulse Time, to trigger an alarm. The Pulse Count Timer starts when the first Pulse Count Input is triggered. If the timer expires, and the Pulse Count is not reached, the Pulse Counter is reset. Enter Pulse Time in Hours, Minutes, Seconds. A value of up to 1 h, 49 m, 13 s can be entered.
	Test Time.	Sets the maximum time for Zone Walk Testing. Enter a value in Hours, Minutes, and Seconds. Maximum value is 1 hr, 49 min, 13 sec.
	Arm Self Test Count	Determines the number of times this Area must be switched ON before a Zone self-test is performed. If left at 0, Zone Self Test is disabled. If set to a non-zero value, then every nominated number of arms, at the end of exit delay, any input that has “Zone self test” enabled and has not had a seal to alarm transition since the last Zone Self-Test will assert the ZST fail state, or de-assert the ZST fail state if it passed. In addition a review message will be saved.
	Re-arm options	The Re-arm options provide a feature whereby the Area can be programmed to automatically re-arm if a specified period of Input inactivity has elapsed.

	Re-arm Time	Program a re-arm time. If there is no Input activity in this Area for the nominated period of time, the Area will re-arm. If left at 0, the Area will never re-arm automatically.
	Re-arm Qualifier	A Re-arm Qualifier may be assigned to the re-arm operation. This entity must be valid for Rearm to occur. e.g. Another Area must already be On. Additional options may be presented depending on the Qualifier Type selected.
	Invert Re-arm Qualifier.	If enabled, the Re-arm Qualifier must be Invalid for Area Re-arm to occur.
	Battery Test on Area Arm	Forces a short Battery Test on all Batteries in the System on an Area Arming.
	Arm 2nd Stage Delay	Allows a 2nd Stage Arm delay time to be entered. When 2nd Stage Arm is started, the process will be delayed by this time before Inputs are tested to allow any Input contacts to settle. (e.g. Because someone just left the Area and closed the Door). "Arm 2nd Stage Delay" is only relevant to systems in which "Enable EN50131 processing" has been selected in the Control Module options. *See Control Module and Process Group programming for more details.*
	Soak Test Time	Program the duration required to Soak test Inputs. *See "ISOLATE/SOAK TEST AN INPUT" for details.*
Event Tones		Select the Siren Tone to be sounded for any of the Area Event Tone options required. Siren Tones are the same as those available in "Sirens" above.
	Exit Tone	Siren tone to sound during Exit Delay period.
	Entry Tone	Siren tone to sound during Entry Delay period.
	Arm Problem Tone	Siren tone to sound if there is a problem during the arming procedure. E.g. Unsealed Zones.
	Arm Fail Tone	Siren tone to sound if the Area failed to Arm.
	Arm OK Tone	Siren tone to sound when the Area successfully Arms.
	Warn Tone	Siren tone to sound during the Defer Arm warning period.
Verify Options	Confirm	Select this option to enable Alarm Confirmation logic for this Area.
	Verify Group	Enter the Verify Group number for this Area.
	Confirmed Alarm Time	Program the Confirmed Alarm Time in Hours, Minutes and Seconds.
	Confirmed Alarm Options Prevent Lockout this Area allowed Isolate Extended Entry	

Inputs	Area Input assignment.	Select an Input to be assigned to this Area, then select the Process Group that will be used for the Input. Note that an Input can be assigned to a maximum of eight (8) different Areas. Additional pairs of Input and Process Group selections are made for each Area that the Input is assigned to.

Modules

Entity/Feature	Option	Description
Modules		The following Modules are currently supported in Integriti Controller Firmware V3.2.1 or later: The default Module name displayed in the navigation pane is shown in brackets. "nn" is the Module number.
	LCD Terminal	Concept 3/4000 Elite LCD Terminal. (C3K-LcdTerm: nn) Concept 3/4000 Terminal Emulator. (C3K-LcdTerm: nn)
	Graphic Terminal (Prisma)	Integriti Graphic Terminal. (Graphic Terminal: nn)
	Expander	Integriti 8-Zone Expander. (WiredExp: nn) Integriti 16-Zone Expander. (WiredExp: nn) Concept 3/4000 Universal Expander, 32Z. (C3K-BigExp: nn) Concept 3/4000 Universal Expander, 16Z. (C3K-SmallExp: nn) Concept 3/4000 Mini Expander. (C3K-MiniExp: nn) Concept 3/4000 Analogue Module. (C3K-Alog: nn)
	Radio Expander	Concept 3/4000 Visonic Wireless I/F. (C3K-RadioExp: nn) Concept 3/4000 Paradox Wireless I/F. (C3K- RadioExp: nn)
	Reader	Integriti Smart LAN Access Module (2 Door). i.e. SLAM. (2DoorRdr: nn) Not yet available. Concept 3/4000 2-Door Access Module. (C3K-2DAM: nn) Concept 3/4000 Single Door Access Module. (C3K-2DAM: nn) Concept 3/4000 Weatherproof Terminal. (C3K-2DAM: nn)
	Intelligent Reader	Integriti Intelligent LAN Access Module. i.e. ILAM/Salto (8DoorRdr: nn) Concept 3/4000 Intelligent 4-Door Access Module. (C3K-IRdr: nn)
	LAN Power Supply	Concept 3/4000 LAN Power Supply Module. (C3K-PwrSupply: nn)
	Control Module	

LCD Terminal

LCD Terminal programming is relevant to the following hardware Modules:

- Concept 3/4000 / Integriti Elite LCD Terminal.
- Concept 3/4000 Terminal Emulator Module.

Entity/Feature	Option	Description
Create/Find LCD Term		'Add New' or select a record to Alter.
LCD Terminal Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
General Options	Associated Area	Determines the Associated Area for this LCD Terminal. Used in conjunction with other LCD Terminal options.
	Associated Area List	Determines the Associated Area for this LCD Terminal. Used in conjunction with other LCD Terminal options.
	LCD Terminal Options No Keypad Beep. No Immediate Entry Disarm Single Area Tenancy Exit Display. Exit Beep.	Select the general LCD Terminal options required. No feedback beep when keys are pressed. Note that some alerts will still cause the keypad to beep. No Area Off allowed if the Entry Timer for the Associated Area still has more than 30 seconds remaining. Terminal is used in a single Area Tenancy. Only Area operation is allowed. Show Exit Timer countdown for the associated Area. Beep during exit timer for the associated Area. Exit display/beep options Cont. F/ware V2.5 or later only.
	LED Mode. None Area Array	Select the default LED operation for this LCD Terminal. LEDs are controlled by the associated Auxiliary only. LEDs will display Area status by default.
Logged Off Display Options.	Idle Display System Ready System Time Single Area Area Array	This message will be displayed on the LCD whilst logged off. The text "System Ready" is displayed The current system time and date is displayed. The status of the Associated Area is displayed A status array for the Associated Area and the subsequent 7 Areas is displayed.
	Display options Display Alarm Messages. Display Status Messages. Display LCD Messages. Display Input Levels. Display Single Message. Display Area Arm Warning.	Select the types of messages that the LCD Terminal is allowed to accept. Area Alarm Messages allowed. Area Alarm Message Categories must also be programmed. Select whether terminal will display System Status messages such as Power Supply, Battery, Communication or LAN Network problems. Select whether terminal will display custom LCD Messages. An LCD Message, if Valid, will override the selected Idle Display. Input Level messages allowed. Terminal will display a Single Message for the Associated Area. (Limited Messages) Restricts the LCD Messages to the Defer Arm Warning ("Area about to turn on") and LCD Message 1 broadcasts.
	Alarm Message Categories	Message Categories 1-8 determine which Area Zone state messages will be displayed on this LCD terminal. Messages will be displayed for Zones that have a matching category set in their Process Group.

Logged Off Keys	Up/Down Arrow Mode None Area Array Area Text	Select the Up/Down Arrow key operation for Area Status. No Area status available via the Up/Down Arrow keys. Up/Down Arrow keys will display Area status as an array of 8 Areas per screen. Up/Down Arrow keys will display Area status as a text message, one Area at a time.
	Logged Off Operations. Allow Quick Alarm Review Allow Named Actions Allow Aircon Control Allow Show Info Allow Logged Off Panic	Select the LCD Terminal operations allowed when logged off. Quick Alarm Review allowed via <MENU>, <1>. Named Actions allowed via the > key. Note that the named action must have the "Allow Logged Off Access" option enabled. Aircon Control (Not yet implemented) System Information allowed via <MENU>, <2> . The LCD Terminal "Panic" System Input can be triggered by pressing the <HELP> key 3 times in succession. Note that since this is a "logged off" operation, the LCD Terminal rather than the User will be identified in Review and Reporting messages.
Access Control	Associated Door	Select a Door to be associated to this LCD terminal. The Door nominated will be controlled and monitored by this terminal.
	Access Control Options. Access Only. No Lock. *(V1 to V2 only)* Enable Reed Input Enable Tongue Input. Zone 2 Rex Zone 2 Opposite Side	 This Terminal may only be used for access control. **CAUTION:** Once set, you will not be able to access other operations or Menus from this Terminal. Set to 'Y' if there is no lock hardware for this Door. Allow Door Reed Switch logic for this Door. Allow Tongue Sense logic for this Door. LCD Terminal Zone 2 functions as the Exit (REX) button LCD Terminal Zone 2 REX/REN button is on the Opposite side of the Door to where this Terminal is installed.
	Reader 01 Purpose Control a Door Control a Lift Log On Area Toggle	Reader Purpose defines how the Reader will be used. Door access control. Lift access control. Terminal Logon. A Valid Card presentation logs the User on to the associated LCD Terminal. Controller Firmware V3.1.0 or later recommended if this feature is used. Area On/Off only. No access control operations. "Keypad Area" below must be programmed.
	Reader 01 Location None Inside Door 1 Outside Door 1	Determines the location of the Terminal in relation to the associated Door; Inside or Outside. Only the Door 1 options are relevant to an LCD Terminal.
	Keypad Area.	Reader Keypad Area. Select the Area to control when the Reader purpose is "Area Toggle".

	Card Format. Direct Entry Wiegand 26Bit Wiegand (H10301) Indala 27 Bit – Wiegand Keri 30 Bit Wiegand etc…	This screen allows the Card Format to be selected. Card Formats are programmed separately. A wide range of default Card Formats are available. Not relevant to LCD Terminals at present. *See 2 Door Reader Module programming for the full list of default card formats and their details.*
	Any Card Mode.	If enabled, any card of the correct type will be allowed access and the card data will be logged to Review. Not relevant to LCD Terminals at present.
	PIN Device (Entity for PIN Code Entry)	Select a Module/Reader to be used for entering the PIN Code when Card + PIN is required. Controller Firmware V3.1.0 or later recommended if this feature is used with an Elite LCD or Integriti Prisma Graphic Terminal. Not relevant to LCD Terminals at present.
	Wiegand PIN Mode. None Motorola HID Reader MR Access Model Reader 26 Bit Wiegand Keypad IR Weatherproof Terminal 26 Bit Wiegand Keypad Forced	Select the PIN data mode if a Reader" was selected in the "PIN Device" option above. No PIN entry requirement. Motorola/Indala ARK-501 HID 5355 or iClass with 4 Bit Burst PIN output format. MR Access Magnetic Swipe & PIN code Reader 26 Bit Wiegand Keypad. Inner Range Weatherproof Terminal. 26 Bit Wiegand Keypad Forced. Not relevant to LCD Terminals at present.

	Reader Arming Mode No Reader Arming User Area w/button Area Empty Exit Area w/button Entry Area w/button Exit Area on 3 Swipes Entry Area on 3 Swipes Arm Users 'Tenancy Area' on 3 Swipes.	Select the Area Arming Mode if the Reader is to be used for Area Arming on Access Control operations. No Arming. Arm the User Area if the "Arm" button is pressed while the Card is presented. Arm the Exit Area (Area you are leaving) if the Area User Count decrements to zero when the Card is presented. Arm the Exit Area if the "Arm" button is pressed while the Card is presented. Arm the Entry Area if the "Arm" button is pressed while the Card is presented. Arm the Exit Area if Card presented 3 times within 5 seconds. Arm the Entry Area if Card presented 3 times within 5 seconds. Arm the User's Tenancy Area if Card presented 3 times within 5 seconds. (Cont F/ware V3.2.1 or later only) NOTES: 1) SOME OF THESE OPTIONS NOT RELEVANT TO LCD TERMINAL. E.g. ARM BUTTON OPERATION. 2) Exit Area / Entry Area. The Exit Area is the Area you are leaving. i.e. The Area the Reader is installed in. The Entry Area is the Area on the opposite side of the Door to where the Reader is installed. 3) 3 Swipe Arming. V3.3.0 firmware or later provides a Controller option for setting a different "Three Badge Wait" time.
	Ask PC	This option allows User Credentials presented at this Reader to be utilized in the Active User Rotation Module (AURM) feature and/or the Operator Challenge feature if necessary. *AURM* *See the "Enable AURM" option in the Controller General Behaviour options for more details.* *OPERATOR CHALLENGE* *See the Integriti Software "Guide - Operator Challenge" document for more details.*
Security (Incorrect PIN Lockout)	Lockout attempts	The number of incorrect PIN entries before the LCD terminal is Locked Out. The number of tries must occur within the Attempts Time.
	Lockout Time	Defines how long this LCD terminal will reject PIN operations once the number of Lockout Attempts has been reached within the Attempts Time.
	Attempt Timeout	PIN attempts Timer. The amount of time in which the Lockout Attempts must be reached before the LCD terminal becomes Locked Out. This is the time required to elapse before the lockout count is reset after an illegal PIN has been entered.
LAN Module settings	LAN Poll Time	Enter a Poll Time in Minutes, Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module.

	Battery Test Time	Not applicable to Concept LCD Terminals.
	Unibus Modules	Not applicable to Concept LCD Terminals.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the "Navigation" Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.
Extra Restrictions.	 What When	Up to 6 Permissions can be assigned to an LCD Terminal to place additional restrictions on the operations allowed to be performed. e.g. A limited permission set may be required at particular LCD Terminals during certain times of the day, or while a particular Area is armed or disarmed. Defines the entity for this Permission. e.g. Menu Group, Area List, etc. Defines when the entity is valid for this Permission. e.g. Time Period, Area state, etc. *See Permission programming in "Generic Programming Operations" for details.*

Integriti Graphic Terminal

Entity/Feature	**Option**	**Description**
Create/Find Graphic Terminal		'Add New' or select a record to edit.
Module Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
General Options	Associated Area	Determines the Associated Area for this Terminal. Used in conjunction with other Terminal options.
	Graphic Terminal Options No Keypad Beep. Entry Display. Entry Beep. Exit Display. Exit Beep.	Select the general Terminal options required. No feedback beep when keys are pressed. Show Entry Timer countdown for the associated Area. Beep during entry timer for the associated Area. Show Exit Timer countdown for the associated Area. Beep during exit timer for the associated Area.

	LED Mode. None Area Array (Red / Off) Area Array (Red / Green) Auxiliary Idle Entities	Select the default LED operation for the eight LEDs across the top of the Graphic Terminal. For the purposes of this option, the LEDs are numbered 1 to 8 from Left to Right. No LED control. LEDs will display Area status by default with Red LEDs only. (Red = Armed) LEDs will display Area status by default with Red and Green LEDs. (Red = Armed) LEDs are controlled by their associated Auxiliary only. Graphic Terminal Auxiliaries 9 to 16 are used for this purpose. i.e. LED 1=Gnn:X09, LED 2=Gnn:X10, etc. When the Terminal is logged off, the LEDs will display the current state of up to eight entities selected in the "Idle Entities" option described below. If more than eight Entities are selected, the LEDs will display the status of the first eight.
	EOL Index (EOL [End-Of-Line] Resistor Scheme for Zone Inputs)	Select the End Of Line Resistor scheme to be used for the Zone Inputs on this Integriti Graphic Terminal.
	Air-Conditioner	Air-Conditioner to be controlled by this Terminal.
	Air-Conditioner Zone	Air-Conditioning Zone to be controlled by this Terminal.
Logged Off Display	Idle Entities.	Up to 10 entities may be chosen for which the Graphic Terminal will display the current state. Currently, Areas are the only Entity relevant to this option. Via the Screen: NOTE: If using this option, only 6 Entities may be selected. The state of the selected Entities will be displayed in the selected circumstances on the Colour Graphic Screen when the Terminal is logged off and the "Idle Entities" setting is chosen in one or more of the Logged Off Display options. Via the LEDs: The state of up to 8 of the selected Entities will be displayed on the LEDs when the Terminal is logged off and the "Idle Entities" setting is chosen in the "LED Mode" option.
	Idle Display. System Ready System Time Single Area Idle Entities Time Digital Time Analogue Zones Icons	This message will be displayed on the Graphic Terminal Colour display whilst logged off. The Integriti logo is displayed. The current system time and date is displayed. The status of the Associated Area is displayed The Icons, Names and Status of up to 6 selected "Idle Entities" is displayed. *See "Idle Entities" above.* Time & Date is displayed as a large digital clock with the date displayed below. Time is displayed in analogue (clock face) format in the top left of the screen. Not currently supported. Four logged off menu icons are displayed. (PIN Code, Review, Information and Control)

	Idle Area Off Display.	This alternative message will be displayed on the Graphic Terminal if an associated Area has been assigned to the Terminal, and that Area is Off. Options as above.
	Display options Display Alarm Messages. Display Status Messages. Display LCD Messages. Display Input Levels. Display Area Arm Warning.	Select the types of messages that the Terminal is allowed to accept. Area Alarm Messages allowed. Area Alarm Message Categories must also be programmed. Select whether terminal will display System Status messages such as Power Supply, Battery, Communication or LAN Network problems. Select whether terminal will display custom LCD Messages. An LCD Message, if valid, will normally be displayed in addition to the selected Idle Display. If "Idle Entities" has been chosen for the Idle display, and there are 4 or more Idle Entities selected, LCD messages cannot be displayed. Input Level messages allowed. (Limited Messages) Restricts the LCD Messages to the Defer Arm Warning ("Area about to turn on") and LCD Message 1 broadcasts.
	Alarm Message Categories	Message Categories 1-8 determine which Area Zone state messages will be displayed on this Terminal. Messages will be displayed for Zones that have a matching category set in their Process Group.
Logged Off Keys	Logged Off Key Operations. Allow Quick Alarm Review Allow Named Actions Allow Aircon Control Allow Show Info Allow Logged Off Panic	Select the Terminal operations allowed when logged off. Quick Alarm Review allowed via <MENU>, <2>. Named Actions allowed via <MENU>, <1>. Note that the named action must have the "Allow Logged Off Access" option enabled. Aircon Control allowed via <MENU>, <3>. System Information allowed via <MENU>, <4>. The Terminal "Panic" System Input can be triggered by pressing the <HELP> key 3 times in succession. Note that since this is a "logged off" operation, the Terminal rather than the User will be identified in Review and Reporting messages.
Access Control	Associated Door	Select a Door to be associated to this Terminal. The Door nominated will be controlled and monitored by this terminal.
	Access Control Options. Access Only. No Lock. *(V1 to V2 only)* Enable Reed Input Enable Tongue Input.	 This Terminal may only be used for access control. **CAUTION:** Once set, you will not be able to access other operations or Menus from this Terminal. Set to 'Y' if there is no lock hardware for this Door Allow Door Reed Switch logic for this Door. Allow Tongue Sense logic for this Door.
	Dual Code Wait Time.	Enter a Dual Code Time in Minutes and Seconds. Determines how long this Terminal will wait for the second PIN Code in a dual PIN entry.

	Reader 01 Purpose Control a Door Control a Lift Log On Area Toggle	Reader Purpose defines how the Reader will be used. Door access control. Lift access control. Terminal Logon. A Valid Card presentation logs the User on to the associated LCD Terminal. Controller Firmware V3.1.0 or later recommended if this feature is used. Area On/Off only. No access control operations. The "Keypad Area" option below must also be programmed.
	Reader 01 Location None Inside Door 1 Outside Door 1	Determines the location of the Terminal in relation to the associated Door; Inside or Outside. Only the Door 1 options are relevant to a Graphic Terminal.
	Keypad Area.	Reader Keypad Area. Select the Area to control when the Reader purpose is "Area Toggle".
	Card Format. Direct Entry Wiegand 26Bit Wiegand (H10301) Indala 27 Bit – Wiegand Keri 30 Bit Wiegand etc…	This screen allows the Card Format to be selected. Card Formats are programmed separately. A wide range of default Card Formats are available. Not relevant to Graphic Terminals at present. *See 2 Door Reader Module programming for the full list of default card formats and their details.*
	Any Card Mode.	If enabled, any card of the correct type will be allowed access and the card data will be logged to Review. Not relevant to Graphic Terminals at present.
	PIN Device (Entity for PIN Code Entry)	Select a Module/Reader to be used for entering the PIN Code when Card + PIN is required. Controller Firmware V3.1.0 or later recommended if this feature is used with an Elite LCD or Integriti Prisma Graphic Terminal. Not relevant to Graphic Terminals at present.
	Wiegand PIN Mode. None Motorola HID Reader MR Access Model Reader 26 Bit Wiegand Keypad IR Weatherproof Terminal 26 Bit Wiegand Keypad Forced	Select the PIN data mode if a Reader" was selected in the "PIN Device" option above. No PIN entry requirement. Motorola/Indala ARK-501 HID 5355 or iClass with 4 Bit Burst PIN output format. MR Access Magnetic Swipe & PIN code Reader 26 Bit Wiegand Keypad. Inner Range Weatherproof Terminal. 26 Bit Wiegand Keypad Forced. Not relevant to Graphic Terminals at present.

	Reader Arming Mode No Reader Arming User Area w/button Area Empty Exit Area w/button Entry Area w/button Exit Area on 3 Swipes Entry Area on 3 Swipes Arm Users 'Tenancy Area' on 3 Swipes.	Select the Area Arming Mode if the Reader is to be used for Area Arming on Access Control operations. No Arming. Arm the User Area if the "Arm" button is pressed while the Card is presented. Arm the Exit Area (Area you are leaving) if the Area User Count decrements to zero when the Card is presented. Arm the Exit Area if the "Arm" button is pressed while the Card is presented. Arm the Entry Area if the "Arm" button is pressed while the Card is presented. Arm the Exit Area if Card presented 3 times within 5 seconds. Arm the Entry Area if Card presented 3 times within 5 seconds. Arm the User's Tenancy Area if Card presented 3 times within 5 seconds. (Cont F/ware V3.2.1 or later only) NOTES: 1) SOME OF THESE OPTIONS NOT RELEVANT TO GRAPHIC TERMINAL. E.g. ARM BUTTON OPERATION. 2) Exit Area / Entry Area. The Exit Area is the Area you are leaving. i.e. The Area the Reader is installed in. The Entry Area is the Area on the opposite side of the Door to where the Reader is installed. 3) 3 Swipe Arming. V3.3.0 firmware or later provides a Controller option for setting a different "Three Badge Wait" time.
	Ask PC	This option allows User Credentials presented at this Reader to be utilized in the Active User Rotation Module (AURM) feature and/or the Operator Challenge feature if necessary. *AURM* *See the "Enable AURM" option in the Controller General Behaviour options for more details.* *OPERATOR CHALLENGE* *See the Integriti Software "Guide - Operator Challenge" document for more details.*
Security (Incorrect PIN Lockout)	Lockout attempts	The number of incorrect PIN entries before the Terminal is Locked Out. The number of tries must occur within the Attempts Time.
	Lockout Time	Defines how long this Terminal will reject PIN operations once the number of Lockout Attempts has been reached within the Attempts Time.
	PIN Attempt Timeout	PIN attempts Timer. The amount of time in which the Lockout Attempts must be reached before the Terminal becomes Locked Out. This is the time required to elapse before the lockout count is reset after an illegal PIN has been entered.
LAN Module settings	LAN Poll Time	Enter a Poll Time in Minutes, Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module.

	Battery Test Time	Not applicable to Graphic Terminals.
	Unibus Modules	Not currently applicable to Graphic Terminals.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the "Navigation" Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.
Extra Restrictions.	 What When	Up to 6 Permissions can be assigned to a Graphic Terminal to place additional restrictions on the operations allowed to be performed. e.g. A limited permission set may be required at particular Terminals during certain times of the day, or while a particular Area is armed or disarmed. Defines the entity for this Permission. e.g. Menu Group, Area List, etc. Defines when the entity is valid for this Permission. e.g. Time Period, Area state, etc. *See Permission programming in "Generic Programming Operations" for details.*

Expander

Expander programming is relevant to the following Modules:

- Integriti 8-32 Zone Expander.
- Integriti 16-Zone Expander.
- Concept 3/4000 Universal Expander, 32 Zone (B).
- Concept 3/4000 Universal Expander, 16 Zone (E).
- Concept 3/4000 Mini Expander.
- Concept 3/4000 Analogue Module.

Entity/Feature	Option	Description
Create/Find Expander		'Add New' or select a record to edit.
Module Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.

Inputs	EOL for Zones… (EOL [End-Of-Line] Resistor Scheme for Zone Inputs)	Select the End Of Line Resistor scheme to be used for the Zone Inputs on this Integriti Expander. An EOL scheme can be selected for each block of 8 Zone Inputs: Block 1: Zones 1 to 8 Block 2: Zones 9 to 16 Block 3: Zones 17 to 24 Block 4: Zones 25 to 32 *See "Inputs" in the Controller "Module Details" programming for details of the EOL Scheme options.* Note that this option is only relevant to: • Integriti 8-32 Zone Expander. • Integriti 16-Zone Expander (No longer available). • Concept 3/4/5000 Universal Expander V8.0 or later. P/N: 995004EUPCB&K (Europe only) With the exception of the Universal Expander listed above, legacy Concept 3000/4000 Universal Expanders Rev H or later have EOL scheme selection available via on-board DIPswitch options. Other legacy Concept 3000/4000 Expanders that are compatible with Integriti, do not have selectable EOL.
Advanced Settings.	Analogue Hysteresis	Enter an Analogue Hysteresis value. This is the sensitivity to changes in analogue values to initiate a change of state. NOTE: Used for legacy Concept 3000 Analogue Modules only. For Integriti Expanders, this option is set in the relevant Input programming.
Obsolete Options	AC Hold-Off Time	Specifies the period that an AC Fail condition may exist before the AC Fail System Input is triggered for this Module. Only required in Controller Firmware up to V3.0. In Controller Firmware V3.1 or later, this option is programmed in the General Controller Programming.
LAN Module settings	Poll Time	Enter a Poll Time in Minutes, Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module.
	Battery Test Time	Enter a Battery Test Time in Hours and Minutes. Determines the battery test time for this Module.
	Unibus Modules	Define the Unibus Modules installed on relevant types of Integriti Expander Modules. Not relevant for Concept Expanders.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the "Navigation" Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.

Radio Expander

Radio Expander programming is relevant to the following Modules:

- Concept 3/4000 Visonic Wireless I/F.
- Concept 3/4000 Paradox Wireless I/F.

Entity/Feature	Option	Description
Create/Find Radio (RF) Module.		'Add New' or select a record to edit.
Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
Inputs	EOL	Not relevant to RF Expanders.
Advanced Options	OK Feedback Action None Control Area Control Area List Control Aux Control Aux List Etc.	Allows an entity to be chosen to provide feedback for "OK" indication. e.g. A Siren Chirp, or an Auxiliary that controls a Beeper. When an action entity is selected additional options will be displayed to program the remaining action settings. *See Action programming in "General Programming Operations for programming details.*
	RF Poll Time.	Enter a Transmitter Poll Time in Hours. The Poll time is the maximum amount of time an RF device can remain out of communication with the RF Expander Module.
	US Jamming	Enable US Jamming detection algorithm.
Logging	Log Missed RF. Log RF Zone Details. Log RF Remote Details.	An event is logged to Review to indicate re-synchronizing of a Fob that is slightly out of sync with the Receiver. Logs Wireless Sensor activity to Review. Logs Wireless Remote activity to Review.
Sensor Registry.	RF Sensor ID 1 to 32 (HEX)	View or Enter the RF device IDs for registration with this module. The device ID is entered in HEXADECIMAL format. Up to 32 devices can be registered with an RF Expander Module.
LAN Module	Poll Time	Enter a Poll Time in Minutes and Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module.
	Battery Test Time	Not relevant to the current range of RF Expander Modules.
	Unibus Modules	Not relevant to the current range of RF Expander Modules.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the "Navigation" Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.

Reader Module

Reader Module programming is relevant to the following 2-Door and Single Door Modules:

- Concept 3000/4000 2-Door Access Modules.
- Concept 3000/4000 Single Door Access Modules.
- Concept 3000/4000 Weatherproof Terminal.
- Integriti SLAM. (Smart LAN Access Module). Not yet available.

Entity/Feature	Option	Description
Create/Find Reader Module		'Add New' or select a Record to edit.
Module Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
Readers. These options are programmed separately for Reader 1 and Reader 2.	Reader Purpose Control a Door Control a Lift Log On Area Toggle	Reader Purpose defines how the Reader will be used. Door access control Lift access control Terminal Logon. A Valid Card presentation logs the User on to the associated LCD Terminal. Controller Firmware V3.1.0 or later recommended if this feature is used. Area On/Off only. No access control operations.
	Reader Location None Inside Door 1 Outside Door 1 Inside Door 2 Outside Door 2 Inside Door 3…etc.	Determines which Door the Reader is associated with, and the location of the Reader in relation to the Door; Inside or Outside. Typically, Access Control Readers are Entry Readers, and are therefore located 'Outside' the nominated Door. A Reader can also be located 'Inside' the nominated Door when the Reader is an Exit Reader, or when there are Readers on both sides of a Door. Reader is not associated with a Door. Reader is located Inside the 1st Door. Reader is located Outside the 1st Door. Reader is located Inside the 2nd Door. (2-Dr Modules only) Reader is located Outside the 2nd Door. (2-Dr Modules only) Options for Doors 3 to 8 are not relevant to Reader Modules.
	Keypad Area.	Reader Keypad Area. Select the Area to control when the Reader purpose is "Area Toggle".

	Card Format.	This option allows the Card Format to be selected. Card Formats are programmed separately and are used to define the Card Type, bit length and Site Code parameters (if relevant) within a single Entity. A wide range of default Card Formats are available. If the required format is not in the list, additional Card Formats can be added via Card Format programming.
	Direct Entry Wiegand 26Bit Wiegand (H10301) Indala 27 Bit - Wiegand Keri 30 Bit Wiegand Ind/Kant KSF 32Bit Wiegand HID 32 Bit Wiegand KASTLE 32Bit Wiegand HID 34Bit Wiegand (H10306) Indala 34Bit Wiegand HIDCorp1000 35Bit (H50360) HID 35 Bit Wiegand Indala 36 Bit Wiegand HID 36Bit Wieg (Std) HID 36Bit Wiegand (S906133A) HID 37Bit No SC (H10302) HID 37Bit SC (H10304) HID iClass 37Bit Wiegand BQT 38Bit Wiegand HID 40Bit Wiegand IR Secure40 Wiegand IRMag Secure C3K Mag Direct Integriti Mag Direct	Direct Entry Wiegand HID 26 Bit Wiegand (H10301) Indala 27 Bit Wiegand Keri 30 Bit Wiegand Indala / Kantech KSF 32 Bit Wiegand HID 32 Bit Wiegand KASTLE Wiegand Swipe Card 32 Bit HID 34 Bit Wiegand (H10306) Indala 34 Bit Wiegand HID Corporate 1000 35 Bit Wiegand (H50360) HID 35 Bit Wiegand Indala 36 Bit Wiegand HID 36 Bit Wiegand (Std) HID 36Bit Wiegand (S906133A) HID 37 Bit Wiegand with No Site Code (H10302) HID 37 Bit Wiegand with Site Code (H10304) HID iClass 37 Bit Wiegand BQT 38 Bit Wiegand HID 40 Bit Wiegand Inner Range Secure40 Inner Range Magnetic Card Secure Site Code Concept 3000/4000 Magnetic Card Direct Entry Integriti Magnetic Card Direct Entry
	Any Card Mode.	Any card of the correct type will be allowed access and the card data will be logged to Review.
	PIN Device (Entity for PIN Code Entry)	Select a Module/Reader to be used for entering the PIN Code when Card + PIN is required. Controller Firmware V3.1.0 or later recommended if this feature is used with an Elite LCD or Integriti Prisma Graphic Terminal.

	Wiegand PIN Mode. None Motorola HID Reader MR Access Model Reader 26 Bit Wiegand Keypad IR Weatherproof Terminal 26 Bit Wiegand Keypad Forced	Select the PIN data mode if a Reader" was selected in the "PIN Device" option above. No PIN entry requirement. Motorola/Indala ARK-501 HID 5355 or iClass with 4 Bit Burst PIN output format. MR Access Magnetic Swipe & PIN code Reader 26 Bit Wiegand Keypad. Inner Range Weatherproof Terminal. 26 Bit Wiegand Keypad Forced. This reader can only be used for PIN codes. If enabled, any 26 bit Wiegand data received from this Reader will be processed as a PIN Code regardless of the Site Code. Cards will not be able to be used at this Reader. If disabled, only 26 bit Wiegand data with Site Code 255 (FF) will be processed as a PIN Code and any other Site Code will be processed as a Card. Normally a 26bit Wiegand Keypad has the site code $FF (255) with the card number representing the PIN code. If the reader sends some other site code with a PIN or $FF is actually a site code used by the system, then this option can be used to force any 26bit card number to be treated as a PIN code.
	Reader Arming Mode No Reader Arming User Area w/button Area Empty Exit Area w/button Entry Area w/button Exit Area on 3 Swipes Entry Area on 3 Swipes Arm Users 'Tenancy Area' on 3 Swipes.	Select the Area Arming Mode if the Reader is to be used for Area Arming on Access Control operations. No Arming. Arm the User Area if the "Arm" button is pressed while the Card is presented. Arm the Exit Area (Area you are leaving) if the Area User Count decrements to zero when the Card is presented. Arm the Exit Area if the "Arm" button is pressed while the Card is presented. Arm the Entry Area if the "Arm" button is pressed while the Card is presented. Arm the Exit Area if Card presented 3 times within 5 seconds. Arm the Entry Area if Card presented 3 times within 5 seconds. Arm the User's Tenancy Area if Card presented 3 times within 5 seconds. (Cont F/ware V3.2.1 or later only) NOTES: 1) Exit Area / Entry Area. The Exit Area is the Area you are leaving. i.e. The Area the Reader is installed in. The Entry Area is the Area on the opposite side of the Door to where the Reader is installed. 2) 3 Swipe Arming. V3.3.0 firmware or later provides a Controller option for setting a different "Three Badge Wait" time.

	Ask PC	This option allows User Credentials presented at this Reader to be utilized in the Active User Rotation Module (AURM) feature and/or the Operator Challenge feature if necessary. *AURM* *See the "Enable AURM" option in the Controller General Behaviour options for more details.* *OPERATOR CHALLENGE* *See the Integriti Software "Guide - Operator Challenge" document for more details.*
Door Access Control	Door 1 (First Associated Door)	Select the first Door to be assigned to this Reader Module. The Door nominated will be controlled and monitored by this Module.
	Settings for first Door. No Lock. *(V1 to V2 only)* Enable Reed Input Enable Tongue Input	 No Lock. Set to 'Y' if there is no lock hardware for this Door Reed Switch. Allow Door Reed Switch logic for this Door. The state of the Reed Switch Input will be utilized in functions such as Forced Door, DOTL, Interlocking, etc. Tongue Sense. Allow Tongue Sense logic for this Door. The state of the Tongue Sense Input will be utilized in functions such as Forced Door, DOTL, Interlocking, etc.
	Door 2 (Second Associated Door)	Select the second Door to be assigned to this Reader Module if required. If this Reader Module is providing Entry and Exit Readers for the same Door, then a second Door is not assigned. The Door nominated will be controlled and monitored by this Module.
	Settings for second Door. No Lock. *(V1 to V2 only)* Enable Reed Input Enable Tongue Input	 No Lock. Set to 'Y' if there is no lock hardware for this Door Reed Switch. Allow Door Reed Switch logic for this Door. The state of the Reed Switch Input will be utilized in functions such as Forced Door, DOTL, Interlocking, etc. Tongue Sense. Allow Tongue Sense logic for this Door. The state of the Tongue Sense Input will be utilized in functions such as Forced Door, DOTL, Interlocking, etc.
	General Door options. No LEDs Override EOL	 Disable LED Outputs. LEDs will not provide Valid/Invalid indication and will only be controlled by the associated Auxiliary. Overrides the EOL Resistor requirement for the REX (Request to Exit) and REN (Request to Enter) Inputs on all Doors. When enabled, the Normally Open contacts of the switch can be wired directly into the REX and/or REN Inputs with no EOL resistors.
Lift Access Control	Lift Car 1 (First Associated Lift)	Select the first Lift to be assigned to this Reader Module. The access control Reader interface for the nominated Lift will be provided by this Module.

	Lift Car 2 (Second Associated Lift)	Select the second Lift to be assigned to this Reader Module. The access control Reader interface for the nominated Lift will be provided by this Module. Note that Reader Modules for Lift Control are often installed in the Lift Car. This means that a second Lift Car is usually not assigned to a Reader Module.
Offline Operation	Card Cache Time None 1 Hour 4 Hours 8 Hours 1 Day 2 Days 4 Days 1 Week 2 Weeks 1 Month 2 Months 4 Months	Select the period for which a Cached Card will be retained in the Cache from the last time it was used. Integriti Modules only. Not relevant for Concept 3/4000 Reader Modules.
	Button Cache Time	Select the period for which a Cached Button operation will be retained in the Cache from the last time it was used. Integriti Modules only. Not relevant for Concept 3/4000 Reader Modules. Options are the same as those for Card Cache Time above.
	Offline Function. None First 2 Credentials Pass Use Cached Credentials	Determines which card credentials the reader will process in offline mode. No Card access when Module is offline. Allow access for the first 2 Backup Cards only when Module is offline. Allow access to Cards stored in the local Cache when Module is offline.
	    Door 1 Entry dual user Door 2 Entry dual user Door 1 Exit dual user Door 2 Exit dual user Door 1 Entry ren button Door 2 Entry ren button Door 1 Exit rex button Door 2 Exit rex button	Standalone Operation options for the Doors assigned to the Module. These requirements will only be relevant while the Module is Offline. Dual User requirement for Entry at first Door. Dual User requirement for Entry at second Door. Dual User requirement for Exit at first Door. Dual User requirement for Exit at second Door. REN button will operate at first Door. REN button will operate at second Door. REX button will operate at first Door. REX button will operate at second Door.

Inputs	EOL for Zones. (EOL [End-Of-Line] Resistor Scheme for Zone Inputs)	Select the End of Line Resistor Scheme for an Integriti Standard (2-Door) LAN Access Module (SLAM). *See "Inputs" in the Controller "Module Details" programming for details of the EOL Scheme options.* Note that this option is only relevant to the Integriti 2-Door Reader Module (SLAM). Legacy Concept 3000/4000 Reader Modules that are compatible with Integriti, do not have selectable EOL.
LAN Module	Poll Time	Enter a Poll Time in Minutes, Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module
	Battery Test Time	Enter a Battery Test Time in Hours and Minutes. Determines the battery test time for this Module. Integriti Modules only. Not relevant for Concept 3/4000 Reader Modules.
	Unibus Modules	Define the Unibus Modules installed on Integriti Reader Modules. Not relevant for Concept 3/4000 Reader Modules.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the "Navigation" Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.

Intelligent Reader Module

Intelligent Reader Module programming is relevant to the following hardware Modules:

- Integriti ILAM
- Integriti Salto Interface
- Concept 3/4000 Intelligent 4-Door Controller V5.0 or later.

Entity/Feature	**Option**	**Description**
Create/Find Intelligent 4-Door Access Module		'Add New' or select a record to edit. Integriti ILAM requires Integriti Controller Firmware V3.0.0 or later. V3.1.4 or later recommended. Concept 3/4000 Intelligent 4-Door Access Module must be V5.0 or later and the Integriti Controller Firmware must be V2.5.0 or later.
Module Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
Readers. These options are programmed separately for Readers 1 to 16.	Reader Purpose Control a Door Control a Lift Log On Area Toggle	Reader Purpose defines how the Reader will be used. Door access control Lift access control Terminal Logon. A Valid Card presentation logs the User on to the associated LCD Terminal. Controller Firmware V3.1.0 or later recommended if this feature is used. Area On/Off only. No access control operations.

	Reader Location	Determines which Door the Reader is associated with, and the location of the Reader in relation to the Door; Inside or Outside. Typically, Access Control Readers are Entry Readers, and are therefore located 'Outside' the nominated Door. A Reader can also be located 'Inside' the nominated Door when the Reader is an Exit Reader, or when there are Readers on both sides of a Door.
	None	Reader is not associated with a Door.
	Outside Door 1 Outside Door 2 Outside Door 3 Outside Door 4 Outside Door 5 Outside Door 6 Outside Door 7 Outside Door 8	Reader is located Outside the nominated Door.
	Inside Door 1 Inside Door 2 Inside Door 3 Inside Door 4 Inside Door 5 Inside Door 6 Inside Door 7 Inside Door 8	Reader is located Inside the nominated Door.
	Keypad Area.	Reader Keypad Area. Select the Area to control when the Reader purpose is "Area Toggle".

	Card Format. Direct Entry Wiegand 26Bit Wiegand (H10301) Indala 27 Bit - Wiegand Keri 30 Bit Wiegand Ind/Kant KSF 32Bit W... HID 32 Bit Wiegand KASTLE 32Bit Wiegand HID 34Bit Wiegand (H1... Indala 34Bit Wiegand HIDCorp1000 35Bit (H5... HID 35 Bit Wiegand Indala 36 Bit Wiegand HID 36Bit Wieg (Std) HID 36Bit Wiegand (S9... HID 37Bit No SC (H10302) HID 37Bit SC (H10304) HID iClass 37Bit Wiegand BQT 38Bit Wiegand HID 40Bit Wiegand IR Secure40 Wiegand IRMag Secure C3K Mag Direct Integriti Mag Direct	This screen allows the Card Format to be selected. Card Formats are programmed separately. A wide range of default Card Formats are available. If the required format is not in the list, additional Card Formats can be added via Card Format programming. Direct Entry Wiegand HID 26 Bit Wiegand (H10301) Indala 27 Bit Wiegand Keri 30 Bit Wiegand Indala / Kantech KSF 32 Bit Wiegand HID 32 Bit Wiegand KASTLE Wiegand Swipe Card 32 Bit HID 34 Bit Wiegand (H10306) Indala 34 Bit Wiegand HID Corporate 1000 35 Bit Wiegand (H50360) HID 35 Bit Wiegand Indala 36 Bit Wiegand HID 36 Bit Wiegand (Std) HID 36Bit Wiegand (S906133A) HID 37 Bit Wiegand with No Site Code (H10302) HID 37 Bit Wiegand with Site Code (H10304) HID iClass 37 Bit Wiegand BQT 38 Bit Wiegand HID 40 Bit Wiegand Inner Range Secure40 Inner Range Magnetic Card Secure Site Code Concept 3000/4000 Magnetic Card Direct Entry Integriti Magnetic Card Direct Entry
	Any Card Mode.	Any card of the correct type will be allowed access and the card data will be logged to Review.
	PIN Device (Entity for PIN Code Entry)	Select a Module/Reader to be used for entering the PIN Code when Card + PIN is required. Controller Firmware V3.1.0 or later recommended if this feature is used with an Elite LCD or Integriti Prisma Graphic Terminal.

	Wiegand PIN Mode. None Motorola HID Reader MR Access Model Reader 26 Bit Wiegand Keypad IR Weatherproof Terminal 26 Bit Wiegand Keypad Forced	Select the PIN data mode if a Reader" was selected in the "PIN Device" option above. No PIN entry requirement. Motorola/Indala ARK-501 HID 5355 or iClass with 4 Bit Burst PIN output format. MR Access Magnetic Swipe & PIN code Reader 26 Bit Wiegand Keypad. Inner Range Weatherproof Terminal. 26 Bit Wiegand Keypad Forced. This reader can only be used for PIN codes. If enabled, any 26 bit Wiegand data received from this Reader will be processed as a PIN Code regardless of the Site Code. Cards will not be able to be used at this Reader. If disabled, only 26 bit Wiegand data with Site Code 255 (FF) will be processed as a PIN Code and any other Site Code will be processed as a Card. Normally a 26bit Wiegand Keypad has the site code $FF (255) with the card number representing the PIN code. If the reader sends some other site code with a PIN or $FF is actually a site code used by the system, then this option can be used to force any 26bit card number to be treated as a PIN code.
	Reader Arming Mode No Reader Arming User Area w/button Area Empty Exit Area w/button Entry Area w/button Exit Area on 3 Swipes Entry Area on 3 Swipes Arm Users 'Tenancy Area' on 3 Swipes.	Select the Area Arming Mode if the Reader is to be used for Area Arming on Access Control operations. No Arming. Arm the User Area if the "Arm" button is pressed while the Card is presented. Arm the Exit Area (Area you are leaving) if the Area User Count decrements to zero when the Card is presented. Arm the Exit Area if the "Arm" button is pressed while the Card is presented. Arm the Entry Area if the "Arm" button is pressed while the Card is presented. Arm the Exit Area if Card presented 3 times within 5 seconds. Arm the Entry Area if Card presented 3 times within 5 seconds. Arm the User's Tenancy Area if Card presented 3 times within 5 seconds. (Cont F/ware V3.2.1 or later only) NOTES: 1) Exit Area / Entry Area. The Exit Area is the Area you are leaving. i.e. The Area the Reader is installed in. The Entry Area is the Area on the opposite side of the Door to where the Reader is installed. 2) 3 Swipe Arming. V3.3.0 firmware or later provides a Controller option for setting a different "Three Badge Wait" time.

	Ask PC	This option allows User Credentials presented at this Reader to be utilized in the Active User Rotation Module (AURM) feature and/or the Operator Challenge feature if necessary. *AURM* *See the "Enable AURM" option in the Controller General Behaviour options for more details.* *OPERATOR CHALLENGE* *See the Integriti Software "Guide - Operator Challenge" document for more details.*
Door Access Control.	Door 1 to Door 8 assignment. (Associated Doors)	Select the Doors to be assigned to this Reader Module. The Doors nominated will be controlled and monitored by this Module.
	Settings for Individual Doors. No Lock. *(V1 to V2 only)* Enable Reed Input Enable Tongue Input	The Door settings are programmed separately for each of the eight Doors. Set to 'Y' if there is no lock hardware for this Door Reed Switch. Allow Door Reed Switch logic for this Door. The state of the Reed Switch Input will be utilized in functions such as Forced Door, DOTL, Interlocking, etc. Allow Tongue Sense logic for this Door. The state of the Tongue Sense Input will be utilized in functions such as Forced Door, DOTL, Interlocking, etc.
	General Door options. No LEDs Override EOL	 Disable LED Outputs. LEDs will not provide Valid/Invalid indication and will only be controlled by the associated Auxiliary. Overrides the EOL Resistor requirement for the REX (Request to Exit) and REN (Request to Enter) Inputs on all Doors. When enabled, the Normally Open contacts of the switch can be wired directly into the REX and/or REN Inputs with no EOL resistors.
Access Control: Lift Cars.	Lift Car 1 to Lift Car 8 assignment. (Associated Lift Cars)	Select the Lifts to be assigned to this Reader Module. Access control for the nominated Lifts will be provided by this Module.
Offline Options.	Card Cache Time None 1 Hour 4 Hours 8 Hours 1 Day 2 Days 4 Days 1 Week 2 Weeks 1 Month 2 Months 4 Months	Select the period for which a Cached Card will be retained in the Cache from the last time it was used.
	Button Cache Time	Select the period for which a Cached Button operation will be retained in the Cache from the last time it was used. Options are the same as those for Card Cache Time above.
	Verbose Review	The IFDAM Review Log will include extra detail that may be useful during commissioning and troubleshooting.

Standalone Operation.		Standalone Operation options for the Doors assigned to the Module. These requirements will only be relevant while the Module is Offline. The four standalone operation options are programmed separately for each of the eight Doors.
	Door 1 Entry dual user Door 2 Entry dual user Door 3...	Dual User requirement for Entry at first Door. Dual User requirement for Entry at second Door. Dual User Entry options continue for Doors 3 to 8.
	Door 1 Exit dual user Door 2 Exit dual user Door 3...	Dual User requirement for Exit at first Door. Dual User requirement for Exit at second Door. Dual User Exit options continue for Doors 3 to 8.
	Door 1 Entry ren button Door 2 Entry ren button Door 3...	REN button will operate at first Door. REN button will operate at second Door. REN button options continue for Doors 3 to 8.
	Door 1 Exit rex button Door 2 Exit rex button Door 3...	REX button will operate at first Door. REX button will operate at second Door. REX button options continue for Doors 3 to 8.
	Historic Review download pace time (ms)	If the Module has been offline and reconnects, the Review Events logged locally while offline need to be transferred to the Controller. These “historic review” messages are “paced” in order to minimise disruption to normal LAN traffic. This pace time setting sets the time the Module waits between sending each review event to the Controller.
Inputs	End Of Line Config. (EOL [End-Of-Line] Resistor Scheme for Zone Inputs) Concept3K 8-State Tecom Compat	Select the End Of Line Resistor scheme to be used for the Zone Inputs on this Intelligent LAN Access Module (ILAM). *See “Inputs” in the Controller “Module Details” programming for details of the EOL Scheme options.* Note that this option is only relevant to the Integriti Intelligent LAN Access Module (ILAM). Legacy Concept 3000/4000 Intelligent Reader Modules that are compatible with Integriti, do not have selectable EOL.
Connectivity. Serial Reader Settings.	Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	Selects the Serial Channel or Port. Not relevant to Concept Intelligent 4 Door Access Module. No Modem connection. On-board “Port 0” connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4. Port 1 Unibus UART 4, Port 2

	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	Selects the Baud Rate. Not relevant to Concept Intelligent 4 Door Access Module.
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	Selects the number of Bits. Not relevant to Concept Intelligent 4 Door Access Module.
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	Selects the Parity scheme. Not relevant to Concept Intelligent 4 Door Access Module.
	Stop Bits 1 Bit 2 Bits	Selects the number of Stop Bits. Not relevant to Concept Intelligent 4 Door Access Module.

Access Control Hardware Mapping	Door Mapping	Door Mapping is used to map the logical Door number on this Module to the Hardware that is to be used for that Door. There are 8 logical Doors on an Integriti Intelligent LAN Access Module. There are 4 logical Doors on a Concept Intelligent 4-Door Access Module. The Door mapping is programmed by defining the following parameters for each logical Door to be used: - The hardware "Device Type". - The "DIP Switch Setting" on the device (if relevant) - The number of the entity on the device. i.e. Number 1 or 2 if the device supports 2 Readers, or 2 Doors.
	Device Type: Not Present Onboard Hardware Unibus Reader Unibus Door Salto Aperio Serial Reader OSDP	 Not present Onboard Hardware. Unibus Reader (2 Readers). Not relevant to C3K IFDAM. Unibus Door (2 Readers / 2 Doors) Not relevant to C3K IFDAM. Salto RS485. Not relevant to C3K IFDAM. Aperio. Not relevant to C3K IFDAM. Serial Reader. Not relevant to C3K IFDAM. RS485 Reader. e.g. HID OSDP Reader or Inner Range SIFER Reader. (Requires V4 or later)
	DIP Switch Setting	Enter a value between 1 and 8. Not relevant to C3K IFDAM.
	Number on Device	Enter a value between 1 and 2. Not relevant to C3K IFDAM.

	Reader Mapping	Reader Mapping is used to map the logical Reader number on this Module to a hardware Reader Port. There are 16 logical Readers on an Integriti Intelligent LAN Access Module. There are 8 logical Readers on a Concept Intelligent 4-Door Access Module. The Reader mapping is programmed by defining the following parameters for each logical Reader to be used: - The hardware "Device Type". - The "DIP Switch Setting" on the device (if relevant) - The number of the entity on the device. i.e. Number 1 or 2 if the device supports 2 Readers, or 2 Doors.
	Device Type: Not Present Onboard Hardware Unibus Reader Unibus Door Salto Aperio Serial Reader OSDP	 Not present Onboard Hardware. Unibus Reader (2 Readers). Not relevant to C3K IFDAM. Unibus Door (2 Readers / 2 Doors) Not relevant to C3K IFDAM. Salto RS485. Not relevant to C3K IFDAM. Aperio. Not relevant to C3K IFDAM. Serial Reader. Not relevant to C3K IFDAM. RS485 Reader. e.g. HID OSDP Reader or Inner Range SIFER Reader. (Requires V4 or later)
	DIP Switch Setting	Enter a value between 1 and 8. Not relevant to C3K IFDAM.
	Number on Device	Enter a value between 1 and 2. Not relevant to C3K IFDAM.
LAN Module	Poll Time	Enter a Poll Time in Minutes, Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module
	Battery Test Time	Enter a Battery Test Time in Hours and Minutes. Determines the battery test time for this Module.
	Unibus Modules	Define the Unibus Modules installed on Integriti Reader Modules. Not relevant for Concept Intelligent 4-Door Access Modules.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the "Navigation" Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.

Concept Intelligent 4-Door Access Module Notes

V5 or later Concept IFDAM Firmware release introduces support for Integriti Controllers V2.0 or later.

To enable Integriti mode.

Before power-up, set Switch 4 on the Options DIPswitch (S1) to ON.
i.e. S1 Switch 4 OFF = Concept 4000. Will need to have its DB defaulted 1st time, see installation manual.
S1 Switch 4 ON = Integriti Security Controller.
All other switches on S1 are set to OFF, unless the alternate AC Fail Delay time is required via Switch 2.

This setting causes the IFDAM to act similar to an Integriti 2-Door Reader with an offline cache of 2000 Users.
Note that the mode must be selected to match the type of Control Module that the IFDAM is to be used with.
If the mode does not match the Controller, the IFDAM Fault LEDs will indicate “Module Unknown”
(L2 = OFF, L3 = ON).

Operation in an Integriti System.

GENERAL OPERATION:
• Battery testing is operational.
• The fast unlock time option via Switch 8 on DIPswitch S1 is not supported.

ACCESS CONTROL OPERATIONS WHEN ONLINE:
In online mode, operation should be identical to an Integriti Two-Door Reader or Four-Door Reader Module.

ACCESS CONTROL OPERATIONS WHEN OFFLINE:
In offline mode, the IFDAM can use cached User/Button operations to provide access as follows:
• The cache contains up to 2000 User credentials.
• The cache can be cleared by setting Switch 8 on the Options DIPswitch (S1) to ON (as well as Switch 4) and power cycling the IFDAM. If Switch 8 is left on, then every power cycle will clear the cache.
• When a User is granted access whilst online, the User will be cached for that Door. If the cache is full then the oldest User will be replaced by the new User.
• If a User is denied access, then that User will be removed from the cache for that Door. If they are not in the cache for any other Doors on that Module, then they will be removed from the cache completely on that Module.
NOTE. Certain types of “access denied” events will not cause the User to be removed from the cache. E.g. Denied because the Door is interlocked, Denied because Area is On and User does not have permission to turn off that Area, etc.
• When a User is added to the cache, if the User programming has the “permanent cache” option set, then that User cannot be replaced by a newer User. The User will remain in the cache until removed by a power cycle with Switch 8 on, or if denied access at a Door and also not in the cache for any of the other Doors on that Module.
• In addition to Users being removed if a new User is added when the cache is full, Users can also be automatically removed if they have been in the cache for too long. This time is programmable between 1 hour and 4 months. Note that permanent Users are not removed by time.
• The caching of Users can also be disabled completely.

Note that Users are only added when online and access is granted.
Users are only removed from the Module cache:
• When access is denied for all the Doors on that Module on which the User had previously had an access granted event.
• Via time for non-permanent Users.
• Using a Switch 8 power cycle.

If Users are deleted from the Integriti Database whilst online, they are not removed from the cache. If Users are created whilst online they are not automatically added to the cache.
REX and REN button operations are also cached separately, per Door as follows:
- Whenever a REX/REN is allowed whilst online, the REX/REN for that Door is added to the cache.
- Whenever a REX/REN is denied whilst online, the REX/REN for that Door is removed from the cache.
- Cached buttons are also removed by time, programmable from 1 hour to 4 months (separate to User cache time) or can be disabled completely.
Whilst offline, whatever is in the cache determines access permissions.
Whatever REX/REN buttons are in the cache will remain operational until they time out.
Whatever Users are in the cache will remain operational until they timeout, unless they are permanent.
“Dual User” and “Card plus PIN” or “PIN only” is not supported in offline mode.
“PIN only” will not work. If a legal card was presented whilst online, even if a PIN was required but was incorrect, the card will still be added to the cache.

No record of User operations is kept whilst off line.
The Door unlock time is set to 5 seconds when offline.

Checking IFDAM Firmware Version.

The IFDAMcan be confirmed via an LCD Terminal as follows:
INTEGRITI:
NOTE: ISC Firmware must be V2.0 or later, and IFDAM Firmware must be V5.0 or later.
• Logon to the LCD Terminal and select Module Info. [MENU, 1, 8]
• Press the Down Arrow key (V) as often as required to locate the IFDAM to view. e.g. C3K-IRdr: 03
• Press the OK key. The display will show the current status of the selected IFDAM. e.g. Present and Secure.
• Press the OK key. The display will now show the current firmware version and build number of the selected IFDAM. e.g. 5.0.0_1

LAN Power Supply Module

LAN Power Supply Module programming is relevant to the Concept 3/4000 LAN Power Supply.
Integriti Smart Power Supplies are integrated with their host Module and do not require separate programming.

Calibration

LAN Power Supply Modules are calibrated at the factory during the manufacturing process. The Module does not normally require any further calibration unless the Module's firmware is upgraded, or a repair has been carried out that required components to be replaced.

Any Firmware upgrade or repair work performed by the manufacturer will also include re-calibration of the Module.

In the rare event of a firmware upgrade being performed in the field, a calibration procedure is available from the Distributor. The following equipment is required to perform the calibration procedure:
- A Digital Multimeter capable of measuring 0 to 20V DC and 0 to 1999mA DC.
- Dummy load. 10 to 15 Ohms. 15W. e.g. 12V, 15Watt Automotive lamp.
- Heavy guage (14/020) test leads for connection of Dummy load and Multimeter.

Entity/Feature	Option	Description
Create/Find LAN Power Supply Module		'Add New' or select a record to edit.
LAN Power Supply Name		Program a name of up to 32 characters in length. Use this feature to describe the location and/or purpose of the Module.
LAN Power Supply Options	Invert Auxiliary 1 Invert Auxiliary 2.	Invert the operation of Auxiliary 1. Invert the operation of Auxiliary 2. Normally set to "Y" when a Satellite Siren is connected to this output. *See Note below.* **IMPORTANT NOTE:** Auxiliary 2 is not an Open Collector output. It provides a switched +12V output via an on-board relay and can therefore be used to control a Battery-backed Satellite Siren or other similar controlled device. - When used for controlling a Battery-backed Satellite Siren, the 12V output normally needs to be present when the Auxiliary is Off, and removed when the Auxiliary is On. Therefore, the "2" option must be set to "Y". - When controlling a device such as a Strobe or Piezo Siren (where the 12V output needs to be present when the Auxiliary is ON) the "2" option must be set to "n".

LAN Module	Poll Time	Enter a Poll Time in Minutes and Seconds. The Poll time is the maximum amount of time a module can remain out of communication with the Control Module.
	Battery Test Time	Enter a Battery Test Time in Hours and Minutes. Determines the battery test time for this Module.
	Unibus Modules	Define the Unibus Modules installed on relevant types of Integriti Expander Modules. Not relevant for Concept LAN Power Supply Modules.
	Enable on LAN Disable on LAN	This operation is available by Right-clicking on the Module in the "Navigation" Pane. Provides a facility to temporarily disable a faulty Module on the LAN and Isolate its Inputs while awaiting service.
Miscellaneous LAN Power Supply Options.	Number of Slaves	Specifies the number of Slave Modules connected to a Master LAN Power Supply Module. Up to 3 Slave Modules can be connected. The default setting of 0 indicates that no Slave Modules are connected and disables the Slave Fail System Input for this LAN Power Supply Module. Slave Modules are connected to provide additional Battery charging current AND/OR Detector current on a LAN Power Supply Module. This is done by connecting additional "Slave" LAN Power Supply Modules to the 2-wire Slave Bus connection provided, and connecting the "+B" and "DET+" outputs of the Slave Module to the "+B" AND/OR "DET+" output of the Master Module. **IMPORTANT NOTE:** *See the Installation Manual for DIPswitch settings, wiring information and additional details.*
	Battery Overcurrent Detector Overcurremt	These options allow the Installer to independently specify the maximum current allowed from the Battery Charger circuit and the Detector Supply circuit before Over-current System Input Alarms are activated. NOT YET IMPLEMENTED. The value is programmed in milliAmps, and can be set from 0.1A (100mA) to 9.9 Amps in 100mA increments. A value of 00 means that the Over-current condition is not monitored. *See Important Notes below.*

	IMPORTANT NOTES: 1. 2. 3. CALCULATING THE MAXIMUM CURRENT AVAILABLE. Example 1: Example 2:	 - If using the Standard version of the Module, or an Enhanced version with no Slave Modules connected, the value should be set to no more than 4A. - If the Enhanced version is used, and Slave Modules are connected, a value of up to 9.9A may be set depending on the number of Slave Modules connected and the wiring configuration. - If the Master/Slave configuration chosen is designed to deliver more than 9.9A on a particular circuit, then Over-current monitoring for that circuit must be disabled. (Set value to 00) *See examples below.* The Maximum Battery Current or Detector Current available is calculated as follows: I max. = 2 + 2n. Where "n" is the number of Slave Supply outputs ("+B" and/or "DET+" outputs) connected to the specified Master output. If one Slave is connected, set to "Charger Only Mode" and +B / -B of the Slave is connected to +B / -B on the Master, then the maximum Battery current available would be 2 + (2x2) = 6A. "Charger Only Mode" combines the current available from the 2 outputs into the specified output. (In this case, the maximum guaranteed Detector current available would remain at 2A) If three Slaves are connected, set to "Split Mode" and: - +B / -B from all Slaves is connected to +B / -B on the Master. - DET+ / 0V from all Slaves is connected to DET+ / 0V on the Master. Then; The maximum Battery current available would be 2 + (2x3) = 8A; And the maximum Detector current available would also be 2 + (2x3) = 8A.
	Aux 2 Undercurrent	Specifies the minimum current required to prevent a Satellite Siren Tamper Alarm condition. The value should be set from 20 to 50mA in 1mA increments. The default value of 00 means that Aux2 Tamper current is not monitored. NOTE: Any value less than "20" disables Aux2 Tamper current monitoring. NOT YET IMPLEMENTED.

Communications Programming

Entity/Feature	Option	Description
Comms Tasks		Program/Edit the Communications Tasks. e.g. Integriti software interface, Alarm reporting, etc.
Telephone Numbers		Program/Edit any Telephone numbers that may be required for Dialler Comms Tasks.
DTMF Remote Control		Not yet implemented.
Network Interface Controllers (NICS)		Program/Edit Network Interfaces.
DNS Names (DNS Servers)		Program/Edit DNS Names.

Comms Tasks

Important Upgrade Notes.

In V3.0.0 and later Firmware, the “Comms Task Group” programming field in the GSM, SkyTunnel & Securitel Comms Task formats has been moved to the Review Filtering that is available within these Comms Task formats.
To upgrade the Integriti Controller firmware without any loss of functionality, one of the following methods can be taken:

- When upgrading the Integriti Controller firmware via the Integriti System Designer, if the Integriti System Designer is updated first to V3.0.0 or later then it will automatically migrate any existing Comms Task Group programming into the review filtering programming.
- When upgrading the Integriti Controller firmware manually (e.g. using an LCD Terminal and a USB memory stick), the existing programming will need to be re-entered using the LCD Terminal after the firmware update has completed. Before starting the firmware update process take note of the existing Comms Task Group programming. Then after the firmware update process has completed re-enter the Group programming into the review filter programming for the comms task. NOTE: If upgrading to this firmware from V2.5.2 firmware or later, then the Group programming can be entered in the review filter for the comms task before starting the firmware update process.

Comms Task Status Monitoring.

Where relevant to their operation, many Comms Task formats allow unused Zone Inputs to be assigned to monitor status conditions as shown in the following table.

This allows the Installer to assign the nominated Inputs to a “System” or “Comms Monitor” Area with an appropriate Process Group (e.g. “Comms Problem”) for local &/or remote annunciation/reporting or to trigger other actions or operations.

Notes:
1) Some of these options were not available prior to firmware V3.3.0
2) Any Zones used for this purpose must have the “Ignore Physical Input” option enabled in Input programming.

Format	Online Input	Fail Input	Backup Input
Integriti	Yes		
Monitor			
Dialler	Yes	Yes	Yes
GSM	Yes	Yes	Yes
Automation	Yes		
EMS	Yes		
Securitel	Yes		Yes
Intercom	Yes		
BMS	Yes		
EN32Pin			
SkyTunnel Reporting		Yes	Yes
E Modem			
Peer Reporting		Yes	Yes

Entity/Feature	Option	Description
Comms Tasks	Comms Task to Program: CT01	Select Communications Task to program. Use <UP>/<DOWN> Arrows to scroll, or use digit keys to enter the number.

Comms Task Setup	Type (format).	Select the Communications format for this Comms Task.
	None	No Comms Task format selected.
	Integriti	Integriti Software communications.
	Monitor	Monitor Comms Task. Only use if advised by Tech Support.
	Dialler	Digital Dialler Alarm Reporting. E.g. IRfast, Contact ID, SIA, etc.
	GSM	Multipath STU or GSM primary or backup reporting.
	Automation	Control, status monitoring and event logging communication protocol for 3rd Party Systems. e.g. Home/Building Automation, HVAC, etc.
	EMS	High-level interface for Elevator (Lift) Management Systems.
	Securitel	Securitel Serial STU format. While the Securitel network is no longer available, the Securitel Serial format is still utilized as the interface to some 3rd Party communicators.
	Intercom	Serial interface to 3rd Party Intercom products to facilitate integrated access control functionality.
	BMS	Allows an Integriti Controller to communicate directly with a 3rd party BMS system. e.g. Clipsal C-Bus.
	EN 32 Pin	Provides an interface to activate Auxiliaries or Zone Inputs for different types of alarms with Alarm confirmation (verification) logic for "Intruder" alarms. This allows reporting of alarm pin data via: - 3rd party communicators that support pin inputs for reporting. e.g. Redcare STU, 8-pin STU, GSM STU, etc. - Integriti Zone Inputs for reporting via any other Comms Task such as Contact ID or IRfast.
	SkyTunnel	A service provided by Inner Range that allows: - Temporary connection of an Integriti Controller to Integriti software or the Integriti Mobile App provided there is internet connectivity at both ends. - Alarm Reporting.
	E Modem	Answers calls from Integriti Software via a separate line connected to an external modem. Not yet supported.
	Peer Reporting	Allows an Integriti Controller to perform alarm reporting on behalf of other Integriti Controllers connected via the Peer Reporting Comms Task. e.g. Where multiple IAC and/or ISC Controllers are installed on the same site. Controller Firmware V3.2.1 or later required. Once the required format is selected, ensure that the Comms Task is currently “Idle”.

	Mode Normal Backup	Select whether this Comms Task is a normal Task or a Backup Task. This Comms Task is a Primary reporting Comms Task. This Comms Task is a Backup Comms Task to another Comms Task. e.g. It will only be used if the Primary Reporting Comms Task fails to communicate with the monitoring station.
	Backup Comms Task	Specifies the Comms Task number that will be used as the Backup Comms Task if required. The Backup Task will be triggered after the specified number of Attempts on the Primary Task has failed. When programming the nominated Backup Comms Task, it must be set to "Backup" mode.

INTEGRITI FORMAT		The Integriti Comms Task format allows communications with the Integriti Management Software via one or more prioritised communications paths including Ethernet, USB, RS-232 and Modem. Note that if multiple Integriti Comms Tasks are programmed, they cannot normally run simultaneously. Firmware V3.3.1 or later does allow Integriti Pro software and Integriti CS software to connect to an Integriti Controller simultaneously.
Ethernet Connection	Server IP Address	View or Enter the IP Address of the Integriti Server PC.
	TCP Port	View or Enter the Server TCP Port Number. The default Port number (004711) does not normally need to be changed.
	DNS Name	Select required DNS Server Name. DNS Servers are programmed separately.
Connectivity Paths	Path 1 Path 2 Path 3 Path 4	Select a primary communications path (Path 1) and any secondary communications paths to be used for communications with Integriti Management Software. The path number defines the priority. The options below are programmed separately for each of the four Communications Paths that can be used in the system.
	Type None TCP USB Serial IModem EModem SkyTunnel Phantom	Select the communications path to be used for communications with Integriti Management Software. No Path selected. Ethernet. USB Host Port. RS232 Serial Port. (Not currently supported) Internal Modem. On-board PSTN modem. External Modem. PSTN or GPRS Modem on a UniBus UART Port. Inner Range SkyTunnel service Factory debugging path only.

	Call	The Controller will call the Integriti Management Software Server.
	Answer	The Controller will answer a call from the Integriti Management Software Server.
Advanced Options	Encryption Type None AES128 AES128_Private	Select the type of encryption (if any) to be used. No encryption AES 128 AES 128 Private
	Product Edition None Installer Professional	Select whether the Insight Management Software package is the Professional edition or an Installer edition.
	Encryption Key	Optional Site-based encryption key that is used with AES128 Private. Enter the 32 characters encryption key in HEXADECIMAL format.
	Encryption Pairing Code	A unique key generated for the connection between the Server and the Panel.
Modem connection: General	Telephone Number.	Enter a Telephone Number for the Controller's modem to call the Integriti Server back on when the Integriti Server requests a Call-back type connection.
Modem connection: Internal modem Options	First Telephone Number. Telephone Number 1 Qualifier (When) Invert Qualifier	 Select a Telephone Number or Telephone Number List to use as the primary Telephone Number in this Comms Path. If required, select a Qualifier to define when this Telephone Number will be valid. Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Second Telephone Number. Telephone Number 2 Qualifier (When) Invert Qualifier	 Select a Telephone Number or Telephone Number List to use as the secondary Telephone Number in this Comms Path. If required, select a Qualifier to define when this Telephone Number will be valid. Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Maximum Online Time	Determines the maximum time that the Integriti Management Software is allowed to remain connected via this Modem Path. **NOT YET IMPLEMENTED.**
	Maximum Dial Attempts	Determines the maximum dial attempts this Comms Task will use to contact the Integriti software. When the maximum attempts are reached, the Backup Task, if defined, will be triggered. **NOT YET IMPLEMENTED.**

	Decadic Dial. Dumb Dial. Long Pace Dial.	Selects Pulse ("decadic") dial when dialling, rather than tone (DTMF) dialing. Selects Dumb dialling. Normally the Comms Task will monitor the line for line faults, dial-tone, busy etc. and make dialling decisions accordingly. When Dumb dialling is selected, the Comms Task does not make "smart" decisions based on sensed tones. All tones sensed and dialer progress are still recorded to review. Forces the Comms Task to wait 60 seconds between any redial attempts.
Modem connection: External modem Options. **NOT YET IMPLEMENTED**	First Telephone Number. Telephone Number 1 Qualifier (When) Invert Qualifier	 Select a Telephone Number or Telephone Number List to use as the primary Telephone Number in this Comms Path. If required, select a Qualifier to define when this Telephone Number will be valid. Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Second Telephone Number. Telephone Number 2 Qualifier (When) Invert Qualifier	 Select a Telephone Number or Telephone Number List to use as the secondary Telephone Number in this Comms Path. If required, select a Qualifier to define when this Telephone Number will be valid. Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Maximum Online Time	Determines the maximum time that the Integriti Management Software is allowed to remain connected via this Modem Path.
	Maximum Dial Attempts	Determines the maximum dial attempts this Comms Task will use to contact the Integriti software. When the maximum attempts is reached, the Backup Task, if defined, will be triggered.
	RS232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Master USB Slave Onboard RS485 Reader Port	 Select the Port that the Modem is connected to. No Modem connection. On-board "Port 0" connection. Unibus UART 1, RS232 Port 1 Unibus UART 1, RS232 Port 2 Unibus UART 2, RS232 Port 1 Unibus UART 2, RS232 Port 2 Unibus UART 3, RS232 Port 1 Unibus UART 3, RS232 Port 2 Unibus UART 4. RS232 Port 1 Unibus UART 4, RS232 Port 2

	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	
	Stop Bits 1 Bit 2 Bits	
	Modem Type PSTN GPRS	
	Modem Initialization String.	Enter a custom modem initialization string if required.
Options.		Sets General Comms Task connection options.
	Permanent	If selected, the Controller will try to reconnect with the Integriti Server if it becomes disconnected. i.e. The Controller will try to maintain a permanent connection. If this option is not selected, the Controller will only attempt one connection when the Comms Task is started.
	Temporary Comms Ta	If selected, the Comms Task will be deleted upon completion of a communication session. e.g. When the Integriti Comms Task using a modem connection disconnects from the Integriti Server.
	Online Input	An unused Zone Input may be assigned to monitor the "Online" status. The Input will be sealed while the Integriti Comms Task is online and in alarm when offline. Any Zones used for this purpose must have the "Ignore Physical Input" option enabled in Input programming.

DIGITAL DIALLER FORMATS		The Dialler format allows reporting via a range of Digital Dialler protocols.
	Dialler Common Settings	**The following settings are common to all Dialler formats.**
Reporting	Dialler Format None IRFast Co SIA Four Plus Two	Select Reporting Format for this Comms Task. No format. IR fast. Contact ID. SIA 4+2.
	Client Code	Determines the account code sent when reporting events to the Central Station. This is the default Client Code for this Comms Task which will be used if there is no Client Code programmed in the Area in which the event to report has occurred. If a Client Code has been programmed for an Area, then that Client Code will take precedence when events are reported for that Area. Options are provided to enter the Client Code in Hexadecimal and Decimal formats. Enter a Decimal value between 0 – 65535, or a Hexadecimal value between 0 – FFFF. (Hexadecimal available in Controller Firmware V3.2.1 or later only) Account Codes are typically provided by the Central Monitoring Station. The number of digits required will depend on the reporting format.
	Telephone Number 1 (Primary Telephone Number)	Use this setting to select the primary Telephone Number for this Comms Task if the Telephone number does not need to be qualified in any way. Note: If the Telephone Number needs to be Qualified, use the Telephone Number settings in the Advanced Options instead. A Telephone Number or Telephone Number List may be selected.
	Telephone Number 2 (Secondary Telephone Number)	Use this setting to select the secondary Telephone Number for this Comms Task if the Telephone number does not need to be qualified in any way. Note: If the Telephone Number needs to be Qualified, use the Telephone Number settings in the Advanced Options instead. A Telephone Number or Telephone Number List may be selected.
Review Options	Review Filter	The Review Filter options may be programmed to determine the events that will be reported based on parameters such as specific entities, entity types, Comms Task Groups, Event type, etc.

	Entity 1 Entity 2 Entity 3 Entity 4 Entity 5 Entity 6	Allows up to 6 specific Entities to be nominated for reporting via this Comms Task so that only review entries that reference these entities will get reported.
	Comms Task Groups	Option to allow Input event reporting to be filtered based on the type of Input. Up to 16 separate Comms Task reporting Groups can be established. If one or more Groups are enabled in these options, an Input event will only be reported by this Comms Task if it has: - At least one matching Comms Task Group enabled in its associated Process Group. - No Comms Task Groups enabled in its associated Process Group. If no groups are enabled in these options, any Input events can be reported, regardless of how the Comms Task Group options have been set in the Input's Process Group.
	Review Classification	Select the Review classifications to filter the events reported by this Comms Task. *See Menu Group programming for a list of the Review Classifications available.*
	Review Level Everyone User - Essential User - Standard User - Detailed Installer - Standard Installer - Detailed Inner Range - Debug	Select the Review Level to filter the events reported by this Comms Task. This option is normally only used for Comms Task formats such as Automation, Printer, BMS, etc. formats. This option determines the amount of detail that will be accepted for this Comms Task. Lowest level of detail. Highest level of detail.
	EN Review	Only EN Review will be used by this Comms Task.
	Historic Review	Allows buffered events that are made redundant by a subsequent event and normally discarded, to be reported. e.g. For an Input that has been Isolated. Normally if you have a lot of queued events and then you get an event such as a closing for the Area those events are in, or an isolate on the Input causing the events, the relevant buffered events are discarded up until the Isolate or Close. If enabled, this option forces those buffered events to be reported. Use this option with caution. Under certain circumstances it can contribute to a run-away dialer condition.

Options	Delay Report Time	Enter a Delayed Report Time in Hours, Minutes and Seconds, if required. Determines the duration of delay when reporting alarms to the Central Station if the Process Group "Delay Report" option is enabled.
	Look Ahead. General Open/Close. Xmit Historic	New Alarm events will be reported ahead of multi-break reports on Inputs that have already been reported. Area Open/Close reporting will only be done on the 1st Area to Open and the last Area to Close, with the exception of Areas with the "Not General Area" option enabled. Sends buffered events for an Input that has since been isolated or is in an Area which has been disarmed. Normally (this option disabled), when there are events buffered for an input, if the input is then isolated or the Area is disarmed, only the final event is sent. When this option is enabled, this functionality is not executed and all buffered events are sent.
	Maximum Online Time (ms)	Program the maximum online time in milliSeconds.
	Maximum Events to send per call.	Program the maximum number of events allowed to be reported per call.
	Maximum Dial Attempts	Determines the maximum dial attempts this Comms Task will use to contact the Central Station.
Miscellaneous	Status monitoring options. Online Input Fail Input Backup Input	Unused Zone Inputs can be assigned to monitor the status of the Dialler Comms Task. Note that any Zones used for this purpose must have the "Ignore Physical Input" option enabled in Input programming. An unused Zone Input may be assigned to monitor the Dialler On-hook/Off-hook" status and operates as follows: Seal: Dialler is Off-hook (not making a call) Alarm: Dialler is On-hook (making a call) An unused Zone Input may be assigned to monitor the Dialler "Fail" status. An alarm will be triggered on this Input on dialler failure. An unused Zone Input may be assigned to monitor the "Backup" status. An alarm will be triggered on this Input when the Backup Comms Task (if assigned) is triggered.
Advanced Settings		
	Primary Telephone Number. Telephone Number 1 Qualifier (When) Invert Qualifier	Allows the primary Telephone Number or Telephone Number List to be selected and paired with a Qualifier to define when it will be used. If a Qualifier is not required, use the Telephone Number settings in the Reporting Options instead. Select a Telephone Number or Telephone Number List to use as the primary Telephone Number in this Comms Task. If required, select a Qualifier to define when this Telephone Number will be valid. Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.

	Secondary Telephone Number. Telephone Number 2 Qualifier (When) Invert Qualifier	Allows the secondary Telephone Number or Telephone Number List to be selected and paired with a Qualifier to define when it will be used. If a Qualifier is not required, use the Telephone Number settings in the Reporting Options instead. Select a Telephone Number or Telephone Number List to use as the secondary Telephone Number in this Comms Task. If required, select a Qualifier to define when this Telephone Number will be valid. Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	Seize Action.	Select the Line Seize Action. The selected Entity will be controlled when the line is seized / unseized. *See Action Programming in "Generic Programming Operations" for details.*
	Pass Action	Select the Comms Pass Action. The selected Entity will be controlled when the dialler successfully sends a report to the Central Station. *See Action Programming in "Generic Programming Operations" for details.*
	Dialling options. Dial Decadic. Dumb Dial. Long Pace Dial.	 Selects Pulse ("decadic") dial when dialling, rather than tone (DTMF) dialing. Selects Dumb dialling. Normally the Comms Task will monitor the line for line faults, dial-tone, busy etc. and make dialling decisions accordingly. When Dumb dialling is selected, the Comms Task does not make "smart" decisions based on sensed tones. All tones sensed and dialer progress are still recorded to review. Forces the Comms Task to wait 60 seconds between any redial attempts.
	Handshake Wait Time (mS)	A longer handshake wait time may be programmed if required. The handshake wait time is the time the task will wait for an initial handshake after dialling the Central Station. If left set to 0, the following default time will be used; Contact ID: 20 Seconds. IR fast: 20 Seconds. SIA: 15 Seconds. A value of up to 65 Seconds can be programmed in 1 milliSecond increments. e.g. For a wait time of 35 seconds, enter 35000. The default time listed above is also the minimum time allowed. A programmed time that is less than the default time will be ignored and the default time will be used.

	Acknowledgement Wait Time (mS)	The amount of time that the Panel will wait for the Receiver to Acknowledge an alarm. If left set to 0, the system's default value will be used. A value of up to 65 Seconds can be programmed in 1 milliSecond increments. e.g. For an Ack. time of 10.5 seconds, enter 10500. NOT YET IMPLEMENTED
	Maximum Time until Backup Task (mS)	The maximum amount of time before the Backup Comms Task will be triggered when the Primary Comms Task fails. If left set to 0, the default time of 60 Seconds will be used. A value of up to 65 Seconds can be programmed in 1 milliSecond increments. e.g. For a Backup Comms Task trigger time of 45 seconds, enter 45000.
	Callback Telephone Number	Select a Telephone Number to use for the Callback function in this Comms Task.
	Client Telephone Number	Record the Panel's telephone number here for reference.

	Dialler Format Settings	**These are the settings unique to each of the Dialler formats.** **The format is chosen in the 'Reporting' options above.**
IRFast Settings. (Only displayed if IRFast format selected)	Send Text.	Send Review text for each event reported.
	Send Contact ID.	Send an equivalent Contact ID string for each event reported, using the mapping option selected. This is useful when the automation system cannot understand native IRfast information.
	Send Time.	Send a text string of the Time/Date the event was recorded into review.
	C3K Compatible.	The C3K Compatible Map is implemented for reporting Input events to Receivers and/or Automation Software that have not yet been updated for Integriti IRFast mapping.
	300 Baud.	Forces all communications to 300 Baud instead of the default 1200 Baud. This need only be set if there are communication difficulties at 1200 Baud
	XMIT Info.	Send miscellaneous panel information before hanging up, including panel serial number, software version and security option settings.
	Save time.	Causes the Receiver to Update the panel time and date from its system clock prior to hanging up. NOTE: An IRFast Receiver can set any of the above options to Yes on a per receiver basis. The above options should only be enabled upon instruction from the Central Station.

Contact ID Settings. (Only displayed if Contact ID format selected)	Contact ID Map	Select Contact ID Mapping for this Comms Task. Determines which zones are uniquely reported. *Refer to Contact ID Map documentation.*
	Standard	Standard Mapping oriented towards Intruder Alarm monitoring.
	Access	Access Mapping oriented towards Access Control with 2-Door Reader Modules.
	SIMS II	SIMS II Mapping for use with the SIMS II Central Station Automation Software. Allows all Inputs, on up to 35 Modules of every Module Type to be reported uniquely.
SIA Settings. (Only displayed if the SIA format selected)	Map	
	0	Hex digits are used for the Address field.
	1	Decimal digits will be used for the Address field.
	2	Not yet implemented.
		Note that if the Decimal Map option is selected, the address mapping alters and the maximum number of Modules of any one type is limited to 32. *See the Tables section of the rear of this manual for SIA address mapping.*
	RTC	If enabled, a time modifier (ti) prefixes every Event Data Code to provide the historical time stamp of the event. Note that this option may considerably slow down the rate of alarm transmission.
	ASCII	If enabled an ASCII text block is appended to the data to provide textual information from the system. **NOTES:** 1) This option may considerably slow down the rate of alarm transmission. 2) When this option is selected, the appropriate text for the first event will be sent in an ASCII block. Each subsequent event in the same phone call will only have ASCII text sent if it varies from the previous events. i.e. Only differences are sent to save on transmission time. 3) This option also has the effect of forcing one alarm event per packet. 4) With an opening/closing event, the following ASCII text may be appended if the related Area Communications options are selected. "Sys still open" At least one nominated System Area is Open (Off). "24Hr Partition" The 24 Hour (Tamper) part of the Area is Open (Off).
	Peripheral Identifier	Send Peripheral Identifier modifier. Use decimal addresses instead of hexadecimal.
	Decimal Address	Don't output the address of events that can be considered a 'General Fault'. e.g. AC Fail, System Power-up, etc.
	Obey Address	
Four Plus Two Settings. (Only displayed if the Four Plus Two format selected)	No options at present	

GSM Comms Task Notes

- The format (IRfast or ContactID) used to communicate the normal event data to the FE3000 is determined by the FE3000. If the FE3000 tells the GSM Comms Task to use IRfast, then IRfast is what the GSM Comms Task sends. Note that the new Integriti IRfast may not be implemented in the Central Monitoring Station whereas the C3K IRfast may be. An option is provided for "C3k compatible IRfast" data to be sent.
- There is currently no option in the Comms Task to disable SMS control commands. Restricting SMS control of an entity is achieved via the User's Menu Group.
- When GSM Comms Task is configured as a Backup Comms Task, under normal "idle" conditions, no events are reported but SMS control messages are still processed.
- See information following the GSM Comms Task programming for full details of the SMS Command feature.
- The connection between the Integriti Controller and the FE3000 is made via a serial interface, by connecting one of the Integriti Controller's UARTs to the FE3000. FE3000s are capable of communicating at 600, 1200 or 2400 BAUD. The recommended port configuration for communications between the Integriti Controller and an FE3000 is 1200,N,8,1
- If upgrading the Integriti Controller Firmware from a Version prior to V3.0.0, to V3.0.0 or later, see the "Important Upgrade Notes" at the beginning of the "Communiations Programming" chapter.

GSM FORMAT		The GSM format allows primary or backup reporting via compatible Fratech Multipath IP STU or FE3000 products. It is used to communicate reportable events to a Central Monitoring Station, to send reportable events via SMS message and/or to receive SMS control messages.
Connectivity	RS232 Serial Interface Serial Channel	Select the Port that the Modem is connected to. GSM Format utilizes the following connection options: 1) "Uart 0" with Cable P/N: 996790 Integriti Port 0 to Multipath IP Interface Cable. 2) UniBus UART RS232 Port with Cable P/N: 994092 Serial Interface Cable.
	None	No Modem connection.
	Uart 0	On-board "Port 0" connection.
	Unibus Uart1(1)	Unibus UART 1, RS232 Port 1
	Unibus Uart1(2)	Unibus UART 1, RS232 Port 2
	Unibus Uart2(1)	Unibus UART 2, RS232 Port 1
	Unibus Uart2(2)	Unibus UART 2, RS232 Port 2
	Unibus Uart3(1)	Unibus UART 3, RS232 Port 1
	Unibus Uart3(2)	Unibus UART 3, RS232 Port 2
	Unibus Uart4(1)	Unibus UART 4. RS232 Port 1
	Unibus Uart4(2)	Unibus UART 4, RS232 Port 2
	USB Master	Not relevant to this format.
	USB Slave	Not relevant to this format.
	IAC Onboard RS485	Not relevant to this format.
	Modem	Not relevant to this format.

	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	The next four options configure the serial port. The recommended port configuration for communications between the Integriti Controller and an FE3000 is: • 1200 baud • 8 Bits • No Parity • 1 Stop Bit
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	
	Stop Bits 1 Bit 2 Bits	
Reporting	Client Code	Determines the account code sent when reporting events to the Central Station. This is the default Client Code for this Comms Task which will be used if there is no Client Code programmed in the Area in which the event to report has occurred. If a Client Code has been programmed for an Area, then that Client Code will take precedence when events are reported for that Area. Options are provided to enter the Client Code in Hexadecimal and Decimal formats. Enter a Decimal value between 0 – 65535, or a Hexadecimal value between 0 – FFFF. (Hexadecimal available in Controller Firmware V3.2.1 or later only) Account Codes are typically provided by the Central Monitoring Station. The number of digits required will depend on the reporting format.
	SMS Number 1 (Primary SMS Telephone Number)	Use this setting to select the primary Telephone Number for this Comms Task if the Telephone number does not need to be qualified in any way. Note: If the Telephone Number needs to be Qualified, use the Telephone Number settings in the Advanced Options instead. A Telephone Number or Telephone Number List may be selected.

	SMS Number 2 (Secondary SMS Telephone Number)	Use this setting to select the secondary Telephone Number for this Comms Task if the Telephone number does not need to be qualified in any way. Note: If the Telephone Number needs to be Qualified, use the Telephone Number settings in the Advanced Options instead. A Telephone Number or Telephone Number List may be selected.
	General Reporting Options Enable SMS Alarms.	 When this option is set, the Comms Task waits for an event to transfer to the FE3000. When an event is detected it is sent to the FE3000 to be reported to the nominated SMS Telephone Number or Telephone Number List as an SMS Text message. The FE3000 will attempt to send the SMS message and will report back whether or not it was successful. If the FE3000 could not successfully send the message, no further action is taken by the GSM Comms Task. When there is an SMS message pending to be sent, if the FE3000 takes longer than 30 seconds to be free to accept the next SMS message then the pending SMS message will be discarded. Note: Prior to V3.1.3 SMS messages were sent with UTC time instead of the local time.
	Enable Alarms.	When this option is set, the Comms Task waits for an event to transfer to the FE3000. When an event is detected it is sent to the FE3000 to be reported to the Central Monitoring Station. The FE3000 will attempt to report the event via one of its many communication paths. The FE3000 reports back whether or not it was successful with its attempt to communicate the event(s). If the FE3000 could not successfully communicate the event(s) to the Monitoring Station then the GSM Comms Task can pass the event(s) to its programmed Backup Comms Task.
	Reporting Format None IRFast Contact ID SIA Four Plus Two	If “Enable Alarms” above is selected, select the Reporting Format that will be used to send alarm information to the Monitoring Station. No format. IR fast data will be sent. Contact ID data will be sent. SIA 4+2.

Options	SMS General Open/Close	Enables General Open/Close reporting for SMS Reporting. See "General Open/Close" below for details.
	SMS Xmit Historic	Enables Xmit Historic reporting for SMS Reporting. See "Xmit Historic" below for details.
	Update Time.	The Integriti Controller's Real-time clock will be updated from the FE3000 status packet every hour on the hour.
	Save RSSI	Save RSSI information to Review allows the Received Signal Strength Information to be logged to Review.
	Alarm Look Ahead.	New alarms will be reported ahead of multi-break messages for Inputs that have already reported.
	SMS Look Ahead.	New SMS alarm messages will be reported ahead of multi-break messages for Inputs that have already reported.
	General Open / Close.	Whenever all Areas that are programmed to report Open/Close are turned On, a general Area close is reported. As soon as the first Area is turned Off, a general Area open is reported. In Area Programming, some Areas can be nominated to be ignored in the general Area calculation allowing them to still be reported individually.
	Need PIN	A PIN Code is required to be sent with SMS commands.
	SMS Error Reply.	If SMS commands are received that result in some sort of error (e.g. Command Syntax, Permissions deny control, etc.) then this option allows an error reply to be sent back to the Sender.
	Xmit Historic	Sends buffered events for an Input that has since been isolated or is in an Area which has been disarmed. Normally (this option disabled), when there are events buffered for an input, if the input is then isolated or the Area is disarmed, only the final event is sent. When this option is enabled, this functionality is not executed and all buffered events are sent.
	Maximum Messages	Maximum SMS messages allowed to be sent in a 60 second period. Note that messages will bank up if they are occurring faster than this rate. The default setting of 0 means that the maximum messages will be 10 per 60 seconds.
Contact ID.	Contact ID Map	Select Contact ID Mapping for this Comms Task. Determines which zones are uniquely reported. *Refer to Contact ID Map documentation.*
	Standard	Standard Mapping oriented towards Intruder Alarm monitoring.
	Access	Access Mapping oriented towards Access Control with 2-Door Reader Modules.
	SIMS II	SIMS II Mapping for use with the SIMS II Central Station Automation Software. Allows all Inputs, on up to 35 Modules of every Module Type to be reported uniquely.
Advanced Settings	First SMS Number.	
	SMS Number 1	Select a Telephone Number or Telephone Number List to use as the primary Telephone Number in this Comms Task.
	Qualifier (When)	If required, select a Qualifier to define when this Telephone Number will be valid.
	Invert Qualifier	Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.

	Second SMS Number. SMS Number 2 Qualifier (When) Invert Qualifier	 Select a Telephone Number or Telephone Number List to use as the secondary Telephone Number in this Comms Task. If required, select a Qualifier to define when this Telephone Number will be valid. Select Invert Qualifier to enable the Telephone Number when the Qualifier is invalid.
	CID Telephone Number	Select a Telephone Number to use for reporting to a Central Station Digital Receiver.
	Service Telephone Number	Select a Telephone Number for the SMS service centre. This number can be obtained from the Network you subscribe to and is mandatory for any SMS operations.
	SMS Control Number	Select a Telephone Number to define a number that is allowed to perform SMS Control operations if the "Need PIN" option is not enabled.
	Status monitoring GSM Reg Input. GSM Signal Input GSM Fail Input GSM Backup Input GSM Online Input	Allows Inputs to be specified for monitoring a number of GSM Comms Task states. Unused Zone Inputs can be assigned to these functions. Any Zones used for this purpose must have the "Ignore Physical" option enabled. This Zone will indicate changes in the state of the GSM modem registration. The Input is alarmed when the modem de-registers and sealed when the modem re-registers. This Zone will be put into Alarm when the FE3000 reports to the Integriti Controller that it has low signal strength. The Zone will restore when the FE3000 reports that the signal strength is satisfactory. This Zone is will be put into Alarm when some error conditions occur between the Integriti Controller and the FE3000. This Zone will indicate when the Backup Comms Task is Triggered. This Zone will be Sealed when communications with the FE3000 are working and in Alarm when they are not.
Review Options	Review Filter	The Review Filter options may be programmed to determine the events that will be reported based on parameters such as specific entities, entity types, Comms Task Groups, Event type, etc. *See "Digital Dialler Formats" for details of the Comms Task Review Options.*
	SMS Review Filter	The SMS Review Filter options may be programmed to determine the events that will be reported via SMS based on parameters such as specific entities, entity types, Comms Task Groups, Event type, etc. *See "Digital Dialler Formats" for details of the Comms Task Review Options.*

IRFast Settings. (Only required if IRFast format selected)	Send Text. Send Contact ID. Send Time. C3K Compatible. 300 Baud. XMIT Info. Save time.	Send Review text for each event reported. Send an equivalent Contact ID string for each event reported, using the mapping option selected. This is useful when the automation system cannot understand native IRfast information. Send a text string of the Time/Date the event was recorded into review. The C3K Compatible Map is implemented for reporting Input events to Receivers and/or Automation Software that have not yet been updated for Integriti IRFast mapping. Forces all communications to 300 Baud instead of the default 1200 Baud. This need only be set if there are communication difficulties at 1200 Baud Send miscellaneous panel information before hanging up, including panel serial number, software version and security option settings. Causes the Receiver to Update the panel time and date from its system clock prior to hanging up. NOTE: An IRFast Receiver can set any of the above options to Yes on a per receiver basis. The above options should only be enabled upon instruction from the Central Station.
GSM SMS options	Enable SMS Control Allow Help Allow Area Allow Isolate Allow Reset SMS Allow Named Actions Allow Auxiliary Control Allow Status Query Allow On Control Allow Off Control	All SMS Remote Control commands are allowed. If “Enable SMS Control” is <u>not</u> enabled, select the specific types of SMS commands that will be allowed from the list below. Allow the SMS User to request the Help message. Allow Area control. Allow Input Isolate & De-Isolate. Allow the Reset SMS Messages command. This allows buffered SMS messages to be cleared. Allow Named Action control. Allow Auxiliary control Allow the status of an entity to be requested. Allow Entities to be turned On if control of the entity type is enabled. Allow Entities to be turned Off if control of the entity type is enabled.

SMS Control

The GSM Comms Task can be used to turn Areas on/off, turn Auxiliaries on/off and to trigger Named Actions via SMS control commands. Inputs can also be Isolated or de-Isolated. The GSM Comms Task can be configured to authenticate an SMS command either via a Telephone Number or via a User PIN.

If only the Telephone Number is used as the authentication method then there is no restrictions applied to the SMS control command. This means that as long as the command syntax is correct the SMS control action is carried out (E.g. any Area can be turned ON/OFF or any Input can be Isolated/de-Isolated etc.).

If a User PIN is provided as part of the SMS control command then the User's permissions governs the level of control that the SMS control command can execute. If the User does not have access to control the entity type in their Remote Access Permissions of their Menu Group, then they cannot control the entity. Some SMS control commands also have additional checks, for example:

- When controlling an Area ON the User must have the Area in their "Area ON List".
- When controlling an Area OFF the User must have the Area in their "Area OFF List".
- When Isolating or De-Isolating an Input the User must have the Input in their "Area OFF List".
- When triggering a Named Action, if the Named Action has an "Action Group" set then the User must have at least one matching "Action Group" set to that of the Named Action.

When a valid SMS control command has been received and processed, an SMS reply will be sent back to the original SMS phone number. In most cases the SMS reply will be the review associated with the action that was performed, however in some circumstances an error reply may be sent or even no reply will be sent.
Examples of these exceptions are:

- SMS Alarms are being sent instead of SMS replies (SMS Alarms are a higher priority than SMS replies)
- The review for the executed action was not detected or the FE3000 was full and unable to accept additional SMS messages.

As with SMS Alarms, if there is an SMS reply message pending to be sent and the FE3000 takes longer than 30 seconds to be free, then the pending SMS reply message will be discarded.

See the following table for the command set.

SMS Control Command Syntax

Command Syntax	Command Description
[<PIN>] ?	Display SMS Help
[<PIN>] A <Area ID> <N/F>	Control an Area using its ID
[<PIN>] A <Area Name> <N/F>	Control an Area using its Name
[<PIN>] A <Area ID> L	List 4 Area Names starting at Area ID
[<PIN>] A <Area Name> L	List 4 Area Names starting at Area Name
[<PIN>] A ?	Display Area Help
[<PIN>] I <Input Address> <I/D>	Isolate an Input using its ID
[<PIN>] I <Input Name> <I/D>	Isolate an Input using its Name
[<PIN>] I <Input ID> <L>	List 4 Input Names starting at Input ID
[<PIN>] I <Input Name> <L>	List 4 Input Names starting at Input Name
[<PIN>] I ?	Display Isolate Help
[<PIN>] P <Named Action Address> <N/F>	Trigger a Named Action using its ID
[<PIN>] P <Named Action Name> <N/F>	Trigger a Named Action using its Name
[<PIN>] P <Named Action ID> <L>	List 4 Named Actions starting at Named Action ID
[<PIN>] P <Named Action Name> <L>	List 4 Named Actions starting at Named Action Name
[<PIN>] P ?	Display Named Action Help
[<PIN>] X <AUX Address> <N/F>	Control an Auxiliary using its ID
[<PIN>] X <AUX Name> <N/F>	Control an Auxiliary using its Name
[<PIN>] X <AUX ID> <L>	List 4 Auxiliary Names starting at Auxiliary ID
[<PIN>] X <AUX Name> <L>	List 4 Auxiliary Names starting at Auxiliary Name
[<PIN>] X ?	Display Auxiliary Help
[<PIN>] R	Reset the SMS buffer to the latest review
[<PIN>] R ?	Display Reset SMS Help

Example SMS Control commands

Example	Example Description
01?	01=User PIN, ?=Display the SMS Help message
01A001N	01=User PIN, A=Area Control, 001=Area #001, N=Turn ON
AHouseF	A=Area Control, House=Area Name, F=Turn OFF
A1L	A=Area Control, 1=Area #1, L=List 4 Area Names starting at Area 1
AHouseL	A=Area Control, 1=Area #1, L=List 4 Area Names starting at House
A?	A=Area Control, ?=Display the Area Help message
01IC01:Z05I	01=User PIN, I=Isolate Control, C01:Z05=Input C01:Z05, I=Isolate
IEntry PIRD	I=Isolate Control, Entry PIR=Input (E.g. C01:Z05), D=DeIsolate
IC01:Z05L	I=Isolate Control, C01:Z05=Input C01:Z05, L=List 4 Input Names starting at C01:Z05
IEntry PIRL	I=Isolate Control, Entry PIR=Input (E.g. C01:Z05), L=List 4 Input Names starting at Entry PIR
I?	I=Isolate Control, ?=Display the Isolate Help message
01P001N	01=User PIN, P=Named Action Control, 001=Named Action #001, N=Trigger ON
PUnlockF	P=Named Action Control, Unlock=Named Action Name, F=Trigger OFF
P1L	P=Named Action Control, 1=Named Action #1, L=List 4 Named Action Names starting at 1
PUnlockL	P=Named Action Control, Unlock=Named Action Name, L=List 4 Named Action Names starting at Unlock
P?	P=Named Action Control, ?=Display the Named Action Help message
01XC01:X07N	01=User PIN, X=Auxiliary Control, C01:X07=Auxiliary C01:X07, N=ON
XStrobeF	X=Auxiliary Control, Strobe=Auxiliary (E.g. C01:X07), F=OFF
XC01:X07L	X=Auxiliary Control, C01:X07=Auxiliary C01:X07, L=List 4 Auxiliary Names starting at C01:X07
XStrobeL	X=Auxiliary Control, Strobe=Auxiliary (E.g. C01:X07), L=List 4 Auxiliary Names starting at Strobe
X?	X=Auxiliary Control, ?=Display the Auxiliary Help message
01R	01=User PIN, R=Reset SMS command
R?	R=Reset SMS, ?=Display the Reset SMS Help message

AUTOMATION FORMAT	NOTE: All letters in valid commands sent to the Automation Comms Task must be uppercase only.	The "Automation" communication format allows the Integriti Controller to connect to a 3rd party Home/Building Automation system via an RS232 Serial or Ethernet connection. The protocol is ASCII based for ease of use and is designed primarily to enable home automation or building management system (BMS) connectivity. Firmware V3.1.7 or later recommended.
Review Options	General Review Options	
	Send Review	Enables Review streaming output.
	Acknowledge Review	The Automation Comms Task will expect an acknowledge message to be returned following each Review event sent.
	All Review	This option starts the Comms Task with the review pointer at the oldest event, allowing the user to print all review. Normally review is sent from the time the CT was started. If all review is selected, it is sent from the earliest review record in the buffer, which could date back to when the panel was first manufactured, depending on how many review events have ever been generated and how many review events are licensed.
	Transfer Checksum	Insert a checksum field in all transmissions. A checksum field comprises a "~" character followed by two hexadecimal digits inserted just prior to the end of frame character "}".
	Receive Checksum	The Automation Comms Task will expect a checksum field in all received packets, and will reject any packet that has a bad checksum.
	Transmit Auxiliary	Auxiliary changes will be sent.
	Transmit Auxiliary Acknowledge	Send Auxiliary changes with acknowledgement.
	No Line Breaks	Do not send line breaks between Review messages.
	No Headers or Braces in Review	Select this option to only show text in Review messages.
	Header Format	Select the option for the Review Header format.
	Tstamp	Timestamp only.
	DateTime	Date and Time only.
	Sequence	Sequence Number only. (Event ID)
	LCD Sequence	Match the sequence number as it would appear on the LCD screen at Menu, 1, 1.
	LCD DateTime	Match the Date/Time formatting as it would appear on the LCD screen at Menu, 1, 1.
	Sequence DateTime	Match the sequence number and Date/Time formatting as it would appear on the LCD screen at Menu, 1, 1.
	Body Format	Select the option for the Review Body format.
	Raw	Only Raw Hexadecimal Review data will be output after the Event ID. No text will be output.
	Full Text	Full text with entity names as stored in panel.
	LCD Full Text	Format as it would appear on the LCD screen at Menu, 1, 1 depending what display option was set.
	LCD Abbrev Text	Review events will be sent in an abbreviated form. Any relevant entity names (if programmed) will be replaced with the entity ID. e.g. Normal Review log entry: Auto Comms Task O/P: Alarm on Roller Door Reed in Garage Alarm C01:Z15

	Review Filter	The Review Filter allows up to 5 Entities to be selected to restrict the system entities that are e.g. Area List, Auxiliary List, etc. The Review Filter options may be programmed to determine the events that will be sent via the Automation Comms Task Review streaming based on parameters such as specific entities, entity types, Comms Task Groups, Event type, etc. *See "Digital Dialler Formats" for details of the Comms Task Review Filter Options.*
Connectivity (Serial RS-232)	RS232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	 Select the Port that the Automation Comms Task will use. No connection. On-board "Port 0" connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4. Port 1 Unibus UART 4, Port 2 Not relevant to this format. Appears as a Virtual Comm Port in Windows and may be used for this format. Not relevant to this format. Not relevant to this format.
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	
	Stop Bits 1 Bit 2 Bits	

Ethernet Connection	Server IP Address	View or Enter the IP Address of the Server PC.
	TCP Port	View or Enter the Server TCP Port Number. The default Port number does not normally need to be changed.
	DNS Name	Select required DNS Server Name. DNS Servers are programmed separately.
	TCP Mode None Server Client	
	Retries	Program the number of times to retry connecting upon failing to connect. Only applicable to Client "TCP Mode" if selected above.
	Connection Timeout	**Not used** The timeout period can be programmed in 1 Second increments up to a value of 1 Hour, 49 Mins, 13 Secs (6553 Seconds) V3.1.1 or later.
	Connection Attempt Timeout	**Not used** The connection attempt timeout period can be programmed in 1 Second increments up to a value of 1 Hour, 49 Mins, 13 Secs (6553 Seconds)
Timing	Poll Time	Sets the maximum time allowed between received packets before the Automation Comms Task considers the link to have failed and triggers the "Online Input". The poll time can be programmed in 1 Second increments up to a value of 1 Hour, 49 Mins, 13 Secs (6553 Seconds)
	Pacing Time	Adjusts the rate at which Historic Review events are output when the communications link is re-established. The pacing time can be programmed in 1 milliSecond increments up to a value of 5 Mins, 27.675 Secs
	Repeat Time	If the "Acknowledge Review" option has been selected, then for each review event sent, an acknowledge packet must be received before advancing to the next event. If an acknowledge is not received within 5 seconds, the event will be resent after waiting out the Repeat time. The repeat time can be programmed in 1 Second increments up to a value of 1 Hour, 49 Mins, 13 Secs (6553 Seconds)

Options	Online Input	Select an Input to be used to monitor the Online status of the Automation Comms Task communications link. The Input will be sealed while the Automation Comms Task is online and in alarm when offline. An unused Zone Input can be assigned to this function. Any Zone used for this purpose must have the "Ignore Physical Input" option enabled.

EMS FORMAT		The "EMS" communication format allows the Integriti Controller to provide a high-level connection to an Elevator Management System via an RS232 Serial or Ethernet connection. "Lift Groups" must also be programmed to support this feature. The Integriti Controller lift interface allows for one type of lift interface per controller. If a high-level interface is used, only one EMS Comms Task is allowed per Integriti Controller.
Settings	Protocol None Kone (IP) Kone (RS232) Otis (RS232) ThyssenKrupp DSC (RS232) Kone RCG (IP)	Select the EMS communications Protocol for this EMS Comms Task. No protocol selected. Kone HLI Access Control Protocol V2.6. Kone Access Control Protocol Rev 1.5. Otis RS-232 Thyssen Krupp Destination Selection Control (DSC) Vers 1.0. Kone RCG
	Online Input	An unused Zone Input may be assigned to monitor the "Online" status. The Input will be sealed while the EMS Comms Task is online and in alarm when offline. Any Zones used for this purpose must have the "Ignore Physical Input" option enabled in Input programming.
	RS-232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	Select the Port that the Automation Comms Task will use. No Modem connection. On-board "Port 0" connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4. Port 1 Unibus UART 4, Port 2 Not relevant to this format. USB serial port on Controller. Not relevant to this format. Not relevant to this format.

	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	
	Stop Bits 1 Bit 2 Bits	
ThyssenKrupp Options	Global Lift	Assign the Lift Record that will be used for Thyssen Krupp global permissions.
	ThyssenKrupp Pace Time	Enter the rate limit for messages sent to the Thyssen Krupp system.
Kone IP Options	Car Panel Offline Mask	Select a Floor List for the Car Panel Offline Mask. Floors in this list will be set to Free Access when communications is lost with the Kone IP EMS. The mask affects Car Panels only.
	Destination Panel Offline Mask	Select a Floor List for the Destination Panel Offline Mask. Floors in this list will be set to Free Access when communications is lost with the Kone IP EMS. The mask affects Destination Panels only.
	Offline Lift Group	Select a Lift Group to determine the mapping for the Car Panel Offline Mask and the Destination Panel Offline Mask.
Schindler Options	User Prefix	Prefix to add when sending User names to the Schindler system. (16 characters)
Primary Ethernet Connection	Primary Server IP Address	View or Enter the IP Address of the Server PC.
	Primary TCP Port	View or Enter the Server TCP Port Number. The default Port number (004711) does not normally need to be changed.
	Primary DNS Name	Select required DNS Server Name. DNS Names are programmed separately.

	Primary TCP Mode None Server Client	Select whether the EMS Comms Task is to run as a Server, a Client or neither. *See the Guide: Integriti Communications Tasks –Lift Interfacing (EMS).*
	Primary Retries	The number of times to retry connecting upon failing to connect before it disconnects. Only programmed if "Client" TCP mode selected above.
	Primary Connection Timeout	Programmed in Minutes and Seconds. *See the Guide: Integriti Communications Tasks –Lift Interfacing (EMS).*
	Primary Connection Attempt Timeout	Programmed in Minutes and Seconds. *See the Guide: Integriti Communications Tasks –Lift Interfacing (EMS).*
Secondary Ethernet Connection	Parameters for the Secondary Ethernet connection.	Options are the same as those for the Primary Ethernet Connection.
Tertiary Ethernet Connection	Parameters for the Tertiary Ethernet connection.	Options are the same as those for the Primary Ethernet Connection.
Quartenary Ethernet Connection	Parameters for the Quartenary Ethernet connection.	Options are the same as those for the Primary Ethernet Connection.

Introduction to Securitel Comms Task.

The Securitel format allows connection to 3rd party communicators that use the Securitel Serial protocol as the interface.

The Securitel network that the protocol was originally developed for is no longer in operation, but the protocol is still used in Australia by Subscriber Terminal Units (STUs) to report via communications paths such as GSM, GPRS or IP.

The Securitel network was a "direct-line" alarm transmission network that was supplied and maintained by Telstra Australia. Alarm panels in the field were connected to a Subscriber Terminal Unit (a STU) and the STU would communicate events via the PSTN to Nodes that were hosted by Telstra. These events were then transmitted to a Central Monitoring Station for processing/actioning.
The Alarm panel communicates to the STU via the Securitel communication protocol. The Securitel protocol allows for either Channel/PIN data or Serial data.
The Integriti Securitel format uses Serial data. When an Alarm panel is reporting Serial data to the STU, the event description from the Alarm panel to the STU can describe:

- 255 Inputs being in one of the following states
  - Priority1
  - Priority2
  - Priority3
  - Tamper
  - Trouble
  - Man. Isolate
  - Auto Isolate
- Area 1 to 31 being Open or Close
- General Area Open or Close
- A few other miscellaneous events.

An Integriti Controller can support thousands of Inputs and the STU can only accept an Input number from 1 to 255, so the Securitel Comms Task has the job of collating many Inputs together in an attempt to end up with meaningful event information at the Central Monitoring Station.
See the "Integriti Securitel Comms Task Input Map" document for details.

The Securitel Comms Task also has another collation mechanism that is on a per Area basis. Each time that an Input in an Area reports a new Alarm, Tamper or Isolate, an additional Area Alarm, Area Tamper or Area Isolate can also be generated. When the Area is eventually disarmed, an Area Alarm Restore, Area Tamper Restore or Area Isolate Restore is generated (one Restore event per event type that was reported during this arming cycle).

The Securitel Comms Task has options to report Input events, Area events or both.

When multiple inputs across multiple modules are collated the reporting logic is as follows:

1. If a new input event (E.g. an Alarm) is being reported then the appropriate Securitel Input Number is looked up and the event is sent to the STU.
2. If a new input restore (E.g. going from Alarm to Seal) is being reported, look up all of the other module's inputs of the same type that the Securitel Input Number is collated with. If all of the inputs found are sealed then the restore event is sent to the STU. If an input(s) is unsealed then when the last input seals then the restore event is sent to the STU.

e.g. There are 4 Expander modules and 1 RF module on the Integriti Controller. Expander 2 has a Cabinet Tamper event, this is reported to the STU immediately. Then Expander 3 has a Cabinet Tamper event, this is reported to the STU immediately. Then Expander 3 has a Cabinet Tamper restore, this is not reported to the STU because Expander 2 still has its Cabinet Tamper unsealed. Expander 2 has a Cabinet Tamper restore and this is reported to the STU indicating that all Expander module Cabinet Tamper inputs are sealed.

SECURITEL FORMAT	Australia Only.	NOTE: If upgrading the Integriti Controller Firmware from a Version prior to V3.0.0, to V3.0.0 or later, see the "Important Upgrade Notes" at the beginning of the "Communiations Programming" chapter.
Connectivity	RS232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	 Select the RS-232 Port that the STU is connected to. No Modem connection. On-board "Port 0" connection. Unibus UART 1, RS232 Port 1 Unibus UART 1, RS232 Port 2 Unibus UART 2, RS232 Port 1 Unibus UART 2, RS232 Port 2 Unibus UART 3, RS232 Port 1 Unibus UART 3, RS232 Port 2 Unibus UART 4. RS232 Port 1 Unibus UART 4, RS232 Port 2 Not relevant to this format. Not relevant to this format. Not relevant to this format. Not relevant to this format.
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	STUs using the Securitel Communications Protocol are generally capable of communicating to Alarm panels at 300, 1200 or 9600 Baud. The recommended Baud Rate for communications between the Integriti Controller and a STU is 1200 Baud; however, you should check the Installation and/or Configuration information supplied with the STU to ensure a compatible Baud rate is chosen.

	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	The recommended number of Data Bits for communications between the Integriti Controller and a STU is 8. Check the Installation and/or Configuration information supplied with the STU to ensure a compatible option is chosen.
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	The recommended Parity for communications between the Integriti Controller and a STU is None. Check the Installation and/or Configuration information supplied with the STU to ensure a compatible option is chosen.
	Stop Bits 1 Bit 2 Bits	The recommended number of Stop Bits for communications between the Integriti Controller and a STU is 1. Check the Installation and/or Configuration information supplied with the STU to ensure a compatible option is chosen.
Miscellaneous Settings	Auxiliary Action Hard ID Online Input Backup Input	Selects the system Entity to be controlled by the Securitel Command-back Auxiliary. Sets the Securitel Hard ID to be used for this Comms Task. The Hard ID is the Securitel equivalent to the client code used in other formats and is programmable in HEX from 0001 to FFFF. The Hard ID is provided by the Central Monitoring Station. Note that while the Hard ID is a HEX number, the number provided by the Cenral Station will normally only contain Decimal characters. Simply enter the number as it is provided by the Central Station. The "Multiple Area Client Code" option has no effect when selected for securitel. The Hard ID programmed here is always used. Select an Input to be used to monitor the Online status of the Securitel Comms Task communications link. The Input will be sealed while the Securitel Comms Task is online and in alarm when offline. An unused Zone Input can be assigned to this function. Any Zone used for this purpose must have the "Ignore Physical Input" option enabled in Input programming. An unused Zone Input may be assigned to monitor the "Backup" status. An alarm will be triggered on this Input when the Backup Comms Task (if assigned) is triggered. Any Zones used for this purpose must have the "Ignore Physical Input" option enabled in Input programming.
Options	General Open/Close. Don't Report Area Events. Don't Report Input Events	Area Open/Close reporting will only be done on the 1st Area to Open and the last Area to Close, with the exception of Areas with the "Not General Area" option enabled. Area Open/Close events will not be sent by this Comms Task. Input Events will not be sent by this Comms Task.

Review Options	Review Filter	The Review Filter options may be programmed to determine the events that will be reported based on parameters such as specific entities, entity types, Comms Task Groups, Event type, etc. *See "Digital Dialler Formats" for details of the Comms Task Review Options.*

Introduction to the Intercom Comms Task.

The Integriti Controller has an Intercom Comms Task to provide a high-level interface to a 3rd party Intercom system.
The Integriti system also has an Apartment entity. These features provide an interface that allows an Apartment to grant access to a Call Location.
An Apartment can optionally have a Floor defined as well as having an Intercom System Floor and an Intercom System Unit.
Up to 32 Call Locations can be defined in the Intercom Comms Task and each can optionally have a Door and/or up to 4 Lift Cars defined.
When the Intercom Comms Task detects that an Apartment has granted access to a Call Location, the defined Door and Lift(s) are temporarily unlocked/unsecured to allow access.
At present, the Intercom Comms Task only supports the Kenwei Intercom system. A brief description of the Kenwei system is provided after the Intercom Format programming details.

INTERCOM FORMAT		The Intercom format allows connection to 3rd party Intercom products to allow access control operations to be performed from an Intercom Terminal.
Connectivity	RS232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	Select the Port that the Modem is connected to. No connection. On-board "Port 0" connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4. Port 1 Unibus UART 4, Port 2 Not relevant to this format. Not relevant to this format. Not relevant to this format. Not relevant to this format. **Kenwei:** The Kenwei Intercom can be connected to an Integriti Controller: • Via Port 0 or a UniBus RS-232 Port using an RS485-RS232 Protocol Converter. • Directly to an Integriti Controller RS-485UniBus Port.

	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	Select the Baud Rate for the connection to the Intecom system. **Kenwei:** 9600 Baud.
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	Select the number of Bits for the connection to the Intecom system. **Kenwei:** 8.
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	Select the Parity for the connection to the Intecom system. **Kenwei:** None
	Stop Bits 1 Bit 2 Bits	Select the number of Stop Bits for the connection to the Intecom system. **Kenwei:** 1
Options	Intercom Type Kenwei	Selects the type of Intercom to be connected.
Door / Lift Options	Door / Lift Mappings Call Location number Door to Unlock Lift 1 to Desecure Lift 2 to Desecure Lift 3 to Desecure Lift 4 to Desecure	Each Intercom Call Location can be mapped to a Door and/or up to 4 Lifts to allow the nominated Door to be temporarily unlocked and/or the nominated Lift/s to be temporarily De-secured. The Unlock and De-secure times are programmable specifically for this Comms Task. *See below.* Up to 32 Call Locations can be programmed.
	Door Time	Program the Door Unlock Time. This option applies to all Doors controlled by this Comms Task. If left at 0, the Unlock Time setting in the Door programming will be used.
	Floor Time	Program the Floor Button (De-secure) Time. This option applies to all Floors controlled by this Comms Task. If left at 0, the Button Time setting in the Lift programming will be used.
Miscellaneous options	Online Input	An unused Zone Input may be assigned to monitor the "Online" status. The Input will be sealed while the Intercom Comms Task is online and in alarm when offline. Any Zones used for this purpose must have the "Ignore Physical Input" option enabled in Input programming.

Intercom Comms Task Kenwei Interface.

Description of the Kenwei Intercom system:

The Kenwei Intercom system consists of Indoor Monitor units and Outdoor Camera units. Distributor modules are used to connect the Indoor and Outdoor units.
The standard Distributor module has a DIP switch that is used as the Floor selection for the Kenwei Intercom system and allows for up to 4 Indoor Monitor units connected to a single Distributor module. There is also a special type of Distributor module that allows for up to 4 Outdoor Cameral unit connections. Distributor modules can be connected in series to build up the intercom system to the required size for the installation.
The Kenwei Intercom system addresses the Indoor Monitor units via the Distributor module's Floor and then the terminal location.
e.g. If the Distributor module was set to Floor 17 and the Indoor Monitor was connected to terminal location 3, the Indoor Monitor's address would be 1703.
The Kenwei Intercom system addresses the Outdoor Camera unit as number 1 when it is connected directly to a Distributor module or via the terminal location when connected to a special Outdoor Camera Distributor module.
e.g. If the Outdoor Camera unit was connected to terminal location 3 of an Outdoor Distributor module, the Outdoor Camera's address would be 3.
Refer to the Kenwei Installation manual for full details.

Interface between Integriti and the Kenwei Intercom system:

The Integriti Apartment's Intercom System Floor and an Intercom System Unit equate to Kenwei's Floor and terminal location of an Indoor Monitor unit. The Integriti Intercom Comms Task's Call Location equates to Kenwei's Outdoor Camera address.
The Kenwei Intercom system's RS485 LAN communication protocol has been provided to Inner Range. The Kenwei communication traffic is watched for an "unlock the door" command being sent from an Indoor Monitor unit to an Outdoor Camera unit. When this unlock command is observed, the Integriti Intercom Comms Task searches for an Apartment that matches the Kenwei Indoor Monitor's address. If a match is found the defined Door and/or Lift(s) are temporarily unlocked/unsecured to allow access as well as logging an event to review. If no Apartment is found to match the Kenwei unlock command, then only review is logged.
The Kenwei Intercom's communication traffic is watched by connecting to a segment of the Kenwei RS485 LAN (between the serial Distributors) to a UART on the Integriti Controller. During development/testing this was achieved via an RS485 to RS232 cable connected to UART Port0. The port configuration that is required is 9600,N,8,1 (as per the Figure 2).

Limitations of the Integriti to Kenwei interface:

A typical standalone installation of a Kenwei Intercom system involves a physical electronic lock and/or a lamp to be directly wired to the Kenwei Outdoor Camera unit. There are 3 ways that access through the door can be granted: via the Indoor Monitor unit, via a key fob access at the Outdoor Camera unit and via a PIN password entry at the Outdoor Camera unit. Key fobs are registered with and PINs and are saved to an Outdoor Camera unit.
Using the Kenwei key fob or PIN access from the Outdoor Camera unit cannot be used when using the Integriti to Kenwei interface. This means that the only method to grant access to the Door/Lift(s) is from an Indoor Monitor unit.
To overcome this limitation it would be envisioned that an Integriti access control Reader would be installed alongside the Kenwei Outdoor Camera unit.

BMS FORMAT		The "BMS" communication format allows the Integriti Controller to provide a high-level connection to a 3rd party Building Management System (BMS). e.g. Clipsal C-Bus.
Settings	BMS Protocol None C-BUS Online Input	Select the communications protocol for this BMS Comms Task. No protocol selected. Clipsal C-Bus protocol. Controller Firmware V3.1.0 or later recommended. Select an Input to be used to monitor the Online status of the BMS Comms Task communications link. The Input will be sealed while the BMS Comms Task is online and in alarm when offline. An unused Zone Input can be assigned to this function. Any Zone used for this purpose must have the "Ignore Physical Input" option enabled.
TCP Options	Server IP Address	View or Enter the IP Address of the Server PC.
	TCP Port	View or Enter the Server TCP Port Number. The default Port number (004711) does not normally need to be changed.
	DNS Name	Select required DNS Server Name. DNS Names are programmed separately.
	TCP Mode None Server Client	Select whether the BMS Comms Task is to run as a Server, a Client or neither. *See the Guide: Integriti Communications Tasks –BMS).*
	Retries	The number of times to retry connecting upon failing to connect before it disconnects. Only programmed if "Client" TCP mode selected above.
	Connection Timeout	Programmed in Minutes and Seconds. *See the Guide: Integriti Communications Tasks –BMS).*
	Connection Attempt Timeout	Programmed in Minutes and Seconds. *See the Guide: Integriti Communications Tasks –BMS).*

Connectivity (Serial RS-232)	RS-232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	Select the Port that the Comms Task will use. No Modem connection. On-board “Port 0” connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4. Port 1 Unibus UART 4, Port 2 Not relevant to this format. Not relevant to this format. Not relevant to this format. Not relevant to this format.
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	
	Stop Bits 1 Bit 2 Bits	

EN 32 PIN FORMAT		**NOT YET IMPLEMENTED**
Group Options		Group options are programmed independently for each of the 8 Groups available. The options are the same for each Group.

	Start Auxiliary	Select the first Auxiliary for this Group. The pin Auxiliaries for this group will be a continuous sequence of Auxiliaries starting at this Auxiliary and continuing up to the number of pins enabled in the Pin Map.
	Test Auxiliary	**Not yet implemented.**
	Status Input	**Not yet implemented.** An unused Zone Input can be assigned to this function. Any Zone used for this purpose must have the "Ignore Physical Input" option enabled.
	Pin Map Fire Panic (Personal Alarm) Intruder (Unconfirmed) Open/Close Isolate Fault Confirmed Intruder Power Tamper RF Jam Battery Mask Soak Soaking Primary ATS Secondary ATS (ATS = Alarm transmission system)	Select the pin types to be used in this Group.
	Verify Group	Defines the Verify Group assigned to this Group.
Review Options	Review Filter	The Review Filter options may be programmed to determine the events that will be reported based on parameters such as specific entities, entity types, Comms Task Groups, Event type, etc. *See "Digital Dialler Formats" for details of the Comms Task Review Options.*

SKYTUNNEL FORMAT		NOTES: 1) If upgrading the Integriti Controller Firmware from a Version prior to V3.0.0, to V3.0.0 or later, see the "Important Upgrade Notes" at the beginning of the "Communiations Programming" chapter. 2) In Controller Firmware V3.2.1 or later: - The SkyTunnel Comms Task is only required if Alarm Reporting via SkyTunnel is required. - Configuration of the connection between the Integriti Controller and Integriti Software or Integriti Mobile App via SkyTunnel is now done via "Connection Details" in the General Controller programming and the SkyTunnel Comms Task is not required.
Reporting	Alarm Receiver ID	The Alarm Receiver ID is typically provided by the Central Monitoring Station.
	Map	If Contact ID is to be used as the alarm reporting format, select the Contact ID Map to be used for this Comms Task. Determines which zones are uniquely reported. *Refer to Contact ID Map documentation.*
	Standard	Standard Mapping oriented towards Intruder Alarm monitoring.
	Access	Access Mapping oriented towards Access Control with 2-Door Reader Modules.
	SIMS II	SIMS II Mapping for use with the SIMS II Central Station Automation Software. Allows all Inputs, on up to 35 Modules of every Module Type to be reported uniquely.
	Client Code Prefix	The Client Code Prefix is typically provided by the Central Monitoring Station.
	Client Code	Determines the account code sent when reporting events to the Central Station. This is the default Client Code for this Comms Task which will be used if there is no Client Code programmed in the Area in which the event to report has occurred. If a Client Code has been programmed for an Area, then that Client Code will take precedence when events are reported for that Area. Options are provided to enter the Client Code in Hexadecimal and Decimal formats. Enter a Decimal value between 0 – 65535, or a Hexadecimal value between 0 – FFFF. (Hexadecimal available in Controller Firmware V3.2.1 or later only) Account Codes are typically provided by the Central Monitoring Station. The number of digits required will depend on the reporting format.

	Format None IRFast Contact ID SIA Four Plus Two	Select Reporting Format for this Comms Task. No format. IR fast. Contact ID. SIA 4+2.
Options	Append Text Update Time. Alarm Look Ahead. General Open / Close. IR fast C3k Xmit Historic	Send Review text for each event reported. The Integriti Controller's Real-time clock will be updated New alarms will be reported ahead of multi-break messages for Inputs that have already reported. Whenever all Areas that are programmed to report Open/Close are turned On, a general Area close is reported. As soon as the first Area is turned Off, a general Area open is reported. In Area Programming, some Areas can be nominated to be ignored in the general Area calculation allowing them to still be reported individually. The C3K Compatible Map is implemented for reporting Input events to Receivers and/or Automation Software that have not yet been updated for Integriti IRFast mapping. Sends buffered events for an Input that has since been isolated or is in an Area which has been disarmed. Normally (this option disabled), when there are events buffered for an input, if the input is then isolated or the Area is disarmed, only the final event is sent. When this option is enabled, this functionality is not executed and all buffered events are sent.
Review Options	Review Filter	The Review Filter options may be programmed to determine the events that will be reported based on parameters such as specific entities, entity types, Comms Task Groups, Event type, etc. *See "Digital Dialler Formats" for details of the Comms Task Review Options.*
Miscellaneous options	Backup Input Fail Input	An unused Zone Input may be assigned to monitor the "Backup" status. An alarm will be triggered on this Input when the Backup Comms Task (if assigned) is triggered. Any Zones used for this purpose must have the "Ignore Physical Input" option enabled in Input programming. An unused Zone Input may be assigned to monitor the "Fail" status. An alarm will be triggered on this Input when the SkyTunnel Comms Task fails to report a message. Any Zones used for this purpose must have the "Ignore Physical Input" option enabled in Input programming.

Obsolete	SkyTunnel Password Primary TCP Options Secondary TCP Options	These options are only programmed within the SkyTunnel Comms Task for Controller Firmware prior to V3.2.1. For Controller Firmware V3.2.1 or later, these options are programmed in the General Controller Options. *Refer to the General Controller Options for details.*

E-MODEM FORMAT (External Modem)		The "E-Modem" communication format allows the Integriti Controller to communicate with remote Integriti software via an external Modem connected to a UART Port. **NOT YET IMPLEMENTED**
Connectivity (Serial RS-232)	RS232 Serial Interface Serial Channel None Uart 0 Unibus Uart1(1) Unibus Uart1(2) Unibus Uart2(1) Unibus Uart2(2) Unibus Uart3(1) Unibus Uart3(2) Unibus Uart4(1) Unibus Uart4(2) Modem USB Slave USB Master IAC Onboard RS485	 Select the Port that the Automation Comms Task will use. No connection. On-board "Port 0" connection. Unibus UART 1, Port 1 Unibus UART 1, Port 2 Unibus UART 2, Port 1 Unibus UART 2, Port 2 Unibus UART 3, Port 1 Unibus UART 3, Port 2 Unibus UART 4. Port 1 Unibus UART 4, Port 2 Not relevant to this format. Appears as a Virtual Comm Port in Windows and may be used for this format. Not relevant to this format. Not relevant to this format.
	Baud Rate 1200 Baud 2400 Baud 4800 Baud 9600 Baud 19200 Baud 38400 Baud 57600 Baud 115200 Baud	
	Data Bits 5 Bits 6 Bits 7 Bits 8 Bits	
	Parity None Odd Even Force 1 (Mark) Force 0 (Space)	

	Stop Bits 1 Bit 2 Bits	
Settings	Allow Timed Bypass Rings to Answer	Not yet implemented. Set the number of rings before the External Modem will answer the call.

PEER REPORTING FORMAT		Peer-To-Peer reporting allows relevant Review messages to be sent to another Controller for alarm reporting. *See Peer-To-Peer in General Controller Programming for more information.* Note that if the network connection is lost, the Controller will resend the message twice (3 attempts in total). If the message still fails to reach the Destination Controller no further attempt will be made to resend that message. i.e. Old alarms will not get reported via Peer-To-Peer on network reconnection. A "Backup Comms Task", if programmed, can be used to report alarms that have failed to be reported via Peer-To-Peer reporting. Controller Firmware V3.2.1 or later required.
Miscellaneous Options	Client Code	Determines the account code sent when reporting events to the Central Station. This is the default Client Code for this Comms Task which will be used if there is no Client Code programmed in the Area in which the event to report has occurred. If a Client Code has been programmed for an Area, then that Client Code will take precedence when events are reported for that Area. Options are provided to enter the Client Code in Hexadecimal and Decimal formats. Enter a Decimal value between 0 – 65535, or a Hexadecimal value between 0 – FFFF. (Hexadecimal available in Controller Firmware V3.2.1 or later only) Account Codes are typically provided by the Central Monitoring Station. The number of digits required will depend on the reporting format. For Peer-To-Peer Reporting it is recommended that the Client Codes programmed here and/or in Area programming are different to the Client Codes programmed in the other Controllers in the Peer group. If Client Codes are common to two or more Controllers, then the Monitoring Station will not be able to differentiate between Module/Inputs on different Controllers that have the same Module ID.

	Destination Controller ID	Program the Peer-To-Peer ID of the destination Controller. i.e. The Controller that the review messages will be sent to for reporting. The Peer-To-Peer ID for a Controller can be viewed or programmed in the General Controller programming under Peer-to-Peer options.
Options	General Open / Close.	Whenever all Areas that are programmed to report Open/Close are turned On, a general Area close is reported. As soon as the first Area is turned Off, a general Area open is reported. In Area Programming, some Areas can be nominated to be ignored in the general Area calculation allowing them to still be reported individually.
	Xmit Historic	Sends buffered events for an Input that has since been isolated or is in an Area which has been disarmed. Normally (this option disabled), when there are events buffered for an input, if the input is then isolated or the Area is disarmed, only the final event is sent. When this option is enabled, this functionality is not executed and all buffered events are sent.
Review Options	Review Filter	The Review Filter options may be programmed to determine the events that will be reported based on parameters such as specific entities, entity types, Comms Task Groups, Event type, etc. *See "Digital Dialler Formats" for details of the Comms Task Review Options.*
	Status Monitoring.	Unused Zone Inputs may be assigned to monitor the status of the Peer Reporting Comms Task. Note that any Zones used for this purpose must have the "Ignore Physical Input" option enabled in Input programming.
	Backup Input	An unused Zone Input may be assigned to monitor the "Backup" status. An alarm will be triggered on this Input when the Backup Comms Task (if assigned) is triggered.
	Fail Input	An unused Zone Input may be assigned to monitor the "Fail" status. An alarm will be triggered on this Input when the Peer Reporting Comms Task fails to report a message to the Destination Controller.

Telephone Numbers

Entity/Feature	Option	Description
Telephone Numbers		Select Telephone Number to program.
Name.		Program a name for the Telephone Number up to 32 characters in length.

Telephone Number		Enter the Telephone Number.
		
		The telephone number can include the digits 0 to 9 and the * and # character.
		
		A Pause can be programmed into any part of the telephone number sequence by inserting one or more comma (,) or full-stop (.) characters.
		, (comma) = 125 millisecond pause.
		. (full-stop) = 2 second pause.
		e.g.
		`A 0.5 second pause would be: ,,,,`
		`A 2.25 second pause would be: .,,`
		
		Some Telephone Numbers such as the SMS Service number must be entered in international format starting with the country code.
		e.g. The Telstra Australia SMS service number is entered as "61418706700". (61 is the Country Code for Australia)
		
		Telephone numbers used as SMS numbers should also be entered in the international format.
		Note that when entering a number in international format do not include the + symbol at the beginning.

Telephone Number Lists. *See "Users and Permissions" – "Lists".*

Network Interface Controllers

Entity/Feature	Option	Description
Network Interface Controllers		Select Network Interface to program.
Name.		Program a name for the Network Interface Controller up to 32 characters in length.
IP Address	Local IP Address	Program the static IP address of the local machine (if needed). Only use this option for statically assigned IP addresses. If you do not know the correct value for this setting, see the person responsible for IT infrastructure at the installation site.
	Subnet Mask	Program the Subnet Mask used by this Network Interface. Only use this option for statically assigned IP addresses. If you do not know the correct value for this setting, see the person responsible for IT infrastructure at the installation site.

	Gateway address	Program the Gateway Address used by this Network Interface. Only use this option for statically assigned IP addresses. If you do not know the correct value for this setting, see the person responsible for IT infrastructure at the installation site.
	Use DHCP	If this option is enabled, the DHCP protocol will be used. Disable this option if the static IP Address settings defined above are to be used. If you do not know the setting for this option, see the person responsible for IT infrastructure at the installation site.
DNS Settings	Primary DNS	Program the Primary DNS Address used by this Network Interface. If you do not know the correct value for this setting, see the person responsible for IT infrastructure at the installation site.
	Backup (Secondary) DNS	Program the Backup DNS Address used by this Network Interface. If you do not know the correct value for this setting, see the person responsible for IT infrastructure at the installation site.

DNS Names

Entity/Feature	Option	Description
DNS Name		Select the DNS Name to program.
Name		Program a name for the DNS Name up to 32 characters in length.
DNS Name		Enter the DNS Name text.

System Options Programming

Entity/Feature	Option	Description
Memory Options		Select a Memory Configuration. (Not currently used)
Auxiliary Options		Program/Edit Auxiliary options.
EOL Configurations		Program/Edit Zone Input End Of Line Resistor Schemes.

Memory Configuration

Entity/Feature	Option	Description
Select Configuration		Not currently used.

Auxiliary Options

Entity/Feature	Option	Description
Auxiliary to Edit		Select the Auxiliary to program or edit.
Auxiliary Name		Program a text name of up to 32 characters in length. The name may include the Auxiliary location and/or function.
Options	Auxiliary Options. No Review. Allow Turn On on Reset.	 Activity on this Auxiliary will not be saved to Review. In V3.3.10 or later, this includes Door Lock and DOTL Auxiliaries. On a System Reset, the Auxiliary will be returned to the state it was in prior to the reset.
	Analogue Calibration	Assign a Calibration to this Auxiliary. Determines the calibration parameters for this Auxiliary if it is an Analogue output type. Calibrations are programmed separately.

EOL Configurations

Entity/Feature	Option	Description
EOL Configuration		Select the EOL Configuration to program or edit.. CAUTION: Do not edit the default EOL configurations or create new configurations without a thorough understanding of how the scheme operates, and the ramifications across your system. Note that most legacy Concept Modules do not support alternate EOL schemes.

Name		Program a text name of up to 32 characters in length. The name should unambiguously describe the EOL Configuration.
Debounce Options	Default state debounce time (ms) Alarm state debounce time (ms) Alarm Restore state debounce time (ms)	Minimum time that the Zone Input must remain in an EOL state to process a change. Optional minimum time that the Zone Input must remain in an Alarm EOL state to process a change. Optional minimum time that the Zone Input must <u>not</u> be in the Alarm EOL state to process a change. Note that these options do not apply to legacy Concept Modules.
Ranges	Resistance	Program the eight Resistance settings to define the upper limit of each Band. Eight Bands are available. The resistance range for each Band is from the setting for the previous Band, to the setting of the Band being programmed. e.g. In “Concept3K”, the range for Band 1 is 0 Ohms to 1100 Ohms. For Band 2, 1100 Ohms to 3300 Ohms, etc.
State Mapping	Band States <u>EOL Input States</u> Alarm Tamper Low Tamper High Tamper <u>Logical Input States</u> Zone Self-Test Fail Battery Isolate	Select an EOL Zone “State” for each of the Bands that are to be monitored. There is a range of EOL and Logical Input States to choose from, however, normally only one state from the EOL Input States (Alarm to Tamper) is assigned for a Band. Logical Input States are not relevant to this option and must not be assigned.

Access Control

Entity Types and Groups

Entity/Feature	Option	Description
Entity Types	Door Types Qualified Door Types Lift Types Qualified Lift Types Lift Groups	Edit the names, options and permissions of Access Control Entity Types and Groups. Types & Groups simplify the programming of other entities such as Doors and Lifts by providing pre-programmed entities that define operations.

DOOR TYPES		Door Types provide a simple method of defining how Doors of the same type will operate. Door Types are used to define the operation of Doors where the operation is not required to change due to the status of other entities such as Time Periods. IMPORTANT NOTE: If the operation of certain types of Doors is required to change depending on time/date and/or the status of other entities, then "Qualified Door Types" need to be used. (MENU, 2, 4, 5) e.g. If the credential requirements are "Card Only" to enter and REX button to exit during normal business hours, but "Card & PIN" to enter and "Card Only" to exit at other times. A Qualified Door Type consists of one or more Door Types, each paired with a Qualifying entity such as a Time Period or an Area state, etc.
Find/Create Door Type.		Select the Door Type you wish to edit.
Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Entry Options	User Credential Mode for Entry None Card Only PIN Only Card OR PIN Card AND PIN	Select the User Credential requirement for Entry. None Card must be used. PIN Code must be used. Card or PIN code may be used. User's Card must be followed by the User's PIN Code.
	Dual User. Mask Forced Mode.	Dual User requirement for entry. If enabled, REN will only be used to mask the Forced Door processing and not unlock the Door.

	Anti-Passback Mode for Entry. None Soft Hard Harder Timed	Select the Anti-Passback mode for entry. No Anti-Passback. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is still granted, but an Anti-passback violation is logged to Review. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is denied and an Anti-passback violation is logged to Review. The Area the User is about to enter, and the Area the Reader is located in, are both checked against the User's current location. If the entry Area is the same or the Reader Area is not the same, access is denied and an Anti-passback violation is logged to Review. Same as Hard Anti-passback, except that Amnesty is automatically applied when the Anti-Passback time for that User expires. For "Hard" and "Harder" Anti-passback, amnesty can be provided for an individual User via the "Set Area User is in" (Uarea) Action.
	Entry Button Mode. None Enable Deadlock	Defines Entry button operation. Entry button is Disabled Entry button is Enabled Entry button is Enabled, but only while the Area that the button is located in is Off (Disarmed) i.e. The Area on the same side of the Door.
	Entry Area Disarm Options. Disarm Door Entry Area Disarm User Area	Defines Area Disarm operations on entry. Door Area OFF on entry. User Area OFF on entry.
Exit Options	User Credential Mode for Exit None Card Only PIN Only Card OR PIN Card AND PIN	Select the User Credential requirement for Exit. None Card must be used. PIN Code must be used. Card or PIN code may be used. User's Card must be followed by the User's PIN Code.
	Dual User. Mask Forced Mode.	Dual User requirement for exit. If enabled, REX will only be used to mask the Forced Door processing and not unlock the Door.

	Anti-Passback Mode for Exit. None Soft Hard Harder Timed	Select the Anti-Passback mode for exit. No Anti-Passback. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is still granted, but an Anti-passback violation is logged to Review. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is denied and an Anti-passback violation is logged to Review. The Area the User is about to enter, and the Area the Reader is located in, are both checked against the User's current location. If the entry Area is the same or the Reader Area is not the same, access is denied and an Anti-passback violation is logged to Review. Same as Hard Anti-passback, except that Amnesty is automatically applied when the Anti-Passback time for that User expires. For "Hard" and "Harder" Anti-passback, amnesty can be provided for an individual User via the "Set Area User is in" (Uarea) Action.
	Button Mode for Exit. None Enable Deadlock	Defines Exit button operation. Exit button is Disabled Exit button is Enabled Exit button is Enabled, but only while the Area that the button is located in is Off (Disarmed) i.e. The Area on the same side of the Door.
	Exit Area Disarm Options. Disarm Door Entry Area Disarm User Area	Defines Area Disarm operations on exit. Door Area OFF on exit. User Area OFF on exit.

QUALIFIED DOOR TYPES		Qualified Door Types provide a simple method of defining how Doors of the same type will operate, and allow for circumstances where the operation of certain types of Doors is required to change depending on time/date and/or the status of other entities. e.g. If the credential requirements are "Card Only" to enter and REX button to exit during normal business hours, but "Card & PIN" to enter and "Card Only" to exit at other times. A Qualified Door Type consists of a list of one or more Door Types, each paired with a Qualifying entity such as a Time Period or an Area state, etc. If a Qualified Door Type is assigned to a Door, then on any access attempt, the Door operation is determined by the first Door Type in the list that is currently valid. **IMPORTANT NOTES:** **1.** If more than one Door Type is used in a Qualified Door Type, and there is a possibility that more than one Door Type may be valid at the same time, it is important to consider the order in which the Door Types are assigned. i.e. The Door Types in the Qualified Door Type are prioritised from Q1 to Q8. **2.** If the Door operations are <u>not</u> required to change due to the status of other entities then "Door Types" should be used. (MENU, 2, 4, 2)
Find/Create Qualified Door Type.		Select the Qualified Door Type you wish to edit.
Name.		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Door Types	Door Types What When	Program or Edit the first Door Type for this Qualified Door Type. The "What" <u>must</u> be a Door Type that defines how the Door is to operate. The "When" will be an entity that will define when the Door is to operate in this way. e.g. Typically a Time Period or an Area status. Up to 8 Door Types can be assigned to a Qualified Door Type.

INTERLOCKS		Interlocks provide a simple means of programming Door Interlocking and/or qualifying Door Access with the state of one or more other entities. An Interlock may be assigned to a Door so that access through the Door is qualified by that Interlock Group. The Interlock restricts access through the Door based on the state of entities (typically one or more Doors or Door Lists) in the Interlock Group programming. e.g. Access to a Door into an airlock can be disabled while any other Door into the same airlock is Unlocked and/or Open. Interlock programming also allows other entities to be used to qualify Door access. e.g. The state of one or more Areas, Zone Inputs or Auxiliaries. Once programmed, an Interlock may be assigned to any number of Doors that share the same interlocking requirements. Select the Interlock you wish to edit.
Name.		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Interlock Entities	 What When	Program or Edit the "Interlocked Entities" for this Interlock Group. e.g. To define the Door List, Area, etc., to be applied in the Interlock logic. Defines the entity for this Interlock Entity. e.g. Door List, Area, Input, etc. Defines when the entity is valid for this Interlock Entity. e.g. Time Period, Area state, etc. Up to 16 Interlock Entities can be assigned to an Interlock Group. *See "Permission Programming" for details of how to program this option.*

LIFT TYPES	*See the "Integriti Lift Interfacing" document for a full description of Integriti Lift Access Control.*	Lift Types provide a simple method of defining how Lifts of the same type will operate. Lift Types are used to define the operation of Lifts where the operation is not required to change due to the status of other entities such as Time Periods. IMPORTANT NOTE: If the operation of certain types of Lifts is required to change depending on time/date and/or the status of other entities, then "Qualified Lift Types" need to be used. (MENU, 2, 4, 5) e.g. If the credential requirements are "Card Only" to enter and REX button to exit during normal business hours, but "Card & PIN" to enter and "Card Only" to exit at other times. A Qualified Lift Type consists of one or more Lift Types, each paired with a Qualifying entity such as a Time Period or an Area, etc.
Find/Create Lift Type.		'Add New' or select a Lift Type to edit.
Name		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Entry Options	User Credential Mode for Entry None Card Only PIN Only Card OR PIN Card AND PIN	Select the User Credential requirement for Entry. None Card must be used. PIN Code must be used. Card or PIN code may be used. User's Card must be followed by the User's PIN Code.
	Dual User. Mask Forced Mode	Dual User requirement for entry. REX/REN only used to mask the Forced Door processing and not unlock the Door. **NOT relevant to Lift Access Control.**

	Anti-Passback Mode for Entry. None Soft Hard Harder Timed	Select the Anti-Passback mode for entry. No Anti-Passback. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is still granted, but an Anti-passback violation is logged to Review. The Area the User is about to enter is checked against the User's current location. If these Areas are the same, access is denied and an Anti-passback violation is logged to Review. The Area the User is about to enter, and the Area the Reader is located in, are both checked against the User's current location. If the entry Area is the same or the Reader Area is not the same, access is denied and an Anti-passback violation is logged to Review. Same as Hard Anti-passback, except that Amnesty is automatically applied when the Anti-Passback time for that User expires. For "Hard" and "Harder" Anti-passback, amnesty can be provided for an individual User via the "Set Area User is in" (Uarea) Action. **NOT relevant to Lift Access Control.**
	Button Mode for Entry. None Enabled Deadlock	Defines Entry button operation. Entry button is Disabled Entry button is Enabled Entry button is Enabled, but only while the Area that the button is located in is Off (Disarmed) i.e. The Area on the same side of the Door. **NOT relevant to Lift Access Control.**
	Entry Area Disarm Options. Disarm Door Entry Area Disarm User Area	Defines Area Disarm operations on entry. **NOT relevant to Lift Access Control.**

QUALIFIED LIFT TYPES	*See the "Integriti Lift Interfacing" document for a full description of Integriti Lift Access Control.*	Qualified Lift Types provide a simple method of defining how Lifts of the same type will operate, and allow for circumstances where the operation of certain types of Lifts is required to change depending on time/date and/or the status of other entities. e.g. If the credential requirements are "Card Only" to enter and REX button to exit during normal business hours, but "Card & PIN" to enter and "Card Only" to exit at other times. A Qualified Lift Type consists of a list of one or more Lift Types, each paired with a Qualifying entity such as a Time Period or an Area, etc. If a Qualified Lift Type is assigned to a Lift, then on any access attempt, the Lift operation is determined by the first Lift Type in the list that is currently valid. If more than one Lift Type is used in a Qualified Lift Type, and there is a possibility that more than one Lift Type may be valid at the same time, it is important to consider the order in which the Lift Types are assigned. i.e. The Lift Types in the Qualified Lift Type are prioritised from Q1 to Q8. IMPORTANT NOTE: If the Lift operations are not required to change due to the status of other entities then "Lift Types" should be used. (MENU, 2, 4, 2)
Find/Create Qualified Lift Type.		Select the Qualified Lift Type you wish to edit.
Name.		Program a text name of up to 32 characters in length. This feature can be used to describe the purpose and/or contents of the entity.
Lift Types	Lift Types What When	Program or Edit the first Lift Type for this Qualified Lift Type. The "What" must be a Lift Type that defines how the Lift is to operate. The "When" will be an entity that will define when the Lift is to operate in this way. e.g. Typically a Time Period or an Area status. Up to 8 Lift Types can be assigned to a Qualified Lift Type.

LIFT GROUPS

See the "Integriti Lift Interfacing" document for a full description of Integriti Lift Access Control.

Entity/Feature	Option	Description
Create/Find Lift Group		Select Lift Group to program. Lift Groups are required when a high-level interface (EMS Comms Task format) is used. Not required for low-level interface.

Lift Group Name.		Program a text name of up to 32 characters in length. The name can be used to describe the purpose and/or contents of the entity.
EMS Floor Mapping		Assign each Floor ID of the EMS to the required Integriti Controller Floor record. For each Floor: • Add the Integriti Floor to be mapped. • Enter an EMS Floor number. • If the Floor record is for a Rear Door, then enable the "Rear Door" option.
Settings	EMS Rise	Enter the Rise number to send to an EMS system for Lifts in this Group. The number must be 1 or greater.
	EMS Group	Enter the Group number to send to an EMS system for Lifts in this Group. The number must be 1 or greater.
	Number of Floors	Enter the number of Floors in this Group. If left at 0, the largest EMS Floor number will be used.

CHALLENGE DEFINITIONS

Challenge definitions define the parameters for the Integriti Operator Challenge feature.

Operator Challenge displays information to the operator about a card access request and can be used to passively view or interactively grant/deny access to Users as they pass through one or more doors.
.
The Challenge Definitions can be programmed to:

- Randomly select Users to provide operations such as random bag searches or drug tests to be administered.
- Grant access to Users who do not normally have permissions to access particular Doors.

The Operator Challenge dialogue is completely customizable allowing User Photos, CCTV streams, Allow/Deny buttons, Challenge History, Information display with changeable font/colours and several other items to be arranged and sized as desired. The dialogue can optionally display:
• CCTV footage
• The User's photo
• Custom text
• Challenge history
• Allow button
• Deny button
• A web page

A list of Task Actions can be executed automatically on any challenge, random selection, allow or deny. These Task Actions are the same as used throughout the system, allowing control of entities, sending of messages, etc.

To enable Operator Challenge:
1. Enable the AURM option for any Integriti Controllers on which the Operator Challenge feature will apply.
2. Enable the "Ask PC" option for any Readers on which the Operator Challenge feature will apply.
3. Enable the "Ask PC" option for any Users to which the Operator Challenge feature will apply.

See the Integriti Software "Guide - Operator Challenge" document for more details.

Entity/Feature	**Option**	**Description**

Create/Find a Challenge Definition		Select Challenge Definition to program.
Challenge Definition Name.		Program a text name of up to 32 characters in length. The name can be used to describe the purpose and/or contents of the entity.
What To Challenge		A combination of Doors, Sites/Keywords and Filters can be used to specify what Doors you want to monitor using this Challenge Definition.
	Door	Add one or more individual Doors.
	Sites/Keywords	Add one or more entire Sites or Keywords.
	Filter	Create a Filter to define additional Door selection parameters.
		A combination of Users, Sites/Keywords and Filters can be used to specify what Users you want to monitor using this Challenge Definition.
	User	Add one or more individual Users.
	Sites/Keywords	Add one or more entire Sites or Keywords.
	Filter	Create a Filter to define additional User selection parameters.
Settings	Show Challenge To Operator	This option determines when the Challenge dialogue will appear.
	Never	The Operator Challenge will never display. If Users, Readers, etc. are configured for Operator Challenge ("Ask PC" option) and there is no corresponding Operator Challenge, the Controller will send a challenge request, time out after 20 seconds, then process the User based on their permissions.
	Always	Operator Challenge will appear on every access event.
	Only on Random Selection	Operator Challenge will appear on a random access event based on X occurrences out of Y challenges. *See Random Selection below.*
	Requires Operator Input Never Always Only on Random Selection	Settings for "Requires Operator Input" behave the same way as "Show Challenge To Operator" described above. When an Operator is not required to Input anything, the Controller will continue to process the User based on their permissions.
	Random Selection Select X Occurrences Out of Y Challenges	These options are used to represent the random percentage of access events that will trigger the Operator Challenge. e.g. Select 1 Occurrences Out of 3 Challenges will give you a 33% chance that the User will be picked for Operator Challenge.
	Random Selection Message	Program a simple text string that will be used to display a message to the Operator when an Operator Challenge event occurs.

Challenge Response Layout	*See Integriti Software Documents:* - *"Guide - Operator Challenge"* - *"Integriti GateKeeper"* *for more details.*	The Challenge response layout is configured the same way as an Alert Response Plan: a) Information Boxes display custom text. '%' tags and multiple lines are supported. b) Information Displays support basic HTML tags. The supported tags are listed in the Guide. c) Challenge Pass Button is required for situations where Operator response is required. d) Challenge Deny Button is required for situations where Operator response is required. e) User Image can display either the User image or a custom image field of the User that triggered the Operator Challenge. f) CCTV stream will display live CCTV video from the camera or cameras associated with the door(s) associated with the Operator Challenge. g) Challenge history displays a live stream of past and present Operator Challenges. h) Browser Item will display the web page specified. Keywords associated with the user can be used in the browser URL.
Automatic Actions		Add one or more actions to perform for any of the four types of Operator Challenge events.
	On Challenge	The nominated action/s will occur on every occurrence of the Operator Challenge based on the "What To Challenge" criteria.
	On Random Selection	The nominated action/s will occur whenever a Random Selection occurs on a random Operator Challenge event based on the "What To Challenge" Settings.
	On Allow On Deny	The nominated action/s will occur whenever an "Allow" or "Deny" event occurs when an Operator selects these options via the Operator Challenge dialogue.

Access Control Entities

Card Formats

Entity/Feature	Option	Description
Card Format		'Add New' or select a Card format to edit. Integriti provides an extensive range of pre-programmed Card Formats that will cater for the vast majority of applications. An additional Card format would only need to be programmed to cater for a less common proprietary format or a newly developed format not already provided in the Integriti Card Formats. Please report additional format requirements to Inner Range Support for inclusion in future updates.
Name.		Program a text name of up to 32 characters in length. The name can be used to describe the data protocol, bit length and/or provider of the format.

Options	Card Type	Each card format has a card type defined. The Card Type will tell the reader how to operate, including whether to expect Magnetic Stripe or Wiegand card data, whether it needs to convert the raw data to site code, card number and issues number, or if it needs to hash or decrypt the card data (e.g. Credit Card or IR Secure40). The additional programming fields displayed will vary depending on the Card Type chosen in this option. Select the Card Type to be used in this format.
	None	No Card Type selected.
	Wiegand Raw Data	For direct entry Wiegand cards of any length. (If migrating the card database from a Concept 3000/4000 system you may wish to use the “Legacy: C3k Raw Data” Type.)
	Wiegand Site Code	Allows user credentials to be entered as site code and card number providing the format is known.
	IR Secure 40	Decrypts an IR Secure 40 card and matches it on Site Code and Card Number.
	Mag Swipe Raw Data	Reads up to the first 22 characters of a mag card, until it gets an end or separator sentinel character.
	IR Mag Swipe (Site Code)	Decrypts a Concept Secure Magnetic card and returns its site code, card number and issue number.
	Mag Swipe Site Code	Reads magnetic cards in character mode. Allows user definable site code parameters to be programmed, except lengths and offsets are specified in characters instead of bits.
	Hashed Credit Card	Reads the first 22 characters from a mag card and generates a 5 byte hash from this using the same algorithm as the Concept "Credit Card" format.
	Wiegand Site (Complex)	Allows for Site Code formats unknown to Inner Range. This is the recommended format when only one card format is used throughout the system.
	40 Bit Mag Raw Data	This magnetic swipe card format reads the first 10 characters (40 bits) from a mag card, nibble swapping each byte (ie: swapping each character pair). This allows for compatibility in migrations where Concept Mag Direct was used.
	Mag Swipe Site Code (bits)	This format makes the reader return the binary data from the card instead of characters. This supports non "ISO Track 2" cards where the site code and card number info is stored as binary data instead of characters.
	Legacy: C3k Raw Data	Reads the Wiegand card data and removes the start bit. This helps migrations from Concept direct entry Wiegand systems where the start bit was not used (i.e. Most C3k/C4k Wiegand Direct Entry installations). Note: If a “Raw Data” Card Type is selected, and the data on the Cards to be used will be of different bit lengths, ensure that the “Total Bits” option below is set to “0”.
Site Code Parameters		The Site Code Parameters options will vary depending on the Card Type selected above.

	Wiegand Raw Data Mag Swipe Raw Data Hashed Credit Card 40 Bit Mag Raw Data Legacy C3k Raw Data Total Bits	If one of these Raw Date Card Types is selected above, this option allows the Card data parameters to be defined. The total number of bits present in the Card's data.
	Wiegand Site Code Mag Swipe Site Code Mag Swipe Site Code (bits) Total Bits Site Code Offset Site Code Length Card Number Offset Card Number Length Issue Number Offset Issue Number Length	If one of these Site Code Card Types is selected above, this option allows the Card data parameters to be defined. The total number of bits present in the Card's data. The number of bits in the string prior to the Site Code data. The number of bits in the Site Code data. The number of bits in the string prior to the Card Number data. The number of bits in the Card Number data. The number of bits in the string prior to the Issue Number data. (If used) The number of bits in the Issue Number data. (If used) e.g. If the card data string is 38 bits where Bit 1 is Parity, Bits 2 to 17 are Site Code Data, Bits 18 to 37 are Card Number and Bit 38 is Parity, the settings would be programmed as follows: Total Bits: 38 Site Code Offset: 1 Site Code Length: 16 Card Number Offset: 17 Card Number Length: 20 Issue Number Offset: 0 Issue Number Length: 0
	Wiegand Site Complex Encoding Method Standard Total Bits Site Code Offset Site Code Length Card Number Offset Card Number Length Issue Number Offset Issue Number Length	If this Site Code Card Type is selected above, this option allows the Card data parameters to be defined. Select the encoding method used for this format. Only the 'Standard' method is available at this time. The remaining parameters in this option are the same as described for "Wiegand Site Code" above.

	IR Secure 40 Standard Registered Site Enterprise	If the Inner Range Secure 40 Card Type is selected above, choose the IR Secure 40 scheme that will apply to this Card Format. The Scheme is shown on the label affixed to the box that the cards were supplied in. The Site Code (Hex) is 10 characters in length and also indicates the scheme type as follows: • 00nnnnnnnn = Standard • 01nnnnnnnn = Registered Site • 02nnnnnnnn = Enterprise "Registered Site" and "Enterprise" Cards will also have the text "RS[nn]" printed on them, where nn is the production batch number. Standard. Over 32,000 Site Codes and Card Numbers up to 65,535. Registered Site. Unique Client Site Codes factory registered and Card Numbers up to 65,535. Enterprise. Unique Client Site Codes factory registered and Card Numbers up to 1,048,575.
Card Programming	Wiegand Card Type 26 Bit 27 Bit 30 Bit 32 Bit 34 Bit 35 Bit 36 Bit 37 Bit N Bit Secure 40	For all Card Types in a Wiegand format, an option is provided to select a Wiegand Card Type. This can be N Bit meaning that any bit length is allowed or it can be set to a particular bit length. N Bit will always return all the bits read. For fixed bit lengths, the behaviour varies between legacy Concept Modules and Integriti Modules. **Legacy Modules:** For cards equal to or longer than the bit length, it will return the first n bits, as if the card read were n bits long. If the card is shorter than the bit length, it is ignored. **Integriti Modules:** If the card is not equal to the bit length, it is ignored completely. If a Wiegand Card Type is selected above, select the Wiegand Card Type required. 26 Bits 27 Bits 30 Bits 32 Bits 34 Bits 35 Bits 36 Bits 37 Bits Any bit length is allowed. Inner Range Secure 40 Bits

Photo ID Designs

Entity/Feature	Option	Description

Photo ID Designs		Photo ID Designs can be programmed to create design templates for different types of User Cards to be used in the system. A Photo ID Design is then assigned to a Card Template so that a default Photo ID Design will be provided when printing a Card for any User associated with that Card Template.
Name.		Program a text name of up to 32 characters in length. The name can be used to describe the design, or in the case of multi-tenancy systems, the name may be used to identify the Tenant.
Card Properties and Elements.		Refer to the Integriti Software Manual for details of programming and layout of the Card Properties and Elements. Some default designs are included in the Software which can be used as a guide when creating new designs.

Locations

Entity/Feature	Option	Description
Location		'Add New' or select a Location to edit. Controller Firmware V3.0 or later only. Locations provide an entity to facilitate the global anti-passback feature when the access control system consists of multiple Integriti Controllers. It is only necessary to program Locations if global anti-passback is required across Integriti Controllers linked via the Peer-To-Peer feature. Once programmed, Locations can then be assigned to the Inside and/or Outside of each Door on which global anti-passback functionality is required.
Location Name		Program a text name of up to 32 characters in length. The Location Name would typically include the physical location that it represents.

Door Programming

Entity/Feature	Option	Description
Door		'Add New' or select a Door to edit.
Door Name		Program a text name of up to 32 characters in length. The Door Name would typically include the location and possibly the type of the Door.

		Door programming has been divided into two tabs:
	Door Programming	"Door Programming" allows all the basic parameters to be programmed easily within a simple graphical representation of the Door. If basic access control is required, most of the programming can be done here.
	Advanced	"Advanced" allows the basic options and all other options associated with a Door, to be programmed. If basic access control is required, and the Door Programming tab has already been used, you may only need to program a few parameters on the Advanced tab such as "Door Unlock Time", "Door Open Too Long Time" and "Warn Time".
	DOOR PROGRAMMING	
Module		Select the Module that the Door Reader and hardware are connected to.
Relay	No Lock Lock 1 Lock 2 Lock 3 Lock 4 Lock 5 Lock 6 Lock 7 Lock 8	Select the Lock Relay to be used for this Door. The number of locks displayed in the drop-down list will vary according to the type of Module chosen above.
Door Type	Default Door Types: Entry Door Exit Door Internal (RIRO) Door Card+PIN Entry Door Card+PIN Exit Door Card+PIN Internal (RIRO) Door	Select the Door Type or Qualified Door Type for use with this Door. The selected Door Type or Qualified Door Type will determine how this particular door will function. Door Types and Qualified Door Types are programmed separately The 6 default Door Types shown opposite cover common Door Access Control requirements. Additional Door Types or Qualified Door Types may be programmed. If a Qualified Door Type is assigned, then on any access attempt, the Door operation is determined by the first Door Type in the list that is currently valid.
Outside Settings	Reader None Reader 1 Reader 2 ... Reader 16	Select the Module Reader Port to be used for the Outside Reader. From 1 to 16 Readers may be available depending on the Module Type.

	PIN Device. None Motorola HID Reader MR Access Model Reader 26 Bit Wiegand Keypad IR Weatherproof Terminal 26Bit Wiegand Keypad Forced	If the Outside Reader is a PIN code device, select PIN device type. No PIN device. Motorola/Indala ARK-501 HID 5355 or iClass with 4 Bit Burst PIN output format. MR Access Magnetic Swipe & PIN code Reader 26 Bit Wiegand Keypad. Inner Range Weatherproof Terminal. If enabled, any 26 bit Wiegand data received from this Reader will be processed as a PIN Code regardless of the Site Code. Cards will not be able to be used at this Reader. If disabled, only 26 bit Wiegand data with Site Code 255 (FF) will be processed as a PIN Code and any other Site Code will be processed as a Card. Normally a 26bit Wiegand Keypad has the site code $FF (255) with the card number representing the PIN code. If the reader sends some other site code with a PIN or $FF is actually a site code used by the system, then this option can be used to force any 26bit card number to be treated as a PIN code.
	Location	Select the Location to be associated with the Outside of this Door. (The “Exit” Location) This option is only required for operations in which User Location Tracking is needed such as Global Anti-passback. Note that the Entry &/or Exit Area is still used to prevent access if the Area is armed and the User does not have permission to disarm, and Area User counting still occurs regardless of whether Global Anti-Passback is used.
	Area	Select the Area to be associated with the Outside of this Door. (The “Exit” Area) Required for operations and functions that use the Area status or data such as Reader Arming/Disarming, Anti-passback, User Counting, etc. Normally left set to “None” if the Door is a perimeter Door. i.e. If exiting through the Door takes you out of all areas being protected by the system.
	Arm Mode None Button 3 Badge Area Empty	Select the Area Arming Mode for this Reader if required. No Area Arming via this Reader The “Arm” button must be held on while the Credential (i.e. Card) is presented. The Credential (i.e. Card) is presented to the Reader 3 times within a 5 second period. The Area will Arm when the User Count within that Area transitions from 1 to 0. i.e. When the last person exits the Area.
Inside Settings	Reader	Select the Module Reader Port to be used for the Inside Reader. Options as above.

	PIN Device	If the Inside Reader is a PIN code device, select PIN device type. Options as above.
	Location	Select the Location to be associated with the Inside of this Door. (The "Entry" Location) This option is only required for operations in which User Location Tracking is needed such as Global Anti-passback. Note that the Entry &/or Exit Area is still used to prevent access if the Area is armed and the User does not have permission to disarm, and Area User counting still occurs regardless of whether Global Anti-Passback is used.
	Area	Select the Area to be associated with the Inside of this Door. (The "Entry" Area) Required for operations and functions that use the Area status or data such as Reader Arming/Disarming, Anti-passback, User Counting, etc.
	Arm Mode	Select the Area Arming Mode for this Reader if required. Options as above.
Door Options		This option defines which Inputs on the nominated Module will be used when processing various operations such as Forced Door, DOTL monitoring, Door re-locking, Interlocking, Door Not Opened Review, etc.
	Enable Reed Input	The "Reed" Input for this Door will be used.
	Enable Tongue Input	The "Tongue Sense" Input for this Door will be used.
	ADVANCED	
Door Configuration	Door Type	*See above.*
	Inside Area	*See above.*
	Outside Area	*See above.*
	Inside Location	*See above.*
	Outside Location	*See above.*
	Leaf Door	This option is required if the Door is part of a set of double doors, where the other Door is independently controlled (separate Lock relay) using the same Card Reader. The option is programmed by assigning the Door that is associated with the other Lock relay.
	Door State Follows Area State	Select if the Door state is to be controlled by the Inside and/or Outside Area. i.e. Door will Unlock if Area Disarmed, and will Lock if Area is Armed.
	None	Door state does not follow Area State.
	Inside Area	Door state follows Inside Area State.
	Outside Area	Door state follows Outside Area State.
	Either Area	Door state is Locked when either the Inside or Outside Area is Armed, and will Unlock when both Areas are Disarmed.
	Both Areas	Door state is Locked when the Inside and Outside Areas are both armed, and will Unlock when either Area is Disarmed.

	Physical Type Normal Roller (Up – Down) Roller (Toggle)	Select the physical type of the Door. Normal Door. A Roller Door that requires separate outputs from the controller for Up and Down control. A Roller Door that requires a single timed output from the controller on which each activation toggles between Up and Down. *See "Roller Doors" following the Door programming for details.*
	Inhibit Input	If a Roller Door type is selected above, an Inhibit Input may be programmed. The Inhibit Input is installed to detect something blocking the physical path of the Roller Door. e.g. A PE (Photo Electric) beam installed immediately inside the Roller Door to detect the presence of a pedestrian or vehicle under the raised Door.
Advanced Door Configuration	Lock Auxiliary	Hardware Auxiliary address for Door lock. Programmed only when the door does not use the predefined local lock auxiliary of the Reader Module or Terminal.
	Door Unlock Time	Determines how long the door lock auxiliary remains On when the Door is accessed. Programmed in Hours, Minutes and Seconds up to a maximum of 18 Hrs, 12 Mins and 15 Seconds.
	Disability Unlock Time	Determines how long the door lock auxiliary remains On when the Door is accessed by Users that have the "disabled" option enabled. Programmed in Hours, Minutes and Seconds up to a maximum of 18 Hrs, 12 Mins and 15 Seconds.
	Door Open Too Long (DOTL) Time.	Determine how long a door may remain open until a DOTL warning or alarm is generated. If the Door remains open longer than this time, then: - If a DOTL Warning Time is <u>not</u> programmed, the relevant DOTL (Door Held) System Input on the Module will go into alarm. - If a DOTL Warning Time <u>is</u> programmed (see below), the relevant local DOTL Warning output on the Module will be turned on for the Warning Time. If the Door continues to remain open for longer than the warning time, the relevant DOTL (Door Held) System Input on the Module will go into alarm. Programmed in Hours, Minutes and Seconds up to a maximum of 18 Hrs, 12 Mins and 15 Seconds.
	Warn Time (Door Open Too Long [DOTL] Warning Time)	Determines the DOTL Warning timer period. *See "Door Open Too Long (DOTL) Time" above for details.*

	Interlock	Defining an Interlock restricts access through this Door based on the state of entities in the Interlock Group programming. e.g. Access to a Door into an airlock can be disabled while any other Door into the same airlock is Unlocked and/or Open. Interlock Groups are programmed separately.
Anti-Passback	Entry Area Anti-Passback Minutes (For "Timed" Anti-passback only)	Defines the Timed Anti-Passback period for an anti-passback violation on the Entry Area. *See "Anti-Passback Mode" in Door Types programming for details.*
	Exit Area Anti-Passback Minutes (For "Timed" Anti-passback only)	Defines the Timed Anti-Passback period for an anti-passback violation on the Exit Area. *See "Anti-Passback Mode" in Door Types programming for details.*
Options	Tenancy Area Counting.	If enabled: On a successful Door access control operation, and the direction is leaving, then the number of Users in the User's Tenancy Area will be decremented. Any resultant Area User Count Action will also be invoked. If direction is entering then the number of Users in the User's Tenancy Area will be incremented. Any resultant Area User Count Action will also be invoked. i.e. The User Count will be updated in the User's Tenancy Area instead of the Door Inside Area. Notes: 1. The User's Tenancy Area must be defined. 2. The Dual User option should not be used with Tenancy Area Counting. If not enabled: On a successful Door access control operation, the number of Users in the Door Area that you are leaving will be decremented (twice if Dual User) and the number of Users in the Door Area that you are entering will be incremented (twice if Dual User). Any resultant Area User Count Action will also be invoked. i.e. User counting is performed on the Area/s assigned to the Door.
	Door Not Opened Review	If enabled, causes a Review Message to be logged whenever this Door is unlocked, but then not subsequently opened.
	No Passback On Entry	When selected, a User 'entering' via this Door will not have their anti-passback area changed. The Area User counts and the software's User status remain unaffected. Controller firmware V3.2.3 or later only.
	No Passback On Exit	When selected, a User 'exiting' via this Door will not have their anti-passback area changed. The Area User counts and the software's User status remain unaffected. Controller firmware V3.2.3 or later only.

Debounce	Force Debounce.	This option will shunt the reed/tongue for this time after the door is unlocked. This is to stop the panel accidentally relocking the door due to bounce as it is opened. While the door is unlocked if the panel senses the door open, it will wait for it to close again. When it closes the panel will automatically relock the door, even if the lock timer hasn't expired.
Behaviour	When Offline	Select an Offline option for this Door to define how it will operate if the host Module is offline.
	Permissive	Normal offline access mode based on a subset of the User's permissions.
	Restrictive	Any Doors to which the User has unqualified access (i.e. access all the time) will be allowed. Any Doors to which the User has time-period qualified access (i.e. access only at certain times) will not be allowed.
	No Access	Access will be denied to all Users at this Door if the host Module is offline.
	Free Access	If the Door is required to be in Free Access under certain conditions, select the Time Period that will define the Free Access conditions.
Card Format	Card Format.	This screen allows the Card Format to be selected. Card Formats are programmed separately. A wide range of default Card Formats are available.
	Direct Entry Wiegand 26Bit Wiegand (H10301) Indala 27 Bit – Wiegand Keri 30 Bit Wiegand etc…	*See 2 Door Reader Module programming for the full list of default card formats and their details.*

Roller Doors

Options are provided in Door programming to define a physical Door type of "Roller (Up – Down)" or "Roller (Toggle)". Roller (Up – Down) is a Roller Door that requires separate outputs from the controller for Up and Down control. Roller (Toggle) is a Roller Door that requires a single timed output from the controller on which each activation toggles between Up and Down.

To implement Roller Door control, a Reed Switch is installed (door reed input) that seals when the door is fully closed, and an optional reed switch is installed (tongue sense input) that seals when the door is fully open.

The complete list of Input and Output states used for Roller Doors is as follows:

Door reed sealed	Roller door fully down (locked)
Door reed in alarm	Roller door not fully down
Tongue reed sealed	Roller door fully up (locked) (tongue input must be enabled)
Tongue reed in alarm	Roller door not fully up (tongue input must be enabled)
Door Lock output	Roller up output (or toggle output for toggle type doors)
Door DOTL output	Roller down output (only for up/down type doors)
Door Tamper Input	Alarms when a roller door fault occurs, seals when tries again
Door DOTL Input	Alarms at start of down warning, seals at end of down warning (Program an action to the Door DOTL Input to annunciate a door down warning)

Door Forced Input	Alarms if the door is currently fully opening, and is being prevented from closing by the Door inhibit input (see below)
Door Inhibit Input	Pauses a door going down via an input (e.g. safety beam) When input re-seals door continues down Doesn't work for toggle mode doors

The following Door and Reader Module programming options are required to implement Roller Door control:

- Set the Physical Door Type option to Up/Down roller door or Toggle roller door.
- Set the “Door Unlock Time” to the maximum time it takes to open the roller door, or if tongue sense is not enabled, the time that the roller door requires to reach its desired open position.
- Set the “Extended Unlock Time” to the maximum time it takes to close the roller door.
- Set the “Door Open Too Long Time” to the maximum time it takes the roller door to signal it is now opening/closing via the reed or tongue inputs.
- Set the “Warn Time” to the time that the DOTL input will remain in alarm as a warning prior to the roller door closing (going down warning)
- Set “Force Debounce” time to set the time the toggle relay turns on for in toggle mode (Also sets the gap between toggles)
- Select the “Inhibit Input” if being used.
- The Reader Module “Enable Tongue Input” option is set for the appropriate Door if a reed is installed to indicate the roller door is fully open (connected to the tongue sense input).

The roller state machine is designed to try and get the roller door either open (if the door is unlocked) or closed (if the door is locked).
The roller state machine does not alter the lock status of the door - it simply tries to manipulate the roller door to get it into the correct state.
If the roller doors cannot be got into the correct state to match the lock status of the door, then a "Fault" state is assumed and no more effort is made to get the roller door to match the door lock status until another lock(or relock) or unlock (or re-unlock) attempt is made.
Whilst in the "Fault" state, the door tamper input is in the alarm condition indicating a problem. If a door is currently up and is being prevented from closing because of the inhibit input, then the door forced input will be in alarm.
All attempts to close (lock) a roller door are preceded by a "Down Warning" state. This state puts the door DOTL input into alarm which can be used to warn personnel that the door is about to close. At the end of the warning time the door attempts to close. Once the door direction down is established, if the inhibit input is sensed in alarm then the door will revert to going up.
When a card is presented or REX/REN button pushed and the door is a roller door, then the current lock state of the door is toggled. i.e. Lock to unlock or unlock to lock.

A Motor overload output can be wired to tamper either reed or tongue input to immediately cause the fault input state.

Note on Inhibit Input and Roller Door toggle mode: In toggle mode, the lock output pulses to reverse the direction of the door, i.e. going up or going down. The roller state machine attempts to deduce the correct direction the door is travelling, however, it is possible under abnormal circumstances that the door direction is not ascertained correctly. This can result in the inhibit input not successfully stopping a closing door. When using toggle mode, another means must also be used to sense door obstructions.

Note on tongue sense: If tongue sense is disabled, then the state machine uses the “Door Unlock Time” to determine when the door is considered to be fully open from fully closed. Note that subsequent locks and unlocks could result in the door going higher than desired.

It is not recommended to have tongue sense disabled in toggle mode because when the door is in the open state, there is no way to see if the toggle state is correct by monitoring for an alarm on the tongue reed switch (door fully open).

Lift Car Programming

See the “Integriti Lift Interfacing” document for a full description of Integriti Lift Access Control.

Entity/Feature	Option	Description
Lift Car		‘Add New’ or select a Lift Car to edit.

Name		Program a text name of up to 32 characters in length. The Lift Car Name may include the location and/or type of the Lift.
Restricted Floors		If the Lift Car does not service all Floors, permissions may be programmed to define one or more Floors or Floor Lists that are serviced (by selecting "Allow") and/or are not serviced (by selecting "Deny) by this Lift Car and when these restrictions apply. Up to 3 Restricted Floor Permissions may be assigned.
Lift Configuration	Lift Mode None Low Level (No Button Feedback) Low Level (Button Feedback) High Level / EMS	Select the Interface Mode used for this Lift Car. None Low Level Lift interface with no Button Feedback Low Level Lift interface with Button Feedback High Level Lift interface via Serial or Ethernet communications.
	Lift Type	Select the Lift Type or Qualified Lift Type for use with this Lift Car. The selected Lift Type or Qualified Lift Type will determine how this particular Lift will function. Lift Types and Qualified Lift Types are programmed separately. There are no default Lift Types. If a Qualified Lift Type is assigned, then on any access attempt, the Lift operation is determined by the first Lift Type in the list that is currently valid.
	Lift Floors	Define the Floors to be serviced by this Lift Car.
	Button On Time	Program the Button time in Hours, Minutes and Seconds.
	Disability Button On Time	Program the Button time for Users with the "Disability" option enabled in their User record. The time is programmed in Hours, Minutes and Seconds.
	Valid Auxiliary	Select an Auxiliary to be used to indicate a valid User Lift access request. Typically used to access a turnstile.
High Level	EMS Type Car Panel Destination Panel Home Floor Caller	 The Reader and Floor selection panel are located within the Lift Car. This Lift Car is logically a Destination Panel. The Reader and Floor selection panel are located in the Lift Lobby (outside the Lift Car) Kone RCGIF. *See the Guide: Integriti Communications Tasks –Lift Interfacing (EMS).*
	Lift Group	Select a Lift Group to define the EMS parameters for this Lift Car. Lift Groups are programmed separately.

	EMS Terminal ID	Identifies the EMS Terminal associated with this Lift Car if required. *See the Guide: Integriti Communications Tasks –Lift Interfacing (EMS).*
	EMS Lift ID	Program an EMS Lift number to identify this Lift Car to the EMS. If the EMS Type is a Destination Panel, program the Destination Panel ID for this Lift Car. *See the Guide: Integriti Communications Tasks –Lift Interfacing (EMS).*
	EMS Floor Number	If the EMS Type "Destination Panel" or "Home Floor Caller" has been selected, program this option to identify the Floor number to the EMS.
	Valid Auxiliary Time	Program an On time for the Valid Auxiliary when using High Level Lift mode.
Low Level	Hardware Interface UniBus Lift Interface board. LAN Zone Expanders	If a Low Level interface is in use, select the hardware that will be used for Floor button enables for this Lift. If UniBus Lift Interface Boards are used, select the host LAN Module that the Lift Interface board/s are connected to. Note that UniBus Lift Interface outputs are not Auxiliaries. If LAN Zone Expanders are used, select the first Auxiliary. The Floor Button enable Relays will be a continuous sequence of Outputs starting at this Auxiliary and continuing up to the number of Floors defined in "Lift Floors". After the last Auxiliary on the Module, you move to the next Auxiliary on the next sequential module (E01:32 to E02:X01)
	Error Auxiliary	Select an Auxiliary to be used to indicate an Invalid User credential or an error in the Lift access control process.
	Add Floors	Set to Yes IF you require additional Floor buttons to immediately be enabled when another User presents their Card to the Reader while the previous User's buttons are still enabled.
	Use 2nd Enables	Set to Yes if you require the previous User's enabled buttons to be cancelled when another User presents their Card to the Reader.
	Button Enable Hold Time	If Button Feedback is in use, program the Button Enable Hold Time in Days, Hours, Minutes and Seconds. This option defines the time that the Floor buttons remain enabled after button feedback is received.

Floor Programming

See the "Integriti Lift Interfacing" document for a full description of Integriti Lift Access Control.

Entity/Feature	Option	Description

Floor		'Add New' or select a Floor to program.
Name		Program a text name of up to 32 characters in length. The Floor Name may include the location of the Floor.
Associated Area		Select an optional Area to be associated with this Floor if required.

Automation and Logic Functions

Entity/Feature	Option	Description
Auxiliary Lists		Create a list of Auxiliaries.
Named Actions		Program/Edit Named Actions.
Action Lists		Enables up to 8 actions to be combined in a single entity.
Macros		
Air-conditioning		
Comparisons		Program/Edit Comparisons.
Calibrations		
Compound Entities		Allows multiple entities to be combined logically for use as a Qualifier in Permissions.
General Variables		
General Timers		
Automation Points		Defines the relationship between Integriti and entities on 3rd Party products communicating with Integriti via the BMS Comms Task format. e.g. C-Bus.

Auxiliary Lists. See "Users and Permissions", "Lists".

Named Actions

Entity/Feature	Option	Description
Named Action		Select the Named Action to program or edit. Named Actions allow Users to perform predefined actions from a Terminal. Options are also provided to allow the Named Action to be controlled by another Entity.
Name		Program a text name of up to 32 characters in length.
Action to Take		Select the Entity Type to be controlled or operation to be performed by this action. Once an Entity Type or operation is selected, additional fields are displayed to program the Action details and any action Qualifier parameters. *See Action Programming in "Generic Programming Operations" for more details.*

Optional Trigger		Select an Entity that will trigger this Named (Predefined) Action. e.g. An Input, Time Period, Auxiliary, Door, etc. that will trigger the Named Action. NOTES: • Any entity can be used as the trigger entity. • The trigger entity and the action qualify entity (if defined) are continuously tested to see whether the action needs to be asserted or de-asserted. • On power-up, after 20 seconds, all Named Actions with trigger entities will assert or de-assert the action depending on the combined state of the trigger entity and the action qualify entity. • Action processing only checks the action qualify entity on assert, not de-assert. • If the trigger entity is a User or Permission Group, then the Named Action is asserted at the time of User logon.
User Interface	Interface Style None On / Off Open / Close Air Conditioning Auxiliary Control Trigger Secure	Select the User Interface style to be used when this Named (Predefined) Action is operated manually via a Terminal. i.e. What the icons look like or what terminology is used to show the state of the action. No style On / Off Open / Close Air-conditioning Auxiliary Trigger Secure
	Sense Entity 1.	Select the Entity to display the state of this Named Action. e.g. An Auxiliary or a Zone Input. Typically this entity is simply the target of the action, but it could be something else. e.g. A Relay controls a motor and a Zone Input is wired to a tachometer which senses when the motor is running. Instead of having the state of the auxiliary display the state, you could use the Input to give you a truer display of state so that you know when the motor is actually spinning.
	Invert Sense Entity.	Allows the result of the Sense Entity to be inverted. e.g. If an Auxiliary is chosen as the Sense Entity, then inverting the Sense Entity will allow the Auxiliary to be turned On when the Action is de-asserted instead of when asserted. e.g. If the NC contacts instead of the NO contacts of a relay are used, so on means off, etc.
	Allow Logged off access.	The Named Action can be controlled from a Terminal without the User logging on.

User Access	Action Groups	This option allows Named Actions to be grouped together in up to 16 Action Groups for the purpose of defining which Users and Entities are allowed to control which Actions. The Named Actions allowed to be controlled from an LCD or Graphic Terminal, or by particular Users or Types of Users are defined via similar screens in Menu Group programming. The Menu Group can then be assigned to an LCD Terminal or Graphic Terminal, a User and/or Permission Group. Select which of the 16 Action Groups this Named Action will belong to.

Action Lists

Entity/Feature	Option	Description
Action List		Select the Action List to program or edit. Action Lists enable up to eight separate Actions to be combined in a single entity. Action Lists are supported in Controller Firmware V3.2.1 or later. If upgrading from a firmware version prior to V3.2.1, a Controller memory default will need to be performed to add Action Lists to the memory configuration.
Name		Program a text name of up to 32 characters in length. The name may include the purpose of the Action List and/or a summary of the actions associated with it.
Define Actions		Up to 8 Actions may be assigned to an Action List. For each Action, once an Entity Type or operation is selected, additional fields are displayed to program the Action details and any action Qualifier parameters. *See Action Programming in "Generic Programming Operations" for more details.*

Macros

Entity/Feature	Option	Description
Macro		Select the Macro to program or edit.
Name		Program a text name of up to 32 characters in length. The name may include the purpose and/or some details of the Macro.

Type	- Do an Action - Do an Action when the Expression Changes - Goto <label> If - Pause for Time - Define a Label - Set Entity to Expression - Wait for Condition - Execute Modified Action - End Current Macro	Select the Type of Macro to program.
Action		If the Macro Type is: - Do an Action - Do an Action when Expression changes - Execute Modified Action… Select the Entity Type to be controlled by this action. Once an Entity Type is selected, additional fields are displayed to program the Action details. *See Action Programming in "Generic Programming Operations" for more details.*
Expression		If the Macro Type is: - Do an Action when Expression changes - Goto <label> if… - Pause for Time… - Set Entity to Expression - Wait for Condition Program the Expression. Expressions can evaluate to true or false, or to a number, depending on the context in which they are used.
Label		If the Macro Type is: - Goto <label> if… - Define a Label Program the Label.
Entity to Set		If the Macro Type is: - Set Entity to Expression Select the Entity. Nearly all entities can return a numerical value. For instance an Input can hold a count value. This statement changes the entities value to the value returned by the expression, which could be a constant, another entity, or a maths formula involving any of these. This is primarily how GVars get set to a value.

Entity 1 Entity 2 Entity 3 Entity 4		If the Macro Type is: - Execute Modified Action… Select up to 4 Entities to define the numeric parameters for the action. The numeric value returned by the first entity will set the first numeric parameter for the action, the second entity the second parameter. So if the action were "control an auxiliary" and the first entity is a count Input, the on time of the aux action would be determined by the count value in the Input.
Comment		If the Macro Type is: - Do an Action - Do an Action when Expression changes - Goto <label> if… - Pause for Time… - Define a Label - Set Entity to Expression - Wait for Condition - Execute Modified Action… - End Current Macro You may enter a comment in this field. Just like comments in programming language, allows the programmer to document the intended functionality of each line.
Statements		

Air-conditioning

Entity/Feature	Option	Description
Air-conditioner		Select the Air-conditioning Unit to program or edit.
Name		Program a text name of up to 32 characters in length.
Temperature Sensors		Select the Inputs to be used for Temperature Sensing. Up to 8 Inputs may be selected, one for each Air-conditioning Zone.
Damper Auxiliaries		Select the Auxiliaries to be used to control the Zone Dampers. Up to 8 Auxiliaries may be selected, one for each Air-conditioning Zone.
Compressor Auxiliary		Select the Auxiliary to be used to control the Compressor.
2nd Compressor Auxiliary		Select an optional 2nd Compressor Auxiliary to be used to control a Compressor.
Reverse Cycle Auxiliary		Select the Auxiliary to be used to control Reverse Cycle On/Off.
Fan Auxiliary		Select the Auxiliary to be used to control the Fan.
Fresh Air Damper Auxiliary		Select the Auxiliary to be used to control the Fresh Air Damper.

Bypass Damper Auxiliary		Select the Auxiliary to be used to control the Bypass Damper.
Minimum Compressor ON Time.		Determines the Minimum Compressor On Time. Enter a value in Hours, Minutes and Seconds. A Value of up to 1 Hr, 49 Min and 13 Seconds can be entered.
Minimum Compressor OFF Time.		Determines the Minimum Compressor Off Time. Enter a value in Hours, Minutes and Seconds. A Value of up to 1 Hr, 49 Min and 13 Seconds can be entered.
Damper Time		Determines the Damper On Time. Enter a value in Hours, Minutes and Seconds. A Value of up to 1 Hr, 49 Min and 13 Seconds can be entered.
Return Air Zone		Defines the Air-conditioning Zone where the Return Air Damper is located.
Minimum Zones for Bypass		Defines the minimum number of zone dampers that can be open before the compressor bypass damper will be closed. If less than this number of zone dampers are open, the bypass damper output will turn off thus opening the bypass damper to lessen air flow from the fan. If this option is left at 0, the bypass damper will remain closed.
Dead-band		Defines the dead-band between heating and cooling mode in degrees Celcius.

Comparisons

Entity/Feature	Option	Description
Comparison to Edit		Select the Comparison to program or edit. Comparisons provide the ability to trigger actions when certain analogue or count values are reached on an Input.
Comparison Name		Program a text name of up to 32 characters in length.
Input and Thresholds	Input to Monitor	Select an Analogue or Counter type Input to Monitor.
	Threshold 1	Enter the Threshold 1 value. The un-calibrated Analogue or Count value representing the required threshold must be used.
	Threshold 2	Enter the Threshold 2 value.
Inputs to Trigger	Input for Threshold 1	Select an optional Input to Trigger for Threshold 1. The alarm state of the selected Input will be asserted if the monitored Input is above Threshold 1. The alarm state will be de-asserted if the monitored Input is below or equal to Threshold 1. An Input trigger will be required if you wish the event to be reported.

	Input for Threshold 2.	Select an optional Input to Trigger for Threshold 2. The alarm state of the selected Input will be asserted if the monitored Input is above Threshold 2. The alarm state will be de-asserted if the monitored Input is below or equal to Threshold 2. An Input trigger will be required if you wish the event to be reported.
Threshold 1 Action.	Action 1	Select Entity Type for Threshold 1 Action. Once an Entity Type is selected, additional fields are displayed to program the Action details. *See Action Programming in "Generic Programming Operations" for more details.*
	When Above Threshold 1. None Assert De-assert	Choose what to do for Action1 when Above Threshold 1. No state triggered when above Threshold 1. State Asserted when above Threshold 1. State De-asserted when above Threshold 1.
	When Below Threshold 1. None Assert De-assert	Choose what to do for Action1 when Below Threshold 1. No state triggered when below Threshold 1. State Asserted when below Threshold 1. State De-asserted when below Threshold 1.
Threshold 2 Action.	Action 2	Select Entity Type for Threshold 2 Action. Once an Entity Type is selected, additional fields are displayed to program the Action details. *See Action Programming in "Generic Programming Operations" for more details.*
	When Above Threshold 2. None Assert De-assert	Choose what to do for Action2 when Above Threshold 2. No state triggered when above Threshold 2. State Asserted when above Threshold 2. State De-asserted when above Threshold 2.
	When Below Threshold 2. None Assert De-assert	Choose what to do for Action2 when Below Threshold 2. No state triggered when below Threshold 2. State Asserted when below Threshold 2. State De-asserted when below Threshold 2.

Compound Entities

Entity/Feature	Option	Description
Compound Entity		Select the Compound Entity to program or edit. Compound Entities enable up to eight different Entities to be logically combined for use as a Qualifier in Permissions. How cool is that?

Name		Program a text name of up to 32 characters in length. The name may include the purpose of the Compound Entity and/or a summary of the entities associated with it.
Define Entities and Relationships		Up to 8 Entities may be assigned to a Compound Entity. For each Entity assigned, an "Invert" option and logical relationship may be defined. The programming options below are repeated for each of the eight Entities.
Entity Selection		Select an Entity to include in this Compound Entity.
Invert Entity		Enable this option if you require the logic for this Entity to be Inverted. Normally the different Entity types will be considered Valid in the state shown in the table below. Enable this option if you require the Entity to contribute a Valid condition to the Compound Entity when in the opposite state.
	User	Programmed.
	Door	Locked and Closed.
	Door List	All Locked and Closed.
	Area	Armed
	Area List	All Armed
	Input	Sealed
	Auxiliary	On
	Time Period	Valid
	Schedule	Valid
	Holiday	Valid
Logical Relation		Select the logical relationship of this Entity to the next Entity. This Entity is ANDed with the following Entity This Entity is ORed with the following Entity XOR logic is applied to these Entities. i.e. The result is Valid if either entity is Valid and Invalid when both Entities are either Valid or Invalid. The logic is applied in the order in which it is entered. The first two Entities take the first Logical Relation (operator). The second Logical Relation is applied to the result of the first two entities and the third entity. The third Logical Relation is applied to the previous result and the fourth entity, etc. Imagine A, B, C, D, and E are entities 1 to 5 respectively and 1, 2, 3 and 4 are Logical Relations 1 to 4 respectively. The expression would be: ((((A 1 B) 2 C) 3 D) 4 E).
	And	
	Or	
	eXclusive OR (XOR)	

Foreign Entities

Entity/Feature	Option	Description

Foreign Entity		Select the Foreign Entity to program or edit. Foreign Entities enable Entities from one Controller to be used in operations on another Controller. *See "Peer-To-Peer" in General Controller Programming for details.*
Name		Program a text name of up to 32 characters in length. The name may include the purpose of the Foreign Entity and/or a summary of the entities associated with it.
Miscellaneous Options	Target Entity	Select an Entity from another Controller that will be represented by this Foreign Entity.

General Variables

Entity/Feature	Option	Description
General Variable		Select the General Variable to program or edit. General Variables provide a place to store a value and perhaps do something when that value reaches a certain threshold.
Name		Program a text name of up to 32 characters in length.
Test Value		Program a Test Value. The Variable will be True if the General Variable value is greater than this number.
Calibration		Select a Calibration for this General Variable to define the formatting of the General Variable. Calibrations are programmed separately.

General Timers

Entity/Feature	Option	Description
General Timer		Select the General Timer to program or edit. Normally a general timer is valid, which means it can trigger or qualify an action. There is an action which can set the time for a timer. When set, the timer is invalid, so would de-assert or not qualify an action, and begins counting down its timer. When its timer expires, it goes valid again, so would assert or qualify another action.
Name		Program a text name of up to 32 characters in length. The name may be used to describe the purpose and/or period of this timer.

Calibrations

Calibrations define processing and display parameters and options for analogue inputs in an Integriti system.

A number of default Calibrations are provided to cover common requirements as follows:

Configuration	**Description/Purpose.**
Raw Value	Raw value 00000 – 65535.
IR 994089 Temp Sensor	Inner Range Serial Temperature Sensor. 0 to +40 °C.
C3K Alog 0-5 Volts	Concept Analogue Module Input configured for voltage sense.
C3K Alog 4-20mA as mA	Concept Analogue Module Input configured for current loop.
C3K Alog 4-20mA as %	Concept Analogue Module Input configured for current loop displayed as a percentage.
GT Light %	Integriti Graphic Terminal light sensor.
GT Temp DegC	Integriti Graphic Terminal temperature sensor. -10 to +50 °C.
Unibus Alog 0-10 Volts	Integriti Unibus Analogue board Input configured for voltage sense.
Unibus Alog 4-20mA as mA	Integriti Unibus Analogue board Input configured for current loop.
C3k Alog IR 994089 Freezer Mode	Inner Range Serial Temperature Sensor. -55 to +70 °C. (V3.3.13 or later only)

Summary descriptions of the parameters and options are provided below.
See the "Integriti System Configuration Handbook" for full details.

Entity/Feature	**Option**	**Description**
Calibration ID		Select the Calibration to program or edit.
Name		Program a text name of up to 32 characters in length.
Calibration	Offset	Offset to add to Raw multiplied to Gain.
	Overall Shift	The entire result will be divided by 2 to the power *this value*
	Calibrate Calculation	This is the calculation that will be used in this Calibration where 'R' is the raw value. This equation is derived from the parameters programmed in the options above.
Calibration Linear Component	Gain	Factor by which the Raw value is multiplied.
	Shift	Denominator (as a power of 2) for the Gain / Offset calculation.
	Linear effective Gain	The gain that would achieve the same result (without the shift)
Calibration Quadratic Component	Quadratic Gain	Factor by which the Raw value is multiplied.
	Quadratic Shift	Denominator (as a power of 2) for the Gain / Offset calculation.
	Quadratic Effective Gain	The gain that would achieve the same result (without the shift).
Calibration Cubic Component	Cubic Gain	Factor by which the Raw value is multiplied.
	Cubic Shift	Denominator (as a power of 2) for the Gain / Offset calculation.

	Cubic Effective Gain	The gain that would achieve the same result (without the shift).
Display	Format / Scale	Used to determine how the analogue value is to be displayed. It includes the scaling, sign if required and text for the desired units. Example 1. units = COMMON_UNIT_MILLIKELVIN and we want to display between -30.0 and +10.0 degrees C. -30C=243000, 0C=273000, +10C=283000 Format string = "K3 Z273000 S2.1 DegC" Where: K3 - indicates scale is 3 decimal places. Z273000 - indicates the sign transition is 273000 COMMON_UNIT_MILLIKELVIN. S - Means display sign. 2.1 - Indicates the format. DegC - Is displayed as is. Example 2. units = COMMON_UNIT_MILLIVOLTS and we want to display between 00.00 and 99.99 Volts. Format string = "K3 F2.2 Volts" Where: K3 - Indicates scale is 3 decimal places. F - Means do not display sign. 2.1 - Indicates the format. Volts - Is displayed as is.
	Display String	Units or gauge ID text to display.
	Minimum String	Minimum value in XXX.YYY format, matching scale_string.
	Maximum String	Maximum value in XXX.YYY format, matching scale_string.

Automation Points

An Automation Point defines the relationship between Integriti and entities on 3rd Party products that interface to Integriti via the BMS Comms Task format. e.g. C-Bus.

Entity/Feature	Option	Description
Automation Point		Select the Automation Point to program or edit.
Name		Program a text name of up to 32 characters in length.
BMS Type	 C-Bus Lighting C-Bus Custom	Select the Automation Type required for the interface. Selects the C-Bus "Lighting" Application. Selects the C-Bus Custom type which allows an Application ID and parameters to be programmed for C-Bus Applications other than lighting.

C-Bus Lighting

C-Bus Lighting Options	Group	Program the C-Bus Group Address for this Automation Point. Commands will be sent to this Group Address.
	Ramp Threshold	Program a Ramp Threshold value between 0 and 255 to define when the C-Bus entity will alter the state of the Integriti entity. When the level on the nominated C-Bus Group Address: - Falls below this value, the mapped Integriti entity is deasserted. - Rises to this value or higher, the mapped Integriti entity is asserted. The "Update Entity" option described below must be enabled.
	Assert Command On Off Stop Ramp Ramp	Select the C-Bus command to perform when the nominated Integriti entity is asserted.
	Assert Ramp Rate	Select the ramp rate to be used when the "Ramp" command is selected above. This is the period that it will take for the nominated C-Bus entity to ramp from its current level to the "Ramp Level" specified below. 16 pre-defined ramp rates are available. Instant (0s) and 15 periods ranging from 4 Seconds to 17 Minutes.
	Assert Ramp Level	Program a Ramp Level to be used when the "Ramp" command is selected above. This is the final level that the C-Bus entity will ramp to.
	Deassert Command	Select the C-Bus command to perform when the nominated Integriti entity is deasserted.
	Deassert Ramp Rate	Select the ramp rate to be used when the "Ramp" command is selected for the Deassert command above. This is the period that it will take for the nominated C-Bus entity to ramp from its current level to the "Ramp Level" specified below. 16 pre-defined ramp rates are available. Instant (0s) and 15 periods ranging from 4 Seconds to 17 Minutes.
	Deassert Ramp Level	Program a Ramp Level to be used when the "Ramp" command is selected for the Deassert command above. This is the final level that the C-Bus entity will ramp to.
	Custom App Code	Allows a different Application Code to be sent/monitored for this Automation Point. A Custom Application Code may be entered as a Decimal number. If left at 0, the default "Lighting" App Code will be used.

C-Bus Custom

C-Bus Custom Options	Custom App Code	Commands will be sent with this C-Bus Application Code. The value is programmed in hexadecimal format. These options should only be attempted by experienced C-Bus integrators. Distributor/Factory Technical Support is not available for this feature.

	Assert String	Program a C-Bus message that will be sent when the Integriti Mapped entity is Asserted. Do not include the Application Code or Route. The string will automatically be prefixed with these according to the settings in those options.
	Deassert String	Program a C-Bus message that will be sent when the Integriti Mapped entity is Deasserted. Do not include the Application Code or Route. The string will automatically be prefixed with these according to the settings in those options.

C-Bus Route

C-Bus Route	First Route Hop Second Route Hop Third Route Hop Fourth Route Hop	These options are available to allow C-Bus commands to be sent to different C-Bus networks across C-Bus Network Bridges. Using these options it is possible to specify up to four Network Bridges for the command to traverse.

Common Options

Common Options	Update Entity	Select this option if the Integriti Mapped Entity is to be controlled by the nominated BMS entity. In the case of C-Bus, the Integriti entity will be controlled by the C-Bus Group Address according to the "Ramp Threshold" option programmed above.
	Mapped Entity	Select the Integriti entity to be mapped to the BMS entity. Whenever this entity changes state, an update may be sent to the BMS according to the command options programmed above for the type of BMS selected.
	Qualifier	Select a qualifier entity if required. If a qualifier is selected, changes in state on the Mapped Entity will be ignored unless the Qualifier is valid.
	Associated Action	If required, select an action to perform when the Mapped Entity is asserted as a result of a change of state of the BMS entity.

Inner Range Pty Ltd
ABN 26 007 103 933

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