



TECOM Discovery Control Panel Programming Manual

Copyright	©2025 Aritech, All rights reserved.
Trademarks and Patents	The TECOM Discovery name and logo are trademarks of KGS Fire & Security Australia Pty Ltd. Aritech is a Global Trademark of Kidde Global Solutions. Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.
Design	Designed in Australia by: KGS Fire and Security Australia Pty. Ltd. Suite 4.01, 2 Ferntree Place Notting Hill, Victoria 3168 Melbourne, Australia
Manufacturer	Made in Australia by: SRX Global Electronics Manufacturing Services Australia & Malaysia 8 – 10 Kitchen Road Dandenong Victoria 3175 Melbourne, Australia
ACMA compliance	
Contact information	For contact information, see www.aritech.com.au

Table of Contents

Contents

- Important information14**
 - Limitation of liability14**
 - Agency compliance14**
 - Regulatory requirements for New Zealand14**
- Preface.....15**
- Chapter 1 Introduction1**
 - The Discovery system2**
 - Overview.....2**
 - Keychanges between ChallengerPlus and Discovery.....3**
 - Key features.....3**
- Chapter2 Overview7**
 - Product overview8**
 - Discovery Web Interface8**
 - LCD RAS.....8**
 - Management software8**
 - Planning the system.....8**
 - Enclosure Access Restrictions9**
- Chapter 3 Programmingbasics.....10**
 - User menu structure11**
 - Install menu structure12**
 - Disarming the system13**
 - Accessing the Install menu13**
 - Reset to default13**
 - Navigating via RAS.....14**
 - Common navigation techniques.....14**
 - Model-specific navigation techniques.....14**
 - The LCD screen14**
 - Programming the options15**
 - Selectingareas by searching.....15**
 - Programming sequence.....16**

Default installer PIN	16
Changing the default installer PIN	16
Restoring the default installer PIN	17
Chapter 4 Commontasks	18
Setting up a basic alarm system	19
Overview	19
Default programming values	21
Programming users	23
Programming relays	24
Overview	24
Programming steps	24
Example	25
Connecting to a printer	27
Printer output via RS-232	27
Printer output via IP	28
Connecting to software	29
Programming arming stations	29
Introduction	29
Keypad arming stations	29
Card reader arming stations	31
Using card readers for alarm control	32
Alarm control with key switches	32
Camera control and monitoring	34
Overview	34
Programming steps	34
Programming delayed holdup inputs	36
Programming automatic arming and disarming	38
Disarming and arming of common areas	41
Programming macros	41
Overview	41
Example of macro logic programming	42
Examples of macro function selections	43
Programming service technician access	47
Triggering console (RAS) beepers	48
Using keypad duress	48

Programming common areas	50
Using Area Search	50
Area search procedure for standard systems (not financial institutions).....	51
Area search procedure for financial institutions	51
Configuring IP connections	52
Overview.....	52
Advanced network administration	53
Using timed input testing	53
Programming text via RAS	54
Automation overview.....	55
Controlling automation zones via RAS	56
Control via User menu.....	57
Control via Quick Control	57
Control via Install menu	58
Programming twin trip inputs	58
Connecting via UltraSync	60
Chapter 5 Programming Reference.....	61
Inputs	64
Programming Inputs	64
Programmable event.....	66
Test type	68
Pre-defined events to activate (check boxes).....	69
Areas.....	71
Programming areas	71
Area name	72
Exit time (sec).....	72
Entry time (sec)	72
Account code.....	73
Disarm time (min)	73
Perimeter area	73
Out of hours' time zone.....	74
Siren.....	74
Secure alarm	74
Entry timer	75
Access alarm	75
Local alarm.....	75
Exit timer	75
Warning timer	76
Input isolated	76

Pre-alarm	76
Input unsealed	76
Area accessed.....	76
Camera	77
Preferred video camera	77
RAS	77
Operations.....	78
RAS programming options	78
RAS number.....	79
RAS name	79
Poll RAS	79
Model number.....	80
Alarm group.....	81
Menu alarm group	81
RAS Relay.....	82
Doorevent	82
RAS Flags	82
DGP	87
Operations.....	87
Programming DGP's.....	87
Sync DGP	88
DGP number	88
Poll DGP (checkbox)	88
DGPName	89
Device model.....	89
Programming tiles for Configurations.....	89
Alarm group.....	90
Alarm group application.....	91
Programming alarm groups.....	92
Alarm group.....	92
Alarm group name	92
Assigned area or area group.....	92
Enter Area / Area group	93
Arm.....	93
Reset.....	93
Disarm	93
Timed area.....	93
Time zone.....	93
Alternate alarm group	93
Options (checkboxes) Users alarm group	93
Remote access	94
Alarm system control	94
Reset system alarms	94
Prompt with list of areas	95

Keypad duress	95
Usercategories (1 through 8).....	95
Auto isolate	96
Forced arming.....	96
Prevent forced disarming	96
Prevent area arming if not timing	96
Disable auto-deisolate	97
Enable area search	97
Menu (checkboxes).....	97
Timers	100
Programming timers	100
Siren time (min)	100
RAS door open (sec).....	101
RAS card and PIN timeout (sec).....	101
Twin trip maximumtime (sec).....	101
Usercategory 1 – 8 time (min).....	101
Warning time (min).....	101
Suspicion (sec)	101
Service (min)	102
Access test (min)	102
Secure test (min)	102
Localalarm reminder (min).....	102
Mains fail time (min).....	102
Delay holdup (sec)	102
Individual test (min)	102
Tester event (sec).....	102
Min area search (min).....	102
Max area search (min).....	103
System options	103
Auto reset	115
Programming Auto reset	116
Reset time (mins).....	116
Alternate alarm group	116
Comm device.....	117
Programming Comms devices	117
Programming comm paths	125
Selecting comm path number	125
Select configuration type.....	125
Enable connection	126
Connection control	129
Filter	131
Test calls	133
Test call day	134

Test call time.....	134
Programming	139
Enable UltraSync	139
Passcode	139
Allow remote connection.....	139
Allow programming if any area armed	139
Allow firmware upgrade if any area armed	139
Allow remote control.....	139
Restrict control if any area armed.....	139
Enable web interface.....	139
Siren beep on alarm	139
Monitor secondary SIM link.....	139
Alternate location setting Location.....	140
URL / Port 1 & URL / Port 2.....	140
Filter event to area or area group	140
Enter time zone	140
Multi Break Alarm Time.....	140
Checkboxes – tick box to enable Report alarm events	140
System alarms report.....	141
Buffer outside time zone.....	141
Common Open Close	141
Report Communication Event.....	141
Report Access Events	141
Report Event TZ Invalid	141
Multi Break Alarms	141
Multi Break Restores.....	141
Report Open Close	142
Disarm Clears Pending Alarms.....	142
Test calls	142
Test call option	142
Test call time.....	142
Programming	143
To create a new report press the + Add and fill out the Add Report.....	143
Report numbers.....	143
User number	143
Address	144
Event check boxes	144
Time zones	144
Programming time zones	145
Time zone number	145
Time zone name.....	146
Holiday types	146
Segment two to eight.....	147
Relays	147
Programming	148

Relay number	149
Relay name	149
Relay inverted	149
Inactive during time zone	149
Event flag.....	149
Time zone.....	149
Vaults	150
Programming vault areas	151
Area links	151
Programming	152
Area link number	152
Linked area name.....	152
Assigned area or area group	153
Input shunts.....	153
Programming	154
Shunt name	155
Input number to shunt	155
Relay number	155
Shunt time.....	155
Event flag	156
Warning time	156
Warning flag	156
RAS	156
Shunt flags (Check boxes).....	156
Door shunted in access	156
Door shunted in secure.....	157
Input hold event	157
Entry/exit shunt.....	157
Report door open/close	158
Soft time zones	158
Programming	159
Time zone number	159
Time zone name.....	159
Relay	159
Battery test	160
Programming	160
Frequency	160
Start hour and minutes.....	160
Run time (mins)	161
Custom RAS message	161
Next service	162
Date	162

Text	162
Summary event flags.....	163
Programming	164
Mains fail.....	164
Low battery	164
Fuse fail	164
Tamper.....	164
DGP isolate	164
DGP fail	164
RAS fail	164
Duress	165
Film out	165
Report fail	165
Test mode.....	165
All secured	165
Console trigger	165
Area search running	165
Area search done	165
Panel macro logic.....	165
Macro number	167
Macro name.....	167
Macro type	167
Macro Duration (sec/min)	168
When.....	168
Input 1 -4 Type.....	168
Macro inputs	169
Macro logic equation.....	169
Area group.....	170
Programming	170
Area group name.....	171
Area.....	171
Automation zone.....	171
Programming	172
Automation zone number	172
Automation zone name	172
Enable (Checkbox)	173
Trigger level (%).....	173
Reset level (%)	173
Trigger time (sec).....	173
Ramp rate	173
Trigger time zone	174
Disable trigger TZ (Time zone)	174
Event to trigger time zone	174

Tick boxes to enable	174
Enable logging	174
Automation only on for mask	175
Enable quick control	175
Enable manual control	175
Manual on control	175
Manual off control	176
RAS number	176
Protocol type	176
Activates event flag	176
Set event flag level (%)	176
Reset event flag level (%)	177
BUS number	177
Group number	177
App number	177
Event flag	178
Programming	178
Event flag number	178
Event flag name	179
Discovery name	179
Standard lifts	179
Chapter 6 Maintenance	191
Troubleshooting	192
Maintenance	196
Introduction	196
Standards	196
Peripheral devices	197
Automated testing	197
Recommended routine maintenance procedures	198
Contacting technical support	201
Appendix A Reference materials	202
System numbering	203
Overview	203
Zone input numbering	203
Relay and output numbering	205
Siren output numbering	206
Door and lift numbering	206
Time zone numbering	207
Input types	208
Input tamper monitoring	209

Application notes.....	209
List of input types	210
Alarm group default settings	219
Event flags.....	222
Reporting	224
CID reporting codes for input events	224
CID reporting codes for system events.....	225
STU serial reporting formats	225
Programming map	225
AppendixBProgramming worksheets.....	227
Input worksheet	228
Area worksheet	229
Area group worksheet	230
RAS worksheet.....	231
DGPs worksheet	233
Alarm group worksheet	234
Timers worksheet.....	235
System options worksheet	236
Auto reset worksheet.....	238
Communications worksheets	239
Time zones worksheet	245
User categories worksheet	246
Relay mapping worksheet	247
Arm or disarm via time zone worksheet.....	248

Arm or disarm via time zone worksheet	248
Vaults worksheet.....	249
Area linking worksheet	249
Input shunt worksheet.....	250
Soft time zones worksheet	251
Battery testing worksheet	251
Custom message worksheet.....	252
Next service date worksheet	252
Event flags worksheets.....	252
Macro logic worksheet.....	255
Users worksheet	256
Door groups worksheet	257
Floor groups worksheet.....	259
Holidays worksheet.....	260
Automation zones worksheet.....	262
Doors & lifts worksheet.....	263
Glossary	266
Index	275

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will KGS Fire & Security Australia Pty Ltd be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of KGS Fire and Security Australia Pty. Ltd. shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether KGS Fire and Security Australia Pty. Ltd. has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

The customer is responsible for testing and determining the suitability of this product for specific applications. The customer is responsible for testing the product at least once every three months.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, KGS Fire and Security Australia Pty. Ltd. assumes no responsibility for errors or omissions.

Agency compliance

This product conforms to the standards set by Standards Australia on behalf of the Australian Communications and Media Authority (ACMA). We recommend enclosure covers remain fitted to maintain ACMA compliance.

Regulatory requirements for New Zealand

Some parameters required for compliance with Telecom's Telepermit requirements are dependent on the equipment (PC) associated with this device. In order to operate within the limits for compliance with Telecom's Specifications, the associated equipment shall be set to ensure that:

- There shall be no more than 10 call attempts to the same number within any 30 minute period for any single manual call initiation.
- The equipment shall go on-hook for a period of not less than 30 seconds between the end of one attempt and the beginning of the next attempt.
- Automatic calls to different numbers are spaced such that there is no less than 5 seconds between the end of one call attempt and the beginning of another.

- This equipment shall not be set up to make automatic calls to the Telecom '111' Emergency Service.
- The associated equipment shall be set to ensure that calls are answered between 3 and 30 seconds of receipt of ringing.

Preface

This manual applies to the Discovery control panels:

The product name "Discovery" will often be used in this manual.

The *Discovery Programming Manual* is for system administrators and installers who need to manage the Discovery system, typically via either the web-based user interface or a text-based keypad terminal (in particular via the "Install menu").

Refer also to other Discovery manuals in the suite:

- The *Discovery Installation and Quick Programming Manual* is for installation technicians to install and commission a Discovery panel.
- The *Discovery User's Manual* is suitable for most users of the Discovery system to perform everyday tasks.
- The *Discovery Administrators Manual* is for users and system administrators who need to manage the Discovery system via its text-based user interface (in particular the User menu).

Chapter 1

Introduction

Summary

This chapter provides an overview of the Discovery system.

Content

The Discovery system	2
Overview	2
Key changes between ChallengerPlus and Discovery	3
Key features.....	3

The Discovery system

Overview

The TECOM Discovery Control Panel is a scalable intrusion detection and access control system. Key TECOM Discovery Control Panel features and benefits include:

- Supports TECOM Challenger system components and peripherals
- DIN rail mounting (DIN adaptor kit for existing enclosures)
- 12 / 24 VDC primary power supply
- 8 individually fused power outputs supporting 3A of peripheral load
- 2 siren and 1 strobe outputs
- 16 on-board alarm inputs
- 4 general purpose relays (e.g., doors)
- Expansion port for additional relays
- 3* LAN (RS485) busses supporting existing and new TECOM high speed protocols
- 2 reader terminals supporting Wiegand and OSDP* protocols
- All LAN and OSDP ports have on-board protected, SW controlled termination
- Ethernet NIC
- 2 USB host ports for additional communications (4G / 5G / Wi-Fi / 2nd NIC)*
- STU interface
- I/O status indication LEDs
- Web browser for configuration options

* Certain functionality will be available in the future by firmware updates.

Key changes between ChallengerPlus and Discovery

Discovery has the following new features over ChallengerPlus:

- Onboard status indicator LEDs
- 4 onboard dry-contact relays
- 2 onboard Wiegand reader inputs
- 2 USB interfaces (1 x USB-A, 1 x USB-C)
- Integrated web interface for configuration of the Discovery panel
- Software-driven RS-485 termination

Additionally, Discovery modifies some existing ChallengerPlus functionality:

- Default user capacity has increased from 2,000 users to 65,535 users
- PSU input changed from 16 VAC to 12 / 24 VDC
- Strobe relay has been modified from relay 2 to relay 15
- Onboard dialler has been removed
- USB connectivity to software is not available
- Existing expansion ports for 3G/4G comms and user expansion have been removed
- Support for TS0866 / TS0867 Four door controllers, and TS0869 Four lift controllers has been removed

Key features

Experienced Discovery users, installers, and administrators will feel at home with Discovery control panels because most of the fundamental concepts are very similar to the Challenger Series.

The following sections briefly describe the main differences that a programmer will need to know about Discovery control panels.

Multiple communication paths

Ten communication paths are available for simultaneous management software connections, reporting via UltraSync, and so on. The status of each path can be quickly displayed via the Discovery web interface or RAS to facilitate installation and troubleshooting.

Users

All Discovery users have user names stored on hardware, and can have PINs up to 10 digits long and up to 48 bits of raw card data.

Inputs

The Discovery panel has 16 inputs. Every DGP address (31 in total) supports 32 inputs for a maximum of 1008 zone inputs.

Notes:

- Some DGP models do not support expansion to 32 inputs, so the number of physical inputs at that address is reduced accordingly.
 - Input numbers in the range 1000 to 1008 will not report CID alarms (Ademco CID format supports 999 zones).
-

End-of-line (EOL) resistor selection

The Discovery panel can be configured (via system options) for alternative EOL resistor values (default is 10K) for the zone inputs connected directly to the Discovery panel. Alternative EOL resistor values may also be used with inputs connected to TS1020 Analogue DGPs.

Areas

The total number of areas is 99. By default, the first 16 areas are mapped to RAS area LEDs in the same manner as in *ChallengerPlus*. If needed, any area number can be mapped to an individual RAS area LED. One entity will be visible and more can be added by selecting + Add.

Area groups

Area groups are collections of areas that can be more easily managed, for example armed or disarmed simultaneously.

Each area in an area group must be configured to allow certain users (as specified by the user's alarm group) to have permissions for arming, disarming, alarm reset, and for timing.

Alarm groups

An alarm group can be linked to an area or to an area group:

- If an alarm group is linked to a single area, then the alarm group controls the area's settings for arming, disarming, alarm reset, and timing (see "[Alarm group](#)" on page 90).
- If an alarm group is linked to an area group (one or more areas), then the area group controls each area's settings for arming, disarming, alarm reset, and timing (see "[Area groups](#)" on page 170).

User categories

Discovery user categories consist only of a number and a name. All eight user categories can be used for timing via the user category time programmed in Timers.

Holidays

Holidays can be defined for multiple days, and can automatically be repeated annually (on the same dates). A holiday must be assigned a holiday type.

Holiday types

Holiday types consist only of a number and a name. There can be up to eight holiday type records.

Holiday types 1 to 8 are not programmable at the panel (they pre-exist). Each holiday type can optionally have a name in management software, or listed on the [Holiday types worksheet](#) (Figure 62 on page 261).

Holiday types provide the ability to grant access for users on some holidays and not others. For example:

- We want cleaning staff to have access during school holidays, but not on public holidays.
- We want maintenance staff to have access during both school and public holidays.
- School holidays can be designated H1 type, and cleaning staff time zone must contain H1 type.
- Public holidays can be designated H2 type, and maintenance staff time zone must contain H1 and H2 types.

Time zones

Time zones can have eight segments, and each segment can be assigned to one or more holiday types.

Area search functionality

Area search is a special disarming process to ensure that a facility is safe to enter at the start of the day.

Timed input testing

Timed input testing allows zone inputs to be tested during normal operation within a specified number of days. The Discovery panel can report when an input has been tested and will report an alarm for inputs that haven't been tested as specified.

Automation zone programming and control

Discovery panels provide configuration and control of automation zones (one or more building devices) via technologies such as C-Bus®.

Standard lifts

Discovery panels can support up to 32 Total - which 32 Doors, of which 2 can be standard lifts with ten floors each, without requiring a Network Access Controller. See "[Standard lifts](#)" on page 179 for more information.

Standard doors

Discovery panels can support up to 32 Total - which is 32 Doors of which 2 can be Standard Lifts, without requiring a Network Access Controller. See "[Standard doors](#)" on page 183 for more information.

Chapter 2

Overview

Summary

This chapter provides an overview of the Discovery system and instructions for planning the best approach to programming the system.

Content

Product overview	8
LCD RAS	8
Management software.....	8
Planning the system	8
Enclosure Access Restrictions.....	9

Product overview

The Discovery panel is the heart and soul of the Discovery alarm and access control system. The Discovery system is essentially a collection of databases that are stored in the panel's onboard memory and can be programmed by the installer (or administrator, as applicable) using the tools described in the following sections.

Discovery Web Interface

A Discovery system can be programmed via the Discovery Web Interface.

LCD RAS

A Discovery system can be operated via a remote arming station (RAS), and limited programming / initial configuration done using a keypad with an LCD screen.

The RAS's text-based user interface provides a numbered menu structure for rapid access to the menus ([see Table 3 on page 12](#)). Even if you plan to use management software for most tasks, some initial Discovery system programming must be done using an LCD RAS before it can communicate with management software.

Management software

A Discovery system that is configured and programmed to be accessed via management software (such as CTPlus and WMS Pro) may be programmed (in part or whole) and operated via the management software, Discovery web interface, and RAS.

The management software user interface is graphical and broadly follows the RAS programming map. Menu numbers are not typically used in the graphical interface, and the descriptions of the programming options may vary slightly depending on the method used.

Management software also enables the use of the TS0870P Smart Card Programmer, used to program Smart Cards. Smart Cards can be used for unlocking doors, arming, and disarming areas, and for operating 'credit applications' such as drinks dispensers, copiers, lighting, and so on.

This manual is based on the programming options as displayed on the Discovery web interface - Web User Interface (WebUI). Options listed as YES or NO on the RAS correspond with enabled or disabled, and are typically shown as ticked or unticked in the management software user interface.

Planning the system

You should create a system plan prior to installing and programming a Discovery system. A system plan should include:

- **Site map:** Create a basic drawing that shows the premises with the location

of all required system equipment (labelled with name and input number). If the anti-passback function is required for the system, regions and IN/OUT reader addresses should be defined on the site map.

Equipment list: Use the site map to create a list of all equipment needed for the system.

- **Naming convention:** Use the site map to create names for the system's equipment, inputs, relays, areas, and so on. The Discovery panel supports 30 characters for most items.
- **Programming worksheets:** Use worksheets to record programming details and to help understand how the various programming options relate to each other. Worksheets (typically completed by the installer) may be found in "[Appendix B "Programming worksheets"](#)" on page 227.

In planning the system make sure you define what outputs (siren, strobe, relays) will be required. This will determine the event flags that will need to be programmed in the input, area, arming station, summary event flags, and shunt timer databases.

Refer to the *Discovery Installation and Quick Programming Manual* for installation and setup information.

Enclosure Access Restrictions

According to the requirements of AS/NZS 62368-1, the interior of the enclosure presents hazards to general users and thus physical access restrictions must be instituted to ensure safety. To comply with the requirements related to safety:

- Access to the interior of the Enclosure must be limited to suitably trained and qualified installation and maintenance technicians.
- Access to the interior of the enclosure should require the use of a key and/or tool.

These restrictions can be met by implementing one or more of the following options:

- Fit a lock to the enclosure. Ensure that it is always locked when not under the immediate control of suitably qualified technicians.
- Seal the enclosure door using standard head (non-knurled) screws, firmly tightened.
- When using finger operable screws (knurled head, etc) to seal the enclosure door, tighten to 2Nm (typically >1/4 turn beyond the finger tight point).

Chapter 3

Programming basics

Summary

This chapter provides instructions for getting started with programming the Discovery system.

Content

User menu structure	11
Install menu structure.....	12
Disarming the system	13
Accessing the Install menu	13
Reset to default.....	13
Navigating via RAS.....	14
Common navigation techniques	14
Model-specific navigation techniques	14
The LCD screen	14
Programming the options	15
Selecting areas by searching.....	15
Programming sequence.....	16
Default installer PIN.....	16
Changing the default installer PIN.....	16
Restoring the default installer PIN.....	17

User menu structure

There are 24 top-level User menus in the Discovery system ([see Table 2 below](#)).

Most of the programming described in this manual is in sub-menus accessed via option 19. Install Menu ([see Table 3 on page 12](#)). However, you may need User menu options 14, 15, 20, and 21 when programming the system. Refer to the *Discovery Administrators Manual* for information about these top-level menus.

Table 2: User menu (top level)

User menu option	Description
1. Panel Status	Lists inputs in alarm, tamper, isolated, unsealed, and system alarms.
2. Input Unsealed	Lists unsealed inputs, for example, an open door contact or an input in tamper condition.
3. Input In Alarm	Lists inputs in alarm.
4. Input Isolated	Lists inputs that are isolated.
5. History	Lists events of system history, including alarms, menu access, etc.
6. Test Report	Displays the results of the access test or secure test.
7. Service Menu	Request a service call or connect/disconnect to management software.
8. Film Counters	Display the frame number position on security camera films.
9. Input Text	Display the description of the inputs.
10. Isolate	Isolate inputs.
11. Deisolate	Deisolate inputs.
12. Test Input	Test an individual input device.
13. Start Auto Access Test	Start the access test.
14. Program Users	Create, modify, or delete user records.
15. Time and Date	Program the panel's time and date.
16. Isolate/Deisolate RAS/DGP	Isolate or deisolate RASs or DGPs.
17. Enable/Disable Service Tech	Enable and disable the service technician's PIN.
18. Reset Cameras	Reset the film frame count on security cameras.
19. Install Menu	See Table 3 on page 15.
21. Holidays	Record the dates of holidays.
22. Open Door	Open a door.
23. Unlock, Lock, Disable and Enable	Unlock, lock, disable, or enable a door.

User menu option	Description
24. Automation Control	Turn automation zones (such as lights) on or off.
25. Change PIN	Change default PIN.

Install menu structure

Table 3 below lists the Install menu options, accessed via User menu option 19. The Install menu items are described in detail in [Chapter 5 “Programming reference”](#) on page 61.

The Discovery menus contain numbered options. The option numbers help to navigate the text-based interface on an LCD RAS and not provided as a guide to programming sequence or other workflow. Refer to [“Setting up a basic alarm system”](#) on page 19 for the recommended programming sequence.

Table 3: Install menu

Install menu option	Description
1. Communications	Program the hardware devices and communications paths that the panel will use.
2. Remote Controllers	Access additional programming menus for remote devices such as a RAS, a Network Access Controller DGP, or a TS0862 Smart Door Controller (which is addressed and polled as a RAS).
3. Version	Display the system’s device types and firmware version numbers.
4. Defaults	Reset the panel to default settings.

Disarming the system

The system must be completely disarmed (all areas) before you can access the Install menu. Use the following steps to disarm the system.

1. The default message displays on the top line of the RAS. Depending on the programming of "[Custom message](#)" on page 161, this line may display "There Are No Alarms In This Area", the time and date, or a custom message.

There Are No Alarms In This Area
Code:

2. Press 4346 (the default Installer code), press [OFF] [0] (to select all areas), and then press [ENTER].

Accessing the Install menu

The Discovery menu system, as displayed on an LCD RAS, has a first-level User menu and a second-level Install menu (the Install menu is option 19 of the User menu). Access to the Install menu is typically limited to installers or administrators.

Use the following steps to access the Discovery User menu when the Code prompt is displayed on the bottom line of the RAS.

1. Press [MENU*].

To Access Menu Enter Code
Code:

2. Enter 4346 (default Installer code), and then press [ENTER].

"0"-Exit "ENTER"-Down "*" -Up
0-Exit, Menu:

3. You can now select the programming option you need from the User menu ([see Table 2 on page 11](#)). To access the Install menu, enter 19 (Install menu option number), and then press [ENTER].

Install Menu
0-Exit, Menu:

You can now select the programming option you need from the Install menu (see [Table 3 on page 12](#)).

Reset to default

Sometimes it is necessary to bring the control panel back to factory defaults (for example, if programming a system that has been without power for more than two weeks).

Alternatively, you may need to default the panel without using the Install menu. Refer to "Clearing the memory via the Discovery panel Reset button" in the *Discovery Installation and Quick Programming Manual*.

Navigating via RAS

Common navigation techniques

The following keys are used to move between menus or between menu options in the Install menu:

- Press [ENTER] to scroll forward one menu option.
- Press [MENU*] to scroll backward one menu option.
- Enter the menu number and press [ENTER] to jump directly to a menu.
- Enter [0] and press [ENTER] or press [CLEAR] to exit the menu.

Model-specific navigation techniques

Certain RASs have additional navigation options, as described in the following sections.

TS1001

The TS1001 Touch Screen RAS has a graphical touch screen to simplify navigation, reduce the number of button presses required, and facilitate text entry. It also has a Classic mode that mimics a conventional LCD keypad. Refer to the *TS1001 Touch Screen Arming Station User Manual* for details.

CA111x-series

Use the up and down arrow keys to move backwards and forwards through a record's options. For example, if you are programming an input you can back up to an option if you go past it. Also, you can move backwards instantly from the first option to the last option.

Use the left and right arrow keys to move backwards and forwards between records (such as inputs) for the same field. For example, you can enter a name for input 1, press [ENTER] to save, and then press the right arrow key to enter a name for input 2, and so on. When going backwards between records you can press the left arrow button to move immediately from the first record to the last record.

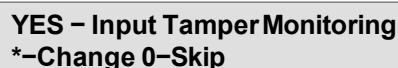
TS0801

Use the up and down arrow keys (ON and OFF keys) to move backwards and forwards through a record's options. For example, if you are programming an input you can back up to an option if you go past it. Also, you can move backwards instantly from the first option to the last option.

The LCD screen

The LCD screen (or touch screen) on the RAS has at least two lines of characters. Each line contains a different type of information.

Figure 1: Sample LCD message to toggle a value



YES – Input Tamper Monitoring
*–Change 0–Skip

For example, the top line in [Figure 1 above](#) contains system information, and the bottom line contains the instructions and characters you can enter on the keypad. For this example, you could:

- Press * to toggle the YES/NO value, and then press [ENTER] when correct.
- Press [0] to skip this option.

Figure 2: Sample LCD message to enter a value



2: Type 1, Access Alarm
Type:

For example:

- The top line in Figure 2 above identifies the item being programmed (in this example, input 2) followed by its currently programmed value.
- The bottom line describes what's being programmed (in this example, input type) followed by the characters (if any) that you entered on the keypad.

Programming the options

In this document, “enter” is used in the following ways:

- Press the key (or sequence of keys) on the RAS keypad that corresponds with the required value. For example, press the [0] key to ‘enter’ the value 0.
- Press the [ENTER] key on the RAS keypad to accept the value that you entered (or to accept the value displayed on the LCD).

To program a YES/NO option ([Figure 1 on page 14](#)), press [ENTER] to accept the displayed value or press [MENU*] to toggle between YES and NO. Press [0] to skip options.

To program a value such as a number or amount (Figure 2 above) enter the value, and then press [ENTER]. The information will be saved and the display will show the next option.

Note: If a value is already programmed and needs to be changed, enter the new value (or toggle, if applicable), and then press [ENTER] to change the value.

Selecting areas by searching

Areas are identified by a number and (optionally) a name programmed by the installer.

When arming or disarming the system, you may want to select a specific area instead of selecting all areas. Some RAS models (such as the CA111x series) allow you to quickly find areas by name.

For example to use a CA1116 RAS to arm an area named “East wing foyer”:

- 1 Press nnnn (where nnnn is your code), and then press [ENTER] or [ON]. Any disarmed areas that are assigned to your alarm group are listed.
- 2 Press the multi-function key to begin (on the CA1116 RAS the multi-function key is the left-hand “—” key).

Area Search is ,(*)-End

- 3 Use the RAS keypad to enter a search character or string. When each character is displayed, press [ENTER] to move to the next position. When finished, press [*] to list all areas that contain the string.

For example, search for “EAST” to find all with area names beginning with that text (including “East wing foyer”). Search is not case-sensitive.

- 4 When the list of areas displays, you can press the area number and then press [ENTER] to arm only that area. Alternatively, press [0] [ENTER] to arm all of the found areas.

- 5 When finished arming areas, press [ENTER] to exit the display.

Refer to Table 5 on page 54 or [“Programming text via RAS”](#) in the *Discovery Administrators Manual* for details.

Programming sequence

Program the system in the order listed in [“Setting up a basic alarm system”](#) on page 19. All remaining Install menu options may be programmed in any order to suit individual installations.

Default installer PIN

Changing the default installer PIN

The default panel programming includes PIN 4346 for user 50. The default PIN must be changed to keep unauthorised persons from modifying your programming or using the system without authorisation.

To change the default installer PIN:

- 1 From the User menu prompt, press [2] [5] [ENTER] to change PIN for the master user
- 2 Enter the old code.
- 3 Enter the new code.
- 4 Re-Enter the new code.
- 5 Press Enter

Note: Unlike previous versions of Challenger panels, you can't actually delete user 50 from the panel (however, user 50 can be deleted from management software). When you 'delete' user 50 from the panel, the user record is voided and not deleted. Doing so can create a user tally that differs between the panel and management software.

Restoring the default installer PIN

If the installer PIN for user 50 has been changed and lost, you may need to reset the PIN to default (4346). This is easily accomplished via management software. However, if necessary, it can be done from the Discovery panel reset button.

Note: This also defaults area group 1 back to areas 1 to 99, and defaults RAS 1 on COMM 1.

To restore the default installer PIN:

- 1 Unseal the tamper switch.
- 2 Press and hold the reset button on the back of the module. Holding the reset button momentarily (0.5 – 2 seconds) will perform a default on the installer PIN and user.

Note: If another user in the system has a PIN of 4346 or 4347, the installer PIN will not be reset.

Chapter 4

Common tasks

Summary

This chapter provides an overview of the programming needed to perform various tasks within the Discovery system. Understanding these tasks helps you to understand how various panel programming concepts are related to each other.

Content

Setting up a basic alarm system	19
Programming relays	24
Connecting to a printer.....	27
Connecting to software.....	29
Programming arming stations.....	29
Alarm control with key switches	33
Camera control and monitoring	34
Programming delayed holdup inputs	37
Programming automatic arming and disarming	38
Disarming and arming of common areas	41
Programming macros.....	42
Programming service technician access.....	47
Triggering console (RAS) beepers	48
Using keypad duress	48
Programming common areas	50
Using Area Search.....	50
Configuring IP connections.....	52
Using timed input testing	53
Programming text via RAS	54
Automation overview	55
Controlling automation zones via RAS	56
Programming twin trip inputs	58
Connecting via UltraSync	60

Setting up a basic alarm system

Overview

This section provides an overview of how to set up a basic alarm system that uses PINs for access control.

Use the following steps to set up a basic alarm system:

- 1 Plan the system and fill out the programming sheets. See [“Planning the system”](#) on page 8.
- 2 Disarm the system. See [“Disarming the system”](#) on page 13.
- 3 Access the Install menu. See [“Accessing the Install menu”](#) on page 13.
- 4 Default the system. See [“Reset to Defaults”](#) on page 13.
- 5 Disarm the system and access the Install menu again, as described above.
- 6 Program the date and time in User menu option 15, Time and Date.
- 7 Optional: Change the default installer PIN. See [“Default installer PIN”](#) on page 16.
- 8 Program the required system options if the default values are not suitable (see [“System option defaults”](#) on page 22). The only options you need to consider for a basic alarm system are as follows:
 - [“Test mode”](#) on page 165.
 - [“No. of Relay controllers”](#) on page 105.
 - [“Input tamper monitoring”](#) on page 209.
 - [“Display one input at a time”](#) on page 113.
 - [“Name file”](#) on page 22.
 - [“System alarms set siren and strobe”](#) on page 111.
 - [“Reset System alarms”](#) on page 94.
 - [“Disable code from displaying”](#) on page 115.
 - [“Disable flashing area LEDs”](#) on page 113.
 - [“Display alarms instantly on LCD”](#) on page 113.
 - [“Sirens only after report fail”](#) on page 111.
- 1 Program time zones using [“Time zones”](#) on page 144.
- 2 Program holidays in User menu Holidays.
- 3 Program areas using [“Area database”](#) on page 71.
- 4 Program alarm groups using [“Alarm group”](#) on page 90.

- 5 If your system requires more than 16 inputs, or requires advanced access control functionality, then you will need to program DGPs (data gathering panels) into the system. Program DGPs using “[DGP database](#)” on page 87.
- 6 Program inputs using “[Input database](#)” on page 64.
- 7 If your system requires more than one arming station, then you will need to program RASs. The only options you need to consider for a basic alarm system are as follows:
 - “RAS model

Select the RAS model attached to the Discovery panel. This will allow certain options in the panel to be configured to ensure optimal communications.

1:RASModel is:
Model No:

The model may be selected from a pre-defined list, as detailed in Table 8 below.

Table 8: RAS models summary

RAS model	LCD	Keypad	Card Reader	LEDs
TS0003		Yes		4
TS0004	Yes	Yes		16
TS0006		Yes		4
TS0801	Yes	Yes		8
TS0804	Yes	Yes		16
TS0862			Yes	2
CA1110	Yes	Yes		16
CA1111	Yes	Yes		16
CA1115	Yes	Yes	Yes	16
CA1116	Yes	Yes	Yes	16
TS0870			Yes	2
TS0870H			Yes	2
TS0870D			Yes	2
TS1001	Yes	Yes		8
TS1162		Yes		3

“Area alarm group” on page 85.

- “[Menu alarm group](#)” on page 81.
 - “[LCD arming station](#)” on page 79.
 - “[Toggle keyboard control](#)” on page 84.
- 1 Program the system’s timers if the default values are not suitable (see “[Timer defaults](#)” on page 22):

- “[User category time](#)” on page 101.
- “[Access test time](#)” on page 102.
- “[Secure test time](#)” on page 102.
- “[Warning time](#)” on page 156.
- “[Delay holdup time](#)” on page 102.
- “[Suspicion time](#)” on page 101.
- “[Service time](#)” on page 102.
- “[Local alarm reminder time](#)” on page 102.
- “[Individual input test time](#)” on page 102.
- “[Tester event flag time](#)” on page 102.
- “[Siren time set to](#)” on page 100.
- “[Mains fail time](#)” on page 102.

Program the communication options to enable the Discovery system to report alarms to the remote monitoring station. See “[Communications](#)” on page 124.

- 1 Program the behaviour of relays using “[Map relays](#)” on page 149.
- 2 Reset all poll error counters when the system is error-free.
Otherwise, errors that occurred during installation and programming could distort future error counts.
- 3 Program (at least) the first user. See “[Programming users](#)” on page 23.

Default programming values

The Discovery panel is supplied with a set of factory defaults in the programming to make initial set-up easier. The default settings are as follows.

Input defaults

- Input type is set to type 2 Secure Alarm (inputs 1 to 16 only)
- Report ID type is set to 25-140, General Alarm
- Assigned to area 1
- Siren event flag is selected
- Event flag 2 Secure Alarm is selected, and is mapped to relay 15 Strobe Output

Area defaults

- Areas 1 to 16 have names
- Exit time is set to 60 seconds

- Entry time is set to 30 seconds
- Siren event flag is set to 1

Area group default

- Area Group 1 (used by master installer, master user, and master RAS alarm groups) contains areas 1 to 99

Arming station defaults

- RAS 1 is polled
- RAS 1 is LCD arming station
- RAS 1 has LEDs 1 to 16 mapped to areas 1 to 16
- RAS 1 has Alarm Group 2 (Master RAS)

System option defaults

- Film Low is set to 800
- Film Out is set to 1100
- Relay Controllers is set to 0
- Input tamper monitoring is selected
- Display one input at a time is selected
- User name file is selected
- EOL Resistor Code is set to 0 (10K Ohm)
- Time zone is set to 0 (not used)
- Area search time zone is set to 0 (not used)
- External siren mode is set to 0 (standard 8 Ω siren speaker)
- Internal siren mode is set to 0 (standard 8 Ω siren speaker)

Timer defaults

- Each user category time is set to 0 minutes
- Access test time is set to 15 minutes
- Secure test time is set to 15 minutes
- Warning time is set to 5 minutes
- Delay holdup time is set to 60 seconds
- Suspicion time is set to 15 seconds
- Service time is set to 30 minutes
- Local alarm reminder time is set to 0 minutes

- Individual test mode time is set to 5 minutes
- Door/s unlock time is set to 5 seconds
- Tester event flag time is set to 15 seconds
- Siren time is set to 8 minutes
- Mains fail time is set to 0 minutes
- Card to code time is set to 8 seconds
- Minimum area search time is set to 0 minutes
- Maximum area search time is set to 0 minutes
- Maximum twin trip time is set to 60 seconds

Relay mapping defaults

- Relay 15 (panel strobe output) is mapped to event flag 2
- Relay 16 (panel siren driver) is mapped to event flag 1. The sixteenth relay assigned to each DGP (DGP siren drivers relay 32, 48, 64 and so on) is also mapped to event flag 1.

User defaults

- User 50, the master code is allocated:
 - Name TECOM Master
 - PIN 4346
 - Alarm Group 3 (containing Area Group 1)
 - Door Group 1
 - Floor Group 1

Programming users

The installer must initially program a user into the system who has the necessary authority to program additional users into their system.

It is important that the client is provided with details of the users' alarm groups to facilitate this. Use "[Alarm group worksheet](#)" on page 234 to list the alarm groups that the client will use when adding or changing users in their system.

Use the following steps to create a user or modify an existing user:

- 1 From the Discovery User menu (see "[User menu structure](#)" on page 11) select option 14. Program Users.
- 2 Select option 3. Create.
- 3 Select a user number to program.

Note: User number 50 is the Master Installer Code. The PIN for user 50 should be changed from the factory default of 4346, but no other parameter should be altered.

- 1 Assign an alarm group to the user to specify the areas and functions allowed. It is not necessary to assign a door group or a floor group for a basic alarm system using PINs for control. See [“Alarm group”](#) on page 90.
- 2 Program the user’s name (applies only to user numbers 1 to 2,000).
- 3 Program the user’s PIN.
- 4 If you want the user to be activated from a particular date, then program a start date and time.
- 5 If you want the user to be deactivated at a later date, then program an end date and time.

Note: When programming a new user record in User menu option 14. Program Users, a list of designated “user alarm groups” are displayed on the RAS for assigning to the new user. The list of designated “user alarm groups” depends on the alarm group (and alternate alarm group, if applicable) of the person doing the programming. You cannot assign an alarm group to a new user that has more permissions than you have.

Programming relays

This section provides an overview of how to program relays and outputs in the Discovery system.

Overview

Relays may be used for a variety of applications, including:

- Sirens (timed or untimed) and strobes.
- Door locks.
- Warning beepers and lamps.
- Activating cameras.
- Mimic LEDs or lamps for inputs, area and system status, system fault indication.
- Automatic testing of input devices (for example, seismic detectors).
- Interface to building management systems (lighting, heating, air conditioning, and so on).
- Activate backup communicators.
- Link functions together within the system (physical relay not required).

If open collector outputs are required for any of these applications (for example, mimic LED panels), a 16-way open collector card is available. For programming purposes, each open collector output is treated as a relay.

Programming steps

- 1 Note the type and quantity of relay cards used and which unit (panel

or DGP), the relay cards are connected to.

- 2 Configure the panel or DGP as required to use the relay cards.
 - To configure the panel, refer to “[No. of Relay controllers](#)” on page 105.
 - To configure a Network Access Controller DGP, refer to the Network Access Controller Programming Manual for details of programming the relay controllers option.
 - For DGPs TS1020, TS0820, or TS0824, set the DIP switch segment 6 to ON if a TS1041, TS0841, or TS0842 relay controller is connected to J8 or J9, or OFF if a TS0840 4-Way Relay Card is connected.
- 1 Determine the number of relays you wish to program. The relay numbers allocated for the panel and each DGP address are listed in [Table 25](#) on page 204.
- 2 Use the 16 predefined event flags ([Table 30](#) on page 223) or program user-defined event flags to activate your relays.
- 3 Determine or program any ‘hard’ time zones that may be required to control your relays (a relay can be programmed to be held active or inactive during a time zone). Time zones are programmed in “[Time zones](#)” on page 144.
- 4 Program the details for each of the relays in your system, in “[Map relays](#)” on page 147.

Example

The “Mulgrave” site has two 8-way relay cards (TS1041) connected to the Discovery panel number 1.

Normal business hours are 8:00 am to 5:30 pm Monday to Friday, and 8:00 am to 12:30 pm Saturday.

Relay 5 is required to interface to a lighting system to automatically turn the lighting on during normal business hours or if the building security is turned off (Area 1 in access).

The relevant programming details in “[System options](#)” on page 103 is:

- Number of relay controllers is 2.

The relevant programming details in “[Area database](#)” on page 71 are:

- Area number is 1.
- Area Accessed Event Flag number is 17 (this is the first user-defined event flag).

The relevant time zone programming details are shown the worksheet example in [Figure 3](#) on page 26.

Figure 3: Time zones worksheet example

Site

Mulgrave

Discovery

1

Time zone no.

1

Time zone name

Lighting control time zone

Sub-time zones				Days							Holiday types												
		hh	mm			hh	mm		S	M	T	W	T	F	S	1	2	3	4	5	6	7	8
.1	Start	08	00	End	17	30			☒	☒	☒	☒	☒	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐
.2	Start	08	00	End	12	30			☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐
.3	Start			End					☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
.4	Start			End					☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
.5	Start			End					☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
.6	Start			End					☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
.7	Start			End					☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
.8	Start			End					☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Mark check boxes to indicate YES ☒

The relevant programming details in “[Map relays](#)” on page 147 are:

- Relay number is 5.
- Event Flag number is 17.
- Time zone number is 1.
- Active during time zone.
- Non-inverted.

In addition, you might want to record the relay’s application such as “lighting control” on the “[Relay mapping worksheet](#)” on page 247. This detail is for future reference only and is not programmed into the system.

Figure 4 below is an example of a worksheet detail for this example of relay mapping.

Figure 4: Relay mapping worksheet example

Site

Mulgrave

Discovery

1

Relay no.

10

Application

Lighting control

Event flag

17

Time zone

1

☐ Inactive during time zone

☐ Relay inverted

Mark check boxes to indicate YES ☒

Connecting to a printer

The Discovery panel's printer output may be used for:

- Printing events on a printer (such as Epson-compatible dot matrix or HP IIP-compatible laser printer) connected by a serial cable to the Discovery panel's Serial (STU) terminals. See "Printer output via RS-232" below.
- Sending events to a computer via IP connection to the Discovery panel's Ethernet port. See "[Printer output via IP](#)" on page 28.

Printer output via RS-232

Use the following steps to print from a printer (such as Epson-compatible dot matrix or HP IIP-compatible laser printer) connected to the Discovery panel's onboard RS-232 STU port (Serial).

You will need to obtain or make a cable to connect the Serial terminals to your printer.

Refer to your printer documentation to determine the settings you will need to program in the Discovery panel.

For Epson printers the range of parameters includes:

- Baud: 9600
- Data bits: 8 (not configurable in Discovery)
- Parity: None, Odd, or Even
- Stop bits: 1

For HP IIP printers the range of parameters includes:

- Baud: 9600 or 19200
- Data bits: 8 (not configurable in Discovery)
- Parity: None
- Stop bits: 1

To connect a printer via RS-232:

- 1 Connect the printer to the Discovery panel's onboard RS-232 STU port (Serial).
- 2 Program a time zone if you require the printer to be enabled or disabled during specific time periods (see "[Time zones](#)" on page 146). Time zone 0 is valid 24 hours every day. It may be used wherever a 24-hour time zone is required.
- 3 From Install menu option 1 Communications, select option 1 Setup, to access the Setup menu.
- 4 From the Setup menu, select option 1 Onboard to configure the

onboard serial port.

- 5 Program the baud, parity, and stop bits to suit your printer.
- 6 Create new comm path record for the printer (for example, path 4 because paths 3, and 8 are set up for reporting by default).
- 7 Press Enter to display the first item in the path menu.
- 8 Select option 1 Main, and then program the format "Printer", program the sub- format to suit your printer, and then select Enable.

Printer output via IP

You can send the Discovery panel's printer data via IP to a computer. The data can be used in third-party applications, such as Nurse Call systems.

Note: Events such as alarms are not acknowledged. The Discovery panel cannot resend events that are not received.

To send printer output via IP:

- 1 Connect the Discovery panel's onboard Ethernet port to the network.
- 2 Program a time zone if you require the printer to be enabled or disabled during specific time periods (see "[Time zones](#)" on page 146). Time zone 0 is valid 24 hours every day. It may be used wherever a 24-hour time zone is required.
- 3 From Install menu option 1 Communications, select option 1 Setup, to access the Setup menu.
- 4 From the Setup menu, select option 1 Onboard to configure the onboard Ethernet port.
- 5 Enable the Ethernet option and program other IP-related options as required.
- 6 Select option 2 Paths, and then create a new (unused) communications path record for the printer (for example, path 4 because paths 1, 2, and 3 are set up for reporting by default).
- 7 Press Enter to display the first item in the path menu.
- 8 Select option 1 Main, and then program the format "Printer", program the sub- format to suit your requirements (typically None), and then select Enable.
- 9 Select option 2 Path Connection Control, and then change the Always Connect option to Yes.
- 10 Select option 6 Path IP Address, and then program the Send to IP address (the IP address of the computer to which you want to send the printer data).
- 11 Program the Send IP Port number (for example, 3001) that will be used for sending data to other devices.

12 Select UDP/IP for the IP mode.

Connecting to software

Discovery panels may connect to computers running management software such as CTPlus or WMS Pro.

Ten communication paths are available for simultaneous management software connections, reporting via UltraSync, printing events, and so on.

Connection options include:

- Ethernet connection via the Discovery panel's Ethernet port
- UltraSync connection via Ethernet

Refer to "Enabling communications" in *Discovery Installation and Quick Programming Manual* for details.

Programming arming stations

This section provides an overview of programming requirements for keypads and card readers.

Introduction

Remote arming stations (RASs) have LEDs to indicate area and system status. The number of area LEDs determines the RAS's suitability for controlling a single area or multiple areas.

The areas that the RAS can control are determined by the area alarm group assigned to the RAS. RASs with 2, 3, or 4 LEDs are suitable for single-area alarm groups (for example, alarm groups 14 to 29). RASs with 8 or 16 LEDs are suitable for multi-area alarm groups because each LED can correspond to an area. Any area LED can be mapped to any of Discovery's 99 areas.

Refer to [Table 8](#) on page 80 for a list of common RASs and related features.

Keypad arming stations

Keypad RASs are used to enter data into the Discovery system. RASs that have only a keypad can be used only for entering a PIN and performing basic alarm control and access control functions. RASs that have a keypad plus LCD, or a touch screen, are used to program the Discovery system.

Use the following steps to program a keypad RAS.

- 1 Determine how the RAS is to be used in the system and fill out the appropriate programming sheets.
- 2 Optionally, specify the alarm code prefix value (see "[Number of prefix](#)" on page 106). The alarm prefix allows a PIN of 5 digits or more to be used for the alarm control functions and a shorter code (minimum 4 digits) to be used just for door access.

- 3 Program any time zones that may be required in order to limit the alarm or access control functions of the RAS to specific time periods. See "[Time zones](#)" on page 146.
- 4 Determine whether an existing alarm group is suitable for the RAS. Program a new alarm group if necessary in "[Alarm group](#)" on page 90.
 - If the RAS does not have an LCD, the alarm group's User menu options do not apply.
 - If alarm control is needed, the alarm group must have Alarm System Control enabled, plus any other options, as required.
- 5 Program the RAS's specific details in "[RAS database](#)" on page 158 including the following:
 - Area alarm group. The area alarm group defines the areas, alarm control and User menu options available at this RAS.
 - Menu alarm group. The menu alarm group specifies User menu options available if requirements are different from those specified in the area alarm group.
 - Door event flag. If the RAS is to activate a relay to unlock a door, then a door event flag number must be entered. Enter any event flag number that is not used elsewhere in the system. If you know the number of the relay that is to be used to unlock the door, you may choose to make the event flag number the same.
 - Relay number. If the open collector output on the RAS is to be used to activate a warning buzzer, relay, and so on, then a relay number must be assigned to the RAS.
 - Other options appropriate to the RAS and its application. See "[RAS programming options](#)" on page 78.
- 6 Program door groups to specify which doors (RASs) a user may access. Door groups are programmed in User menu option 20.
- 7 If the RAS is activating a relay to unlock a door:
 - Program the door's unlock time in "[Timers](#)" on page 101. The default is 5 seconds.
 - Determine the relay number to use. See "[Relay and output numbering](#)" on page 205 for details.
 - Program the details in "[Map relays](#)" on page 147.
- 1 If an input is required to be shunted (disabled) for a period of time when the door access function is performed at the RAS, program shunt options in "[Input shunts](#)" on page 153.
- 2 Ensure that any users who are to perform any access control functions with the RAS have an appropriate door group assigned to them. See "[Programming users](#)" on page 23.

Card reader arming stations

RASs that have card readers or magnetic swipe readers may also have keypads and LCDs. Refer to “[Keypad arming stations](#)” on page 29 for details of programming RASs with a combination of features.

This section describes how to program RAS that have a card reader or magnetic swipe reader (and two LEDs). Such RASs will be called ‘readers’ in this section. Readers are programmed as RASs, and can be used to perform alarm control functions and/or to access a door.

Use the following steps to program a reader.

- 1 Determine how the reader is to be used in the system and fill out the appropriate programming sheets.
 - 2 Program any time zones that may be required in order to limit the alarm or access control functions of the reader to specific time periods. See “[Time zones](#)” on page 146
 - 3 Determine whether an existing alarm group is suitable for the reader. Program a new alarm group if necessary in “[Alarm group](#)” on page 90.
 - If the card reader does not have an LCD, it can't display menus. However, we recommend that the alarm group that is used as the RAS's area alarm group is also used as the menu alarm group.
 - If alarm control is needed, the alarm group must have Alarm System Control enabled, plus any other options, as required.
 - 4 Program the reader's specific details in “[RAS database](#)” on page 158, including the following:
 - Area alarm group. The area alarm group defines the area, alarm control and User menu options available at this reader.
 - Menu alarm group. If the card reader does not have an LCD, it can't display menus. However, we recommend that the alarm group that is used as the RAS's area alarm group is also used as the menu alarm group.
 - Door event flag. If the reader is to activate a relay to unlock a door, then a door event flag number must be entered. Enter any event flag number that is not used elsewhere in the system. If you know the number of the relay that is to be used to unlock the door, you may choose to make the event flag number the same.
 - Relay number. If the open collector output on the reader is to be used to activate a warning buzzer, relay, and so on, then a relay number must be assigned to the reader.
 - Other options appropriate to the reader and its application. See “[RAS programming options](#)” on page 78 and “Using card readers for alarm control” below.
- 1 Program door groups to specify which doors (readers) a user may

access. Door groups are programmed in User menu option 20.

- 2 If the reader is activating a relay to unlock a door:
 - Program the door's unlock time in "[Timers](#)" on page 101. The default is 5 seconds.
 - Determine the relay number to use. See [Table 25](#) on page 204 for details.
 - Program the details in "[Map relays](#)" on page 147.
- 1 If the open collector output on the magnetic card reader or the "LO" open collector output on the Wiegand interface are to be used to activate a relay for the lock, refer to ("[Relay and output numbering](#)" on page 205) for details.
- 2 If an input is required to be shunted (disabled) for a period of time when the door access function is performed at the reader, program shunt options in "[Input shunts](#)" on page 153.
- 3 Ensure that any users who are to perform any access control functions with the reader have an appropriate door group assigned to them. See "[Programming users](#)" on page 23.

Using card readers for alarm control

"[RAS programming options](#)" on page 78 provide a variety of ways to control the alarm system, depending on the options that are available on the reader. This section describes reader behaviour when various RAS programming options are enabled.

Toggle keyboard control: The [ON] and [OFF] keys lose their function. For arm control the user must present their card followed by [ON], [OFF], or [ENTER]. If a list of areas appears, pressing the area number and [ENTER] toggles the status of the area. If no list appears, the status of the areas is toggled immediately.

Card auto disarms: If the reader has buttons, then the user can arm by presenting the card and pressing the [ON] key. The user can disarm by presenting the card.

Card always disarms/arms and Toggle keyboard control: The user can arm and disarm by presenting the card.

Cards arm after three badges: The user can arm by presenting the card three times within 10 seconds.

Alarm control with key switches

This section provides an overview of the programming steps to enable alarm system control functions to be performed with key switches or other devices wired to a Discovery system input, such as:

- Output contacts from a remote control receiver.
- Output contacts from another security system.
- Push button switch for quick arming on exit (programmed to allow arm

but not disarm).

Use the following steps to use an input for alarm control.

- 1 Plan the system and fill out the programming sheets. See "[Planning the system`](#)" on page 8.
- 2 Access the Install menu. See "[Accessing the Install menu](#)" on page 13.
- 3 Program any time zones that may be required in order to limit the alarm control functions of the control input to specific time periods. See "[Time zones](#)" on page 146.
- 4 Determine whether an existing alarm group is suitable for the control input. Program a new alarm group if necessary in "[Alarm group](#)" on page 90.
 - The alarm group will define the areas and alarm control functions available to the key switch or other device connected to a Discovery input.
 - The special input types used for this purpose require an alarm group to be assigned instead of areas. Alarm groups 11 to 13 are assigned Area Group 1 and may be suitable for key switches, and so on, if all areas in Area Group 1 are to be controlled. Alarm groups 14 to 29 are intended for devices that control a single area.
 - User alarm group option is set to no. Alarm system control option is set to yes.
 - Program other alarm group options as required.
- 1 Program the input in "[Input database](#)" on page 63.
- 2 Determine the number of the input you wish to program. The input numbers allocated for the panel and each DGP address are listed in [Table 25](#) on page 204.
- 3 Program a suitably descriptive input name.
- 4 Select one of the "Area Control" input types to suit the purpose of the input (see "[Input types](#)" on page 208). For example:
 - Type 6 "Area Control Input - Momentary" for momentary (spring return) key switches, and so on.
 - Type 31 "Area Control Input - Latching: for latching key switches, and so on.
- 5 Program the input's alarm group.

Camera control and monitoring

This section provides an overview of the programming steps to control and monitor security cameras and CCTV systems.

Overview

The Discovery system provides the following facilities:

- Eight input types are available for camera frame counting, and eight input types are available for film out reporting (see [“Input types”](#) on page 208).
- Camera testing is available utilizing the frame counting feature.
- Special input types are available for suspicion buttons with a timing feature (see [“Input types”](#) on page 208).
- The installer can specify which inputs will activate cameras.
- Cameras can also be activated or inhibited via time zones.
- Cameras can be programmed to be activated or inhibited by virtually any event in the system, such as keypad duress, DGP offline, report fail, and so on.
- Camera event flags to activate relays are programmed for each individual area in the system, i.e. inputs can trigger cameras in a single area or in multiple areas.
- Film out is reported to the remote monitoring station in all reporting formats (some formats also report film low).

Programming steps

Use the following steps to control and monitor security cameras.

- 1 Plan the system and fill out the programming sheets. See [“Planning the system”](#) on page 8.
- 2 Access the Install menu. See [“Accessing the Install menu”](#) on page 13. Program the required system options. The options you need to consider for cameras are as follows:
 - [“Film low”](#) on page 103. Enter a value greater than 0, even if frame counting is not used.
 - [“Film out”](#) on page 165. Enter a value greater than 0, even if frame counting is not used.
 - [“Test mode”](#) on page 165. Camera testing facilities are available, which utilize the frame counting feature. To provide automatic camera testing when area 1 is disarmed, select system test option 1 or 3 incorporating the access test.
 - [“No. of Relay controllers”](#) on page 105.

- [Disable 0 \[ENTER\] for camera reset](#)” on page 112. Set this option to YES if cameras are required to continue operating until the alarm is reset with a PIN.
 - [“Financial options”](#) on page 110. Set this option to YES to enable film counts to be displayed as part of camera testing during access test. (Setting this option to YES will also increase the minimum PIN length to 5 digits when programming users).
- 3 Program any time zones that may be required in order to limit the functions of particular users or arming stations to specific time periods via their alarm groups or to control relays. See [“Time zones”](#) on page 146.
 - 4 Specify the Camera Event Flag number in the area database for the areas in the system where cameras will be used. See [“Area database”](#) on page 71. Scroll through the options to locate the Camera Event Flag record.
 - The Camera Event Flag is activated when an input that has the area assigned to it, and the option Camera Event Flag set to YES on the input database, is in alarm.
 - Program an event flag. For convenience you may wish to use the same number as the relay number that will activate the camera.
 - 5 Determine whether an existing alarm group is suitable for camera control or testing. Program a new alarm group if necessary in [“Alarm group”](#) on page 90. Ensure that the required menu options are available to the user:
 - Option 5. History
 - Option 6. Test Report
 - Option 8. Film counters
 - Option 13. Start Auto Access Test
 - Option 18. Reset Cameras
 - 6 Program the input in [“Input database”](#) on page 63. Inputs can be programmed to provide any of the special input facilities for cameras; or as alarm inputs that will activate the cameras.
 - 7 Determine the number of the input you wish to program. The input numbers allocated for the panel or DGPs are listed in [Table 25](#) on page 204.

Note: Camera frame count inputs can only be connected to the Discovery panel (inputs 1 to 16).

- 8 Program a suitably descriptive input name.
- 9 Select one of the input types suited to cameras (see [“Input types”](#) on page 196). For example:
 - Type 1 (access alarm) may be used for a holdup button.

- Type 2 (secure alarm) may be used for motion detector.
 - Type 7 (camera suspicion) input may be used for a camera suspicion button.
 - Type 8 (delayed access/secure alarm) may be used for a hold-up button on a counter where more than one hold-up button is used.
 - Type 9 (reset delayed input) may be used for reset button for quick cancellation of alarm. This input type stops the cameras from operating if the input is unsealed, but the delayed time continues to run. It is used to reset delayed input types 8, 11, 22, and 40.
 - Types 48 to 55 are used to generate a film out alarm.
 - Types 23 to 26 and 36 to 39 are used to increment the camera's frame count.
- 10 Program the input's areas. The camera input must have at least one area assigned. If the input is programmed to activate cameras, only cameras in the areas assigned to the input will be activated.
 - 11 If you need to test the camera, set the input's test type to 0 (see "Test option" on page 71).
 - 12 If you need the input to activate the siren, strobe, or camera outputs, or if you need the input to activate a relay, then you must assign the appropriate event flags to the input. Set the camera event to YES to enable the input to activate the event flag number specified in the area database for the areas assigned to the input (see "Programming input event flags").
 - 13 Program the relevant timers (see "[Timers](#)" on page 100). In particular, the suspicion time that cameras continue to operate after a suspicion type input (7, 40, and 47) is resealed.
 - 14 If an output is required for a buzzer, lamp, and so on, to indicate the "film out" condition, program the film out event flag (see "[Program summary event flags](#)" on page 163).
 - 15 Determine the number of the relays you wish to program. The relay numbers allocated for the panel or DGPs are listed in [Table 25](#) on page 204.
 - 16 Program the details for each of the relays in your system that will be used to activate cameras (see "[Map relays](#)" on page 147)

Programming delayed holdup inputs

This section provides an overview of the programming steps to use the delayed holdup input facilities.

The delayed holdup input types provide a feature which allows holdup or duress type inputs to be activated and generate an alarm locally (activating cameras and other outputs if required), but not report to the remote monitoring station until after

a pre-programmed delay has expired. This provides personnel on site the opportunity to rectify the cause and/or reset the alarm if it was activated accidentally or by a faulty input device before it is reported. If more than one delayed holdup input type is activated, the system will report the alarm instantly.

Use the following steps to program a delayed holdup alarm input type.

1. Determine the holdup button requirements and fill out the programming sheets. See "[Planning the system](#)" on page 8.
2. Access the Install menu. See "[Accessing the Install menu](#)" on page 13.
3. Program the required system options. The options you need to consider for delayed holdup are as follows:
 - "[No. of Relay controllers](#)" on page 105.
 - "[Financial options](#)" on page 111.
4. Specify the Pre-Alarm Timer Event Flag number in the area database for the areas in the system where delayed holdup input types will be used. See "[Area database](#)" on page 71. Scroll through the options to locate the Pre-Alarm Timer Event Flag record.
 - The Pre-Alarm Timer Event Flag is activated when a delayed holdup input that has the area assigned to it is unsealed. The Event Flag is activated for the delayed period.
 - Program an event flag. For convenience you may wish to use the same number as the relay number that will activate the camera.
 - The Pre-Alarm Timer Event Flag may be used to activate a relay to provide discreet visual indication via a LED, and so on, that the delayed holdup button is active.
5. Program the input in "[Input database](#)" on page 63.
6. Determine the number of the input you wish to program. The input numbers allocated for the panel and each DGP address are listed in [Table 25](#) on page 204.
7. Program a suitably descriptive input name.
8. Select an appropriate input type to suit the purpose of the input (see "[Input types](#)" on page 208). For example:
 - Type 8, "Delayed access/secure alarm" (holdup button)
 - Type 9, "Reset delayed inputs" (button for quick reset & to stop cameras)
 - Type 11, "Delayed access alarm" (holdup button)
 - Type 22, "Delayed access non-latching/secure alarm" (holdup button)
 - Type 40, "Suspicion or delayed access/secure alarm" (special combined suspicion/holdup button)
9. If the system is going to report to the Remote Monitoring Station

using the Contact ID format, then it is necessary to program a report type for the input. The default type is “140 General Alarm” (sub-class General Alarm).

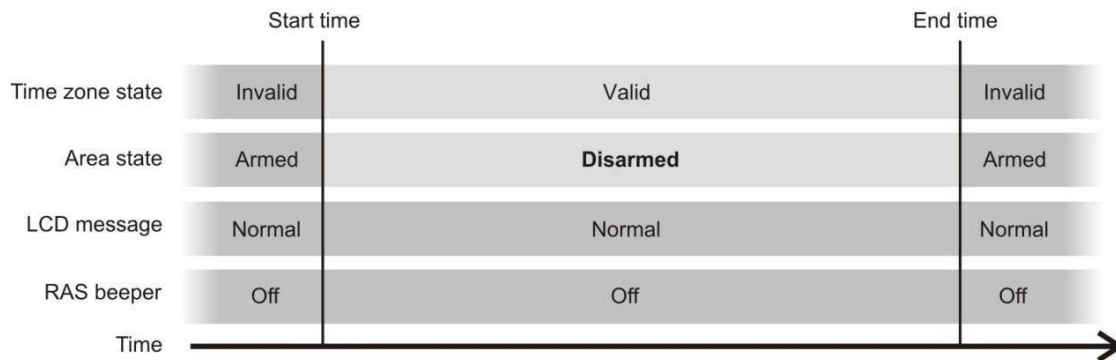
10. Assign an area or area group to the input that must alarm when the input is unsealed and the area status (secured or in access) meets the requirement for the input type.
 - At least one area must be assigned to an input.
 - Where there is more than one area assigned (via an area group), the input is regarded as being in access if one or more of the areas assigned is disarmed, and in secure only if all the areas assigned are armed.
11. If you selected one of the test options when programming the system options, or if the user wishes to use the access test option in the User menu, then you may need to program a test type for certain inputs. Refer to “Test option” on page 71 for details.
12. If you require the input to activate the siren, strobe, or camera outputs, or if you require the input to activate a relay, and so on, then it is necessary to assign the appropriate event flags to the input. Refer to “Programming input event flags” on page 72.
13. Program timers. The relevant timers for delayed holdup are as follows:
 - “Delay holdup time” on page 98.
 - “[Suspicion time](#)” on page 101.
14. Determine the number of the relays you wish to program. The relay numbers allocated for the panel and each DGP address are listed in [Table 25](#) on page 203.
15. Program the details for each of the relays in your system, in “[Map relays](#)” on page 147. Use the Pre-Alarm Timer Event Flag number that you recorded in the area database for the areas in the system where delayed holdup input types will be used.

Programming automatic arming and disarming

The Discovery system can automatically arm and disarm areas based on a time zone (time of day and day of the week). Time zones are effectively on-off switches (valid or invalid), so an alarm group is also used to define (among other things) the areas that are affected. The time zone and an alarm group are linked via an arm/disarm timer program (see “Arm/disarm via TZ” on page 166).

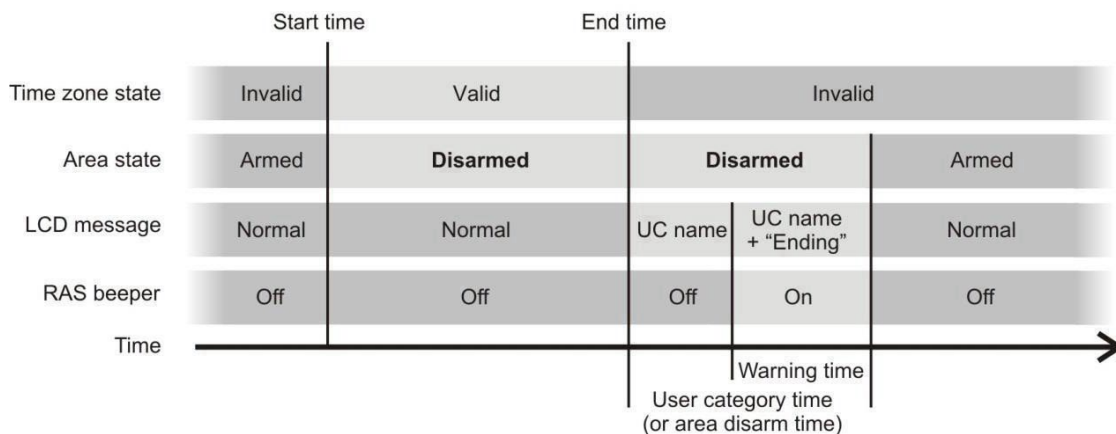
Figure 5 below depicts the effect of the time zone’s state on the area’s armed/disarmed state.

Figure 5: Example of simple arm/disarm timer functionality



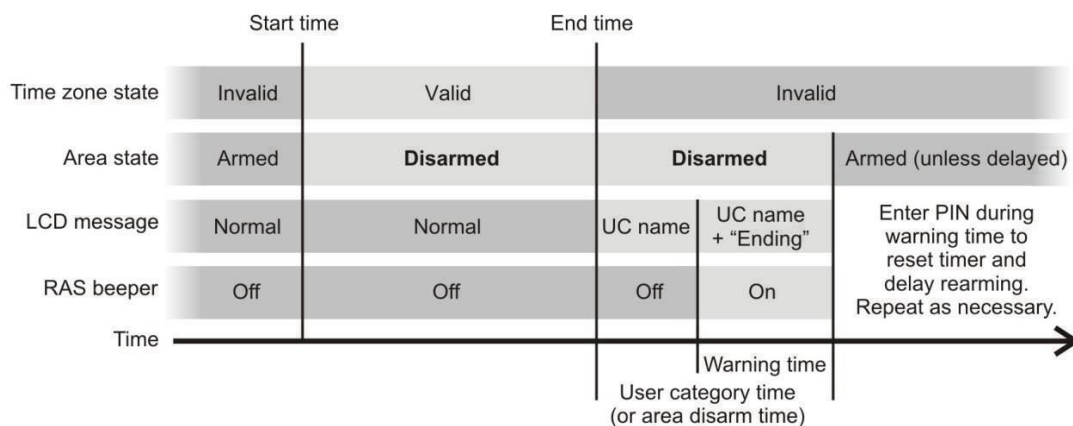
The alarm group can also be linked to a user category in order to provide a warning time, in which the RAS beeper (or other device) sounds to indicate imminent rearming (Figure 6 below).

Figure 6: Example of arm/disarm timer functionality where a user category provides a warning



Users who have the user category in their alarm group can badge or enter their PIN to delay the automatic rearming of areas after the time zone expires (Figure 7 below).

Figure 7: Example of arm/disarm timer functionality where a user can delay rearming



Use the following steps to program automatic arming and disarming.

- 1 Determine the automatic arming and disarming requirements and fill out the programming sheets. See [“Planning the system”](#) on page 8.
- 2 Access the Install menu. See [“Accessing the Install menu”](#) on page 13.
- 3 Program time zones that will specify the arm and/or disarm times. The time zone must specify both start and end times whether both are used or not. See [“Time zones”](#) on page 146.
 - The start time will be the time that the areas specified in the alarm group will disarm.
 - The end time will be the time that the areas specified in the alarm group will arm.
- 4 If a warning prior to arming is required, program a user category so that it can be linked to the alarm group.
- 5 The alarm group will define the areas and alarm control functions that will be performed when the time zone starts and/or ends. Program the alarm group’s alarm control functions for the area or the area group:
 - If an alarm group is linked to a single area, then the alarm group controls the area’s settings for arming, disarming, alarm reset, and timing (see [“Alarm groups”](#) on page 90).
 - If an alarm group is linked to an area group (one or more areas), then the area group controls each area’s settings for arming, disarming, alarm reset, and timing (see [“Area groups”](#) on page 170).
- 6 The following alarm group options may need to be enabled:
 - Reset system alarms—If [“System alarms”](#) on page 94 is enabled, then enabling this option will allow reset of those alarms.
 - Disable auto-deisolate—Enabling this option prevents the alarm group from being able to automatically de-isolate inputs in the areas they disarm.
 - Auto isolate unsealed inputs—Enabling this option allows unsealed inputs to auto-isolate when arming to prevent them causing alarms.
 - Forced arming when inputs unsealed—Enabling this option allows areas to arm regardless of any unsealed inputs which may subsequently cause an alarm.
 - Prevent forced disarming—Enabling this option prevents areas to be disarmed if there are unsealed inputs (access alarms).
- 7 Program the alarm group’s time zone to control when this alarm group is valid (the time zone programmed to specify the arm

and/or disarm times must not be used here).

- The “No Time zone” selection specifies the alarm group is always valid and is the typical setting for this application.
 - The time zone could be used in this application to specify particular automatic alarm control functions for a particular time period and then switch to the alarm control functions as specified in the alternate alarm group when the time zone is not valid.
 - If a time zone restriction has been specified for this alarm group, you may assign an alternate alarm group that will take effect when the time zone on this alarm group is not valid.
- 8 Program the arm and disarm timers in “Arm/disarm via TZ” on page 166.

Disarming and arming of common areas

This section provides an overview of how to enable a common area (or areas) to be disarmed and armed according to the status of other areas (for example, a common reception area in a medical suite shared by several practices will disarm when the first practice is disarmed and re-arms when the last practice is armed).

Use the following steps to program common areas.

- 1 Determine the areas to be considered common and which areas will control the common areas. Fill out the programming sheets. See “[Planning the system](#)” on page 8.
- A common area is an area that will be disarmed and armed automatically according to the status of other specified areas.
- A controlling area is individually armed and disarmed by the users, but will control the status of the common areas.
- 2 Access the Install menu. See “[Accessing the Install menu](#)” on page 13.
- 3 Program area linking in “[Area linking](#)” on page 151

Programming macros

Overview

A macro logic equation is a tool for activating inputs or event flags based on the conditions of one to four macro inputs (event flags or relays). The macro logic equation can combine macro inputs using AND or OR logic, based on the event flag’s or relay’s active or inactive (inverted) state. The output of the macro logic equation is an event flag or input.

This section provides an overview of how to program macro logic. See “[Program macro logic](#)” on page 166.

Use the following steps to program a macro logic equation.

- 1 Determine the macro logic requirements and fill out the programming sheets. See [“Planning the system”](#) on page 8.
- 2 Access the Install menu. See [“Accessing the Install menu”](#) on page 13.
- 3 Program or determine any event flags required for the macro logic equation. See [“Event flags”](#) on page 178.
- 4 Program or determine any relays required for the macro logic equation. See [“Programming relays”](#) on page 147.
- 5 Program the output of the macro logic equation:
 - If the output of the macro logic equation is an event flag, program the event flag. See [“Event flags”](#) on page 178.
 - If the output of the macro logic equation is an input, program the input. See [“Input database”](#) on page 63.
- 6 Program a macro logic equation using [“Program macro logic”](#) on page 166.

Example of macro logic programming

In the following example, we want to prevent door 1 from being unlocked via card reader while door 2 or door 3 is open (for example, airlock doors).

The system is configured in the following manner:

Contacts on doors 2 and 3 are wired to Discovery inputs 1 and 2.

- Discovery inputs 1 and 2 are programmed as input type 20 (Input to activate event flag 24-hour), and are programmed with event flag 17 as their selected event flag.
- The door 1 reader activates event flag 18 to unlock the door when a valid card is presented.
- The relay that activates the door 1 lock is relay 19 and is mapped to event flag 19.

The macro logic program can be used to ensure that event flag 19 does not activate to unlock the door unless the other two doors are closed.

The logic equation described in Figure 8 below states that event flag 19 will only activate to unlock door 1 if:

- Event flag 17, used for inputs 1 and 2, is inactive (inverted), indicating that neither door 2 nor door 3 are open), AND
- Event flag 18 is active (door event flag activated by valid card at reader).

Figure 8: Macro logic worksheet example

Site

Notting Hill

Discovery

1

Mark check box to indicate YES ☒

Macro number

1

Description

AIRLOCK DOOR CONTROL

Macro function:

Disabled

☐

On pulse

☐

Non-timed

☒

On timed

☐

Latched

☐

On delay

☐

Off delay

☐

Time

Seconds

☐

Minutes

☐

Macro output activates:

Event flag

☒

Number

19

Input

☐

Invert

☐

Macro output is generated subject to the following inputs:

Macro input 1

Event flag

☒

Number

17

Relay

☐

Invert

☒

and

☒

or

☐

Macro input 2

Event flag

☒

Number

18

Relay

☐

Invert

☐

and

☐

or

☒

Macro input 3

Event flag

☐

Number

Relay

☐

Invert

☐

and

☐

or

☒

Macro input 4

Event flag

☐

Number

Relay

☐

Invert

☐

Notes:

"Invert" indicates an inactive input or a deactivated output.

Macro input 4 resets the output for latched functionality. The and/or selection does not apply.

Examples of macro function selections

Macro output functions are listed in [Table 18](#) on page 168. The following sections further describe these options.

Nontimed

Nontimed output follows the result of the logic equation only. If an event flag or output for this macro changes, the logic equation will be calculated again.

Figure 10: Graphical representation of nontimed macro function

Time (Seconds)	Result of inputs (True/False)	Output (Active/Inactive)
0 - 10	True	Active
10 - 40	False	Inactive

On pulse

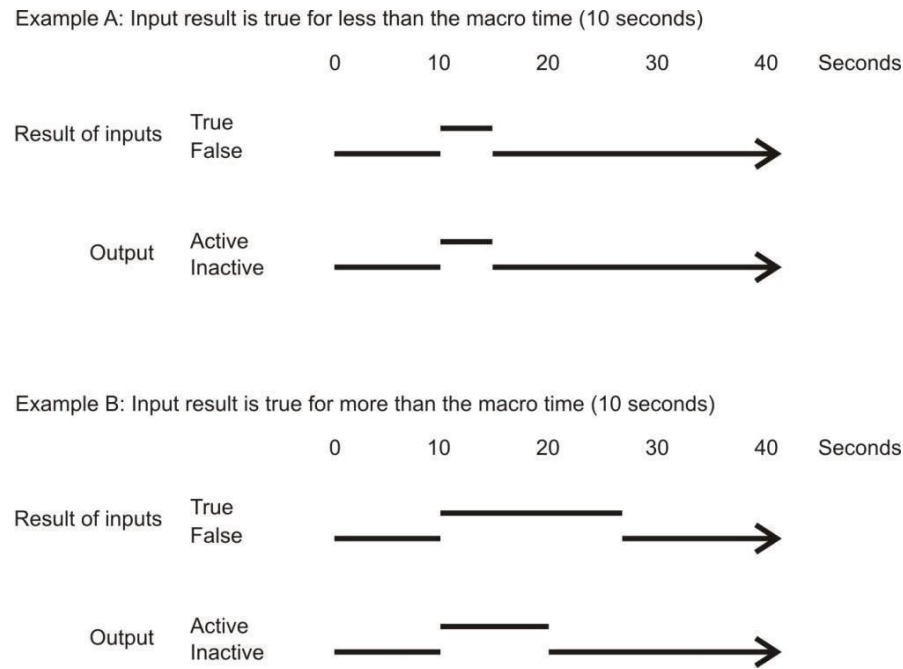
On pulse activates for the programmed time or the active period of the logic result,

MAPROG-TSX10000 TECOM Discovery Programming Manual

43

whichever is shortest (Figure 11 below).

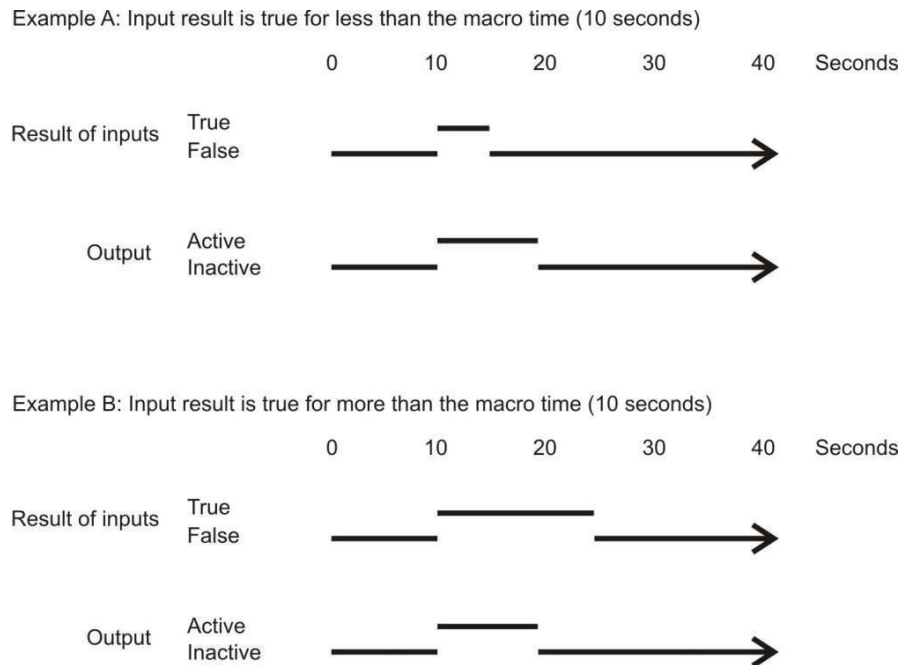
Figure 11: Graphical representation of on pulse macro function



On timed

On timed activates for the programmed time regardless of the macro output changing ([Figure 12](#) on page 45).

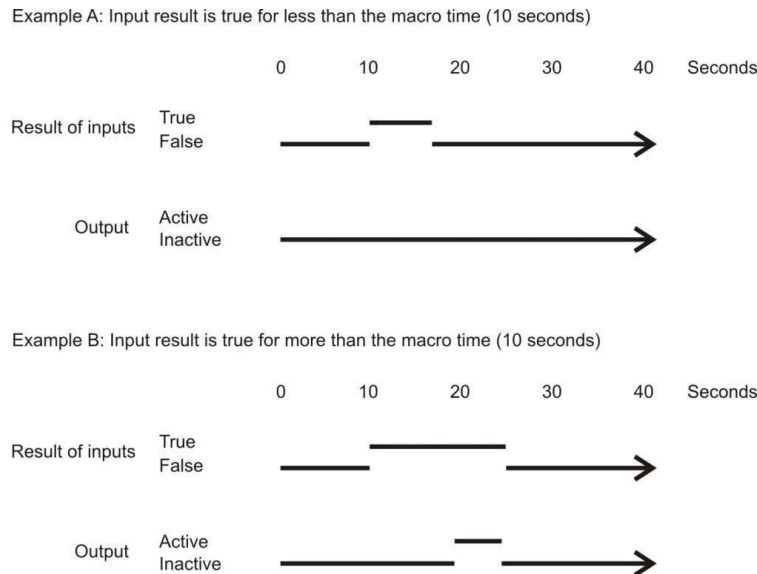
Figure 12: Graphical representation of on timed macro function



On delay

On delay activates after the programmed time unless the result of the logic equation is no longer valid (Figure 13 below).

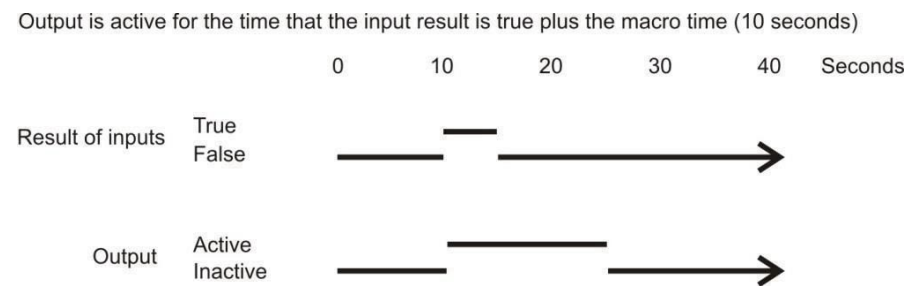
Figure 13: Graphical representation of on delay macro function



Off delay

Off delay follows the result of the logic equation, but remains active for the time programmed after the result of the logic equation is no longer active (Figure 14 below).

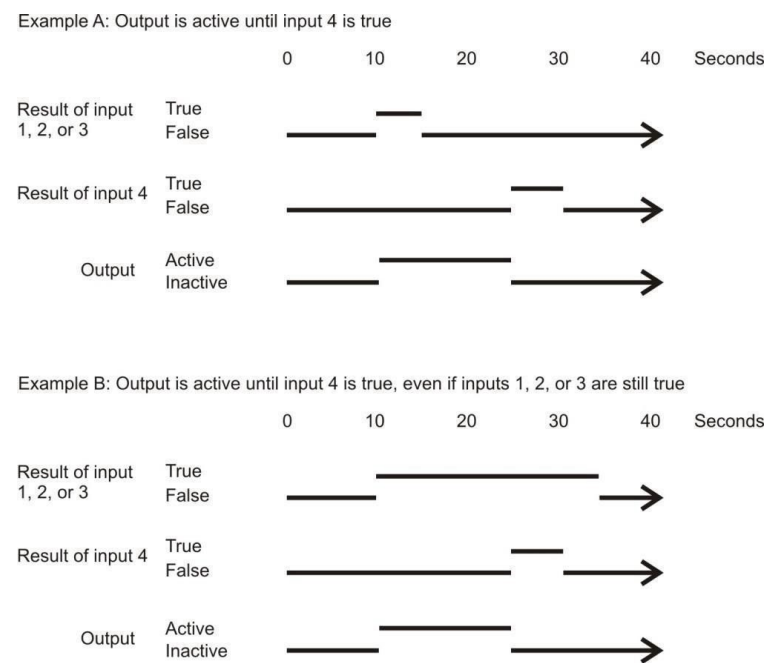
Figure 14: Graphical representation of off delay macro function



Latched

Latched activates on any of the first three macro inputs in the logic equation and is only reset by the fourth macro input. Any programmed AND / OR function is not used (Figure 15 below).

Figure 15: Graphical representation of latched macro function



Programming service technician access

This section provides an overview of the programming required to enable a service technician to access the system functions that they require via a PIN or card, when permitted by an authorised user.

The service technician's PIN or card is valid only when enabled by a user with the appropriate authority via User menu 17. Enable/Disable Service Technician. Once enabled, the service technician's PIN or card will remain valid until disabled by a user with the appropriate authority, or the programmed service time expires (see "[Timers](#)" on page 100).

Enabling the service technician activates the special time zone 25. Time zone 25 is used to enable the service technician's PIN or card, and can also be used to enable or disable any other system functions, relays, and so on, that are required while the service technician is in attendance.

Use the following steps to program service technician access.

- 1 Determine the service technician requirements and fill out the programming sheets. See "[Planning the system](#)" on page 8.
- 2 Access the Install menu. See "[Accessing the Install menu](#)" on page 13.
- 3 Ensure that a user (and a RAS) are assigned an alarm group that has access to User menu 17. Enable/Disable Service Technician in order to provide access for the service technician.
- 4 Program an alarm group suitable for the service technician (the alarm group must have time zone 25 assigned and must not have access to User menu 17. Enable/Disable Service Technician). Program a new alarm group if necessary in "[Alarm groups](#)" on page 90.
- 5 Program the service time (see "[Timers](#)" on page 100). When a user enables the service technician, time zone 25 will be valid until the service time expires or until User menu 17. Enable/Disable Service Technician is used to disable the service technician, whichever occurs first.
- 6 If any relays are required to be held active or inactive when time zone 25 is valid, program the requirements in "[Map relays](#)" on page 147 (you must know which relays are affected). Assign time zone 25 to the relays.
- 7 Program the user record that the service technician will use to access the system (as permitted by the alarm group). Refer to "[Programming users](#)" on page 23 for details.
- 8 Program the system to allow service technician access when the system is armed. See "[Skip access check for service tech](#)" on page 114.

Triggering console (RAS) beepers

This section provides an overview of the programming required to activate the keypad beeper on any RAS connected to the Discovery system LAN.

The keypad beeper is activated automatically when warning timers are running, local alarms are active, or input test procedures are active. Any input can also be programmed to activate the keypad beeper when in alarm. In addition, the system can be programmed to activate on virtually any type of event or condition that can exist in the Discovery system.

Use the following steps to program a keypad beeper.

- 1 Determine the keypad beeper requirements and fill out the programming sheets. See [“Planning the system”](#) on page 8.
- 2 Access the Install menu. See [“Accessing the Install menu”](#) on page 13.
- 3 Program an unused event flag number as the Console trigger event flag in [“Program summary event flags”](#) on page 163.
- 4 Use the console trigger event flag number in any event flag record for the functions that are to activate the keypad beepers. Event flags are used in many parts of Discovery programming and can be seen on the following programming worksheets:
 - [“Input worksheet”](#) on page 228 (selected event flag)
 - [“Area worksheet”](#) on page 229
 - [“RAS worksheet”](#) on page 231 (door event flag)
 - [“Input shunt worksheet”](#) on page 250 (shunt event flag and shunt warning event flag)
 - [“Event flags worksheets”](#) on page 252 (all summary event flags)
 - [“Macro logic worksheet”](#) on page 255
- 5 If more than one event is required to activate the keypad beepers, and those events have already been allocated different event flag numbers for other functions, create a macro logic program that will combine the required event flag numbers to activate the console trigger event flag number. See [“Programming macros”](#) on page 166 for details.

Using keypad duress

An alarm group may be programmed to allow a user to signal a duress condition (for example, a holdup) by entering a special duress code on a keypad RAS (on the Discovery system Comm) instead of their usual door code.

The system will behave as if the user's PIN was entered (for example, to open a door), and it will initiate a duress alarm. The duress alarm can be reset (cancelled) by entering the normal PIN. Duress codes cannot be used to access a RAS menu (for example, to program the system): a duress code is treated as an invalid code for RAS menu access.

When enabled, the special duress code is the user's PIN+1 (last digit only). For example, if the user's PIN is 8914 then the duress code is 8915. If the user's PIN is 8919, then the duress code is 8910 because only the last digit is affected. When a duress alarm is activated from a keypad connected to the Discovery LAN, the characters "...," are displayed on the LCD (Figure 16 below).

Figure 16: LCD RAS indication of keypad duress alarm



..., There Are No Alarms In This Area
Code:

To use keypad duress, enable (set to YES) the following options:

- "[Keypad duress](#)" on page 48 for the user's alarm group and the RAS's alarm group.
- "[User alarm group](#)" on page 90 for the user's alarm group and the RAS's alarm group.
- The user's alarm group and the RAS's alarm group must allow arming and disarming of the applicable areas. If not enabled, the duress code opens the door and activates a duress alarm, but the duress alarm cannot be restored when a normal PIN is entered. Duress can only be reset on a keypad that has alarm system control over at least one area.
- At least one area must be assigned for the RAS's alarm group. If the RAS is assigned an alarm group without any areas, the duress code opens the door but does not activate or report duress.
- Optionally program a summary event flag to be activated when a keyboard duress alarm occurs.

The known limitations of keypad duress are as follows:

- The duress code opens the door but does not activate or report duress if the RAS is programmed for Enter Key Opens Door Only. See "[ENTER key opens door only](#)" on page 84.
- When used on a RAS connected to an Intelligent 4-Door or 4-Lift Controller (with duress enabled), a duress code opens the door, regardless of the user's alarm group and the keypad duress option in the alarm group. The Discovery panel will report the duress alarm; however, there is no way to restore the duress from any door or Discovery RAS, and the RAS on the Discovery LAN do not display "...," to indicate duress.

Programming common areas

Common areas have inputs that can go into alarm only when all areas are armed (for example, the front door in a building provides an entry to two areas, thus the front door needs to be a common area). There are two ways to create inputs in a common area:

- Assign more than one area (via an area group) to an input. The input can only go into alarm if all areas meet the condition (armed or disarmed). The input is disarmed if one area is disarmed and the longest entry and exit time is used. See [“Area or Area Group programming”](#) on page 65.
- Use area linking. The common area is an additional area that automatically secures as soon as the linked areas are secured. See [“Area linking”](#) on page 151.

The common area can be disarmed separately and has its own entry and exit times. For example, if area 1 is a foyer and is linked to areas 2, 3, and 4, then:

- When any of the linked areas (2, 3, or 4) are disarmed, area 1 will be disarmed.
- When all of the linked areas (2, 3, and 4) are armed, area 1 will be armed.

Linked areas also have control over the common area (if programmed in the alarm group). For example, if area 1 is linked to an area group containing areas 2, 3, and 4, then a user with area 3 can reset an alarm in area 1.

Using Area Search

Area search is a process by which a person must ensure that a facility is safe as part of the disarming process. The following programming is required:

- The person’s alarm group must have area search enabled.
- Minimum and maximum area search times must be defined in Timers.
- An area search time zone must be specified in system options.

Note: The area search time zone must not be a 24-hr time zone because the functionality depends on the time zone changing from valid to invalid to reset the functionality for the next time it is needed. Either soft or ‘hard’ time zones may be used.

Two summary event flags can be used to indicate the state of the area search process:

- Area Search Running
- Area Search Done

The area search process has two modes of operation, depending on whether the Discovery system is configured as a financial institution in System Options or a standard system.

Area search procedure for standard systems (not financial institutions)

The process of disarming via area search is:

- 1 The person enters the premises when the area search time zone is valid, and disarms the area (or areas). The area search timer starts. During the area search procedure “Area Search” is displayed via LCD RAS.
- 2 The person searches the premises to determine that there are no threats, and then exits and rearms the premises.

Assuming that the person searched the area, and then exits and rearms the premises between the minimum and maximum area search times, then the premises is deemed to be safe to disarm and enter (open for business).

If rearming occurs before the specified minimum area search time, then an “Area Search Early” alarm is generated (CID 140, point ID 421).

If the area has not been rearmed before the area search timer expires (maximum area search time), then an “Area Search Timeout” alarm is generated (CID 140, point ID 422). The RAS text “Area Search” is replaced with, “..,” until the next time the area is armed or disarmed. After arming or disarming, a “Reset Area Search Failed” message is logged in history.

Area search procedure for financial institutions

The process of disarming via area search is:

- 1 The person enters the premises when the area search time zone is valid, and disarms the area (or areas). The area search timer starts. During the area search procedure “Morning Check x mins” is displayed via LCD RAS (where x is a countdown of the time remaining starting from the maximum area search time). The area cannot be rearmed until the minimum area search time expires.
- 2 The person searches the premises to determine that there are no threats, and then exits and rearms the premises.

Assuming that the person searched the area, and then exits and rearms the premises between the minimum and maximum area search times, then the premises is deemed to be safe to disarm and enter (open for business).

If the area has not been rearmed before the area search timer expires (maximum area search time), then an “Area Search Timeout” alarm is generated (CID 140, point ID 422). The RAS text “Morning Check x mins” is replaced with, “..,” until the next time the area is armed or disarmed. After arming or disarming, a “Reset Area Search Failed” message is logged in history.

Configuring IP connections

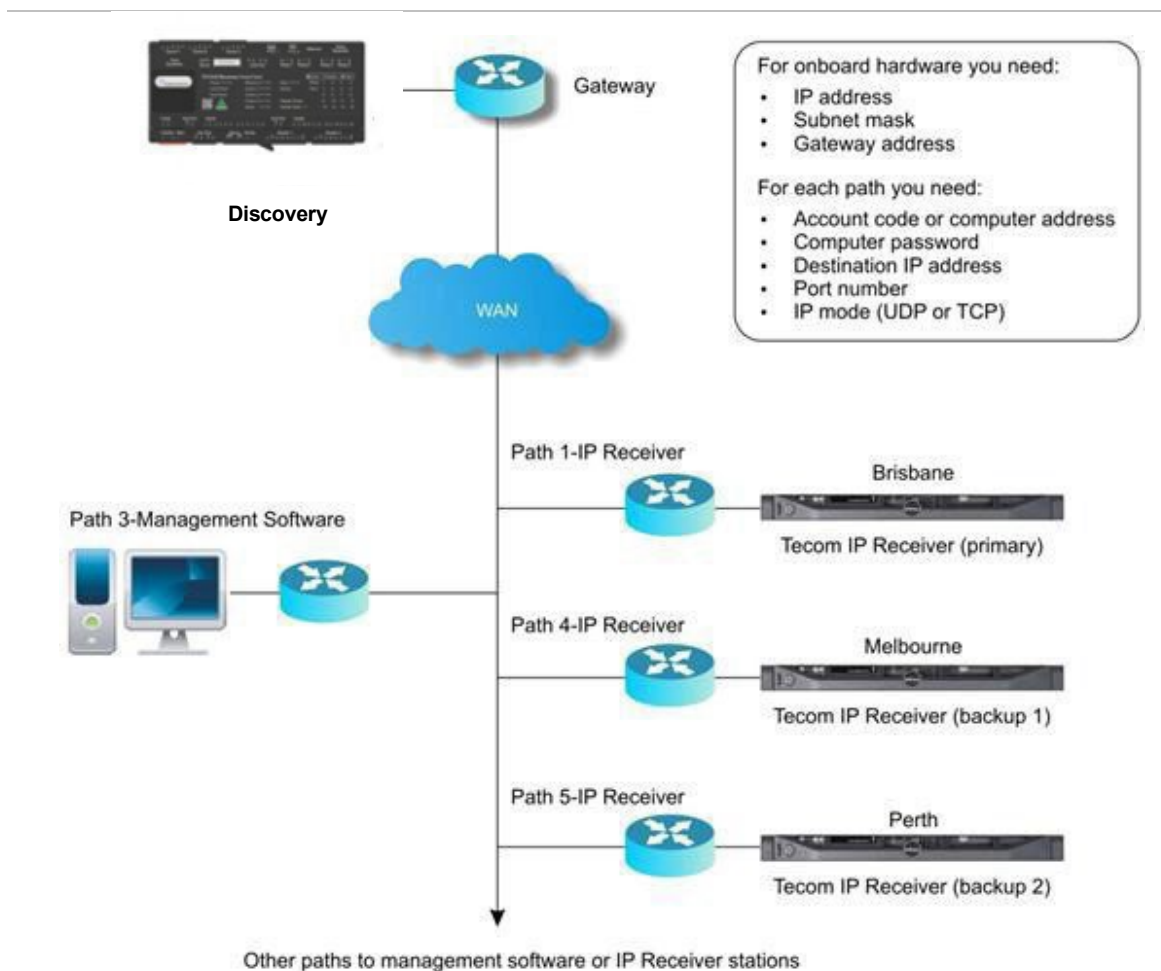
Overview

Discovery panels have native Ethernet support and can communicate with remote computers via one or more of 10 communications paths. Refer to [“Setting up communications paths”](#) on page 124 for additional details.

WARNING: Configuring IP communications requires consultation with the client’s Network Administrator. Failure to gain the essential information from the client may result in the Discovery panel not communicating with the IP Receiver, management software, or introducing data collisions with parts of the client’s existing IP network and possibly a total network shutdown.

Figure 17 below is an example of how the Discovery panel’s Ethernet port can be used for simultaneous connection to multiple computers.

Figure 17: Overview of IP connectivity



Advanced network administration

Enterprise-scale sites may have network security measures in place that need to be considered when configuring Discovery IP communications.

For example, the Discovery panel may be configured to communicate with various devices (on various communications paths) over the “Send IP Port” and the “Listen IP Port” which might both be programmed as port 3001. However, the customer’s network might be configured to block communications based on source ports (also known as local ports).

Source or local IP port assignment

Source ports are assigned by the Discovery panel for each communication path that is configured for IP communication.

The source port for a communication path is assigned when the communication path establishes a connection with its configured destination (or re-establishes communication any time the panel restarts).

For example, on a Discovery panel:

- Communication path 3 is configured to communicate with WMS Pro on Send IP Port 13000.

Using timed input testing

Various options for testing security devices (inputs) are described in the *Discovery Administrators Manual*. This section describes the programming required to configure the Discovery panel to use timed input testing.

Past versions of Discovery panels allowed inputs to be tested (typically unsealed and then resealed) in the following situations:

- On an ad hoc basis when a device appears to be faulty
- During an access test (a timed interval that starts when areas are disarmed)
- During a secure test (a timed interval that starts when areas are armed)

Discovery panels allow inputs to be tested during normal operation within a specified number of days and will report an alarm for inputs that haven’t been tested.

For example, a sensor that is normally activated on a daily basis would be considered to be successfully tested in normal operations. However, a sensor in a room that gets little traffic could be programmed to be tested within seven days so that if a week passes without the sensor being activated, then an input test failed message (CID 307 ‘Self-test failure’) is generated for the input number.

During access tests and secure tests, the Discovery panel’s LCD RASs lists all untested inputs, and removes inputs from the list as they are tested. The list includes inputs that are programmed for timed input testing, and removes these

from the list, even if tested during normal operation (outside of access or secure tests).

Inputs that are programmed for timed input testing have a testing interval timer (for example, 30 days). The timer is reset and the input is considered as untested each time the testing interval expires.

To program timed input testing:

Enable the System option "[Enable expanded test reporting](#)" on page 111.

- 1 For each input to be timed, select option 2 "Tested in Secure Test & Access" in "Test option" on page 71.
- 2 For each input to be timed, specify the testing interval in "[Test input within no. of days](#)" on page 111.
- 3 If you need to time only on certain days of the week (defined by a time zone), then use "[Decrement test days during TZ](#)" on page 107 to assign the time zone.
- 4 Optional: After programming time input testing, reset the timer to 0 before handing over to the customer. See "Option 38: Reset input test days" on page 192.
- 5 Optional: When an input is tested within its specified number of days, you can send a test success message for the input number. See "[Expanded test success reporting](#)" on page 111.

Programming text via RAS

Many entities, such as inputs, areas, and so on, can be programmed with a names to identify them. The initial RAS display for input 1 is shown below.

```
1:
(1)-Edit
```

Press 1 to add (or overwrite) text and numbers via RAS (see [Table 5](#) page 55). The name may contain up to 30 characters (including spaces).

```
1: ,(*)-End
10 Ferntree Place, front door PIR_
```

When each required character is displayed, press [ENTER] to move the cursor to the next position (and to save the characters to the left of the cursor). When finished, press * to save the programming.

Table 5: Key press to get character

Key	1st	2nd	3rd	4th	5th	6th	7th
1	A	B	C	1	a	b	c
2	D	E	F	2	d	e	f
3	G	H	I	3	g	h	i
4	J	K	L	4	j	k	l
5	M	N	O	5	m	n	o
6	P	Q	R	6	p	q	r
7	S	T	U	7	s	t	u
8	V	W	X	8	v	w	x
9	Y	Z	sp	9	y	z	sp
0	.	—	&	0	.	—	&

If the item already has a name (as shown below), and you want to completely delete it, use the following steps.

**1: 10 Ferntree Place, front door PIR
(1)–Edit**

Press 1 to begin editing. Note the flashing cursor below the first character.

**1: 10 Ferntree Place, front door PIR ,(*)–End
10 Ferntree Place, front door PIR**

Press [0] to replace the first character with a “.” (see [Table 5](#) above).

**1: 10 Ferntree Place, front door PIR ,(*)–End
_Ferntree Place, front door PIR**

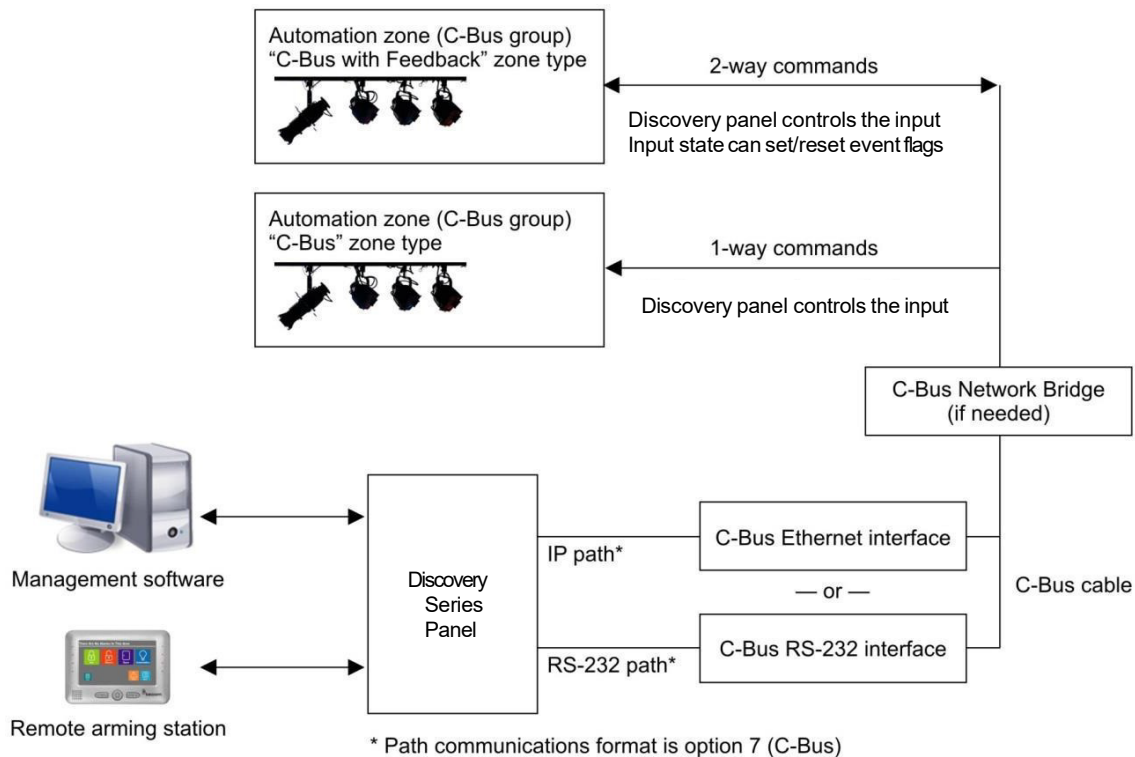
Press * to delete all characters and save the programming.

Automation overview

An automation zone is one or more building devices (including C-Bus® devices) that can be controlled by the Discovery panel via a system RAS or via supported management software or remote devices.

[Figure 18](#) on page 56 is a general overview of the relationship between a Discovery panel and two automation zones (C-Bus groups).

Figure 18: Automation overview diagram



Automation zones are programmed in "[Automation zone](#)" on page 171. Refer to "Controlling automation zones via RAS" below for details about manually turning automation zones on and off via an LCD RAS.

Controlling automation zones via RAS

Subject to the automation zone's programming, a RAS can be used to manually control the zone by activating it, or by immediately turning it on or off.

Figure 19 below depicts the RAS display for automation zone 1 named "Entrance lights".

Figure 19: Automation zone control screen

1: Entrance lights – OFF
1–Trig 2–On 3–Off

The top line indicates the current state of the zone. Press a number to perform the following actions:

- Press [1] to trigger the automation zone according to its programming.
 Press [1] again, or press [MENU*], to update the RAS display.
- Press [2] to turn the automation zone on immediately at 100% until turned off or triggered (in which case the zone's programming will turn it off).
- Press [3] to turn off (reset) the automation zone.

Refer to “[Control via User menu](#)” below, “[Control via Quick Control](#)” below, and “[Control via Install menu](#)” on page 58 for the required programming.

Control via User menu

The relevant programming for controlling automation zones via the User menu 24–Automation Control includes the following items:

- There must be at least one RAS designated to control the zone in “Control zone on RAS” on page 196. If one RAS is designated, then the automation zone can be controlled by a user at only that RAS.
- At least “[Enable manual control](#)” on page 175 must be enabled. If this option is enabled by itself (manual on control and manual off control disabled), then the user can select only RAS option “1–Act” to activate (trigger) the zone.
- If the option “[Manual on control](#)” on page 175 is also enabled, then the user can also select RAS option “2–On” to turn the zone on immediately at 100%.
- If the option “[Manual off control](#)” on page 176 is also enabled, then the user can also select RAS option “3–Off” to turn the zone off immediately.

Refer to the *Discovery Administrators Manual* for details about the User menu.

Control via Quick Control

Quick control uses the CA111x RAS’s multi-function key as a shortcut to the automation zone control screen ([Figure 19](#) on page 56).

Note: Quick control does not require user authentication via PIN. We recommend that control be assigned to a specific RAS (in a secure area) in “Control zone on RAS” on page 196 in order to prevent unauthorised use.

The relevant programming for controlling automation zones via quick control includes the following items:

- There must be at least one RAS designated to control the zone in “Control zone on RAS” on page 196. If one RAS is designated, then the automation zone can be controlled by a user at only that RAS.
- At least “[Enable quick control](#)” on page 175 must be enabled. If this option is enabled by itself (manual on control and manual off control disabled), then the user can select only RAS option “1–Trig” to trigger the zone.
- If the option “[Manual on control](#)” on page 175 is also enabled, then the user can also select RAS option “2–On” to turn the zone on immediately at 100%.
- If the option “[Manual off control](#)” on page 176 is also enabled, then the user can also select RAS option “3–Off” to turn the zone off immediately.

Control via Install menu

Regardless of an automation zone's programmed control options, an installer can use via the Automation Status to select RAS option "1-Trig" to trigger the zone.

The following items allow additional control:

- If the option "[Manual on control](#)" on page 175 is enabled, then the installer can also select RAS option "2-On" to turn the zone on immediately at 100%.
- If the option "[Manual off control](#)" on page 176 is also enabled, then the installer can also select RAS option "3-Off" to turn the zone off immediately.

Refer to the install menu "Automation status" for details.

Programming twin trip inputs

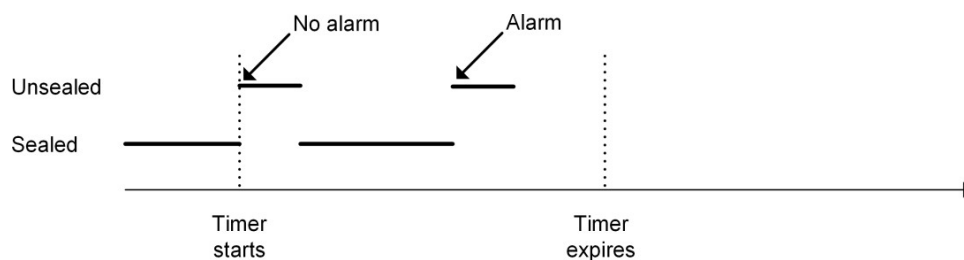
It may sometimes be necessary to allow an input to be briefly unsealed without generating an alarm immediately. In this case, the input can be designated as a **twin trip** input. Twin trip inputs will not generate an alarm if they are unsealed (i.e. tripped) and then re-sealed only once within a specified amount of time (the maximum twin trip time).

A twin trip input will not generate an alarm immediately when it is unsealed and all assigned areas are armed. Instead, it will start a twin trip timer, which runs for the maximum twin trip time.

Note: A maximum of five twin trip timers can run simultaneously. If a twin trip input is unsealed and all five twin trip timers are already running, then the input will generate an alarm immediately.

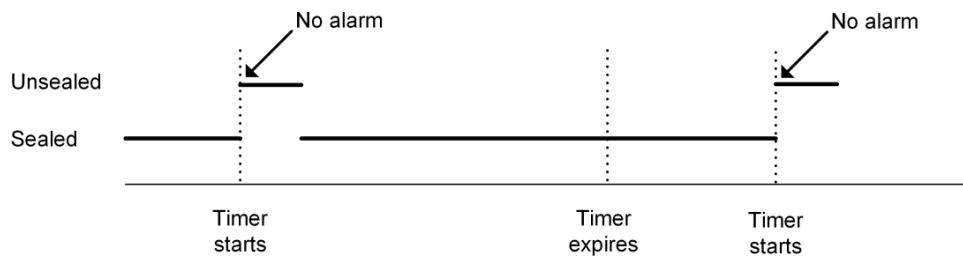
If a twin trip input is unsealed a second time whilst its twin trip timer is running, then it will generate an alarm:

Figure 20: Twin trip input unsealed before timer expiry



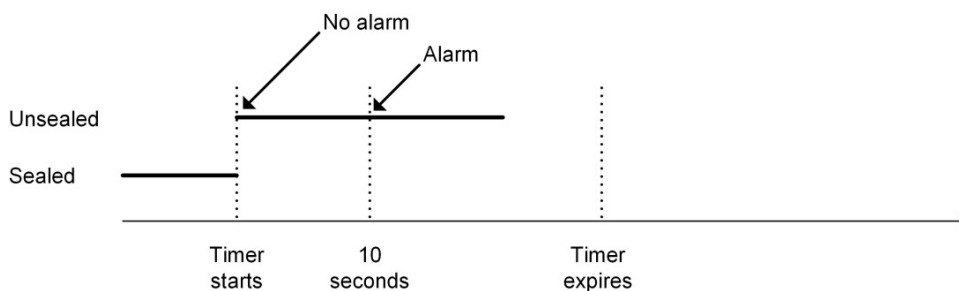
If a twin trip input is unsealed a second time after the twin trip timer has expired, then a new twin trip timer is started (if available) and the input will not generate an alarm:

Figure 21: Twin trip input unsealed after timer expiry



If a twin trip input remains unsealed for longer than 10 seconds then it will generate an alarm:

Figure 22: Twin trip input unsealed for 10 seconds



If a twin trip timer is running and another input (which does not have a twin trip input type) is unsealed in the same area, then both inputs will generate an alarm immediately.

If a twin trip timer is running and another twin trip input is unsealed (whether the second input is in the same area or not), then another twin trip timer will be started (if available). Thus, both twin trip inputs will run a timer and wait for a second unseal before generating an alarm.

If a twin trip input is unsealed when another input in the same area is already in alarm and all assigned areas are armed, then the twin trip input will generate an alarm immediately.

A “twin trip timer started” event will occur when any twin trip timer is started. The event will carry the number of the input that started the timer.

An input can be designated as a twin trip input by setting its input type to one of the following:

- Twin trip secure alarm (input type 60)
- Twin trip entry exit handover (input type 61)
- Twin trip handover no seal check (input type 62)

See “[Input type](#)” on page 208 for instructions on programming the input type of an input.

The maximum twin trip time is configured in “[Timers](#)” on page 100.

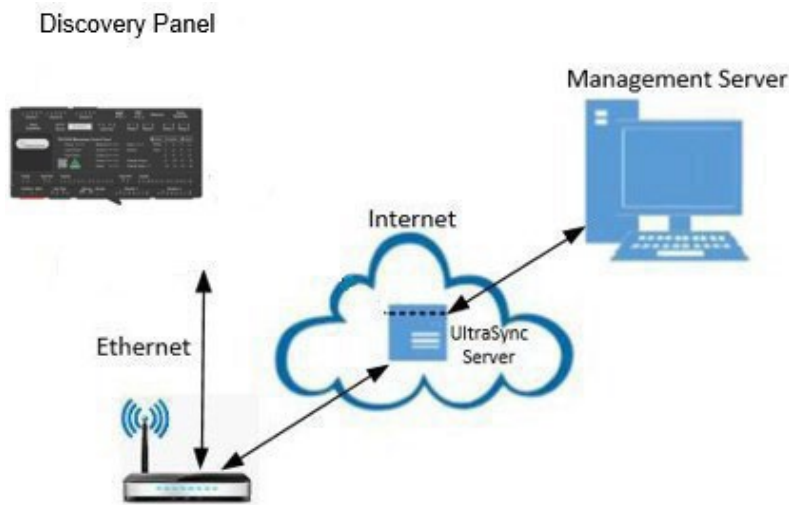
Connecting via UltraSync

Overview

Discovery panels support **UltraSync** communication. UltraSync provides a secure cloud connection between the Discovery panel and management software or monitoring station using an Ethernet and/or 4G connection through the Internet as shown in figure 23 below.

For further information, please refer to the *UltraSync Configuration Guide* document.

Figure 23 UltraSync Connection



Chapter 5

Programming Reference

This chapter describes using the Discovery web interface for programming, and some features on a LCD RAS on the Discovery system LAN.

The Discovery system may contain Network Access Controllers, which have local LANs and their own command structure. In addition, the system may be operated from management software, which also has its own command structure. The details provided in this chapter pertain to the commands that can be performed on the Discovery web interface and system LAN via an LCD RAS.

- If using a Network Access Controller, refer to its programming manual for programming details.
- If using management software, refer to its user guide or online help for programming details.
- For Discovery User menu commands (for example, to program users) refer to the *Discovery Administrator's Manual*.

On each page, Discovery will list the programmed items displaying the Input number (Entity), Name, Status, and icons for managing Operations related to each item's entity:

-  **Copy** (from the selected entity to a new entity number)
-  **Edit** (same as clicking anywhere along the entity row)
-  **Delete** (to remove the entity)

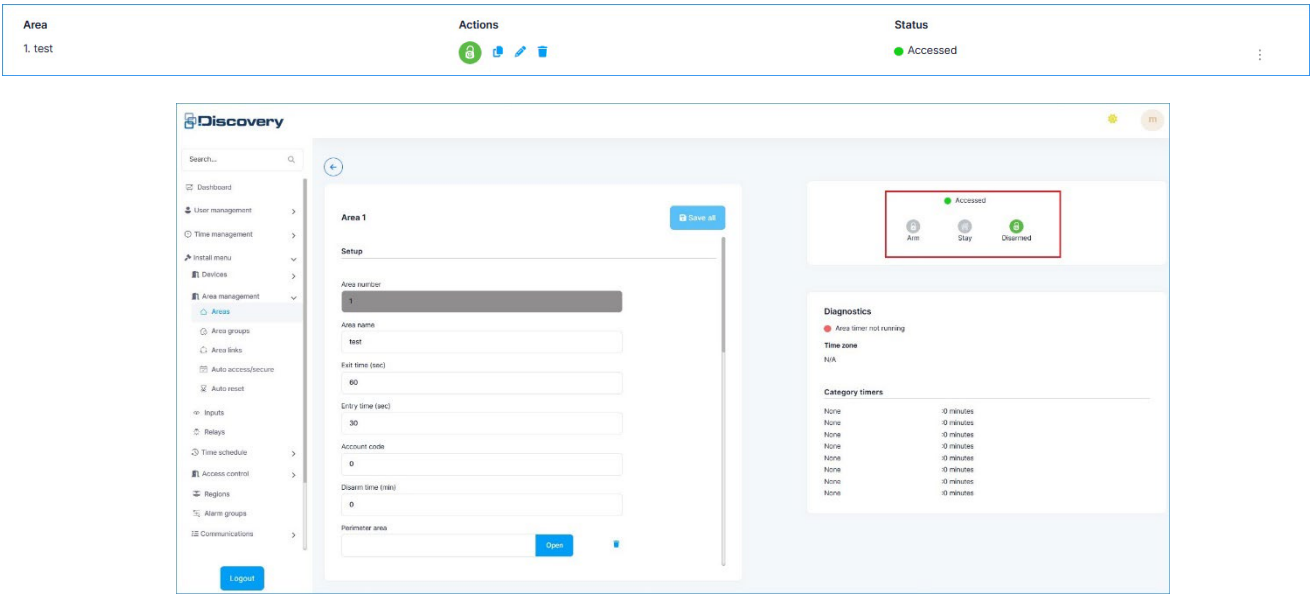
On some Installer menu pages statuses, diagnostics and control are available to most entities

For example:

- Discovery will have locks or power buttons in the Action(s) column, this can have different meaning depending what is being locked or unlocked / deisolated or isolated.



Clicking on the entity line will open up options for this Eg; Area for its Arming, Disarming and Diagnostics.



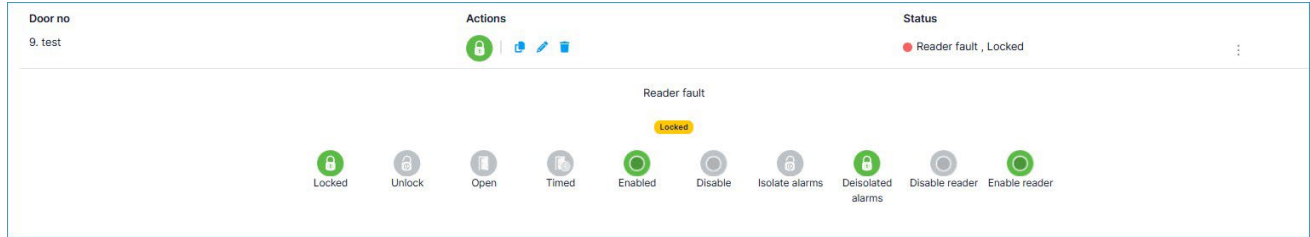
Using the 3 dots at the end of the entity line will expand the line out for the commands for the device.



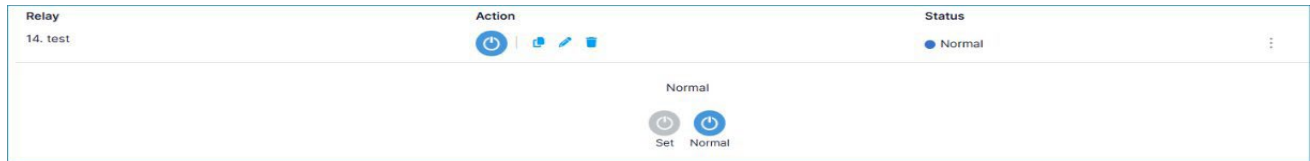
Eg; Accessing or Disarming an Area.



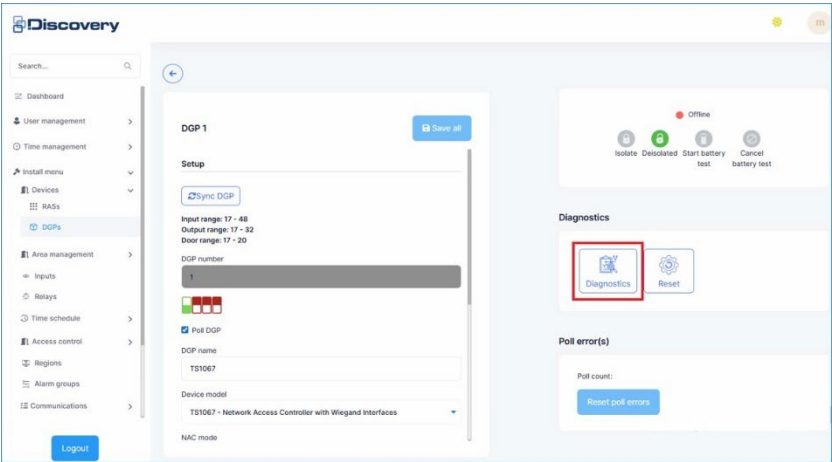
Similar with Locking or Unlocking a Door.



Example below shows a Relay being set / active.



Diagnostics of devices are also available throughout the Installer Menu.



These actions and similar ones are throughout the functions within the Discovery web interface.

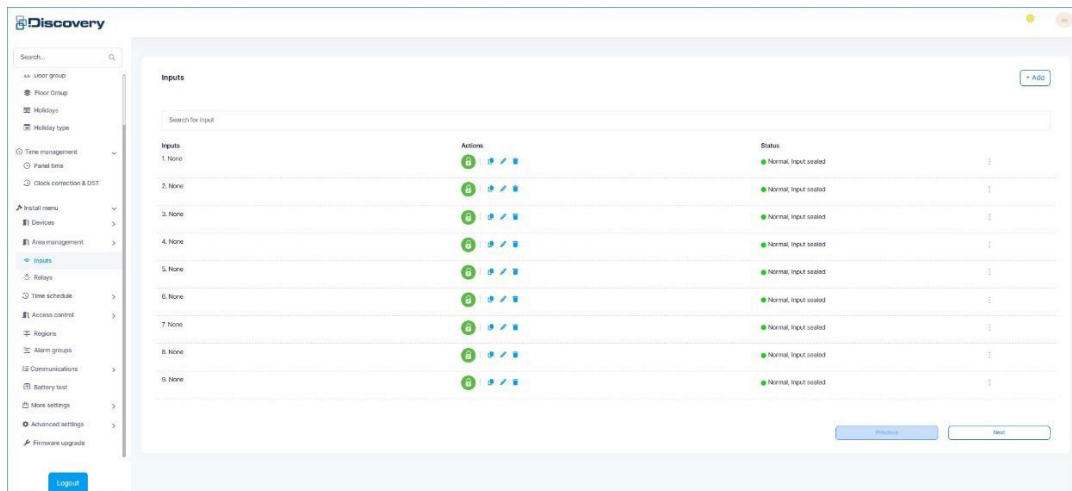
Content

Inputs	64
Areas	72
RAS	78
DGP	88
Alarm group	92
Timers	103
System options	104
Auto reset	118
Comm devices	119
Comm paths	126
UltraSync	139
UltraSync reports	143
Panel time zone	145
Relays	148
Vaults	150
Area links	152
Input shunts	154
Soft time zones	159
Battery test	160
Custom RAS message	162
Next service	162
Summary event flags	163
Panel macro logic	166
Area group	169
Automation zone	171
Event flag	177
Discovery name	178
Standard lifts	178
Standard doors	182

Inputs

INSTALL MENU > INPUTS

Each input device can be physical, or a programming input on the control panel, a DGP, or a plug-in expander. Alternatively, an input can be the output of the macro logic equation (see “[Program macro logic](#)” on page 167).



A worksheet is provided to record programming details and to further describe this option. See “[Input worksheet](#)” on page 228.

Programming Inputs

To program a new Input, click the **+ Add** button to bring up the Setup page.

Setup

Physical location : Panel Onboard

Input number

Must be between 1 and 1008.

Input name

Type

2 - Secure alarm

Area or area group assigned

Area

Enter area

1. None

Open

Contact ID

Save

Cancel

On the Setup page we have the Input's physical location as **Panel Onboard**.

Input number

Select the appropriate input number to program.

Every input has a number, depending on the location in the system.

Input name

Enter a name to identify the input (for example, Front Door).

The name may contain up to 30 characters (including spaces).

Input type

Choose the input type number (see [Table 28](#) on page 210). The input type determines exactly how the input will function in given circumstances. Refer to "[Input types](#)" on page 208 for details.

Note: The input type is important and influences much of the programming and functions of the system. You must be very careful when programming input types. All inputs used for safe or vault monitoring must be a 24-hour alarm input type.

Area or Area group assignment

An area, or an Area group must be linked to the input.

Area or Area Group programming

Except for area control input types, you must assign an area or an area group to the input so that the input can generate an alarm when the input is unsealed and the area status (secured and/or in access) meets the requirement for the input type.

Note: At least one area must be assigned to an input. It is not possible to reset an alarm on an input without an area assigned.

Area groups are used to assign multiple areas to an input. This is typically used:

- To program an additional area that is designated to have overriding control over the alarm functionality for this input. See "Total disarm" on page 107.
- To create a common area. Common areas have inputs that can go into alarm only when all areas are armed. See "[Programming common areas](#)" on page 50.

Select the Area / Area group field or the **Open** button next to it to display a list of Areas / Area groups that may be used with this Input. Select or create the Area / Area group to be used, then press the OK button to save. The Area / Area group may be cleared from this entity by selecting the  trash icon next to the Area / Area group field.

Contact ID

Use this option to select the Ademco Contact ID (CID) message to be reported to the monitoring company if the input or the system generates an event. The details of the data sent to the monitoring company depend on the reporting format.

The example: **140 – GA General alarm** shows the Ademco Contact ID event class “140 General Alarm” (sub-class General Alarm).

Choose a report ID number from the drop down.

Note: Input numbers in the range 1000 to 1008 will not report CID alarms.

Bypass input in stay mode

When enabled, the input will not activate when the associated area(s) are in stay mode. The panel can have areas in stay mode via control using supported software or the Mobile App. Toggle this option to determine the input being bypassed in stay mode.

- Ticked If the areas to which the input is assigned are in stay mode and the input is unsealed, then the input does not generate an alarm.
- Unticked If the areas to which the input is assigned are in stay mode and the input is unsealed, then the input generates an alarm as normal.

Preferred video camera

Enter the preferred video camera number.

Programmable event

An input can have multiple event flags assigned to it, including one event flag assigned by number and pre-defined event flags (YES/NO values). Event flag numbers from 1 to 16 are the system’s predefined event flags, and numbers from 17 to 255 are programmable event flags.

Refer to “[Event flags](#)” on page 222 for details.

Most input types can activate event flags. The event flags that can be programmed for an input are described in the following sections.

Select the Programmable event field or the **Open** button next to it to display a list of Programmable events that may be used with this input. Select or create the Programmable event to be used, then press the **OK** button to save. The Programmable event may be cleared from this entity by selecting the  trash icon next to the Programmable event field.

Selected event flag active when unsealed

When the input is unsealed the selected event flag will be active. Toggle this option to determine whether the selected event flag is active when the input is unsealed.

- Ticked Selected event flag will be active when the input is unsealed.
- Unticked Selected event flag will not be active when the input is unsealed.

Second programmable event

Assign an optional second event flag to be triggered when the input is unsealed, isolated, or in alarm (as determined by the next three options).

Select the Second programmable event field or the **Open** button next to it to display a list of Second programmable events that may be used with this input. Select or create the Second programmable event to be used, then press the **OK** button to save. The Second programmable event may be cleared from this entity by selecting the  trash icon next to the Second programmable event field.

Second event flag for unseal

When enabled, the event flag programmed in “Second event flag” above is triggered when this input is unsealed.

Toggle this option to determine whether the second event flag for unseal is active or not.

- Ticked The event flag is triggered when the input is unsealed (regardless of the status of the area assigned to the input).
- Unticked The event flag is not triggered by this condition.

Note: Not applicable to input types 0, 6, 9, 10, 12, 17, 19, 23, 24, 25, 26, 31, 33,34, 35, 36, 37, 38 or 39.

Second event flag for isolate

When enabled, the event flag programmed in “Second event flag” above is triggered when this input is isolated.

Toggle this option to determine whether the second event flag for isolate is active or not.

- Ticked The event flag is triggered when the input is isolated.
- Unticked The event flag is not triggered by this condition.

Second event flag for alarm

When enabled, the event flag programmed in “Second event flag” above is triggered when this input is in alarm.

Toggle this option to determine whether the second event flag for alarm is active or not.

- Ticked The event flag is triggered when the input generates an alarm.
- Unticked The event flag is not triggered by this condition.

Test type

The test type option value defines the behaviour of this input during a secure test or an access test (input testing interval). Refer to “Testing Input Devices” in *Discovery Administrator’s Manual* for details.

Choose a test type (see Table 6 below).

Table 6: Input Test Types

Test type	Description
No Test	The alarm input is not programmed to be tested during either a secure test or an access test. Select this test type for camera count input types for cameras to be tested during an access test. Example: A button that is active during test mode, siren cover, and panel tamper.
TestDuring Access Test	The input is programmed to be tested during the access test, and is disabled during the access test. Example: Hold-up button.
Tested in Secure Test & Access	The input is programmed to be tested during the secure test, and is considered to be already tested if the input's state is toggled from sealed to unsealed, and then back to sealed during access. Example: PIR detectors, doors.
TestDuring Secure Test	The input is programmed to be tested during the secure test. Example: To enable you to test a door contact at the end of the day when arming the area.
Set Event Flag 13 During Access Test	The input has event flag 13 during the access test. This test type is used for testing devices activated by access alarm input types (e.g. holdup buttons). The device must already be programmed to be activated by access alarm event flag 13.
Set Pre-Alarm During Access Test	The input activates the - event flag during the access test in the areas assigned to the input. This test type is used to test devices that are activated during the delayed hold-up time. The pre-alarm event flag number is programmed in the area database.

Note: During the secure test, the tester event flag (event flag 16) will be activated during half the tester event flag time. Use this event flag to activate devices to generate alarms. The other half of the tester event flag time is used for the device to switch back to sealed state.

See also “[Test mode](#)” on page 165 for related programming.

Test within (days)

Inputs that are programmed as “Test During Access+Secure” test type, can be assigned a timer (number of days). If the input hasn’t been tested within the specified number of days, then the input

reports a 'Self-test failure' alarm.

The input may be tested during an access test, a secure test, or as the result of normal operation outside of the test times. See ["Using timed input testing"](#) on page 53 for details.

Enter a number of days for the input's testing timer.

Notes:

- Use a sufficiently large number of days to accommodate times when there will be no activity, such as weekends or holidays.
 - This functionality requires the System Option "Expanded Test Reporting" to be enabled (the system option "Test Mode" is not relevant).
-

Pre-defined events to activate (check boxes)

Siren event

Program the siren event flag in the area database for each of the areas that activatesirens and that are assigned to the input.

Toggle this option to determine whether the Siren event flag will be activated.

- Ticked The siren event flag specified in the area database is activated when the input generates an alarm, and all the areas assigned to the input are armed.
- Unticked The siren event flag will not be triggered by an alarm in this input.

Console warning

Program the Console warning to trigger a keypad buzzer warning when an input activates an alarm. Toggle this option to determine whether the console warning will trigger a warning.

- Ticked When the input activates an alarm, the console warning (keypad buzzer) is activated on the keypads that control the areas assigned to the input.
- Unticked An alarm on the input will not trigger the console warning.

Print input when unsealed

Program the Printer / computer to receive a message when an input changes to unsealed.

Toggle this option to determine whether the printer or computer receives a warning when a input changes it state.

- Ticked Each time the input changes from sealed to unsealed a message is sent to the printer or computer, as applicable.

- Unticked Changes from sealed to unsealed are not printed or sent to a computer.

Note: Door open and close messages may also be sent for shunted inputs.

Make all events 24-hour

This option causes any event flags assigned to the input to be active when the input generates an alarm, regardless of the secure or access status of the area. For example, the client may want the siren and strobe to activate during the day if the input wiring is tampered or damaged.

Toggle this option to determine whether any event flags assigned to the input to be active when the input generates an alarm, regardless of the secure or access status of the area.

- Ticked All event flags are triggered when the input generates an alarm, regardless of the secure or access status of the area.
- Unticked The event flags are triggered depending on the secure or access status of the area assigned to the input.

Camera event

Program the event flag number in the area database for each of the areas that have cameras that are assigned to the input.

Toggle this option to determine whether the camera will trigger an event flag when an input generates an alarm.

- Ticked The camera event flag programmed in the area database is activated whenever the input generates an alarm.
- Unticked The camera event flag will not be triggered.

Event flags 2, 3, 4, 5, 9, 10, and 11 secure alarm

Program certain inputs to generate an event flag when these input area is secure.

Toggle this option to determine whether an event flag is generated when the input's area is secure.

- Ticked The event flag is triggered when the input generates an alarm and the area is secure.
- Unticked The event flag is not triggered.

Access alarm (event flags 6, 7, and 13)

Program certain inputs to trigger an event flag when their area has been accessed.

Toggle this option to determine whether an event flag is triggered when their area has been accessed.

- Ticked The event flag is triggered when the input generates an alarm and the area assigned to the input is in access.
- Unticked The event flag is not triggered.

Event flag 8, 24 hour alarm

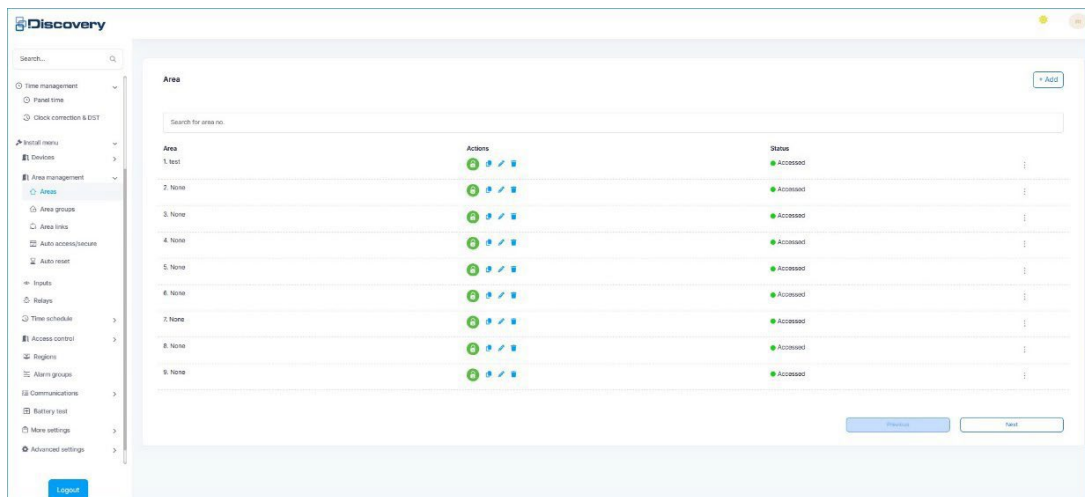
Toggle this option to determine whether the event flag is triggered when the input generates an alarm, regardless of the status of the area assigned to the input.

- Ticked The event flag is triggered when the input generates an alarm, regardless of the status of the area assigned to the input.
- Unticked The event flag is not triggered.

Areas

[INSTALL MENU](#) > [AREA MANAGEMENT](#) > [AREAS](#)

Areas determine how the system is partitioned, and therefore provides the ability to limit users to performing functions only in the areas relevant to their role.



A worksheet is provided to record programming details and to further describe this option. See [“Area worksheet”](#) on page 229.

Programming areas

To program a new Area, click the **+ Add** button to bring up the Setup page.

Setup

Area number

Must be between 1 and 99.

Area name

Exit time (sec)

60

Entry time (sec)

30

Account code

0

Disarm time (min)

0

Save Cancel

Area number

Each Area has a specific number that identifies the Area to the control panel. Enter an Area number.

Area name

Enter a name to identify the area (for example, to select the area to arm or disarm). The name may contain up to 30 characters (including spaces).

Exit time (sec)

This field setting creates a time delay to allow a user to arm an area and leave without generating alarms. If the programmed time is exceeded, an alarm will be activated. Only one exit time can be programmed for each area.

An exit time only applies where the area has been assigned an input which is programmed with input type 3, 4, 13, 14, 41, 42, 61, and 62 (which use the entry/exit timers).

Note: If different areas are programmed with different exit times and a user PIN is programmed to arm more than one area, the longest time is used.

See "[Entry and exit console warning](#)" on page 83 for more information.

Entry time (sec)

This field determines the amount of time (in seconds) allowed between entry to an area and disarming of that area. If the programmed time is exceeded, an alarm will be activated. Only one entry time can be programmed for each area.

An entry time only applies where the area has been assigned to an input which is programmed with input type 3, 4, 13, 14, 41, 42, 61, and 62 (which use the entry/exit timers).

Note: If different areas are programmed with different entry times and a user PIN is programmed to disarm more than one area, the longest time is used.

See [“Entry and exit console warning”](#) on page 83 for more information.

Account code

CID reporting account numbers are four digits long, and are used for reporting via Contact ID Modem format and for reporting via IP Receiver format.

Program area account numbers as follows:

- If the system has account numbers for each area, program the account number for each area on which you want to report alarms.
- If the system has only one account number, program 0000 for each area on which you want to report alarms.

Use “Area account codes” on page 135.

Disarm time (min)

User categories can disarm an area for a timed disarm period. An area disarm time greater than 0 will override any user category time for this area. Enter the time in minutes.

Perimeter area

This option applies only to “internal” areas that contain inputs programmed as handover input types 4, 14, 61 and 62 where you want the internal area to have a designated perimeter area.

Enter the number of the area that contains entry/exit inputs on the perimeter of the premises.

When the entry timer on the perimeter area is activated (for example, by someone opening a door) any internal areas linked by this option are notified. At this point all handover input types in the internal areas will be suppressed for the perimeter area’s entry time.

If the internal area is disarmed while the perimeter area is still entry timing, then the perimeter area will cancel the entry timer and start the exit timer: this allows the perimeter to remain armed while the internal area is occupied.

Arming the internal area when the perimeter area is armed will re-activate the exit timer on the perimeter area to allow people to exit the building without activating an alarm on the perimeter area.

When the perimeter area is disarmed, the internal area’s handover inputs behave like entry/exit inputs.

The internal area and the perimeter area can be armed and

disarmed independently from each other. However, when the internal area is secure (armed), the behaviour of the internal area's handover inputs depends on whether the perimeter area is armed or disarmed:

- If the perimeter area is armed (secure), then the perimeter area's entry or exit timers apply to the internal area.
- If the perimeter is disarmed (in access), then the internal area's entry or exit timers apply to the internal area.

Note: The perimeter area must have longer entry and exit times than any of the internal areas.

Select the Perimeter area field or the **Open** button next to it to display a list of Areas that may be used with this Area. Select or create the Perimeter area to be used, then press the **OK** button to save. The Perimeter area may be cleared from this entity by selecting the  trash icon next to the Event flag field.

Out of hours' time zone

Enter a time zone number if you want to report an out of hours access alarm if the area is in access (disarmed) outside of the specified time zone.

Select the Out of hours' time zone field or the **Open** button next to it to display a list of time zones that may be used with this Area.

Select or create the Out of hours' time zone to be used, then press the **OK** button to save. The Out of hours' time zone may be cleared from this entity by selecting the  trash icon next to the Out of hours' time zone field.

Siren

The siren event flag is set to 1 by default and does not need to be changed unless you want to have different sirens activated for each area.

This event flag is triggered when an input generates an alarm (if the input's siren event flag set to YES). Each area can have its own external siren, using different event flags for each area.

Select the Siren field or the **Open** button next to it to display a list of Sirens events that may be used with this Area. Select or create the Siren event to be used, then press the **OK** button to save. The Siren event may be cleared from this entity by selecting the  trash icon next to the Siren field.

Secure alarm

This event flag activates on an alarm when the area is armed.

Select the Secure alarm field or the **Open** button next to it to display a list of Secure alarm events that may be used with this Area.

Select or create the Secure alarm event to be used, then press the **OK** button to save. The Secure alarm event may be cleared from this entity by selecting the  trash icon next to the Secure alarm field.

Entry timer

This event flag activates when an entry timer for the area is running.

Note: Enter the same event flag number here as for “Console trigger event flag” on page 185 if you want RAS to beep during the entry timer.

Select the Entry timer field or the **Open** button next to it to display a list of Entry timer events that may be used with this Area. Select or create the Entry timer event to be used, then press the **OK** button to save. The Entry timer event may be cleared from this entity by selecting the  trash icon next to the Entry timer field.

Access alarm

This event flag activates on an alarm when the area is disarmed.

Select the Access alarm field or the **Open** button next to it to display a list of Access alarm events that may be used with this Area.

Select or create the Access alarm to be used, then press the **OK** button to save. The Access alarm event may be cleared from this entity by selecting the  trash icon next to the Access alarm field.

Local alarm

This event flag is activated when an input that has this area assigned to it generates a local alarm. For example, fire door, 24-hour local fail input types, and so on (types 15, 16, 18, 21, 30, 41, 42, 44, and 56) in the area. See “[Input types](#)” on page 208.

Select the Local alarm field or the **Open** button next to it to display a list of Local alarm events that may be used with this Area. Select or create the Local alarm event to be used, then press the **OK** button to save. The Local alarm event may be cleared from this entity by selecting the  trash icon next to the Local alarm field.

Exit timer

This event flag activates when the exit timer for the area is running.

Note: Enter the same event flag number here as for “Console trigger event flag” on page 185 if you want RAS to beep during the exit timer.

Select the Exit timer field or the **Open** button next to it to display a list of Exit timer events that may be used with this Area. Select or create the Exit timer event to be used, then press the **OK** button to save. The Exit timer event may be cleared from this entity by

selecting the  trash icon next to the Exit timer field.

Warning timer

This event flag activates to indicate that a user category is running and the area is about to be armed or that a test mode is in progress and the test is about to end.

Select the Warning timer field or the **Open** button next to it to display a list of Warning timer events that may be used with this Area. Select or create the Warning timer event to be used, then press the **OK** button to save. The Warning timer event may be cleared from this entity by selecting the  trash icon next to the Warning timer field.

Input isolated

This event flag indicates an input in this area has been isolated.

Select the Input isolated field or the **Open** button next to it to display a list of Input isolated events that may be used with this Area.

Select or create the Input isolated event to be used, then press the **OK** button to save. The Input isolated event may be cleared from this entity by selecting the  trash icon next to the Input isolated field.

Pre-alarm

This event flag indicates that a delayed holdup alarm input is active and the delay timer is running.

Select the Pre-alarm field or the **Open** button next to it to display a list of Pre-alarm events that may be used with this Area. Select or create the Pre-alarm event to be used, then press the **OK** button to save.

The Pre-alarm event may be cleared from this entity by selecting the  trash icon next to the Pre-alarm field.

Input unsealed

This event flag indicates if any input in the area is unsealed, excluding inputs that can be used to change the status of an area, or used for cameras.

Select the Input unsealed field or the **Open** button next to it to display a list of Input unsealed events that may be used with this Area. Select or create the Input unsealed event to be used, then press the **OK** button to save. The Input unsealed event may be cleared from this entity by selecting the  trash icon next to the Input unsealed field.

Area accessed

This event flag activates when the area is in access.

Select the Area accessed field or the **Open** button next to it to display a list of Area accessed events that may be used with this

Area. Select or create the Area accessed event to be used, then press the **OK** button to save. The Area accessed event may be cleared from this entity by selecting the  trash icon next to the Area accessed field.

Camera

This event flag activates when an input with the appropriate input type and the camera event flag set to YES generates an alarm and the area is disarmed.

Select the Camera field or the **Open** button next to it to display a list of Camera events that may be used with this Area. Select or create the Camera event to be used, then press the **OK** button to save. The Camera event may be cleared from this entity by selecting the  trash icon next to the Camera field.

Preferred video camera

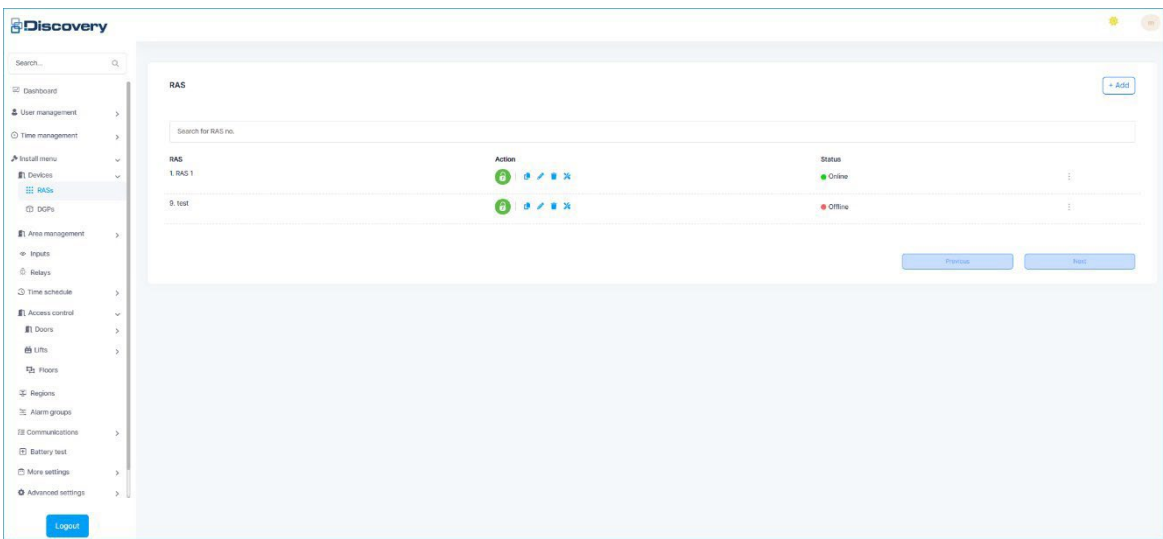
This option allows you to choose the video camera that will be used in the Area. Toggle the arrows to locate the camera number.

RAS

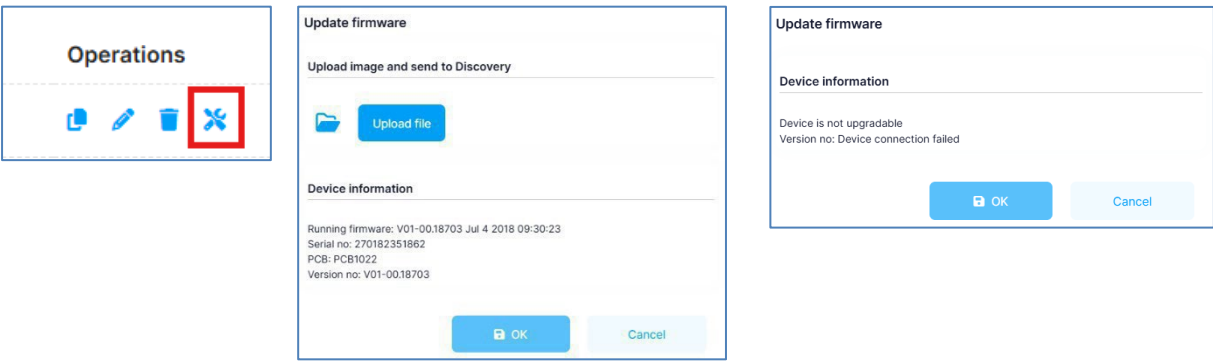
INSTALL MENU > DEVICES > RAS

Remote arming stations (RASs) are devices used to provide alarm system control (such as arming or disarming), to provide access control (such as unlocking a door), and for programming the system.

Alarm groups control what functionality and menu access is available at a RAS, in a similar manner to a user's alarm group controlling what functionality and menu access is available to the user. When a user enters their PIN at an arming station, that user will be able to perform functions (such as alarm control) and see menus (for example, to program users) that are available to both the RAS and the user via their respective alarm groups.



Operations



By clicking on the Spanner / Tools icon on the Operations on the DGP page, it will bring up a 'Update firmware' page where you can update firmware of the DGP. These files must be downloaded first to then be able to upload them to your DGP / NAC. If the device cannot be upgraded there will be a note like in the 3rd image above.

RAS programming options

Program the RAS according to its characteristics (for example, if the RAS has an LCD, set the LCD Arming Station option to YES). Refer to [Table 8](#) on page 80 or the specific RAS's installation guide for details. See also "[Using card readers for alarm control](#)" on page 32.

A worksheet is provided to record programming details and to further describe this option. See "[RAS worksheet](#)" on page 231.

Details of the RAS programming options are:

To program a new RAS, click the **+ Add** button to bring up the Setup page.

The 'Setup' page contains the following fields and options:

- RAS number:** A text input field with a red error message below it: "Must be within: 1-16, 65-80."
- RAS name:** A text input field.
- Options:** Two checked checkboxes: "LCD arming station" and "Poll RAS".
- Model number:** A dropdown menu currently showing "No Model programmed into unit".
- Alarm group:** A dropdown menu showing "2. Master RAS or door" with an "Open" button and a trash icon to its right.
- Menu alarm group:** A horizontal bar with a blue segment on the left.
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

RAS number

Each RAS has a specific number that identifies the RAS to the control panel. RAS numbers may be assigned to physical RAS.

RAS name

Program a name to identify the RAS (for example, to identify its location and type).

The name may contain up to 30 characters (including spaces). To program a name via RAS, see “[Programming text via RAS](#)” on page 54.

Note: The RAS name is the same as the (same numbered) door name, programmed in “Door/lift names and E/F trigger” on page 198.

LCD arming station

Applies to RAS models with LCD or touch screen, see [Table 8](#) on page 80.

Toggle this option to determine if the RAS has a LCD or touch screen.

- Ticked This RAS is an LCD arming station.
- Unticked This RAS does not have an LCD screen or a touch screen.

Poll RAS

In order to be used, a RAS number has to be polled. Polling enables communication between the RAS and the control panel. Discovery automatically uses data encryption when connecting to devices that support encryption.

Toggle the checkbox to Poll the RAS. Repeat for all RAS numbers to be polled.

- Ticked This RAS will be Polled
- Unticked This RAS does will not be Polled

Notes: RASs are config red and polled as follows:

Comm	Configured as	Polled as
1	1 to 16	1 to 16
2	1 to 16	65 to 80

Only polled RASs can be retrieved from the panel (such as by retrieving to management software).

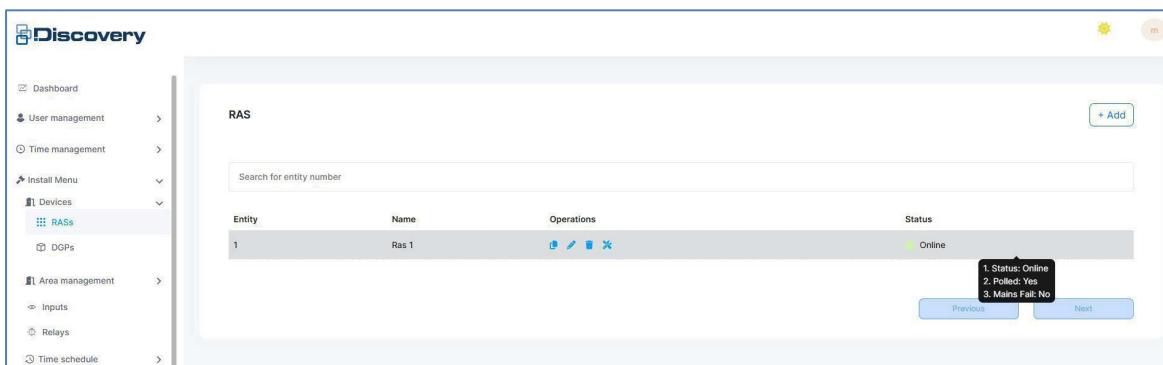
To deactivate a RAS number that is already polled, untick Poll RAS and Save.

Or

Delete the RAS on the RAS page

Notes:

- An offline RAS number initially will displays in the Status area of the RAS page as Offline.
 - If you need to replace the RAS, we recommend that you de- poll the old RAS before removing it. Install the new RAS according to its installation instructions. Some RAS models will not go online otherwise.
-



The RAS status screen shows the different status's that could be:

- 1. Status: Online / Offline
- 2. Polled: Yes / No
- 3. Mains fail: No

Model number

Select the RAS model number attached to the Discovery panel. This will allow certain options in the panel to be configured to ensure optimal communications.

The model may be selected from a pre-defined list, from the drop down:

Table 8: RAS model list

Part number	Description
• TS0003	3/4 LED keypad
• TS0004	4 LED arming station
• TS0006	Heavy Duty keypad
• TS0007	MAG swipe reader with keypad
• TS0008	Mag swipe reader
• TS0801	8 Area RAS
• TS0804	16 Area RAS

- TS0862 Single Door Controller
- CA1110 2 line no reader
- CA1111 4 line no reader
- CA1115 2 line with reader
- CA1116 4 line with reader
- TS0870 Smart card reader range
- TS0870H Smart card reader range
- TS0870D Smart card reader range
- TS1001 Touch Screen RAS
- TS1162 3 LED arming station

Alarm group

With a RAS, you have the option to program an alarm group. See “Area alarm group”. See “[Menu alarm group](#)” below.

A worksheet is provided to record programming details and to further describe this option. See “[RAS worksheet](#)” on page 231.

An area alarm group defines the alarm control functionality that any user can perform at the RAS, subject to the functionality that the user’s alarm group provides. For example, to arm area 1, both the RAS and the user must have alarm system control for area 1. All alarm control options will be taken from the area alarm group programming.

See “[Alarm groups](#)” on page 90 for details.

Select the Alarm group field or the **Open** button next to it to display a list of Alarm groups that may be used with this RAS. Select or create the Alarm group to be used, then press the **OK** button to save. The Alarm group may be cleared from this entity by selecting the  trash icon next to the Alarm group field.

Menu alarm group

A menu alarm group defines which menus that a user can access on the RAS’s LCD screen, subject to the menus that the user’s alarm group provides. For example, to access the Install menu, both the RAS and the user must be permitted to see to the Install menu.

The menu alarm group provides the menus that can be accessed from this RAS regardless of what menus are available in the area alarm group. The alarm group nominated here does not contribute any alarm control functionality to the RAS.

Guidelines for using the menu alarm group:

- The user's alarm group and the RAS's menu alarm group must share at least one area for the user to see any menus on the RAS's LCD screen.
- If different alarm groups are used for the area alarm group and the menu alarm group, then both alarm groups must have the same settings for "alarm system control", "prompt with list of areas", and "keypad duress".
- If two different alarm groups are not needed, then you can assign the same alarm group number to both the area alarm group and the menu alarm group. Alternatively, program the menu alarm group as alarm group 1 (no access) in order to use the area alarm group for both.

Select the Menu alarm group field or the **Open** button next to it to display a list of Menu alarm groups that may be used with this RAS. Select or create the Menu alarm group to be used, then press the **OK** button to save. The Menu alarm group may be cleared from this entity by selecting the  trash icon next to the Menu alarm group field.

RAS Relay

The RAS's output can have any relay number assigned to it that will drive the relay or output on this arming station.

Note: Use a value of 0 for TS0004 and TS0210 RASs.

Select the RAS relay field or the **Open** button next to it to display a list of RAS relays that may be used with this RAS. Select or create the RAS relay to be used, then press the **OK** button to save. The RAS relay may be cleared from this entity by selecting the  trash icon next to the RAS relay field.

Door event

If the RAS is used to unlock a door, assign a door event flag to the RAS. The door event flag will be activated (for the doors unlock time programmed in "[Timers](#)" on page 100) when a valid code is entered at the RAS or a valid card is badged.

Select the Door event field or the **Open** button next to it to display a list of Door events that may be used with this RAS. Select or create the Door event to be used, then press the **OK** button to save. The Door event may be cleared from this entity by selecting the  trash icon next to the Door event field.

RAS Flags

Program the RAS according to its characteristics (for example, if the RAS has an LCD, set the LCD Arming Station option to YES by ticking the checkbox). Refer to [Table 8](#) on page 80 or the specific RAS's installation guide for details. See also "[Using card readers for alarm](#)"

[control](#)” on page 32.

Details of the RAS programming options are as follows:

Reset from RAS without code

Program the RAS to be able to reset without a PIN code.

Note: Applies to RAS models with LCD and keypad, or touch screen, see [Table 8](#) on page 80.

Toggle the option to determine whether a RAS can be reset without a code

- Ticked Reset alarms by pressing [ENTER]
[ENTER] (show alarms) followed by 0 [ENTER].
The areas in alarm must be assigned to the RAS
alarm group.
- Unticked An authorised user code is required to reset
alarms.

Console warning on entry/exit

The RAS can have an audible and visible console warning during entry and exit times.

During the RAS’s entry time period the keypad buzzer will beep and the RAS will display:

Entry,

For the last 10 seconds of the entry time period, the keypad buzzer will sound a constant tone and the RAS will display:

Entry Ending,

Similarly, during the RAS’s exit time period the keypad buzzer will beep and the RAS will display:

Exit,

For the last 10 seconds of the exit time period, the keypad buzzer will sound a constant tone and the RAS will display:

Exit Ending,

The entry time period for the RAS is determined by the maximum of the entry time settings for all associated areas. See [“Entry time”](#) on page 72. Similarly, the exit time period for the RAS is determined by the maximum of the exit time settings for all associated areas. See [“Exit time”](#) on page 72.

Toggle this option to enable or disable console warning keypad buzzer

- Ticked Enable the entry and exit console warnings.
- Unticked Disable the entry and exit console warnings.

Note: Entry and exit console messages are not displayed during alarms.

Door event flag on alarm codes

Door codes must be at least four digits long and are determined by the setting of the alarm prefix length. See [“Number of prefix”](#) on page 106.

Toggle this option to determine whether a door event flag will unlock the door on alarm codes.

- Ticked The door event flag will operate (unlock the door) for either a valid alarm code or a valid door code.
- Unticked The door event flag will operate (unlock the door) only for a valid door code.

Toggle keyboard control

Applies to RAS models with keypad or touch screen, see [Table 8](#) on page 80.

Toggle this option to determine whether or not keypad control is active on this RAS.

- Ticked The [ON] and [OFF] keys lose their function. For arm control the user must enter the user code followed by [ON], [OFF], or [ENTER]. If a list of areas appears, pressing the area number and [ENTER] toggles the status of the area. If no list appears, the status of the areas is toggled immediately.
- Unticked Normal alarm control.

ENTER key opens door only

Applies to RAS models with keypad or touch screen, see [Table 8](#) on page 80. Set this option to YES (tick) for the best user interface on LCD RASs.

Toggle this option to determine whether the ENTER key opens door only.

- Ticked The [ENTER] key unlocks the door but the [ON] and [OFF] keys are used for alarm control. When set to YES, keypad duress functionality requires the use of the [ON], [OFF] or [*] keys — but not the [ENTER] key.
- Unticked The [ENTER] key unlocks the door and also provides alarm control and resets alarms.

Cards arm after three badges

Applies to RAS models with card reader, see [Table 8](#) on page 80.

Toggle this option to allow Badging a card 3 times to arm an area.

- Ticked The assigned areas will arm with three badges of a valid card within 10 seconds (if “[Cards auto disarm](#)” on page 86 is set to YES (ticked)).
- Unticked Normal alarm control.

Card and code

Applies to RAS models with card reader, see [Table 8](#) on page 80.

Toggle this option to allow both a card and PIN code to be entered for access.

- Ticked Both card and PIN are required for access to RAS functions. After the card is presented, the PIN must be entered before the RAS Card and PIN time expires. Card to code time is programmed in timers.
- Unticked PIN alone is required for access to RAS functions.

Restricted user category to disarm

This makes only Restricted user category users to be allowed to disarm.

Toggle this option to only allow restricted user categories users to disarm.

- Ticked Users with user categories cannot manually arm.
- Unticked There is no restriction.

Display shunt on LCD

Applies to RAS models with LCD or touch screen, see [Table 8](#) on page 80.

Toggle this option to show input is shunting on a LCD RAS. Ticked

When an input is shunted, the text ‘Input Shunted’ will appear on the display (LCD RAS only).

- Unticked Nothing is shown when an input is shunted.

Disarm/arm using one key

Applies to RAS models with keypad, see [Table 8](#) on page 80.

Toggle this option to allow users to enter their code followed by a single digit of the area to arm or disarm.

- Ticked After entering the user code, arm or disarm areas by entering the (single- digit) number of the area without pressing [ENTER]. Areas 10 to 99 cannot be controlled from this keypad when this option is set.
- Unticked Normal alarm control.

Note: This option is not compatible with TS1001 Touch Screen RAS.
Do not use.

Cards auto disarm

Applies to RAS models with card reader, see [Table 8](#) on page 80.

Toggle this option to allow cards to auto disarm all areas in a user's area group.

- Ticked The areas assigned to the user and the RAS in their alarm groups will automatically disarm when the card is presented to access.
- Unticked The card only activates the door function unless Card Always Disarms/Arms is set to Yes (ticked), or ON/OFF buttons (TS0064 Expanded Button Interface) are used. Cards always disarm/arms

Applies to RAS models with card reader, see [Table 8](#) on page 80. The card user's alarm group and the RAS's (reader's) alarm group must both allow arm and/or disarm functions before a card can be used to arm and disarm.

Toggle this option to allow cards to always be allowed to disarm / arm.

- Ticked The areas assigned to the user and the RAS in their alarm groups will automatically disarm or arm when the card is presented. Toggle Keyboard Control must be set to YES.
- Unticked The card only activates the door Function unless Card Auto Disarms is set to Yes, or ON/OFF buttons (TS0064 Expanded Button Interface) are used.

LED mapping

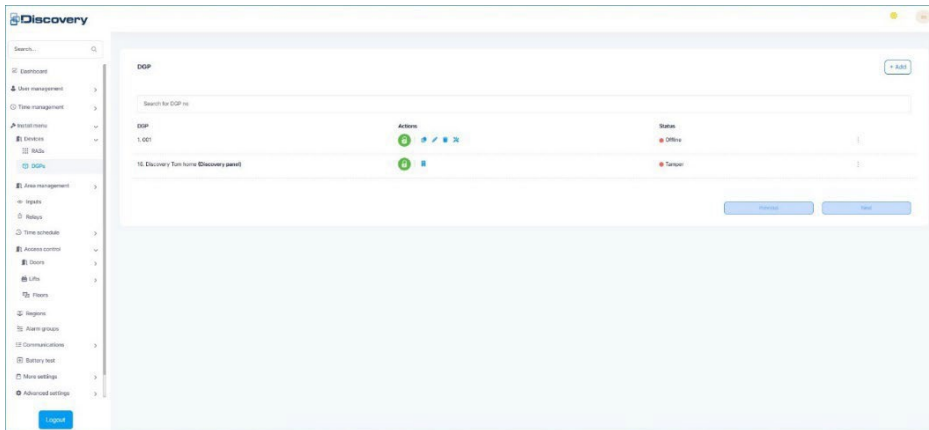
By default, the RAS's area LEDs are mapped to areas 1 to 16.

If you want to assign a different area number to the displayed area LED, choose from the list of LED numbers 1 – 16 and Select the LED (number) field or the **Open** button next to it to display a list of Areas that may be used with this LED. Select or create the Area to be used, then press the **OK** button to save. The Area LED may be cleared from this entity by selecting the  trash icon next to the LED number field.

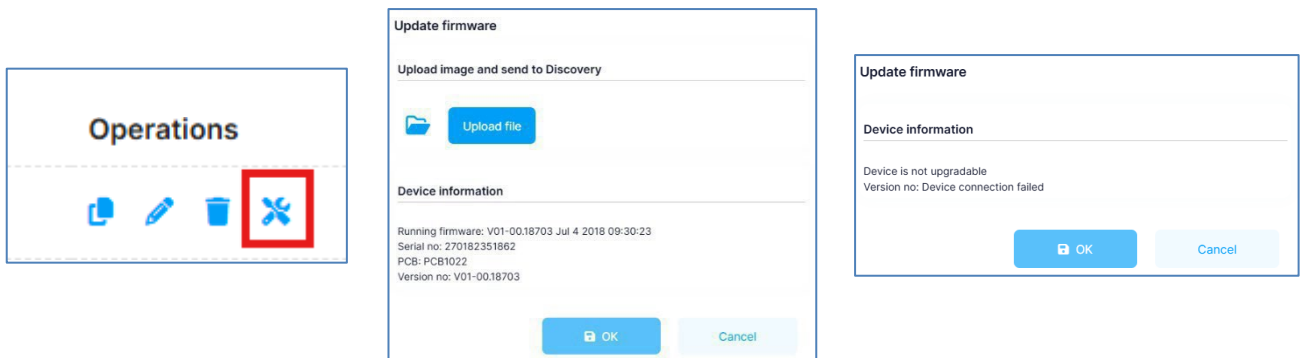
DGP

INSTALL MENU >DEVICES >DGP

Data gathering panels DGP are devices used to send information to the control panel and to provide added access control functionality.



Operations

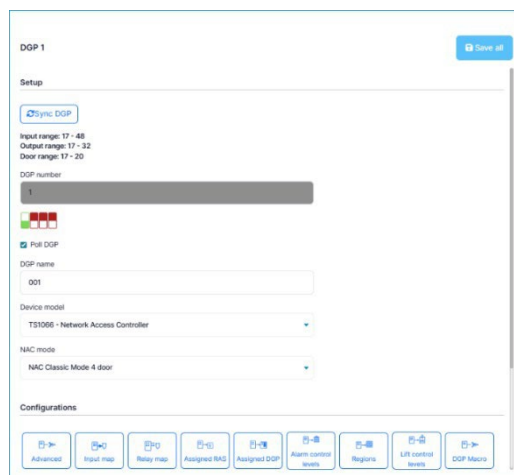


By clicking on the Spanner / Tools icon on the Operations on the DGP page, it will bring up a 'Update firmware' page where you can update firmware of the DGP. These files must be downloaded first to then be able to upload them to your DGP / NAC. If the device cannot be upgraded there will be a note like in the 3rd image above.

Programming DGP's

A worksheet is provided to record programming details and to further describe this option. See [“DGPs worksheet”](#) on page 233.

To program a new DGP, click the **+ Add** button to bring up the Setup page.



Sync DGP

If for example, you have a failure in a DGP and it needs to be replaced, once replaced, click the Sync DGP to send the programming to the new DGP and its connected Devices.

DGP number

Each DGP has a specific number that identifies the DGP to the control panel. DGP numbers must be assigned to physical DGP's.

Enter the DGP's address in the range 1 to 15 on COMM 1 and 17 to 32 on COMM 2.

Poll DGP (checkbox)

Each DGP must be polled to enable communication between the DGP and the control panel. The DGP page display the DGPs status's which can be for example:

- 1. Status: Online
- 2. Polled: Yes
- 3. Mains fail: No

Discovery automatically uses data encryption when connecting to devices that support encryption.

Tick the Poll DGP. Repeat for all DGP numbers to be polled.

Notes:

- DGPs on COMM 1 can be configured with addresses in the range 1 to 15, and DGPs on COMM 2 can be configured with addresses in the range 1 to 16. The first DPG on COMM 1 is configured as DGP 1, and is polled as DGP 1. The first DGP on COMM 2 is configured as DGP 1, but must be polled as DGP 17. Refer to [Table 25](#) on page 204 for details of addressing and polling.
- Only polled DGPs can be retrieved from the panel (such as by retrieving to management software or backing up to SD card).

To deactivate a DGP number that is already polled, untick the Poll DGP on the [Setup](#) page.

Note: Network Access Controllers may be addressed in the range 1 to 12 on COMM 1 and 17 to 28 on COMM 2.

Deactivating a DGP address number clears all alarms for inputs and system points for that DGP address. If the next DGP address number is not polled, alarms on any of the 32 inputs that belong to the DGP are cleared.

DGP Name

Enter a name to identify the DGP (for example, to identify its location and type).

The name may contain up to 30 characters (including spaces).

Device model

Select the DGP model attached to the Discovery panel. This will allow certain options in the panel to be configured to ensure optimal communications.

The model may be selected from a pre-defined list, as detailed in the drop down list:

Table 10: DGP types

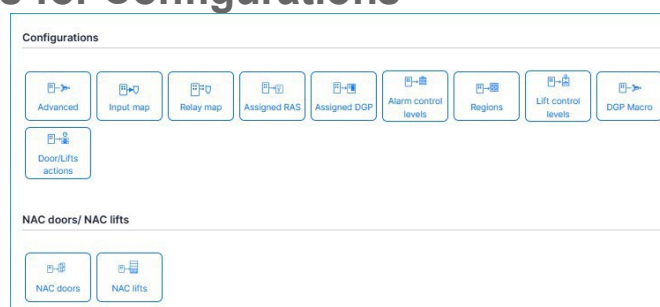
Model number	Description
TS0820	Challenger V8 DGP
TS1020	Challenger10 DGP
TS0825E	Inovonics EchoStream Wireless DGP
TS1066	Network Access Controller <i>Note: When this Model is selected, a Mode number must also be se</i>
TS1061	Dual Wiegand Interface
TS1067	Network Access Controller with Wiegand Interfaces
TS1066-4	4 Door Network Access Controller

NAC mode

This field will self-populate when the NAC Device model is chosen. There is a list consisting of:

- NAC Classic Mode 4 door
- NAC Extended 4 door
- NAC Classic Mode 8 door
- NAC Extended 8 door

Programming tiles for Configurations



More programming can be done for the DGP or NAC and its connected Devices by clicking on these tiles will take to the relevant screen to program and / or add Devices.

Alarm group

INSTALL MENU >ALARM GROUP

Alarm groups enable users, inputs, and RASs to control the system's alarm functions (also called alarm control).

An alarm group's functionality is controlled by the following:

- **Areas**—determines the areas you want this alarm group to control.
- **Time zone**—determines the time zone applicable to this alarm group. Functions assigned via this alarm group will be applicable only for the periods allowed by the time zone (or when the soft time zone is valid). Also, both a user's alarm group time zone and the RAS's (or door's) alarm group time zone have to be valid.
- **Menus**—determines access to the Discovery User menus that the user will have for this alarm group (see [Table 2](#) on page 11).
- **Options**—determines access to system functions that the user or RAS will have for this alarm group. If you do not select User Alarm Group, then you will not be able to assign the alarm group to any user.**Alternate alarm group**—used whenever the original alarm group is disabled due to an invalid time zone.

Alarm groups can be assigned to:

- Users
- RASs 1 to 16 and 65 to 80
- Doors 17 to 64 and 81 to 128
- Area control input types 6, 31, 34 and 35
- Auto reset functionality
- Arm or disarm via time zone functionality

Alarm groups provide enormous flexibility when determining a user's access to, and control of, the system.

Note: You must be extremely careful when changing alarm groups. Both the functions performed by user in the alarm group and the functions available at RASs with that alarm group will be affected.

A function that is provided to users via their alarm group is only valid when:

- Program settings in other sections of the same alarm group allow it. Example: Restricting alarm system control to Reset Only would be invalid unless the alarm group has allowed alarm system control. If Reset Only is set to YES, Alarm System Control must be set to YES.
- The user's alarm group has the same program setting as the alarm

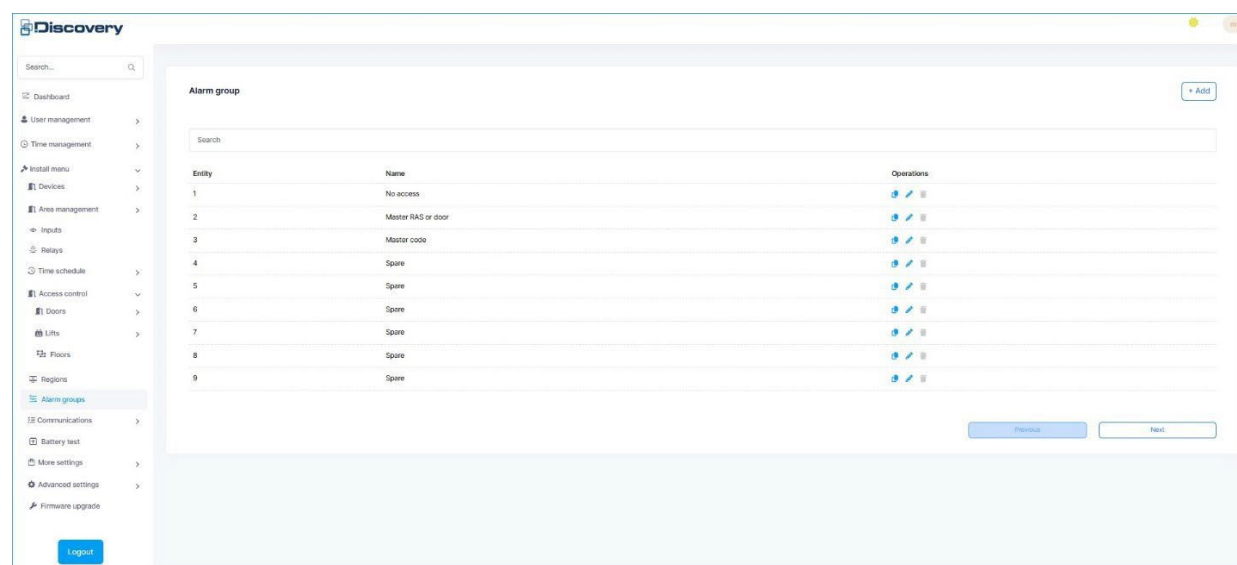
group of the RAS or door the user is using. Example: If the Prompt with List of Areas is set to YES in the user's alarm group, it must also be set to YES in the alarm group of the RAS or door. If it is not, areas are not listed when arming/disarming.

- The user's alarm group includes the areas assigned to the alarm group of the RAS or door the user is using. Example: If a user's alarm group has areas 1, 2, and 3 and the alarm group of the RAS or door has areas 2 and 3, only the functions for areas 2 and 3 are valid.

Alarm group application

Alarm groups may be fixed or have programmable options, as listed in [“Alarm group default settings”](#) on page 219. Alarm groups are used as follows:

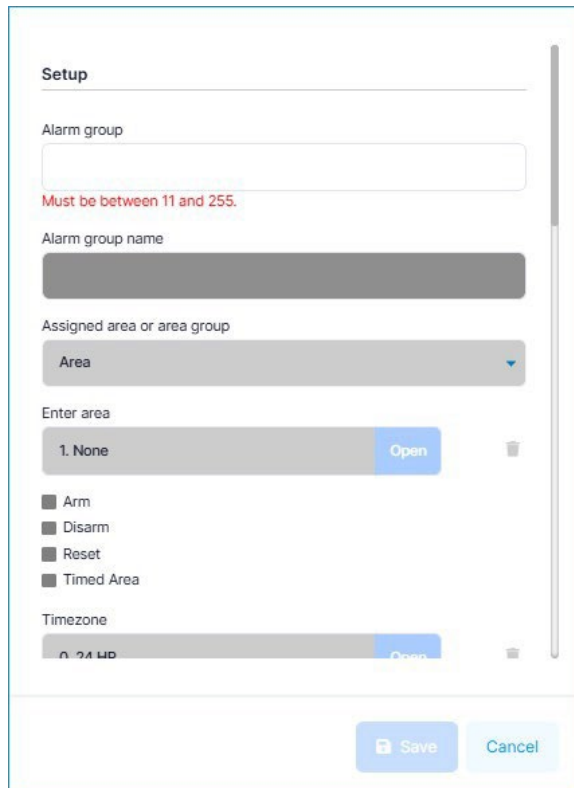
- Alarm Group 1 “No Access”
- Alarm Group 2 “Master RAS or Door” contains Area Group 1 and the default settings for the master RAS (RAS 1 on COMM 1).
- Alarm Group 3 “Master Code” is fixed. It contains Area Group 1 and the default settings for the master user 50 (Installer). Alarm groups 4 to 10 are spare. Do not use.
- Alarm Group 11—High Level User Master contains Area Group 1 and all User menus except 19—Install.
- Alarm Group 12—Low Level User Master contains Area Group 1 and User menus 1, 5, 9, 10, 11, 14, 15, and 16.
- Alarm Group 13—All Area User Code contains Area Group 1 and User menus 1, 5, 9, 10, and 11.
- Alarm Groups 14 to 29 are intended for RASs that control a single area and User menus 1, 5, 9, 10, and 11.
- Alarm Groups 30 to 255 have no default programming and are intended to be programmed for users or RASs according to the system requirements.



Programming alarm groups

A worksheet is provided to record programming details and to further describe this option. See “[Alarm group worksheet](#)” on page 234.

To program a new Alarm group, click the **+ Add** button to bring up the Setup page.



The screenshot shows the 'Setup' page for an alarm group. It includes the following fields and controls:

- Alarm group:** A text input field with a red error message below it: "Must be between 11 and 255."
- Alarm group name:** A text input field.
- Assigned area or area group:** A dropdown menu currently showing "Area".
- Enter area:** A section with a list of areas (currently showing "1. None") and an "Open" button to browse for an area.
- Permissions:** Four checkboxes labeled "Arm", "Disarm", "Reset", and "Timed Area".
- Timezone:** A dropdown menu currently showing "0: 24 HR" and an "Open" button to browse for a timezone.
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

Alarm group

Each alarm group has a specific number that identifies the alarm group to the control panel. Alarm group numbers may be assigned to the Alarm group.

Alarm group name

Enter the Alarm group name, up to 30 characters (including spaces).

Assigned area or area group

An alarm group can be linked to a single area or to an area group.

When linked to a single area, the alarm group controls the area's permissions for arming, disarming, alarm reset, and for timing.

When linked to an area group, the area group controls each area's permissions for arming, disarming, alarm reset, and for timing.

Use the drop-down list to select whether to link the alarm group to an Area or an Area group. Select the area or area group by clicking the Browse button, or type the area or area group number directly into the field.

If a single area is selected, click the check boxes to enable the area's permissions for arming, disarming, alarm reset, and for timing.

Enter Area / Area group

Enter either an area or an area group.

Arm

Tick this check box if the area can be armed.

Reset

Tick this check box if the area can be reset.

Disarm

Tick this check box if the area can be disarmed.

Timed area

Tick this check box if the area may be disarmed for a timed interval. The Disarm check box must also be Ticked.

Time zone

This defines the time zone applicable to this alarm group. Functions restricted/available via this alarm group will be applicable only for the periods allowed by the selected 'hard' panel time zone or soft time zone.

Select the time zone by clicking the Browse button, or type the time zone number directly into the field.

Alternate alarm group

Each alarm group may have an alternate alarm group. These alarm groups are only used when the original alarm group records a time zone with access times which are invalid when a function is attempted. If the time zone of the original alarm group denies access, the alternate is checked.

Note: The alternate alarm group may also be programmed with an alternate alarm group and so on – up to three alarm groups (the original plus two alternates). If a function is denied by the time zone of one alarm group, the next will be checked (and so on). In this way, opposing functions may be made available at different times, days, etc.

Select the alarm group by clicking the Browse button, or type the alarm group number directly into the field.

Options (checkboxes)

Users alarm group

When programming a new user record in the User menu. Program Users, a list of designated “user alarm groups” are displayed on the RAS for assigning to the new user. The list of designated “user alarm

groups” depends on the alarm group (and alternate alarm group, if applicable) of the person doing the programming. You cannot assign an alarm group to a new user that has more permissions than you have.

Toggle this option to allow Alarm groups to be assigned to users

- Ticked This alarm group can be assigned to users.
- Unticked This alarm group is only assigned to an input door, RAS, auto reset, or arm/disarm via time zone.

Remote access

- Ticked UltraSync and modem access with VT100 terminal (or terminal emulation software) is allowed by a user with this alarm group. If using the VT100 terminal, RAS 16 must have a suitable alarm group assigned to specify functions available (for example, alarm group 2) and be programmed as an LCD RAS. The RAS does not need to be polled.

This option does not apply to system management software unless connecting over UltraSync.

Alarm system control

When programming this option a user or RAS with this alarm group can arm or disarm the areas in the alarm group

Toggle this option to allow alarm system control for a User

- Ticked A user or RAS with this alarm group can arm or disarm the areas in the alarm group. This option must be set to YES if any of the user categories in the alarm group are set to YES.
- Unticked Do not enable alarm system control.

Access control functions and user menu options specified are still valid.

Reset system alarms

Programming this option allows a user to reset latching system alarms.

Toggle this option to allow or disallow a user to disarm latching alarms.

- Ticked A user with this alarm group can reset the latching system alarms. The user’s alarm group must allow arming, disarming, and resetting; and “System Alarms” on page 91 must also be set to YES.
- Unticked A user cannot reset latching system alarms.

Prompt with list of areas

Programming this option prompts the user with a list of areas once they have entered their PIN code.

Toggle this option prompts the user a list of areas when PIN is entered.

- Ticked After the user has entered a PIN and pressed [ON] or [OFF], the areas assigned to the user are displayed. The user can then select from the arm/disarm options.
- Unticked The areas assigned to the user are not displayed. Areas are immediately armed/disarmed once the user has entered a PIN and pressed [ON] or [OFF].

Keypad duress

This option allows users to activate a duress alarm on the RAS keypad. Toggle this option to allow a user to be able to activate a duress alarm by using the RAS keypad.

- Ticked A user with this alarm group can enter a duress code on a keypad to activate a Duress alarm.
- Unticked Keypad duress cannot be activated. A duress code is treated as an invalid code. See also “Using keypad duress” on page 48.

User categories (1 through 8)

User categories assigned to an alarm group provide timing functionality via a corresponding user category time (see “[User category](#)” on page 5 and “[User category time](#)” on page 101).

If multiple user categories are assigned to an alarm group, then the lowest user category number applies. System functionality can depend on the alarm group assigned to a user, and the alarm group assigned to a RAS. In these cases, the lowest common user category number applies.

For example, if a user has an alarm group containing user categories 3 and 4, and a RAS has an alarm group containing user categories 1, 2, 3, and 4, then only user category 3 would apply to that user at that RAS.

Toggle this option to allow the user category activates when a user with this alarm group enters their PIN (or badges their card).

- Ticked Activates the displayed user category.
- Unticked The displayed user category is not activated.

Auto isolate

Programming this option will auto isolate alarm inputs when arming starts without causing them to alarm.

Toggle this option to allow this option to auto isolate alarm inputs without making them go into alarm.

- Ticked When the arming starts, all unsealed inputs are automatically isolated and the system is armed without causing an alarm. Alarm system control must also be set to YES.
- Unticked The system cannot be armed if there are unsealed inputs, unless "Forced arming when inputs unsealed" below is set to YES.

Forced arming

Forced arming will force the unsealed alarm inputs to be ignored and cause the alarm.

Toggle this option to allow or disallow the forced arming to occur.

- Ticked The check for unsealed inputs is ignored. If there are unsealed inputs when the arming procedure is started, the system still arms (the unsealed inputs might cause an alarm).
- Unticked The system cannot be armed if there are unsealed inputs, unless "Auto isolate unsealed inputs" on page 40 is set to YES.

Note: See "[Enable exit fault reporting](#)" on page 111 if you want to report alarms from non-entry/exit type inputs as "exit error alarms".

Prevent forced disarming

This setting controls the treatment of unsealed inputs during the disarming procedure and may be used if there are access alarm input types such as type 1 or type 11 in the system.

Toggle this option to prevent forced arming

- Ticked The area cannot be disarmed if there are unsealed inputs.
- Unticked The area can be disarmed even if there are unsealed inputs.

Prevent area arming if not timing

This option prevents the area from being automatically rearmed without a user category. For example, a guard might have a user category that automatically re-arms an area when the user category

timer expires. However, if someone else disarmed the area (the user category timer isn't running), then the guard's user category will not automatically re-arm the area.

Toggle this option to prevent automatic re-arming when an area is occupied by non-user category staff

- Ticked Prevents automatic re-arming when an area is occupied by non-user category staff.
- Unticked Normal user category programming applies.

Disable auto-deisolate

Select this option to prevent certain users (for example, cleaners) from being able to automatically deisolate inputs in the area they disarm.

Toggle this option to disable a user's ability to automatically deisolate inputs in the area they disarm.

- Ticked A user with this alarm group can disarm areas with isolated inputs remaining
Isolated even if the system is programmed to automatically deisolate (sealed) isolated inputs.
- Unticked Disarming the area will automatically deisolate sealed and isolated inputs in the area if the system is programmed to automatically deisolate inputs.

See also "Automatic deisolate".

Enable area search

When enabled, a user with this alarm group must perform an area search as part of the disarming process during the "Area Search TZ" specified in System Options). See "[Using Area Search](#)" on page 50 for details.

- Ticked Enables an area search
- Unticked Disables an area search

Menu (checkboxes)

The Menus tab determines which user functions will be available (via an LCD RAS) to users with this alarm group, or on a RAS with this alarm group. Each user menu option is displayed and must be Ticked for it to be available to the alarm group (and therefore the user or RAS). The user options available for selection are summarised below. Refer to the Challenger Series Administrators Manual or ChallengerPlus Administrators Manual for details.

No.	RAS Menu	Description
1	Panel Status	A user with this option enabled can list any inputs which are in alarm, isolated or unsealed. There are menu options available which display each of these conditions separately, however, this option may be used to check on all inputs which need attention.
2	Input Unsealed	A user with this option enabled can see all unsealed inputs, for example, door open. The function would be used to determine whether you need to check an input in order to maintain security. For example, close the door.
3	Input In Alarm	A user with this option enabled can see details of all inputs which are in alarm and tamper alarm. Alarms should be acknowledged and reset.
4	Input Isolated	A user with this option enabled can see details of all isolated inputs. An isolated input is one which is excluded from functioning as part of the security system. It would be isolated because it is faulty or broken and by isolating it you would stop it causing an alarm. This function would therefore be used to determine which inputs are not operational and need attention.
5	History	A user with this option enabled can see past events of system history, including alarms, access to the menu etc. It can help you determine events such as time that an alarm occurred, the time it was reset and who reset it, the time the system was disarmed in the morning etc. The events are displayed in reverse chronological order, i.e. the last event is the first shown.
6	Test Report	A user with this option enabled can see the results of the Secure Test which is done on specific inputs to see if they were operating correctly. The inputs are those that are programmed to be included in testing and which operate when a building is unoccupied.
7	Service Menu	A user with this option enabled can request a service call or to establish connection to a remote service centre to allow programming over the telephone network.
8	Film Counters	A user with this option enabled can see the current frame number position on each of the security camera films. If you maintain a log on frame counts it will indicate whether the cameras have operated since they were last checked.
9	Input Text	A user with this option enabled can see the text that is programmed as a description of the inputs in your system.

10	Isolate	A user with this option enabled can isolate inputs i.e. exclude them from functioning as part of the security system. An input would be isolated because it is faulty or broken and by isolating it, you would stop it causing an alarm. The function provides a list of unsealed inputs for you to select an input to isolate. A faulty or broken input is usually unsealed; however, sealed inputs may also be isolated if you know the input number.
11	Deisolate	A user with this option enabled can de-isolate inputs, i.e. return them back to functioning as part of the security system. An input is isolated because it is faulty or broken and when it is repaired it must be de-isolated.
12	Test Input	A user with this option enabled can test an individual input device to determine if it is operating correctly.
13	Start Auto Access Test	A user with this option enabled can start the access test.
14	Program Users	A user with this option enabled can add, delete or change a user. Your system may have been set up to require two authorised users to enter this menu.
15	Time & Date	A user with this option enabled can program a new time and date. The time and date are not visible during normal use of the Challenger; however, all internal functions are reliant on them. A new date or time would only need to be programmed when the Challenger is first installed or if the time needs to be adjusted for daylight saving. The time is programmed for a 24 hour clock.
16	Isolate/Deisolate RAS/DGP	A user with this option enabled can isolate or deisolate RASs and DGPs.
17	Enable/Disable Service Tech	A user with this option enabled can enable and disable the service technician's code. (Activates time zone 25 when service is enabled and deactivates time zone 25 when service is disabled).
18	Reset Camera	A user with this option enabled can reset the film frame count on a security camera to zero, or change the frame count number on an individual camera. This would be necessary when you change the film in the camera.
19	Install Menu	A user with this option enabled can access the Install Menu. Caution is to be taken over who is given access to this option.
20	Door and Floor Groups	A user with this option enabled can program door and floor groups.
21	Holidays	A user with this option enabled can record the date of holidays. The holidays recorded here may be used in

conjunction with time zones to control access (for example, staff who are allowed access during normal weekdays can be denied access on weekdays declared a holiday). The Challenger is capable of recording up to 24 holiday dates.

- | | | |
|----|----------------------------------|--|
| 22 | Open Door | A user with this option enabled can open a door via an LCD RAS. |
| 23 | Unlock, Lock, Disable and Enable | <p>A user with this option enabled can unlock, lock, disable, and enable a valid door via an LCD RAS. Depending on the type of panel, the door range this will work with may be different. For example:</p> <p>ChallengerPlus: Doors 1 - 128
 Challenger10: Doors 17 - 64 and 81 - 128
 ChallengerLEPlus: Doors 1 - 18</p> |
| 24 | Automation Control | A user with this option enabled can manually control automation zones via LCD RAS. |

Timers

INSTALL MENU > MORE SETTINGS > TIMERS

Timers are accurate on ± 1 of the value entered, so a timer set for 20 seconds will end somewhere between 19 and 21 seconds. Therefore, avoid using values of 1 second or 1 minute.

Programming timers

A worksheet is provided to record programming details and to further describe this option. See "[Timers worksheet](#)" on page 235.

Enter the timers for each field needed and then click **Save all**

Siren time (min)

Siren time is the interval that the onboard internal siren drivers activate.

Enter the time.

RAS door open (sec)

Door(s) unlock time is the interval that doors will unlock (using the door event flag) to allow doors to be opened. This time value is common for all door event flags from RASs connected to the control panel (doors 1 to 16 and 65 to 80). Doors 17 to 64 and 81 to 128 are connected to DGPs and are individually programmed via the DGP.

Enter the time.

RAS card and PIN timeout (sec)

On RASs where card and PIN code are required, the card to PIN code time is the delay between badging the card and entering the PIN.

Enter the delay time.

Twin trip maximum time (sec)

Enter the maximum amount of time that a twin trip timer may run.

See "[Programming twin trip inputs](#)" on page 58 for details.

User category 1 – 8 time (min)

Program times for user categories 1 through 8 for the time that the user category timer is to run.

Note:

- If set to "0", the areas will not arm automatically.
 - The user category time will be overridden by the area disarmed time (if programmed) in the area database.
-

Enter the time in minutes for user category 1. Repeat for user categories 2 through 8.

Warning time (min)

When user categories are used and areas are timed, a warning will sound (if a warning time is programmed) indicating the areas are about to arm.

Enter the time this warning will sound.

The warning time must always be set for a shorter time than any user category disarmed time. The warning time must always be shorter than the shortest user category time and should be at least 2 minutes.

Suspicion (sec)

Suspicion time is the interval that a camera continues to operate after a

suspicion input type (7, 40, or 47) has switched to sealed state. Enter the time in seconds.

Service (min)

User menu 17 can be used to give access to service technicians. The alarm group for the technician needs time zone 25 to be assigned. When a user enables the service technician, time zone 25 will be valid during the service time.

Enter the service time in minutes.

Access test (min)

Enter the time to perform the access test.

Secure test (min)

Enter the time to perform the secure test.

Local alarm reminder (min)

Local alarm reminder time is the interval that can elapse between acknowledging a local alarm and a re-alarm occurring, including the audible alert. Enter the time.

Mains fail time (min)

Mains fail time is the interval before a mains fail is reported to the remote monitoring company. Enter the delay time. Enter a value of "0" for no delay.

Delay holdup (sec)

Delay holdup time is the interval before an alarm from a delayed input type (for example, a holdup alarm) is reported to the remote monitoring company (the delay time is ignored if another delayed input type has already been activated).

Enter the delay time in seconds.

Individual test (min)

Individual input test time is the interval to perform a test on an individual input, using User menu 12, Test Input. Enter the maximum time.

Tester event (sec)

Tester event flag time is the interval that the tester event flag is triggered to activate devices in order to perform a secure test.

Note: The event flag will only be triggered for half the programmed time; the remaining time is used to allow the device to switch back to sealed state. The event flag used is preset to 16.

Min area search (min)

Enter the smallest amount of time in which an area search may be completed. See "[Using Area Search](#)" on page 50 for details.

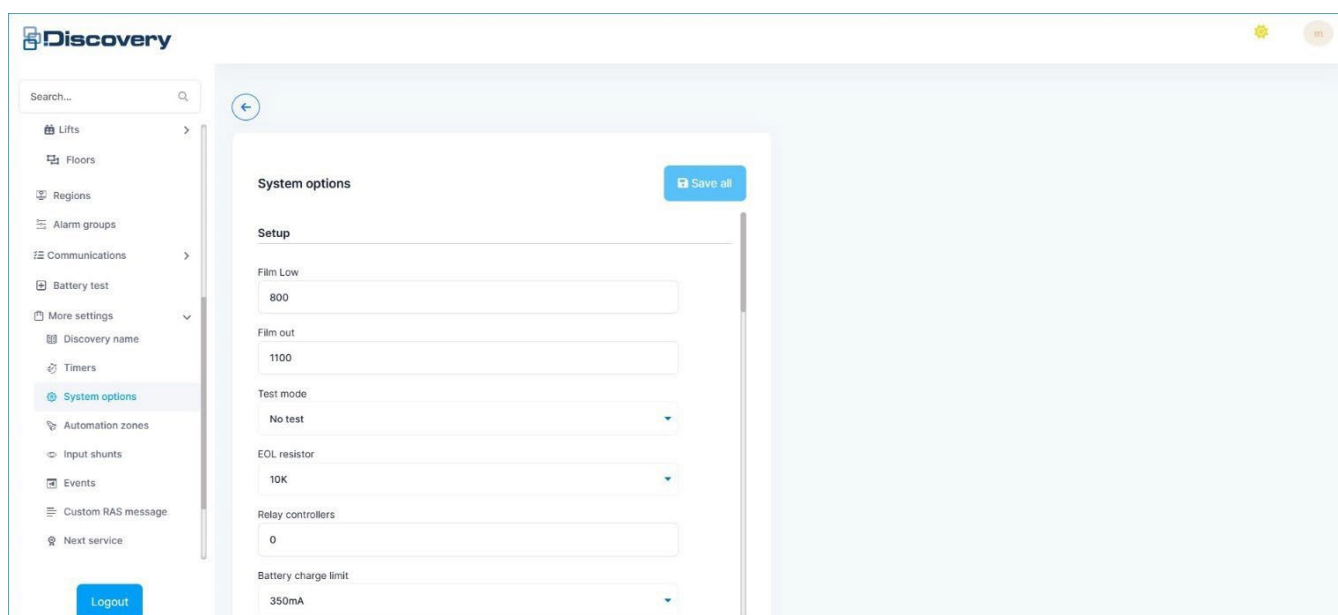
Max area search (min)

Enter the largest amount of time in which an area search may be completed.
See [“Using Area Search”](#) on page 50 for details.

System options

INSTALL MENU > MORE SETTINGS > SYSTEM OPTIONS

The Discovery panel has a series of System options that can be adjusted to suit site conditions and requirements.

The screenshot shows the 'Discovery' web interface. On the left is a sidebar menu with options: Lifts, Floors, Regions, Alarm groups, Communications, Battery test, More settings (expanded), Discovery name, Timers, System options (highlighted), Automation zones, Input shunts, Events, Custom RAS message, and Next service. A 'Logout' button is at the bottom of the sidebar. The main content area is titled 'System options' and contains a 'Save all' button. Under the 'Setup' section, there are several fields: 'Film Low' (text input with value 800), 'Film out' (text input with value 1100), 'Test mode' (dropdown menu with 'No test' selected), 'EOL resistor' (dropdown menu with '10K' selected), 'Relay controllers' (text input with value 0), and 'Battery charge limit' (dropdown menu with '350mA' selected).

Programming system options

A worksheet is provided to record programming details and to further describe this option. See [“System options worksheet”](#) on page 236.

Enter the System options for each field needed and then click **Save all**.

Film low

Film low level is the camera count value for input types 23 to 26 and 36 to 39 at which a film low report is sent to the remote monitoring company.

Film out

Film out level is the camera count value for input types 23 to 26 and 36 to 39 at which an out-of-film report is sent to the remote monitoring company.

Test mode

The test mode setting defines whether a secure test or an access test (input testing interval) starts automatically upon arming or disarming areas that contain the input. Testing of inputs involves monitoring the state of the input whilst changing its state from sealed to unsealed, and then back to the

sealed state.

This is typically done by, for example, opening and closing a door and then checking the LCD screen to verify that the change was correctly reported. Refer to Testing Input Devices in *Discovery Administrator's Manual* for details.

Regardless of the programmed test mode, inputs may also be tested via:

- User menu 12 Test Input
- User menu 13 Start Auto Access Test
- Normal operation over a number of days (see "[Test input within no. of days](#)" on page 68).

See also the chapter "Test option" on page 71 for related programming.

Enter the desired the test mode from the list below.(see Table 11 below).

Table 11: Test modes

Option	Function
No Test	Input testing intervals are not started automatically upon arming or disarming.
Enable Auto Test	The access test starts automatically when the system is disarmed. The secure test starts automatically when the system is armed.
Manual Access Test/Auto Secure Test	The secure test starts automatically when the system is armed.
Auto Access Test Only	The access test starts automatically when the system is disarmed.

For the auto access test to operate, at least one area must be programmed as a vault area. If the system contains a vault area, then the access test operates as follows:

- Disarming the vault area only, starts the access test on the vault area only.
- Disarming all areas (including the vault area), starts the access test on all areas.
- Disarming the non-vault areas only does not start the access test.

EOL resistor

The Discovery system normally uses the default 10 kΩ End-Of-Line (EOL) resistor value to detect the electrical states of input circuits. This option is used to apply a different EOL resistor value to the 16 zone inputs connected to the Discovery panel.

Enter one of the following EOL resistor values:

- 10K (default)
- 4K7
- 2K2
- 6K8
- 5K6
- 3K7
- 3K3
- 2K0
- 1K5
- 1K0
- 2K2/6K8 (see note below)

Relay controllers

The value in this record indicates the number of (8-way) relay controllers that are fitted to the main control panel (do not enter values for relay controllers fitted to DGPs). The range of values begins at 0 to indicate either no relay controller or one TS0840 4-Way Relay Card fitted to the control panel (if a TS0840 is fitted, no other relay controller may be used on the panel simultaneously).

If relay controllers are fitted (other than TS0840), use a value greater than 0 where 1 represents every 8 relays available. For example:

- Enter 1 for one TS0841 8-Way Clocked Relay Card.
- Enter 2 for two TS0841 8-Way Clocked Relay Cards.
- Enter 2 for one TS0842 16-Way Open Collector Card.
- Enter 3 for one TS0841 8-Way Clocked Relay Card and one TS0842 16-Way Open Collector Card.
- Enter 4 for two TS0842 16-Way Open Collector Cards.

The numbering system allows for 32 relay controllers, which is considerably more than is practicable. In reality, the workable limit for a series of relays is about 144, which limits the number of 8-way relay controllers to a total of 18; or 16-way open collector cards to a total of 9. If more than 144 relays are required, it's best to connect the additional relays via DGPs.

Enter 0 if a TS0840 4-Way Relay Card is connected to the panel, and then press [ENTER]. Alternatively, enter a value greater than 0 where 1 represents every 8 relays available, and then press [ENTER].

Note: We recommend powering only one relay controller directly from the Discovery panel via the 10-way ribbon cable. Do not use the 10-way ribbon cable to power daisy-chained relay controllers.

Alarm prefix digits

User PINs (four to ten digits long) may be used for both alarm control and access (door) control, depending on the setting of “[Door event flag on alarm codes](#)” on page 84.

The alarm code prefix value in the range one to four enables users to enter a door code (a shorter PIN) for access control.

For example, if a user’s full PIN is six digits long (for example, 123456), and the alarm code prefix value is 2, then the first two digits are removed for access control, and the user can operate doors by entering only the last four digits of the PIN (for example, 3456).

The door code must be at least four digits long. Table 12 below lists the prefix values that may be used for PINs of various lengths.

Enter the prefix value in the range one to four, and then press [ENTER].

Table 12: Acceptable ranges of alarm code prefix values

User PIN length (digits)	Alarm code prefix value	Resulting door code length
4	0	not applicable
5	1	4
6	1, 2	5, 4
7	1, 2, 3	6, 5, 4
8	1, 2, 3, 4	7, 6, 5, 4
9	1, 2, 3, 4	8, 7, 6, 5
10	1, 2, 3, 4	9, 8, 7, 6

Battery charge limit

Use this option to choose your back up battery’s charging limit. Choose from the following:

- 350 mA
- 550 mA
- 850 mA

Note: Consult your battery specifications and the Discovery Installation an quick programming manual to choose the correct settings.

Time before rotate

LCD RASs that have small displays (for example, 16-character LCD screens) scroll longer strings of text in order to display entire messages. This scrolling is referred to as ‘rotation’.

When a long message displays, the text rotation begins after a configurable delay. If you wish to change the delay time, enter a time value in the range 1 to 15 (a value of 0 uses the default delay time of 8).

Use a value in the range 1 to 7 for delay times less than default, or a

value in the range 9 to 15 for delay times greater than default, and then press [ENTER].

Rotate speed

LCD RASs that have small displays (for example, 16-characters LCD screens) scroll longer strings of text in order to display entire messages. This scrolling is referred to as 'rotation'.

When a long message displays, the speed of the text movement is configurable. If you wish to change the text speed, enter a time value in the range 1 to 15 (a value of 0 uses the default speed of 8).

Use a value in the range 1 to 7 for more speed than default, or a value in the range 9 to 15 for less speed than default, and then press [ENTER].

Area search time zone

If Area Search functionality is required, enter the number of the soft or 'hard' time zone that will be used to trigger area search. See "[Using Area Search](#)" on page 50 for details.

Select the Area search time zone field or the **Open** button next to it to display a list of Area search time zones that may be used with this system. Select or create the Area search time zone to be used, then press the **OK** button to save. The Area search time zone may be cleared from this entity by selecting the  trash icon next to the Area search time zone field.

Card learn RAS

A card reader RAS can be used to enter a user's card data (card bits) into the Discovery system by presenting (badging) the card at the reader during the user creation process via RAS, not via management software.

Enter the card reader's RAS address in the range 1 to 16 or 65 to 80. The default setting is RAS 1.

Select the Card learn RAS field or the **Open** button next to it to display a list of Card learn RAS's that may be used with this system. Select or create the Card learn RAS to be used, then press the **OK** button to save. The Card Learn RAS may be cleared from this entity by selecting the  trash icon next to the Card learn RAS field.

Decrement test days during time zone

When using timed input testing (see "[Using timed input testing](#)" on page 53), you can assign a time zone in order to specify which days the system uses to check whether inputs have been tested. The default is time zone 0. 24 HR (always valid). Enter the time zone (other than 0) that you defined to tell the panel what days of the week to use for timed input testing (for example, Monday through Friday).

Select the Decrement test days during time zone field or the **Open** button next to it to display a list of time zones that may be used with this system.

Select or create the time zone to be used, then press the **OK** button to save. The time zone may be cleared from this entity by selecting the  trash icon next to the Decrement test days during time zone field.

Event text

When input types 57 (Input to report and screen) or 58 (Input to screen text) are active, the text specified here (up to 16 characters including spaces) is displayed on LCD RASs.

External siren mode

Discovery panels can support an 8 Ω external siren or an external device that requires 12 Volt DC power.

Choose either Standard sirens, or DC Volts.

Warning: Specifying an external siren type of DC Volts when there is an 8 Ω external siren connected to the panel may damage the siren.

Internal siren mode

Discovery panels can support an 8 Ω internal siren or an internal device that requires 12 Volt DC power.

Choose either Standard sirens, or DC Volts.

Warning: Specifying an internal siren type of DC Volts when there is an 8 Ω internal siren connected to the panel may damage the siren.

Time zone

Discovery panels may be located in various remote regions. The time zone setting is used to indicate regional time zone (and DST combinations) when events are reported to the central monitoring station.

Choose a time zone to select from the following options:

- TZ_NONE_SET (default)
- Australia/Brisbane
- Australia/West
- Australia/Tasmania
- Australia/Lord_Howe
- Australia/NSW
- Australia/Queensland
- Australia/Lindeman
- Australia/ACT
- Australia/LHI
- Australia/North

- Australia/Perth
- Australia/South
- Australia/Sydney
- Australia/Melbourne
- Australia/Broken_Hill
- Australia/Canberra
- Australia/Victoria
- Australia/Tasmania (Currie, King Island belongs to Tasmania)
- Australia/Darwin
- Australia/Yancowinna
- Australia/Adelaide
- Australia/Hobart
- Australia/West
- NZ

Note: If UltraSync is enabled, please disable it to edit timezone.

Total area or area group disarm

Choose either **Area** or **Area group** from the drop down list.

Area

Select the Area field or the **Open** button next to it to display a list of Areas that may be used with this system. Select or create the Area to be used, then press the **OK** button to save. The Area may be cleared from this entity by selecting the  trash icon next to the Area field

Area group

Select the Area group field or the **Open** button next to it to display a list of Area groups that may be used with this system. Select or create the Area group to be used, then press the **OK** button to save. The Area group may be cleared from this entity by selecting the  trash icon next to the Area group field.

RAS display (checkboxes)

Input tamper monitoring

This setting determines whether the system can detect two input states (sealed and unsealed) or four input states (sealed, unsealed, open, and short). When input tamper monitoring is enabled, open or short conditions are both reported as an input tamper alarm (subject to input type, see “[Input types](#)” on page 208).

The following example is based on a system where every input has two end-of-line (EOL) resistors to enable the panel to detect whether an input is sealed, is in alarm, or is in tamper.

The default EOL resistor value is 10 kΩ, and the details below are based on the default. See “EOL resistor” on page 112.

Toggle this option to reveal input tampering

- Ticked Input tamper monitoring is used:
 - Seal = 10 kΩ
 - In alarm = 5 or 20 kΩ
 - Fault = open or shorted.
- Unticked Input tamper monitoring is not used:
 - Seal = 10 kΩ
 - In alarm = open or shorted or 5 or 20 kΩ

Note: Refer to the *Discovery Installation and Quick Programming Manual* for resistance values for all EOL resistor options.

Auto de-isolate when area accessed

This setting allows automatic deisolation of an area when its accessed.

Toggle this option to allow or not allow areas to be deisolated when area is accessed

- Ticked Inputs that are sealed and isolated are deisolated when any of the areas assigned to the inputs are disarmed.
- Unticked Inputs that are sealed and isolated remain isolated (are not deisolated). See also “Disable auto-deisolate” on page 93.

Disable insert of user category

This setting allows disablement of the special procedures for automatically timing on non-vault areas when arming vaults.

- Ticked Disables the special procedure for automatically timing on non-vault Areas when arming vaults.
- Unticked Enables the special procedure for automatically timing on non-vault

Areas when arming vaults, provided all applicable values are programmed. See also “[Vaults](#)” on page 151.

Financial options

When enabled (**ticked**), the following special options apply (generally applicable to financial institutions):

- Film counters are enabled during the access test mode.
- Minimum PIN length is set to five digits.

The area search procedure for financial institutions applies (see [“Using Area Search”](#) on page 50).

Enable exit fault reporting

Exit fault reporting is used to indicate to the alarm reporting centre that an unsealed input has gone into “exit error alarm” (CID 374) by being unsealed when the exit timer is running. This is typically caused by a user arming the system when inputs are not sealed, as permitted by the user's Alarm Group option [“Forced arming when inputs unsealed”](#) on page 96.

The exit timer suppresses alarms from entry/exit input types (3, 4, 13, 14, 41, and 42) but does not suppress alarms from other inputs.

If exit fault reporting is not used, or if the input is still unsealed after the exit timer expires, then the input's programmed CID code is reported.

Toggle this option to determine if exit fault reporting is enabled.

- Ticked Enables exit fault reporting
- Unticked Exit fault reporting disabled.

System alarms set siren and strobe

Dedicated tamper inputs on the control panel and the DGPs activate the siren and strobe when in alarm.

Toggle this option to enable dedicated tamper inputs to activate the siren and strobe when in alarm.

- Ticked The dedicated tamper inputs on the control panel and the DGPs activate the siren and strobe when in alarm.
- Unticked The system alarms report and activate event flags only.

Enable expanded test reporting

Enables the use of the “Test Input Within No. of Days” functionality (timed input testing), which is programmed individually for inputs. This option provides system-wide control over this functionality.

Toggle this option to enable or disable timed input testing.

- Ticked Timed input testing enabled
- Unticked Timed input testing not used.

Sirens only after report fail

Siren event flags are activated on alarms, and report fail is registered, if the Discovery panel has failed to report to the remote monitoring company, as specified for the communication path's dial settings. The siren activates for the normal siren cut-off time programmed. See [“Report fail event flag”](#) on

page 165. Toggle this option to enable sirens to operate after report failure.

- Ticked Sirens will operate only after report fail
- Unticked Sirens will operate on alarms only.

Delay holdup lock-up

This option is only applicable to latching delayed holdup alarms. If set to YES, an alarm can only be cancelled if the input is in sealed state. A latching holdup alarm is LOCKED OUT until the alarm device is taken out of its latched state (reset).

Toggle this option to enable or disable Delayed holdup alarm lockouts

- Ticked Delayed holdup alarm lockouts are enabled until the alarm device is reset.
- Unticked Delayed holdup alarm lockouts are disabled.

Siren testing

This option allows siren testing for 3 seconds when the secure test is started from either test mode 1 or 2. See also "[Test mode](#)" on page 165.

Toggle this option to allow siren testing when secure testing is started.

- Ticked The sirens are tested for three seconds when the secure test is started (test mode 1 or 2).
- Unticked The secure test is started without the Siren test.

Disable 0 enter for camera reset

This option disables 0 or [ENTER] to be used to stop camera operating after an alarm has occurred. Refer to the *Discovery Administrators Manual* for details.

Toggle this option to Disable 0 or [ENTER] for camera reset.

- Ticked 0 [ENTER] cannot be used to stop cameras operating after an alarm has occurred. The cameras continue to operate until an authorized user resets them.
- Unticked 0 [ENTER] stops the cameras operating (after pressing [ENTER] [ENTER] for the Quick Alarm History)

System alarms latch

System alarms are RAS/DGP Offline, Cabinet Tamper, Siren Tamper, Mains Fail, Fuse Fail, and Low Battery.

- Ticked System alarms latch and require a PIN or card to reset them.
- Unticked System alarms automatically reset and report

restoral when a condition is no longer present.

Menu and RAS (checkboxes)

Display user flags

The special user flags are Dual Custody, Guard, Visitor, Trace User, Card Only, Privileged and Long Access.

Toggle this option to display or not display Special user flags

- Ticked The special user flags are displayed in sequence after the floor group display when programming users.
- Unticked The special user flags are not displayed.

Display user names

This option allows User names to be visible when a user badges in or out of an area on a RAS.

Toggle this option allow or not allow user names to be displayed

- Ticked User names are displayed
- Unticked User names are not displayed

Display alarms instantly on LCD

This option will enable or disable alarms to instantly display on LCD RAS. Toggle this option to enable or disable alarms to instantly display on LCD RAS's.

- Ticked Details of the first alarm are displayed instantly on the LCD RAS. Details of other alarms can be viewed on the LCD RAS by pressing [ENTER] [ENTER].
- Unticked Details of all alarms can be viewed on the LCD RAS by pressing [ENTER] [ENTER].

Disable flashing area LEDs

This option disables flashing area LEDs to display on RAS on alarm or tamper.

Toggle this option to disable or enable flashing LEDs on alarm or tamper.

- Ticked The area LED will not flash on alarm or tamper.
- Unticked The area LED will flash on alarm or tamper.

Display input one at a time

This option allows one input at a time to be displayed even though there may be more than one in the list of inputs to be displayed (the user must

scroll through the inputs).

Toggle this option to Display one input at a time on a RAS.

- Ticked One input at a time is displayed
- Unticked Inputs are displayed as a list of numbers and it is necessary to select the input number to display the input name.

Skip access check for service tech

This option allows Service Technicians to access the system when the system is armed.

Toggle this option to allow service techs to access the system when it is armed.

- Ticked Enables the User menu option Enable Service Tech to be used when the system is armed.
- Unticked All areas must be disarmed before the option can be used to enable service technician access.

Enable V8 multi-break

By default, Discovery reports multi break input alarms such as CID 139 Burglar alarm, Intrusion verifier. If the "Multi break alarms" option is set to YES for any Comm path, you can choose to report multi break alarms in the same manner as a V8 panel (as a multi break event on the input's programmed CID code).

- Ticked Enables V8 multi-break
- Unticked Disables V8 multi-break

Enable V8 numbering

Discovery uses the latest numbering system, but is able to use the V8 input numbering system if required. If this option is set, Discovery will use V8 input numbering.

Toggle this option to enable Discovery to use V8 input numbering.

- Ticked Enabled to use V8 input numbering
- Unticked Disable to not use V8 input numbering

Expanded test success reporting

When timed input testing is used (Expanded Test Reporting set to Yes), and an input is tested within its specified number of days, enable this option to send a test success message (CID 611 'Point tested OK') for the input number.

Toggle this option to enable or disable timed input test success messages.

- YES Timed input test success messages are enabled
- NO Timed input test success messages are disabled.

Disable code from displaying

This option disables PIN code from displaying on entering.

Toggle to disable or enable PIN codes from displaying on entering.

- Ticked PINs are not visible in User menu Program Users (except to master installer). The display shows "PIN codes cannot be viewed".
- Unticked PINs are visible.

Dual custody code programming

This option requires two users to enter their PINs to gain entry. Toggle this option for Dual custody code programming.

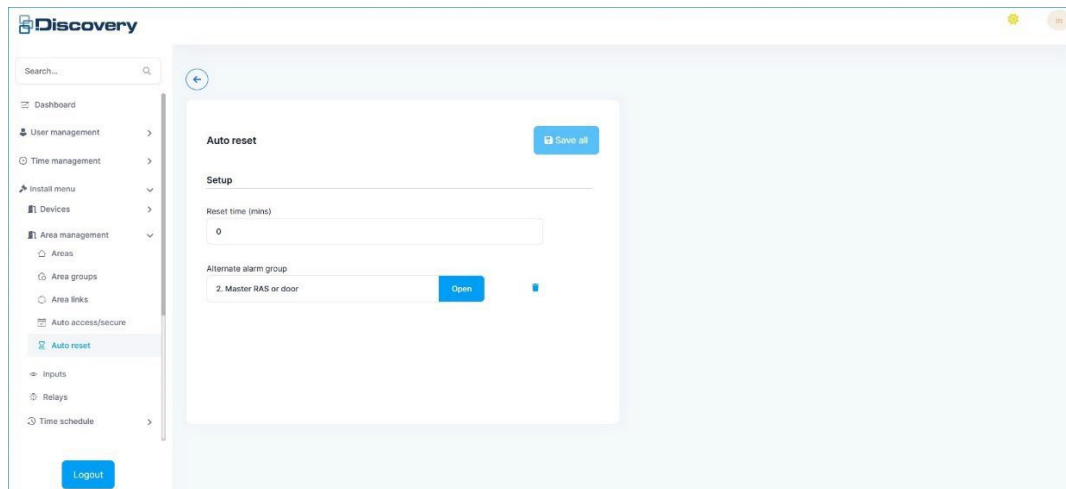
- Ticked Two users are required to enter their PINs before access is granted to program users (user 50, Master Code, is not required to have a second code to program users).
- Unticked Validation is not needed when entering User menu 14, Program Users.

Auto reset

INSTALL MENU > AREA MANAGEMENT > AUTO RESET

This function is used to program the Discovery to automatically reset alarms. The auto reset functionality is typically used for specified areas, and during specified times (for example, at night), each of which is determined by an alarm group.

Note: It may be necessary to program a special alarm group for this function.



Programming Auto reset

Fill out the Setup page and **Save all**.

A worksheet is provided to record programming details and to further describe this option. See “[Auto reset worksheet](#)” on page 238.

Reset time (mins)

Auto reset time is the amount of time that elapses between the alarm occurring and the alarm reset attempt. Enter the amount of time.

Alternate alarm group

An alarm group tells the control panel which areas to auto reset, and the alarm group's time zone tells the control panel the times that this may occur.

Select the Alternate alarm group field or the **Open** button next to it to display a list of Alternate alarm groups that may be used with this system. Select or create the alarm group to be used, then press the **OK** button to save. The Alternate alarm group may be cleared from this entity by selecting the  trash icon next to the Alternate alarm group field.

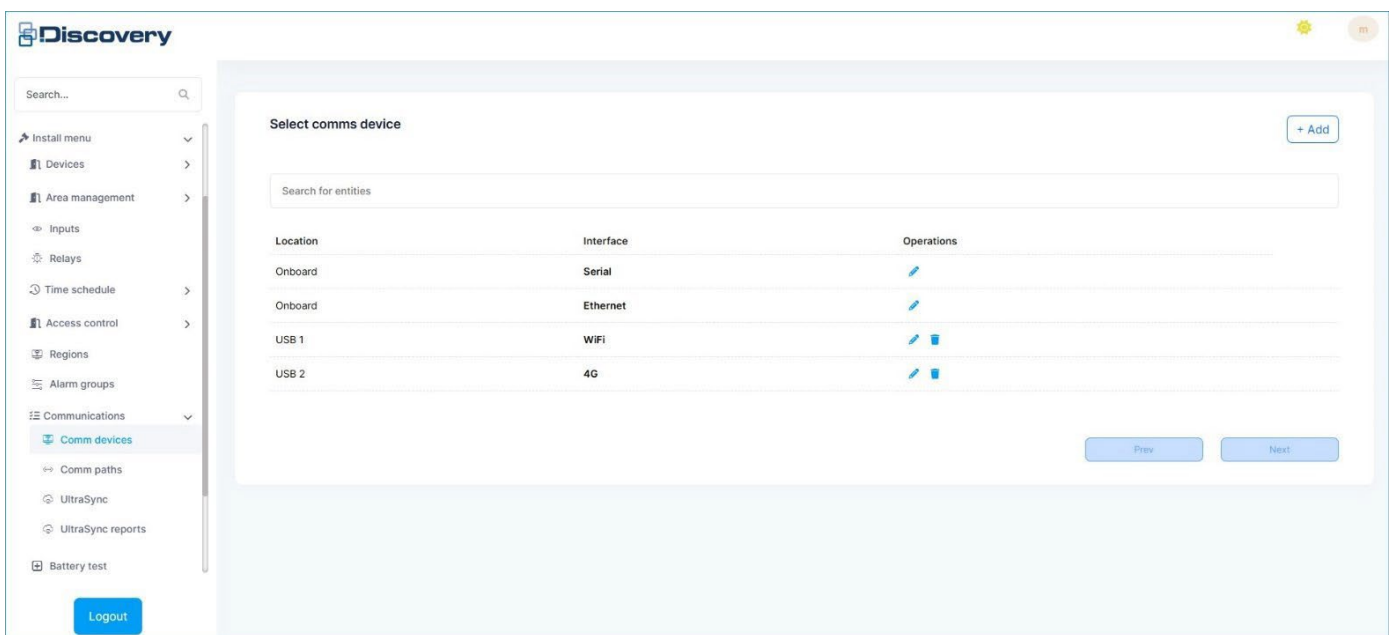
Comm device

INSTALL MENU > COMMUNICATIONS > COMM DEVICES

The Comm devices page allows the operator to program the communication devices on a panel, which supports multiple methods of communication.

Discovery panels running firmware v2 or later utilise modified options on this form compared to ChallengerPlus and Discovery v1 firmware.

Both onboard communications devices and any optional expansion boards are configured using this page. Challenger expansion slots 1 and 2 are used for communications devices, while slot 3 is reserved for the IUM (Intelligent User Memory) Module. Discovery USB slots 1 and 2 can only be configured on Discovery v2 or later firmware, and are used for communication devices.



Programming Comms devices

A set of three worksheets is provided to record programming details and to further describe this option. See:

[“Figure 40: Communications devices worksheet \(onboard hardware\)”](#) on page 240 and [“Figure 41: Communications devices worksheet \(external hardware\)”](#) on page 241 for the hardware setup.

[“Figure 42: Communications paths worksheet”](#) on page 242 for setting up Paths.

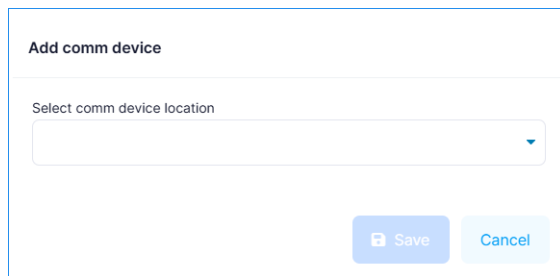
Each of the worksheets is sectioned into areas that correspond to the tabs in the CTPlus software set up screens.

Refer to the following sections for details about these options:

- “Setting up communications hardware” on page 122
- “Setting up communications paths” on page 117
- “Checking communications status” on page 149

- [“UltraSync”](#) on page 138

To program a Comm device, click the **+ Add** button to bring up the Setup page.

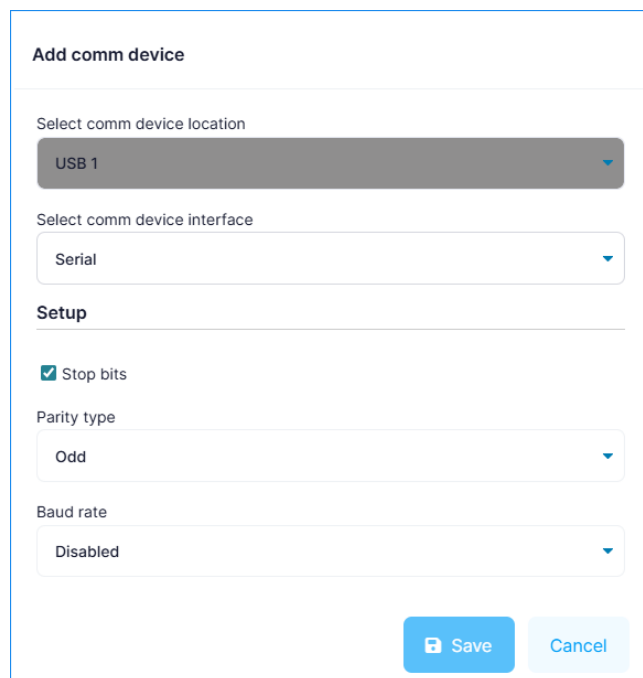


To add a comm device choose from the following 2 options:

- USB 1
- USB 2

When choosing USB 1 it will ask to Select comm device interface, which will be either:

- Serial
- Ethernet



Add comm device

Select comm device location

Choose either **USB 1** or **USB 2**

Select comm device interface

Select either **Serial** or **Ethernet**

Discovery panel comm devices allows you select the Location of the comms device being configured. The available locations are:

- On Board: used for any communications devices which are directly connected to an interface on the panel itself.
- USB 1: used for any communications devices which are connected to the panel via the USB-A port (requires Discovery v2 or later firmware).
- USB 2: used for any communications devices which are connected to the panel via the USB-C port (requires Discovery v2 or later firmware).

On Board

Ethernet

The available configuration options are:

- Enable ethernet: allows the onboard ethernet connection to be used as per configured options.
- Enable access to Web interface from this expander: allows the Web UI to be accessed from this interface.
- Enable DHCP: allows the panel to retrieve IP configuration from a DHCP server. Disable to manually specify IP address and related network configuration options.
- Enable ping: allows the panel to respond to ping requests received on this interface.

The following fields are only editable when 'Enable DHCP' is disabled:

- IP address: The panel's IP address on the network.
- Gateway IP address: The gateway IP address.
- Subnet mask: The panel's subnet mask on the network.
- DNS server 1: The IP address of the primary DNS server.
- DNS server 2: The IP address of the secondary DNS server.
- Ethernet name: The NETBIOS name configured in the device will be displayed as read-only.

Please note: All addresses use IPv4, and DHCP-assigned values are not displayed in this form.

Serial

The available configuration options are:

- Baud rate: Select the desired baud rate (in bits per second) for serial data transmission. The available options are:
 - Disabled
 - 1200

- 2400
- 4800
- 9600
- 19200
- 38400
- 57600
- Parity: Select the required parity config to be used for serial data transmission. The available options are:
 - None
 - Odd
 - Even
- Stop bits: Select the number of stop bits required for serial data transmission. The available options are:
 - 1
 - 2

USB 1

Serial

The available configuration options are:

- Baud rate: Select the desired baud rate (in bits per second) for serial data transmission. The available options are:
 - Disabled
 - 1200
 - 2400
 - 4800
 - 9600
 - 19200
 - 38400
 - 57600
- Parity: Select the required parity config to be used for serial data transmission. The available options are:
 - None
 - Odd
 - Even

- Stop bits: Select the number of stop bits required for serial data transmission. The available options are:
 - 1
 - 2

Ethernet

The available configuration options are: (Tick to enable)

- Enable ethernet: allows the onboard ethernet connection to be used as per configured options.
- Enable DHCP: allows the panel to retrieve IP configuration from a DHCP server. Disable to manually specify IP address and related network configuration options.
- Enable ping: allows the panel to respond to ping requests received on this interface.
- Enable access to Web interface from this expander: allows the Web UI to be accessed from this interface.

The following fields are only editable when 'Enable DHCP' is disabled:

- IP address: The panel's IP address on the network.
- Gateway IP address: The gateway IP address.
- Subnet mask: The panel's subnet mask on the network.
- DNS server 1: The IP address of the primary DNS server.
- DNS server 2: The IP address of the secondary DNS server.
- Ethernet name: The NETBIOS name configured in the device will be displayed as read-only.

Please note: All addresses use IPv4, and DHCP-assigned values are not displayed in this form.

Wi-Fi

The Discovery panel can manage a Wi-Fi network via a supported USB device. This is typically used by installers and technicians requiring temporary access to the panel for programming changes in situations where they are not able to access the panel using the onboard Ethernet or via UltraSync.

The available configuration options are:

- Enable Wi-Fi: allows the Wi-Fi connection to be used as per configured options.
- Enable access to Web interface from this expander: allows the Web

UI to be accessed from this interface.

- Device Mode:

Ad Hoc (Access Point): creates a Wi-Fi network that may be joined by other devices. Typically used to provide temporary access to the panel for programming updates.

- Base IP: (Copy this IP address to your browser)
 - Subnet mask
 - SSID: (Discovery)
 - WIFI Password (PSK): (Discovery123)
- Infrastructure (Client): allows the panel to join an existing Wi-Fi network. May be used in circumstances where a wired network is unavailable or unsuitable for a required task..
 - SSID: (Discovery)
 - WIFI Password (PSK): (Discovery123)
 - Use static IP (Check box)
 - Static IP: The panel's IP address on the Wi-Fi network.
 - Subnet mask: The panel's subnet mask on the network
 - Gateway IP address: The gateway IP address.
 - DNS server 1: The IP address of the primary DNS server.
 - DNS server 2: The IP address of the secondary DNS server.

Please note: All addresses use IPv4, and DHCP-assigned values are not displayed in this form.

USB 2

4G radio

The 4G comms module has the ability to configure up to two SIM cards for connectivity with the panel.

The available configuration options are:

Enable: allows the cellular radio connection to be used as per configured options.

Enable access to Web interface from this expander: allows the Web UI to be accessed from this interface.

SIM 1

- SIM PIN: enter the SIM card's access PIN in this field to enable the panel to access to the cellular network.
- SIM APN: enter the Access Point Name (APN) for the cellular network.
- APN username: enter the username required to access the cellular network access point.
- APN password: enter the password required to access the cellular network access point.
- APN authentication: select the APN authentication required for the SIM card. Available options are:
 - None: this option is selected if no authorisation is required.
 - PAP: select when Password Authentication Protocol (PAP) is required.
 - CHAP: select when Challenge Handshake Authentication Protocol (CHAP) is required.

SIM 2

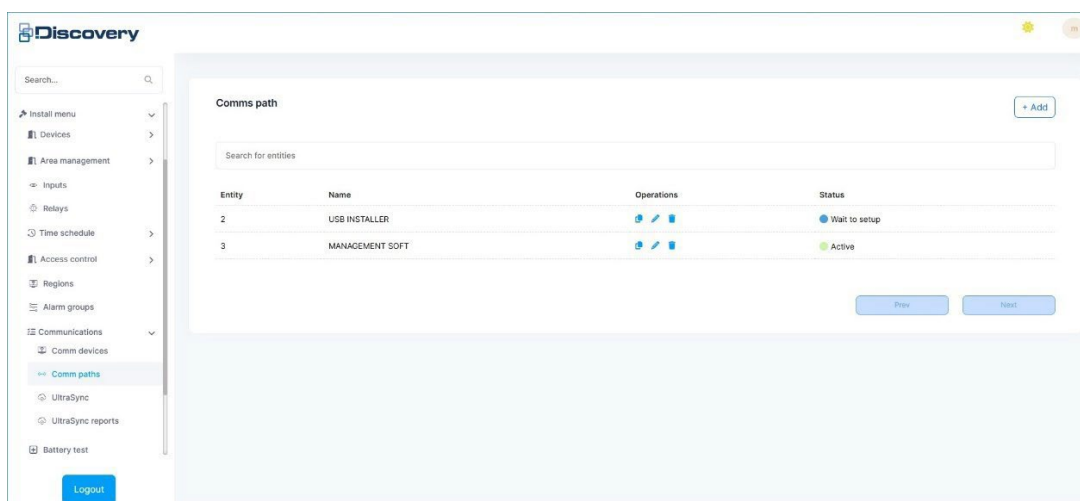
- SIM PIN: enter the SIM card's access PIN in this field to enable the panel to access to the cellular network.
- SIM APN: enter the Access Point Name (APN) for the cellular network.
- APN username: enter the username required to access the cellular network access point.
- APN password: enter the password required to access the cellular network access point.
- APN authentication: select the APN authentication required for the SIM card. Available options are:
 - None: this option is selected if no authorisation is required.
 - PAP: select when Password Authentication Protocol (PAP) is required.
 - PIN: enter the SIM card's access PIN in this field to enable the panel to access to the cellular network.

- Switch between SIM 1 and SIM 2: the panel can periodically toggle which SIM card is being used, which can be useful in areas with unreliable reception.
 - Frequency: select how often the active SIM should be toggled. Available options are:
 - Never
 - Hourly
 - 4-Hourly
 - Daily
 - Weekly
 - Start time: select what time the active SIM should be toggled according to the selected frequency.
 - Day of week: select which day of the week the active SIM should be toggled when Frequency is configured as 'Weekly'.

Comms path

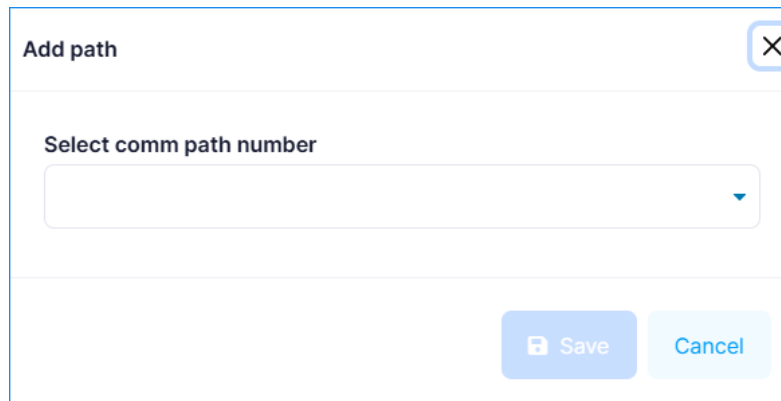
INSTALL MENU > COMMUNICATIONS > COMM PATHS

This section describes how to configure communications path for IP connection to a management software computer. The process for other paths is similar, but details will vary.

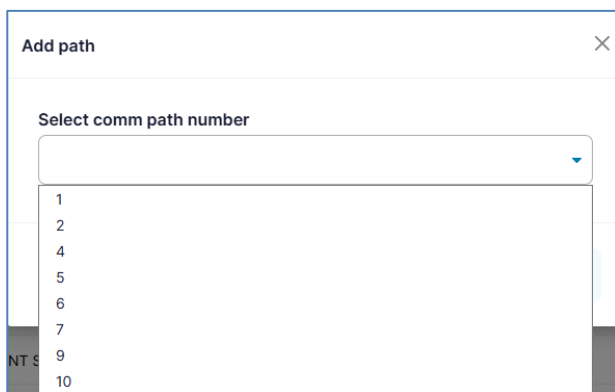


Programming comm paths

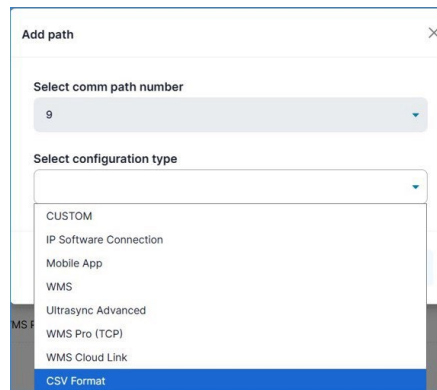
To program a Comms path, click the **+ Add** button to bring up the Add path page.



The 'Add path' dialog box is shown. It has a title bar with a close button (X). Below the title bar is a section labeled 'Select comm path number' with a dropdown menu. At the bottom right are two buttons: 'Save' and 'Cancel'.



The 'Add path' dialog box is shown with the 'Select comm path number' dropdown menu open. The list shows numbers 1 through 10. The number 9 is highlighted.



The 'Add path' dialog box is shown with the 'Select configuration type' dropdown menu open. The list shows options: CUSTOM, IP Software Connection, Mobile App, WMS, Ultrasync Advanced, WMS Pro (TCP), WMS Cloud Link, and CSV Format. The 'CSV Format' option is highlighted.

Example of screens when a path is chosen.

Selecting comm path number

The record number identifies a communication path. Communication paths are numbered in the range 1 to 10.

The following paths have default values and are missing from the Select comm path number list:

- Path 3—MANAGEMENT SOFT is for IP connection to a computer running management software computer such as CTPlus, WMS Pro and Discovery web interface.
- Path 8—MOBILE DEVICE is for use with the Tecom Plus Mobile App, enabling you to view history, alarms, users and control devices such as doors and areas over a TCP/IP connection. Please note that Discovery support in the app is currently limited and will be expanded over time.

Select configuration type

Select the configuration type from the list below:

- CUSTOM
- IP Software Connection
- Mobile App

- WMS
- UltraSync Advanced
- WMS Pro (TCP)
- WMS Cloud Link
- CSV Format

Setup

Enable connection

If you are connecting to the Discovery panel via Ethernet, tick the box for YES and do not tick for NO values (enabled and disabled).

Note: Change this value to YES if connecting to management software via Ethernet.

- Ticked The currently selected path is enabled.
- Unticked The currently selected path is disabled. Note: More than one path may be enabled.

Path name

To assign a custom name to the path, type the name in. Maximum of 16 characters. (including spaces)

Location

This will be self-populate from earlier selections. These can be:

- Onboard if the path communicates via the panel's onboard hardware.
- EXP1 if the path communicates via the first expander module.
- EXP2 if the path communicates via the second expander module.
- EXP3 if the path communicates via the third expander module.
- If the path communicates via an existing UltraSync link path. See "[Connecting via UltraSync](#)" on page 60 for more information.

Slot

After selecting a hardware location, you need to indicate which slot (port) on the hardware the path will use. The options will vary depending on the hardware. The following example is based on location: Onboard.

Select one of the following slot (port) options:

- None - (disabled).

- RS232-STU - if this path uses the panel's J15 connector.
- Ethernet - if this path uses the panel's Ethernet port.

Note: The above options relate only to location: Onboard. Other locations may have their slots named and numbered differently.

Format/Sub-format

Select the communication format. Some formats may be further described by a sub-format.

The formats and sub-formats for each panel type are:

- Discovery / ChallengerPlus
 - None
 - Contact ID Modem
 - None (normal Contact ID)
 - Contact ID Hex
 - Computer Polled
 - Computer Event Driven
 - IP Receiver
 - None (normal Contact ID)
 - Contact ID Hex
 - Securitel STU
 - None
 - Contact ID
 - Contact ID Hex
 - Printer
 - None
 - HP Laser
 - Epson
 - Debug (Note: Use the debug option only if instructed to by Technical Support)
 - C Bus
 - DVMRE Time Stamp

- IP Receiver Names
- Mobile Device
- UltraSync
- High level lift controller
- Network Access Controller (NAC)
 - None
 - Computer Polled
 - Computer Event Driven
 - High level lift controller

Account code

Account code is used in two ways, depending on what this path is used for:

- If connecting to a management software computer, type a number in the range 1 to 1024 to match the computer address.
- If reporting to central station via DTMF dialler, type the four- digit account number provided by that monitoring company that identifies your system to the monitoring company. If not used, enter 0000.

Backup for path number

A path can be designated as a backup for another path. For example, you can program two paths for the same purpose so that if the connection via the primary path is lost then the secondary path takes over until the primary path is restored.

Two levels of backup are supported. For example path 1 can be a backup for path 2, which can be a backup for path 3. So, if path 3 can't communicate, then the panel tries path 2. If paths 3 and 2 can't communicate, then the panel tries path 1.

Notes:

- When a backup path is active, events will be reported according to the backup path's filtering options such as areas, time zones, and so on. We do not recommend using one type of path format to back up a different type of path format due to varied filtering options (for example, using a CID Dialler path as a backup for Management Software path).
 - When using a CID Dialler path as a backup, the dialler will not connect until triggered by an alarm event even if the path it backs up is configured to always connect.
-

Enter the number of the path that this path backs up. Enter 0 if this path doesnot back up another path.

Authentication

Challenger panels, ChallengerPlus panels, NACs, and Discovery panels all support path authentication with a user name and password instead of just a security password (as defined in the Computer password field on the Main tab. This allows connections via the path to be logged against path user names, and allows for more complex passwords, only supported for Mobile App and CTPlus Connection via UltraSync.

Username

Enter a user name for path authentication.

Password

Enter a password for path authentication.

Connection control

Always connect

- Ticked The path remains constantly connected. In the case of a dialler path, it will only disconnect if another higher priority path needs the modem. When the higher priority path's task is complete, it will disconnect and the original dialler path will reconnect.
- Unticked The path will disconnect when not in use (no events to report).

Connect on event

- Ticked Initiate a connection when an alarm event or access event triggered.
- Unticked A connection is not initiated by any event triggered.

Connect on service

- Ticked When requested by the User Service Menu, establish a connection.
- Unticked Do not establish a connection.

Note: Connect on service is only used when the dialler is configured for the panel to dial management software. It will not work for a dialler configured to dial into the panel from management software or any other path comm format.

Connect on buffer at 80%

- Ticked Initiate a connection when the events buffer is at 80%.
- Unticked Do not initiate a connection when the events buffer is at 80%.

Isolated inputs trigger path

This option applies to paths that are not permanently connected.

- Ticked When inputs are isolated, initiate a connection to report.
- Unticked Do not initiate a connection to report when inputs are isolated. Isolated inputs will be reported when the next alarm function triggers the path.

Note: Report alarm events on the Filter tab must be Ticked for this option to work.

Stay connected on empty buffer

- Ticked The path will maintain connection when all events have been sent.
- Unticked The path will disconnect when all events have been sent.

Control command

- Ticked Allows a remote computer to control devices on the panel.
- Unticked The remote computer cannot control remote devices.

Trigger path fail events

- Ticked Comm path fail or restore events for any path are reported out of this path, or displayed on RAS.
- Unticked Comm path fail or restore events are not reported out of this path, or displayed on RAS. Event will still be visible within software.

Use area account code

- Ticked Path uses area Account code, programmed on the Areas form, when reporting to central station.
- Unticked Path does not use area Account code when reporting to central station.

Triggers HB/Link fail events

This option has no effect if 'Report Communication event' is off.

- Ticked The path is triggered (connection is opened) when an Ethernet heartbeat, comm path fail, or link fail condition is detected on any path.
- Unticked The path is not triggered when an Ethernet heartbeat, comm path fail, or link fail condition is detected.

Filter

Filter events to area or area group

Filter events to an area or area group. Use the drop-down list to select whether to filter events to an Area or an Area group. Select the area or area group by clicking the Browse button, or type the area or area group number directly into the field.

If no area or area group is selected, the events from all areas are reported on this path.

Event time zone

To report the event during a specific time (or only outside that specific time), select a 'hard' panel time zone or soft time zone by clicking on the Browse button, or type a time zone number directly into the field. Setting this will report events only during a specified time zone (or outside the time zone if Send events out of time zone, below, is Ticked).

Multi-break alarm time (sec)

If the Multi-break alarms option (below) is Ticked, set a time that will filter out multi-break alarms that are older than the specified time. The time range is from 0 to 255 seconds.

Report communication events

- Ticked Enables the path to report communication faults, including heartbeat, path, link, and too many retries.
- Unticked Disables the path from reporting communication faults.

Disarm clears pending alarms

This option enables the Comm path to clear pending input alarms from history when an area is disarmed.

- Ticked Comm path to clear pending input alarms from history when an area is disarmed enabled
- Unticked Comm path to clear pending input alarms from history when an area is disarmed disabled

Report connection events

RAS menu name: Report computer connected.

- Ticked When a remote computer is connected, send the computer connected event.
- Unticked When a remote computer is connected, do not send the computer connected event.

Notes: This option must be Unticked if this path is used for reporting to a central station or an IP receiver.

This option does not apply if the path Format is Mobile Device.

Report access events

- Ticked Allow the path to report access events.
- Unticked Do not allow the path to report access events.

Report alarm events

- Ticked Report alarm events.
- Unticked Do not report alarm events.

Report open/close

- Ticked The path will report when areas specified in Filter event to area or area group (above) are armed or disarmed.
- Unticked The path will not report when areas specified in Filter event to area or area group are armed or disarmed.

Report system alarms

RAS menu name: System alarm report.

- Ticked The path will report system alarm events, which include all alarm events that are not associated with an area.
- Unticked The path will not report system alarm events, which include all alarm events that are not associated with an area.

Note: Report alarm events (above) must be ticked for this option to work. This is relevant for power low, battery failure, tampers etc. It is not relevant for area type alarms.

Multi-break restores

This check box controls the way in which multiple alarm restorals from one input are reported to the remote monitoring company.

- Ticked If an individual input alarm is restored more than once before being reset by a user, each restoral is reported to the remote monitoring company.
- Unticked If an individual input is restored more than once before being reset by a user, then only the first restoral is reported to the remote monitoring company.

Note: Report alarm events (above) must be Ticked for this option to work.

Multi-break alarms

This check box controls the way in which multiple alarms from one input are reported to the remote monitoring company.

- Ticked If an individual input alarms more than once before being reset by a user, each alarm is reported to the remote monitoring company.

- **Unticked** If an individual input alarms more than once before being reset by a user, then only the first alarm is reported to the remote monitoring company.

Note: Report alarm events (above) must be Ticked for this option to work.

Common open/close

Instead of reporting when individual areas are armed or disarmed a single common event is sent when all the areas (in the area group assigned to the path filter) are armed or any one of those is disarmed.

The area reported as secured/accessed is the area with the lowest index in the area group.

Example:

An area group A is assigned to the path filter and it consists of areas 4, 5, and 6. When the areas are armed in the order 5, 4, 6 a single event for area 4 secured is sent from the panel when the last area is armed. When area 5 is then disarmed a single event area 4 accessed would be sent.

- **Ticked** The path will report open when the first reporting area is disarmed, and close when the last reporting area is armed.
- **Unticked** The will report open or close whenever a programmed area is armed or disarmed.

Remove event when TZ invalid

- **Ticked** The path will ignore events when they are not being reported due to time zone settings. Events that are not reported are removed from the path's queue.
- **Unticked** The path will store events in the queue when they are not being reported due to time zone settings. When the time zone allows reporting then the queued events are sent along with any new events.

Buffer outside time zone

- **Ticked** Report events when the selected time zone is invalid.
- **Unticked** Report events regardless if the selected time zone is invalid.

Test calls

Test call option

This option determines whether the panel activates test calls to the monitoring company

and if so, how often. The test call ensures that communications are operating correctly and can be programmed to only be made if there have been no events to initiate a call since the last test call.

Click the drop down arrow on the right of the field to select the test call type. The options are:

- No test call
- Test once a day
- Test once a week
- Test once a day if no events
- Test once a week if not events
- Test four hourly
- Test four hourly if no event
- Test hourly
- Test hourly if no event

Test call day

Select the day of the week needed, either:

- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

Test call time

Enter the time in HH:MM, 24 hour format or click the up/down counter at the right of the field.

IP Settings

Select to configure either:

- URL name
- IP address

IP Address

Refer Setting up a [Comms path](#) on page 124

This path can connect via IP to a remote computer via:

- A programmed computer IP address (see “Send to IP address” below).
- A dynamically assigned computer IP address (see “Dynamic computer IP address”).

IP address

The Discovery panel can use this IP path to connect to a remote computer, IP Receiver, or other supported software, via:

- An Ethernet cable from the Discovery panel’s Ethernet port. In this case you need to use the IP address of the remote computer.
- A Cellular (wireless) connection from a TSX16000 4G Communication Module fitted to the USB-2 of the Discovery panel. In this case you need to use the IP address of the WAN to access the data KGS Fire & Security Australia Pty Ltd access point (mobile internet).

You do not need to program an IP address for this path if “Dynamic computer IP address” is enabled.

Send Port Number

Enter the port number (for example, 3001) that will be used for sending data to other devices.

Listen IP Port

Enter the port number (for example, 3001) that will be used for receiving requests from other devices.

TCP type

Select UDP/IP if you want the Discovery panel to communicate in event-driven mode with management software, as well as to IP Receiver. In event-driven mode the Discovery panel reports events only as they occur. This prevents the management software and IP Receiver software from continuously polling Discovery panels and therefore minimises network bandwidth requirements.

Select TCP/IP if you want the Discovery panel to communicate in polled mode with management software. Polled mode typically consumes greater bandwidth than event-driven mode. However, this can be useful for panels that deliver little event-driven activity. Some networks require a certain amount of activity in order to maintain an active communications path.

Server/Client mode

If TCP/IP is used, you can configure whether the panel acts in a server or a client capacity. The default setting is server: change it to client for TCP/IP auto-enrol functionality.

Accept incoming connections from any address (checkbox)

Tick to enable

When enabled, this path will allow an IP connection from a computer at any IP address where:

- The connection request is received via the correct port number.
- The path's (non-zero) computer password is correct.

When this option is used, and connects to a remote computer, the path's IP address is populated automatically (see "[Send to IP address](#)" on page 135).

Encryption

Using the path setup. Setting up a [Comms path](#) on page 124

Encryption type

Select from one of the following types of encryption options:

- None
- Twofish - encryption algorithm is required for connection to management software. This option has a 16-character limit on the key length.
- AES 128-bit - encryption algorithm is required for connection to an IP receiver. This option has a 16-character limit on the key length.
- AES 256-bit - encryption algorithm is required for connection to an IP receiver. This option has a 32-character limit on the key length.

Encryption key

The encryption key is programmed as a string of digits, text, a password, or a passphrase. The maximum key length is determined by the encryption type: 16 characters for Twofish or AES 128-bit; or 32 characters for AES 256-bit.

In the following example "Key16" indicates a 16-character limit..

Advanced

From the path set up. Setting up a [Comms path](#) on page 124.

Computer password and Connection attempts

Enter the number of consecutive failed password attempts (in the range 1 to 255) that are permitted before the panel prohibits further attempts. For example, if the number of attempts is set to 3 and the computer has failed to connect 3 times to the Discovery panel, then it will not be able to connect. To re-enable communication you will have to go into this RAS menu option, and then exit.

Note: If the number of attempts is set to 0, then the computer will not connect to the Discovery on this path.

Message ACK timeout (ms)

Communication formats that are used for reporting events will attempt to connect and then wait for an acknowledgement to be received before making another attempt. The length of time that the panel waits is subject to the path's communication format and the programmed number of retries.

The default value for most paths is 0 ms (milliseconds), however, there are other (background) values that determine how long the panel will wait for an acknowledgement to be received. As a result of these background values, you might not need to program a value in the Message ACK Timeout field.

If the path uses format 1 CID Modem, then the length of time that the panel waits for an acknowledgement is a minimum of 1250 ms (this value is compatible with reporting CID via a satellite communications path). If you require a timeout value greater than 1250 ms, then enter the number of milliseconds in the Message ACK Timeout field.

For other applicable communication formats, the length of time that the panel waits for an acknowledgement to be received is comprised of the sum of two values:

- The value of the Message ACK Timeout field, and
- Either 3,000 or 5,000 ms. 3,000 ms is used for the first and second retries; 5,000 ms is used for any further retries.

For example, if the value of the Message ACK Timeout field is 60, and this is the first retry, then the total time that the Discovery panel waits for an acknowledgement to be received is 3,060 ms (3.06 seconds). If you require a timeout value greater than 3,000 or 5,000 ms, then enter the additional number of milliseconds in the Message ACK Timeout field.

Message retries

Message retries is the number of attempts allowed for this path to send an event when the connection is established.

TCP connect timeout (sec)

Connect timeout is the length of time in seconds the panel waits before terminating the connection attempt.

Enter the number of seconds in the range 1 to 255 (0 means wait indefinitely for a connection).

TCP wait time between connections (sec)

Connect retries is the number of times this path is to attempt to reconnect after the initial attempt fails.

Enter the number of attempts in the range 1 to 255 (0 means that only the initial connection attempt will be made).

Note: If this path is used for IP connection, and a non-zero heartbeat timeout is programmed, then a new connection attempt (if programmed) will be made after the heartbeat timeout expires.

Heartbeat timeout (sec)

Heartbeat timeout is optionally used for IP or Cellular (3G & 4G) paths to detect a connection failure. When used, the Discovery panel logs an Ethernet Heart Beat fail message to history (and then an Ethernet Heart Beat restore message when reconnected).

Note 1: The Ethernet heartbeat fail condition is generated only after the path's programmed number of message retries and connect retries have been exhausted.

Note 2: To avoid Ethernet Heart Beat Failed alarms, the Discovery panel's heartbeat value must be greater than the "heartbeat timeout" value in management software or Tecom IP Receiver.

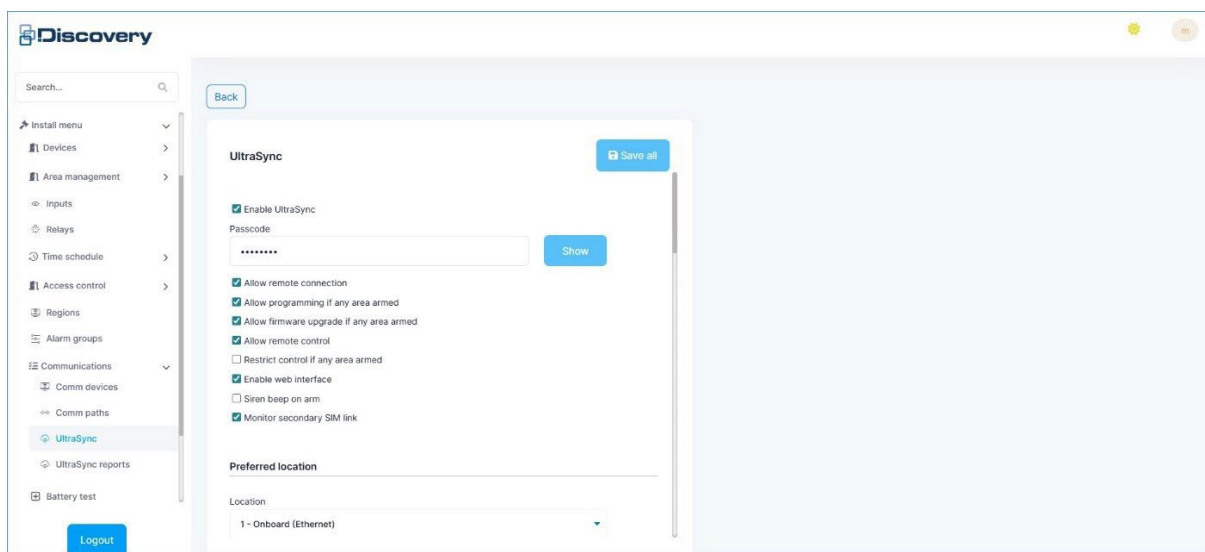
TCP connect retries

TCP connect retries is the number of attempts allowed for this path to send an event when the connection is established.

UltraSync

INSTALL MENU > COMMUNICATIONS > ULTRASYNC

Use this option to configure UltraSync communication. For more information about UltraSync and detailed instructions on setting up an UltraSync connection, refer to the "UltraSync Configuration Guide" document.



Programming

From the Communications menu to UltraSync.

Enable UltraSync

Tick the check box to enable UltraSync communication

Passcode

Enter the 8 digit UltraSync passcode to be used for UltraSync for authentication. This must be any number other than '00000000', otherwise authentication will fail. Click the [Show](#) button to display the current 8 digit passcode.

Allow remote connection

Enables remote access to the panel for user connections, such as the Tecom Plus mobile app and CTPlus. Users requiring remote access must be assigned an Alarm group with the Remote access option enabled.

Allow programming if any area armed

Enables panel programming regardless of area status. When unticked, remote users (e.g. CTPlus or Tecom Plus mobile app connected over UltraSync) cannot modify panel programming unless all areas are disarmed.

Allow firmware upgrade if any area armed

Enables firmware updates regardless of area status, When unticked, remote users cannot upgrade firmware via UltraSync unless all areas are disarmed.

Allow remote control

Enables control commands (e.g. arm/disarm areas, isolate/deisolate devices, open doors, etc.) to be actioned when requested by remote users.

Restrict control if any area armed

When enabled, control commands sent by remote users will only be actioned when all areas are disarmed.

Enable web interface

When enabled the Discovery web interface can be used to program and adjust parameters.

Siren beep on alarm

When enabled, area siren(s) will be briefly activated when an area is armed by remote users.

Monitor secondary SIM link

This will monitor the secondary back up SIM connection for connectivity.

Primary location

Location

Select the device to be used as the preferred path for UltraSync connections:

- 0 – Disabled
- 1 – On-board (Ethernet)
- 3 – USB-2URL / Port 1 & URL / Port 2

URL and Port info have default values and should only be changed if advised by tech support.

Alternate location setting

Location

Select the device to be used as the preferred path for UltraSync connections:

- 0 – Disabled
- 1 – On-board (Ethernet)
- 3 – USB-2

URL / Port 1 & URL / Port 2

URL and Port info have default values and should only be changed if advised by tech support.

Filter settings

Filter event to area or area group

This option enables the events reported to be filtered by either a specified Area or Area group. If no area or area group is selected, the events from all areas are reported. Select the type to be used, then select which area / area group to use by clicking the Browse button or typing the number directly into the field.

Enter time zone

This option enables to events to be reported based on a Panel time zone or Soft time zone. Select which time zone to use by clicking the Browse button or typing the number directly into the field.

Multi Break Alarm Time

When using multi-break alarms, a time between 0 to 255 seconds can be entered to prevent 'old' multi-break input alarms from being reported. For example, if you program a value of 30 seconds, then only multi-break alarms that are less than 30 seconds old will be reported.

Note: This option does not apply if "Enable V8 multibreak" is enabled.

Checkboxes – tick box to enable

Report alarm events

Alarm events will be reported over UltraSync. Report connection event

This option enables the “computer connected” event to be generated and reported to the UltraSync monitoring company when a remote connection has been made to the panel via UltraSync.

System alarms report

This option enables system alarm events to be reported over UltraSync. System alarms include all alarm events which are not associated with an area.

Note: “Report alarm events” must be enabled for this option to work.

Buffer outside time zone

- Ticked Report events when the selected time zone is invalid.
- Unticked Report events regardless if the selected time zone is invalid

Common Open Close

When enabled, this option causes UltraSync to report open when the first reporting area is disarmed, and closed when the last reporting area is armed. In both cases, the lowest reporting area number is used, regardless of when that area was disarmed or armed.

If not enabled, UltraSync will report open / close events whenever a programmed area is armed or disarmed.

Note: “Report open/close” must be enabled for this option to work.

Report Communication Event

This option enables UltraSync to report communications events.

Report Access Events

Access events will be reported over UltraSync.

Report Event TZ Invalid

Only send events over UltraSync when the current date/time is not within the selected Event time zone.

Multi Break Alarms

If enabled, when an individual input goes into alarm more than once before being reset by a user, each alarm is reported to the UltraSync monitoring company. If not enabled, when an individual input goes into alarm more than once before being reset by a user, then only the first alarm is reported to the UltraSync monitoring company.

Note: “Report alarm events” must be enabled for this option to work.

Multi Break Restores

If enabled, when an individual input alarm is restored more than once before being reset by a user, each restoral is reported to the UltraSync monitoring company. If not enabled, when an individual input alarm is restored more than once before being reset by a user, then only the last restoral is reported to the UltraSync monitoring company.

Note: “Report alarm events” must be enabled for this option to work.

Report Open Close

Enable to report when all areas / area group (as specified in “Filter event to area or area group”) open and close (are disarmed and armed).

Note: “Report alarm events” must be enabled for this option to work.

Disarm Clears Pending Alarms

This option enables UltraSync to clear pending input alarms from history when an area is disarmed.

Test calls

The options in this section only apply to panels which have been provisioned in UltraSync. Please note that in the context of UltraSync, a "call" refers to the panel communicating to a control room via an IP connection via the UltraSync network.

Test call option

Test calls can be set to occur on one of the following options:

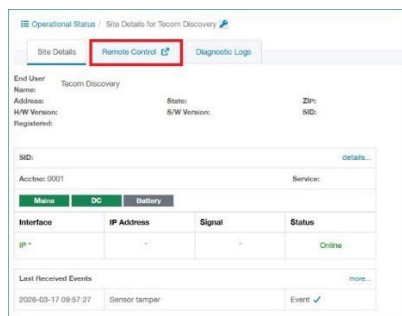
- No test call
- Test once a day
- Test once a week
- Test once a day if no event
- Test once a week if no event
- Test four hourly
- Test four hourly if no event
- Test hourly
- Test hourly if no event

Test call time

Enter the time of day that test calls should be made when enabled.

UltraSync Portal - Discovery Browser Access

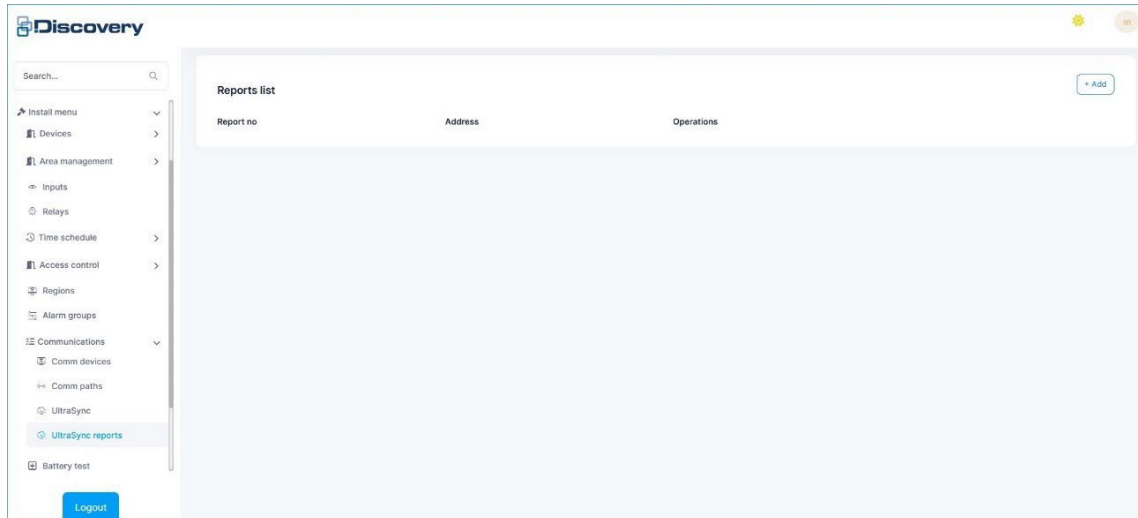
If an Operator has access to the UltraSync Portal as a Dealer and has a Discovery panel assigned, accessing **Live status > Remote Control** will pop out a new window that will allow secure remote connection to the Discovery web interface.



UltraSync reports

[INSTALL MENU](#) > [COMMUNICATIONS](#) > [ULTRASync REPORTS](#)

The UltraSync reports page will show / generate reports that have been initiated for Alarm, System, Power, Arm / disarm, and trace events.



Programming

Add Report

Report number

0

New entity

*User number

Cannot be empty or greater than 65535.

Address

Address is required.

☐ Alarm events

☐ System events

☐ Power events

☐ Arm/Disarm events

☐ Trace events

Save

Cancel

To create a new report press the **+ Add** and fill out the **Add Report**.

Report numbers

Enter a new entity report number

User number

Select the user to report on by entering the user number directly into the field.

Address

Enter the destination email for UltraSync reports.

Event check boxes

To enable the following events on the UltraSync report tick to enable or untick to disable

Alarm events

Tick the check box to report alarm events. For example, when an input goes into alarm.

System events

Tick the check box to report system events. For example, RAS offline, DGP siren fail, and other system events.

Power events

Tick the check box to report power events. For example, Mains fail, low battery.

Arm/disarm events

Tick the check box to report arm/disarm events. This will report when areas in the selected user's alarm group are armed or disarmed.

Trace events

Tick the check box to report trace events (if the user has the "Trace" option enabled on the Cards tab of the Users form). Trace events occur when a user with the trace flag tries to access a door.

Save selection.

Time zones

[INSTALL MENU](#) > [TIME SCHEDULE](#) > [TIME ZONES](#)

Time zones are used to create time slots in which certain events can take place. Time zones are assigned to alarm groups, door groups, floor groups, relays (outputs), arm and disarm timers, and out-of-hours access reporting, to restrict or enable specific operations during specific time periods.

Time zones (also called 'hard' time zones) are numbered 1 to 24 and 42 to 63, and are programmed for specific time periods. Each time zone is made up of one to eight sub-time zones containing:

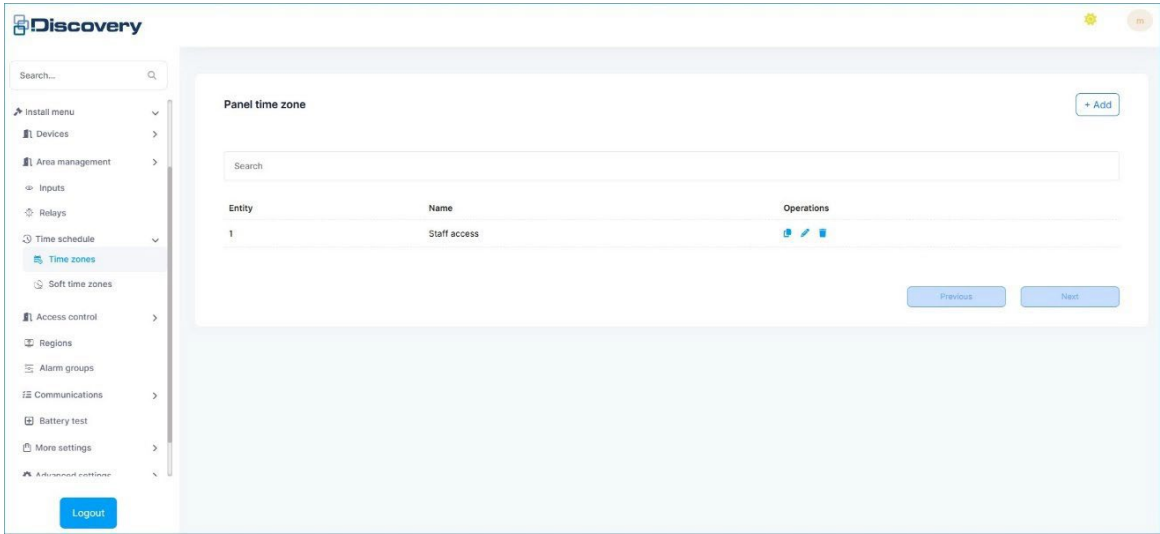
- A start time
- An end time
- The week days that the sub-time zone is valid
- Up to eight holiday types that the sub-time zone is valid

Use consecutive sub-time zones when a time zone start time and end time are on different days. The hours 24:00 and 00:00 are not recognized as end times and can therefore be used to extend a period to the next sub-time zone.

A time zone is invalid on any holiday that has been declared in the

holiday date file unless a corresponding holiday type is included in the sub- time zone. If a holiday type is included, the sub-time zone is valid on defined holiday that have the same type (even if the day of the week that it falls on is not included in the sub-time zone). See [“Holiday types”](#) on page 146.

Time zone 0 is a 24-hour time zone (always valid) and is not programmable.



Programming time zones

A worksheet is provided to record programming details and to further describe this option. See [“Time zones worksheet”](#) on page 245.

To program a new Relay, click the **+ Add** button to bring up the Setup page.

Setup

Timezone number

Must be within: 1-24, 42-63.

Timezone name

Time zones

Add time zone

No.

Start time

End time

Save

Cancel

Time zone number

Enter a Time zone number.

Time zone name

Enter a Time zone name. The name may contain up to 30 characters (including spaces).

Note: From here we now enter start and end times, Days, and Holiday types for up to 8 Segments of Panel time zones. To add a Time zone click on the **Add time zone**.

Add time zones

Start time

12:00 AM

End time

12:00 AM

☐ 24:00 hrs

Days

☐ Sunday

☐ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

Holidays

☐ H1 (None)

☐ H2 (None)

☐ H3 (None)

☐ H4 (None)

☐ H5 (None)

☐ H6 (None)

☐ H7 (None)

☐ H8 (None)

OK

Cancel

Enter the start time Hour and Minutes, and then the end time Hour and Minutes. An option to tick 24:00 hrs. for 24 hour access.

Tick the applicable days of the week, which the Time zone applies to in this segment.

Tick the applicable holiday types between Holiday 1 and Holiday 8.

When one or more holiday types are selected, the sub-time zone will be valid on holidays that contain the same types.

Note: A sub-time zone is invalid on any defined holiday unless the holiday’s type is included as a day in the sub-time zone.

Holiday types

The Discovery concept of holiday types provides greater flexibility in controlling access for users who need to use the Discovery system during holidays.

Holiday types provide the ability to grant access for users on some holidays

and not others. For example:

- We want cleaning staff to have access during school holidays, but not on public holidays.
- We want maintenance staff to have access during both school and public holidays.
- School holidays can be designated H1 type, and cleaning staff time zone must contain H1 type.
- Public holidays can be designated H2 type, and maintenance staff time zone must contain H1 and H2 types.

For each holiday type, enter a description of what the type indicates (for example, “School Holidays”) in the [Holiday types worksheet](#), Figure 62 on page 261.

To keep adding Time zone 2 – 8 click the **Add time zone** button.

Segment two to eight:

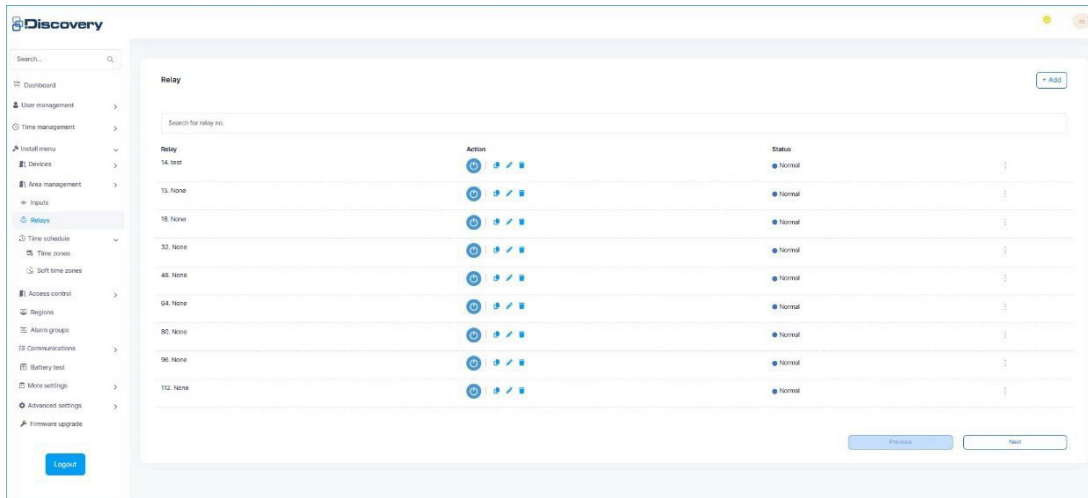
Segments two to eight have the same fields as Segment one. Using the Time zone and Holiday types worksheet, enter the remaining segments. Once completed click on the **Save** button to save the entry.

Once the Panel time zone segments have been finalised time zone to be used, then press the **SAVE** button to save.

Relays

INSTALL MENU >RELAYS

Relays are used by Discovery for a variety of functions, from door locks to switches for external devices, and are available as onboard devices, relay cards (TS1041, TS0840, TS0841, TS0843), and open collector outputs (TS0842).



Programming

Relays are programmed with a name, event flag, and/or a time zone. Relays programmed with an event flag will typically follow the event flag status, and modifiers can be applied to alter how and/or when the relay will be activated.

Discovery has the following default relay entities programmed:

- Relay 15 (panel strobe output) is mapped to event flag 2.
- Relay 16 (panel siren output) is mapped to event flag 1.
- Every 16th relay (32, 48, etc.) is mapped to event flag 1 for the siren output of each DGP address

A worksheet is provided to record programming details and to further describe this option. See [“Relay mapping worksheet”](#) on page 247. See also [“Programming relays”](#) on page 24.

To program a new Relay, click the **+ Add** button to bring up the Setup page.

Setup

Relay number

Must be within: 1-512.

Relay name

☐ Relay inverted
☐ Inactive during timezone

Event flag

Open

Timezone

0. 24 HR

Open

Save

Cancel

Relay number

Each relay has a specific number that identifies the relay to the control panel. Relay numbers may be assigned to physical devices, according to [Table 25](#) on page 204.

Relay name

Enter the name of the relay, up to a maximum of 30 characters (including spaces).

Relay inverted

Toggle this option to determine whether the relay will be inverted.

- Unticked The relay operates normally - on when active, off when inactive.
- Ticked The relay operates opposite to normal – off when active, on when inactive.

Inactive during time zone

Toggle this option to determine whether the relay will be active or inactive when a time zone has been selected and is valid.

- Unticked The relay will be active when the selected time zone is valid, even if the selected event flag is inactive.
- Ticked The relay will be inactive when the selected time zone is valid, even if the selected eventflag is active.

This can be useful to prevent a relay from activating during certain times, for example to ensure a loud siren cannot be activated during business hours when the site is attended.

Relays will be controlled normally when the selected time zone is invalid.

Event flag

An event flag and/or time zone may be used to activate a relay. If an event flag is selected without a time zone, the relay will activate whenever the event flag is active. If no event flag has been selected, the relay will be controlled by the selected time zone and/or standard door/lift programming. See [programming summary event flags](#) on page 163 for more info.

Select the Event flag field or the **Open** button next to it to display a list of event flags that may be used with this relay. Select or create the event flag to be used, then press the **OK** button to save. The event flag may be cleared from this entity by selecting the  trash icon next to the Event flag field.

Time zone

The time zone may be used to control when a relay may be active, for example:

- If a time zone is selected and active, the relay will be active, regardless of the event flag state.
- If a time zone is selected and inactive, the relay will be controlled by the event flag and/or associated standard doors/lifts.
- If a time zone is not selected, the relay will be controlled by the event flag and/or associated standard doors/lifts.

Select the Time zone field or the **Open** button next to it to display a list of time zones that may be used with this relay. Select or create the time zone to be used, then press the **OK** button to save. The time zone may be cleared from this entity by selecting the  trash icon next to the Time zone field.

Vaults

INSTALL MENU > ADVANCED SETTINGS > VAULTS

Vault areas are areas that, when armed, will automatically arm other areas after a specified time. Users that have the vault areas (and a user category) in their alarm group can arm the vault areas. The time starts only if all vault areas are armed. Users do not need to have alarm control over the areas that are automatically armed.

By using a special programming procedure, a user category timer starts when all the vault areas are armed. When the timer expires, a non-vault area linked to the vault areas will automatically arm.

For example: A building has three office areas (areas 3, 4, and 5), a common foyer (area 1) and a common cafeteria (area 2).

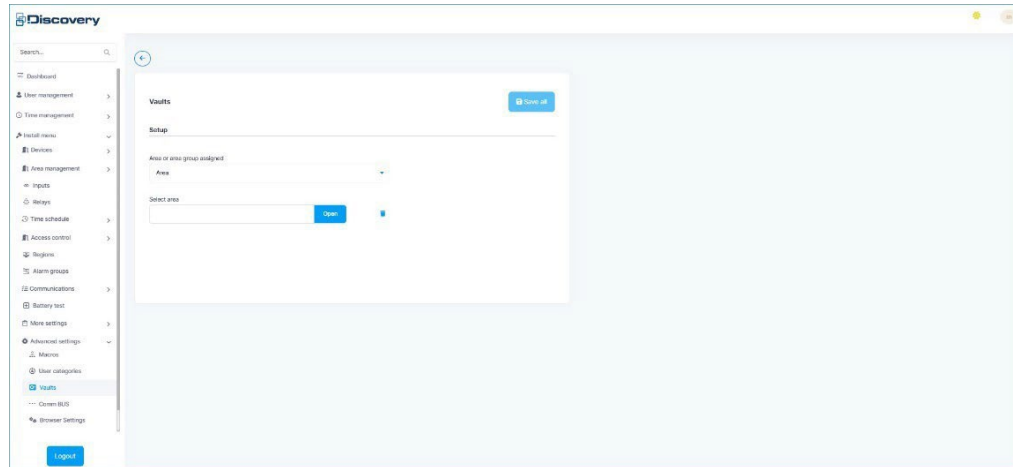
Assigning the office areas as vaults allows the foyer and the cafeteria to be armed at a set time after the last office is armed.

Other programming needed (for this example):

- Use this option to program areas 3, 4, and 5 as vaults. (Because this example is for multiple areas, you will need to create an area group containing areas 3, 4, and 5; and then program the area group as a vault.)
- Set “[Disable insert of user category](#)” on page 110 to NO.
- Link the areas to be timed on (1 and 2) to the areas designated as vaults in “[Area linking](#)” on page 153 (areas 1 and 2 linked to the area group containing areas 3, 4, and 5).
- Program an area group that contains the areas to be automatically armed (1 and 2) so that the areas can be both disarmed and timed.

See [“Area groups”](#) on page 170.

- Program the user category’s time required for delayed arming in [“Timers”](#) on page 100.
- Program the required alarm groups to activate the user category. See [“Alarm groups”](#) on page 90.



Programming vault areas

A worksheet is provided to record programming details and to further describe this option. See [“Vaults worksheet”](#) on page 249.

On the **Setup** page there is a field to choose either an **Area or area group assigned**.

Select the **Area** field or the **Open** button next to it to display a list of Areas that may be used with the Vaults. Select or create the Area to be used, then press the **OK** button to save. The Area may be cleared from this entity by selecting the  trash icon next to the Area field.

Select the **Area group** field or the **Open** button next to it to display a list of Area groups that may be used with the Vaults. Select or create the Area group to be used, then press the **OK** button to save. The Area group may be cleared from this entity by selecting the  trash icon next to the Area field.

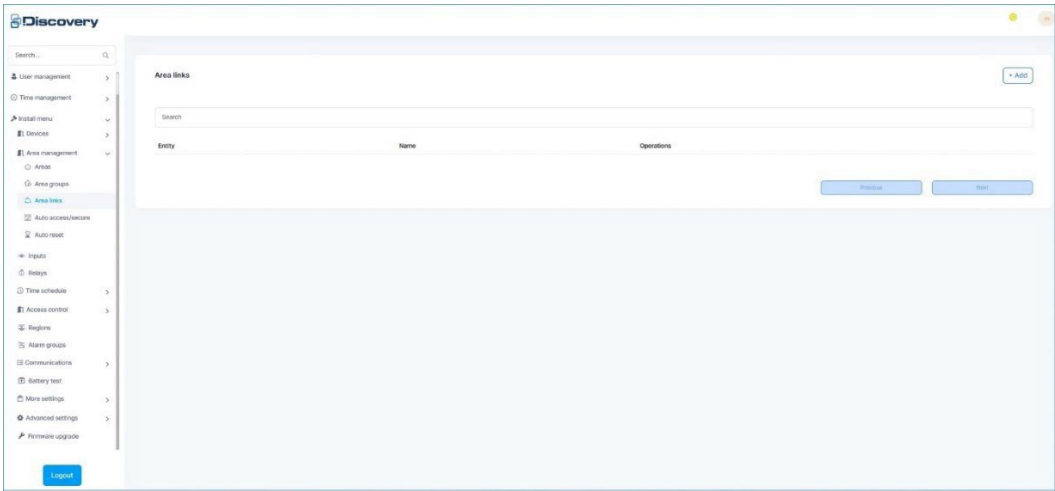
Area links

INSTALL MENU > AREA MANAGEMENT > AREA LINKS

In a facility with multiple areas, the entrance to the facility is usually shared by

all areas. This shared area (common area) should only be armed when the last area is armed. The common area is an additional area that automatically arms as soon as the linked areas are armed.

See “[Programming common areas](#)” on page 50 for details.



Programming

A worksheet is provided to record programming details and to further describe this option. See “[Area linking worksheet](#)” on page 249.

To program a new Area links, click the **+ Add** button to bring up the Setup page.

Area link number

Enter the Area link number, by either typing it in, or using the Up and Down arrows to select the number. The area number must be in the range 1 to 99 to link the area to the common area.

Linked area name

The Linked area name will populate in its field.

Assigned area or area group

In the Assigned area or area group field choose from the drop down arrows of either Area or Area group. Depending on what was chosen the next field will be Area or Area group.

Select the Area field or the **Open** button next to it to display a list of Areas that may be used with this Area link. Select or create the Area to be used, then press the **OK** button to save. The Area may be cleared from this entity by selecting the  trash icon next to the Area field.

Or

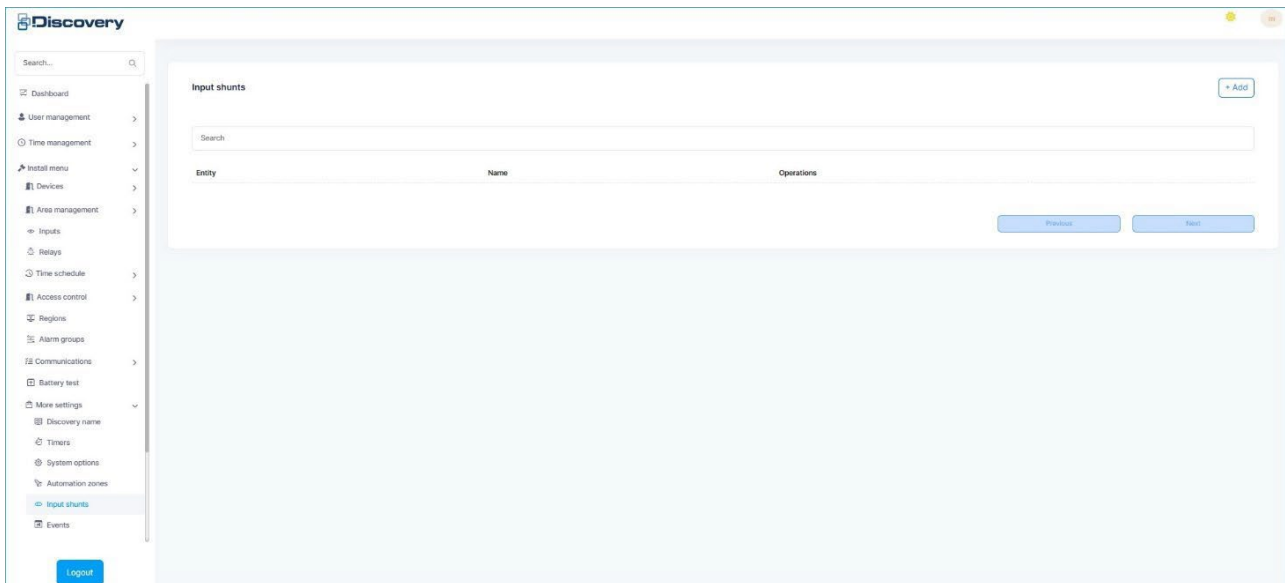
Select the Area group field or the **Open** button next to it to display a list of Area groups that may be used with this Area link. Select or create the Area group to be used, then press the **OK** button to save. The Area group may be cleared from this entity by selecting the  trash icon next to the Area group field.

Input shunts

INSTALL MENU > MORE SETTINGS > INPUT SHUNTS

This option is used to program shunt timers, which control shunt procedures. A shunt procedure inhibits an input from being activated when in an unsealed condition and for a specified interval. For example, a shunt stops a door from generating an alarm when it is opened. If the input is still unsealed after the shunt time expires, the input will generate an alarm, depending on the input type and the status of the area.

A worksheet is provided to record programming details and to further describe this option. See "[Input shunt worksheet](#)" on page 250.



Programming

A worksheet is provided to record programming details and to further describe this option. See “[Input shunts worksheet](#)” on page 250.

To program a new Input shunt, click the **+ Add** button to bring up the Setup page.

This page shows entries for Input shunts. You can Search for a created Entity which will show you its Name and Operations.

Shunt number

Each Shunt has a specific number that identifies the Shunt to the

control panel. Shunt numbers may be assigned to a certain Input shunts.

Shunt name

Enter the Shunt name.

Input number to shunt

The input can be assigned to multiple shunt timers. If the shunt timers have different shunt times, then the shunt time used will be the last one started. The display shows the current input number that relates to this shunt timer.

Enter the input number, and then press **OK**. Add a input by clicking on the **+ Add** input and filling out the required information. See [“Programming Inputs”](#) on page 64 for details. The Input may be cleared from this entity by selecting the  trash icon next to the Input field.

Relay number

The relay condition controls whether or not the input remains shunted.

If the relay is active, the input is always shunted. When the relay deactivates, the shunt timer continues to run for the programmed shunt time.

Enter the Relay number, and then press **OK**. Add a relay by clicking on the **+ Add** relay and filling out the required information. See [“Programming Relays”](#) on page 24 for details. The relay may be cleared from this entity by selecting the  trash icon next to the relay field.

Note: The total shunt time is the time the relay activates plus the shunt time.

Shunt time

If the shunt time expires and the input remains unsealed, an alarm condition occurs, depending on the input type. Shunt time values have special rules, as follows:

- Enter a value of 0 to 225 for shunt times of 0 second to 225 seconds.
- Enter a value of 60 for one minute, and 120 for two minutes.
- Do not enter a value of 128. You cannot create a shunt time of 128 seconds.
- Enter a value of $(128 + n)$ for a shunt time of n minutes. For example, if you want a shunt time of 30 minutes, use $128 + 30$ to give a value of 158.
- The maximum shunt time that can be programmed is 126 minutes (enter a value of 254).

Enter the shunt time.

Note: In Discovery a shunt time of 0 is the same as 1 second.

Event flag

The assigned event flag is activated when the shunt timer is running.

Enter the event flag number, or click **+ Add** event flag to enter an Event flag number. The Event flag may be cleared from this entity by selecting the  trash icon next to the Event flag field.

Warning time

The shunt warning time is the time the shunt warning event flag will be activated before the shunt timer expires. If the shunt time is programmed in seconds (a shunt time value of 1 to 127), the warning time is programmed in seconds. If the shunt time is programmed in minutes (a shunt time value of 129 to 254), the warning time is programmed in minutes. Enter the shunt warning time.

Warning flag

The Warning flag assigned is activated when the shunt warning time is active. Use the Search function to search for an Warning flag. Enter the Warning flag number or click **+ Add**. The Warning flag may be cleared from this entity by selecting the  trash icon next to the Warning flag field.

RAS

A RAS is assigned in order for the shunt messages to show on the RAS (subject to RAS options) and for the shunt to start from the RAS after the door open command. Enter the RAS number or click **+ Add**. See [“Programming RAS”](#) on page 29 for details. The RAS may be cleared from this entity by selecting the  trash icon next to the RAS field.

Shunt flags (Check boxes)

Door open command starts shunt

- Ticked A keypad or shunt relay is required to start the shunt timer. If a keypad is used, the user must have a valid door group assigned. The timer resets if the input does not switch to sealed state within either 3 seconds (a shunt time value of 1 to 127) or 3 minutes (a shunt time value of 129 to 254).
- Unticked The condition of the input (sealed to unsealed) triggers the timer.

Note: If this option is set to YES, then [“Entry/exit shunting”](#) on page 157 must be set to NO.

Door shunted in access

- Ticked The shunt procedure operates when one or more of the areas assigned to the input are in access.

- Unticked The shunt procedure does not operate when the areas assigned to the input are in access.

Note: At least one of Door Shunted In Access or Door Shunted In Secure must be set to YES for the shunt procedure to operate.

Door shunted in secure

- Ticked The shunt procedure operates when all of the areas assigned to the input are in secure.
- Unticked The shunt procedure does not operate when the areas assigned to the input are in secure.

Note: At least one of Door Shunted In Access or Door Shunted In Secure must be set to YES for the shunt procedure to operate.

Cancel door event

- Ticked As soon as the shunted input switches to sealed state, the door unlock event and the shunt timer are cancelled.
- Unticked The door unlock event and the shunt timer are not cancelled if the input switches to sealed.

Input hold event

- Ticked In order to allow time for a door to close, there is a 2-second delay after the input switches to sealed state and before it cancels the door event and shunt timer.
- Unticked There is no delay.

Entry/exit shunt

When entry/exit shunting is set to YES, a valid PIN must be entered at the RAS in order to prevent an alarm from being generated. The code may be entered just prior to the door being opened, or before the shunt time expires after the door has been opened.

- Ticked A PIN (or access card) is required. The user must have a valid door group assigned and the shunt timer number must be the same as the RAS number.
- Unticked Normal shunt procedure operation.

Note: If this option is set to YES, then [“Door open command starts shunt”](#) on page 156 must be set to NO.

Report door open/close

- Ticked Every time the input switches to sealed state and vice versa, it is sent to the printer.
- Unticked Disables the Input status changes being sent to the printer.

Note: If “[Print input when unsealed](#)” on page 69 is set to YES for the input assigned to the shunt timer, a door open message is sent twice.

Soft time zones

INSTALL MENU > TIME SCHEDULE > SOFT TIME ZONE

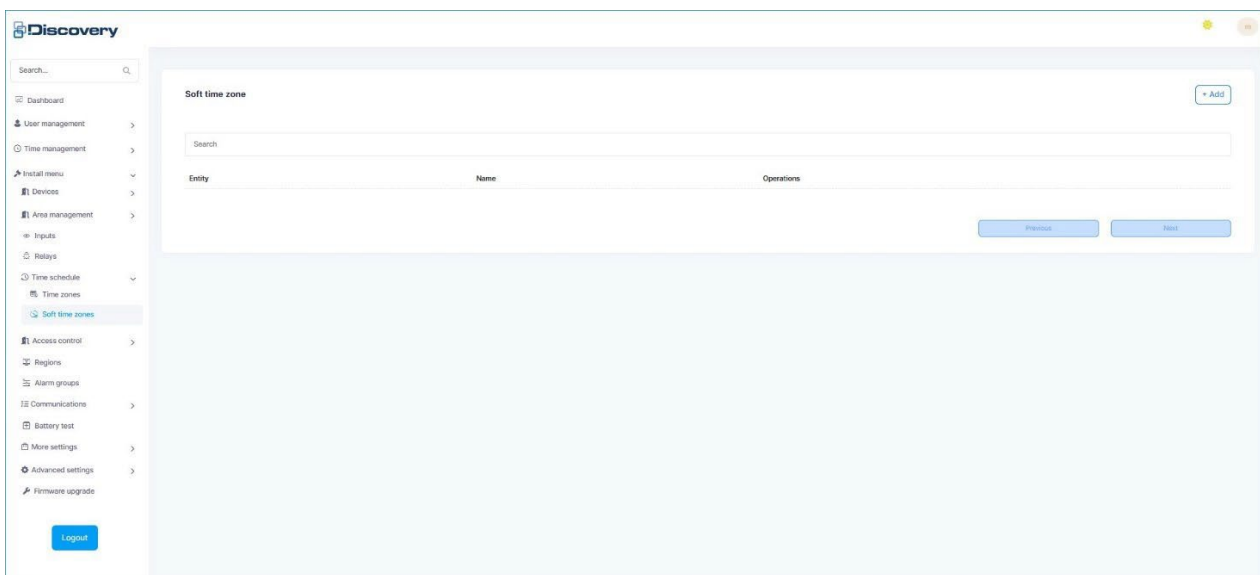
Time zone numbers between 26 to 41 are valid only when a relay or output is active. Soft time zones can be used:

- To control doors via a door group. For example, door 17 could be accessed only when a particular relay is active.
- To control alarm groups. If the time zone is assigned to an alarm group, the functions of the alarm group are enabled only when the relay is active.

Examples:

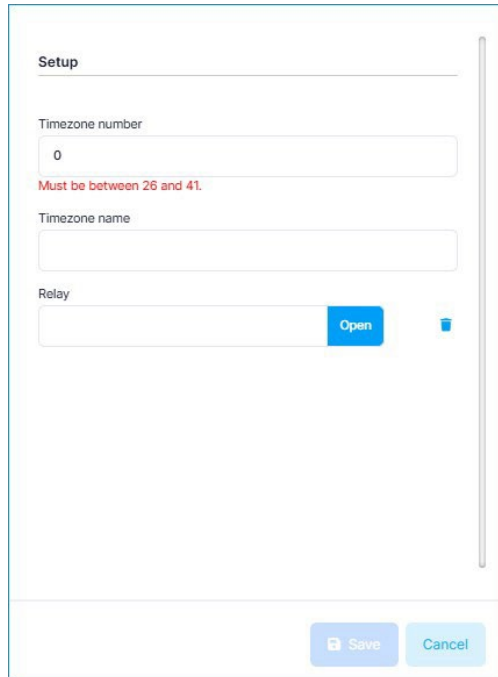
- To prohibit the use of a keypad unless a key switch on an input is active.
- To allow an area to be disarmed only if another area is disarmed first.

A worksheet is provided to record programming details and to further describe this option. See “[Soft time zones worksheet](#)” on page 251. See also “[Time zone numbering](#)” on page 207.



Programming

To program a new Soft time zone, click the **+ Add** button to bring up the Setup page.



The screenshot shows a 'Setup' form with the following fields and controls:

- Timezone number:** A text input field containing the value '0'. Below the field is a red error message: "Must be between 26 and 41."
- Timezone name:** An empty text input field.
- Relay:** A text input field with a blue 'Open' button to its right and a trash icon to its left.
- Buttons:** At the bottom right of the form are two buttons: 'Save' (with a floppy disk icon) and 'Cancel'.

Time zone number

Each time zone has a specific number that identifies the time zone to the control panel. Time zone numbers may be assigned to a certain Time zone.

Time zone name

Enter the Time zone name. The name may contain up to 30 characters (including spaces).

Relay

Enter the Relay that the soft time zone must follow or click **+ Add**. The Relay may be cleared from this entity by selecting the  trash icon next to the Warning flag field.

See "[Programming Relay](#)" on page 24 for details.

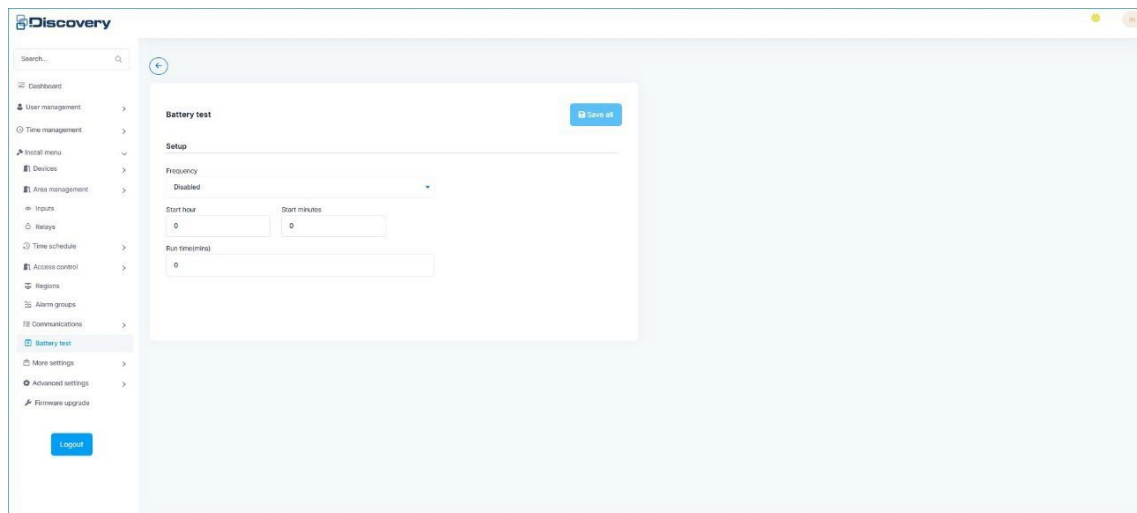
Battery test

[INSTALL MENU](#) > [BATTERY TEST](#)

Use this option to program automatic battery testing.

Note: Battery testing is not enabled as a default setting.

During the battery test, the control panel, DGPs, and all auxiliary driven devices, are powered from the battery. Devices are tested starting at 10 second intervals, ensuring that all devices do not switch to battery test at the same time.



Programming

A worksheet is provided to record programming details and to further describe this option. See "[Battery testing worksheet](#)" on page 251.

Frequency

This option specifies how often the automatic battery test should be performed,. Choose one of the options below and click on the option of choice.

Options:

- Disabled
- Test every working day
- Test every Monday
- Test on the 1st of every month
- Test daily

Note: If an instance of a scheduled battery test falls on a programmed holiday, that instance will not run.

Start hour and minutes

This option shows the start time for a programmed battery test.

Enter the Start time of day, in hours and minutes, when the battery test will start.

Hours option is between 0 hours and 23 hours, and minutes option is between 0 and 59 minutes. This can be entered by using the Up and Down arrows, or typing the value in.

Run time (mins)

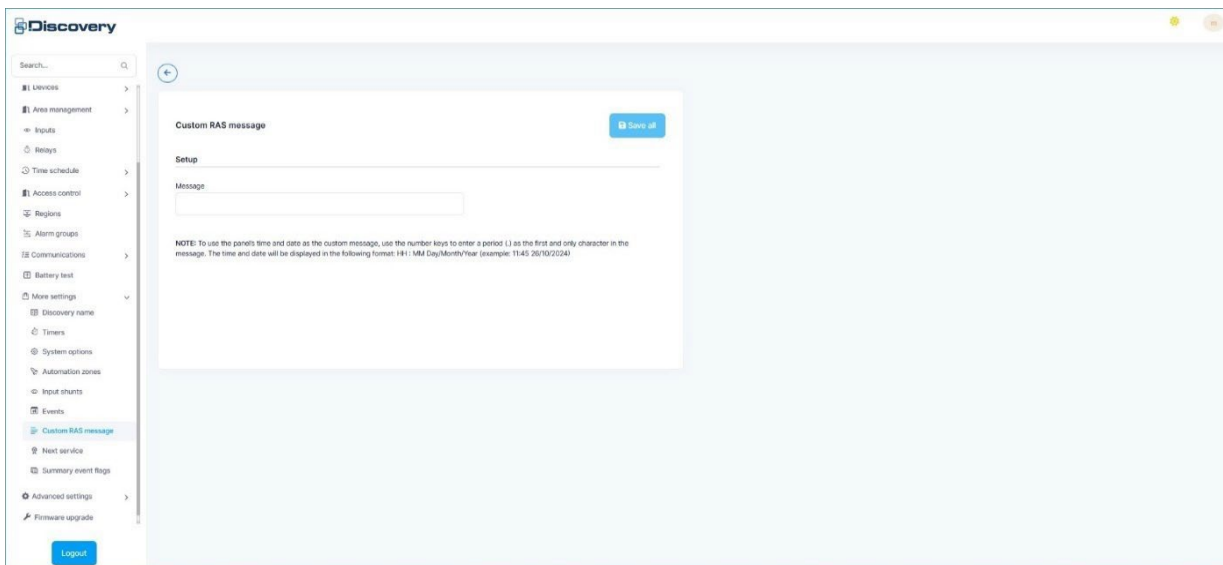
This option displays for a programmed battery test's run time. Enter the period, in minutes, that the automatic battery test will run.

If a battery test on any device fails, that device immediately restores mains power.

Once these values have been entered click on the **Save all** button.

Custom RAS message

INSTALL MENU > MORE SETTINGS > CUSTOM RASMESSAGE



This option creates a customised text message for the top line of the RAS's initial LCD screen. The text message can include numbers, spaces, and punctuation marks.

Use the Message field to enter a text message of up to 32 characters.

Note: To use the panel's time and date as the custom message, type a

period (.) as the first and only character in the message. The time and date will be displayed in the following format: HH:MM Day/Month/Year (example: 11:45 26/06/2013)

A worksheet is provided to record programming details and to further describe this option. See “[Custom RAS message worksheet](#)” on page 252.

Next service

[INSTALL MENU](#) > [MORE SETTINGS](#) > [NEXT SERVICE](#)

This option programs when the next routine service call is due and the display message. The user will be prompted with this programmable message to call the installer.

A worksheet is provided to record programming details and to further describe this option. See “[Next service date worksheet](#)” on page 252.

Date

Enter the date when the user will receive the next message prompt that maintenance is due.

Enter in the format of day, day, month, month, and then the year in its 4 digits (e.g.: 2025) (dd/mm/yyyy). Or use the calendar symbol to then populate the full date.

Text

Use the Text field to enter a message. The message may contain up to 32 characters (including spaces).

To program text via RAS, see “[Programming text via RAS](#)” on page 54.

Once all fields are populated click on the **Save all** button.

Summary event flags

INSTALL MENU > MORE SETTINGS > SUMMARY EVENT FLAGS

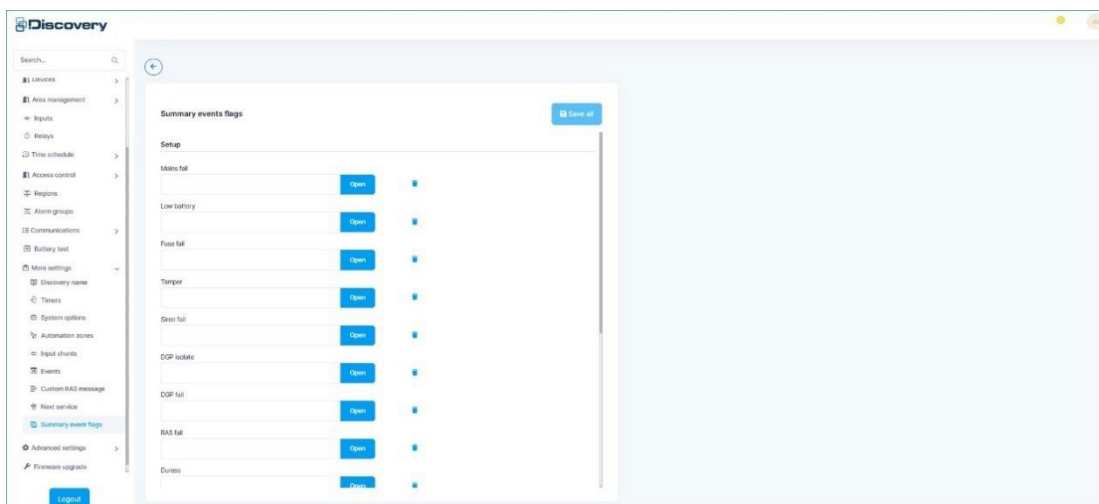
Summary event flags are triggered by system-wide events such as mains failures or DGPs going offline.

For example, to detect mains fail:

- Activate the mains fail summary event flag.
- Trigger a relay in response to the event flag.

The system alarm or fault event flags will be latching if latching system alarms is set to YES (see “[System alarms](#)” on page 112).

Note: User defined event flags are numbered between 1 to 255



Programming

To program the following summary event flags options:

1. Choose an unused event flag number.
2. Record the event flag details on an event flag worksheet.

Refer to “[Event flags](#)” on page 222 for details of these and other types of event flags. A worksheet is provided to record programming details and to further describe this option. See “[Event flags worksheets](#)” on page 252.

In each of these Summary event flags, enter an unused Summary event flag number, and press **OK**.

The Summary event flags may be cleared from this entity by selecting the  trash icon next to the Summary event flag field.

Mains fail

This event flag is activated when a mains failure is detected on the control panel or on a DGP.

Low battery

This event flag is activated when a low battery is detected on the control panel or on a DGP.

Fuse fail

This event flag is activated when a fuse failure is detected on the control panel or on a DGP.

Tamper

This event flag is activated when a panel tamper is detected on the control panel or on a DGP.

Siren fail

This event flag is activated when a siren fail condition is detected on the control panel or on a DGP.

DGP isolate

This event flag is activated when a DGP has been isolated.

DGP fail

This event flag is activated when a DGP programmed to be polled does not respond to polling.

RAS fail

This event flag is activated when a RAS programmed to be polled

does not respond to polling.

Duress

This event flag is activated when a keypad duress alarm occurs.

Film out

This event flag is activated when the film count for a camera exceeds the film out level.

Report fail

This event flag is activated for paths that have Trigger Comms Fail Event enabled to indicate, for example, that the control panel failed to report to the remote monitoring company on the first (and second, if applicable) phone numbers following the number of redial attempts programmed in “Number of redials”.

Test mode

This event flag is activated when the control panel is in test mode.

All secured

This event flag is activated when all areas have been armed, there are no alarm conditions, and no entry/exit timers running.

Console trigger

When this event flag is activated, all RAS buzzers are activated. The event flag also has to be assigned to the events that the RAS buzzer sounds on.

Area search running

The event flag specified here is activated when an area search is active. See [“Using Area Search”](#) on page 50.

Area search done

The event flag specified here is activated when an area search ends, and is deactivated with the area search time zone becomes invalid. See [“Using Area Search”](#) on page 50.

Panel macro logic

INSTALL MENU > ADVANCED SETTINGS > PANEL MACROS

A macro logic equation is a tool for activating inputs or event flags based on

the conditions of one to four macro inputs (event flags or relays).

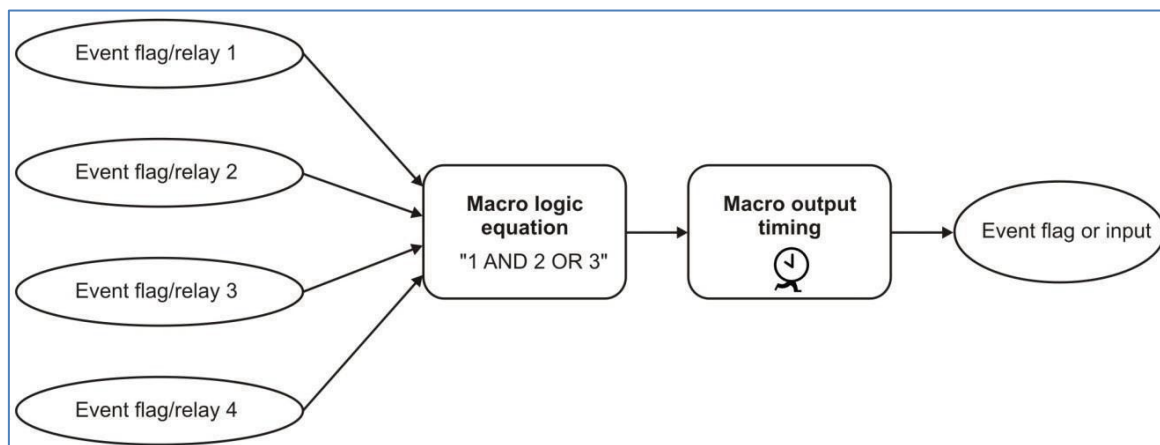
The macro logic equation can combine macro inputs using AND or OR logic, based on the event flag's or relay's active or inactive (inverted) state.

The output of the macro logic equation is an event flag or input. "AND" and "OR" functions can be made by inverting the logic of the particular input.

Programming options are provided so that the macro result will trigger a macro input as a pulse, time, on delay, off delay, or latch, when activated (see [Table 18](#) on page 168).

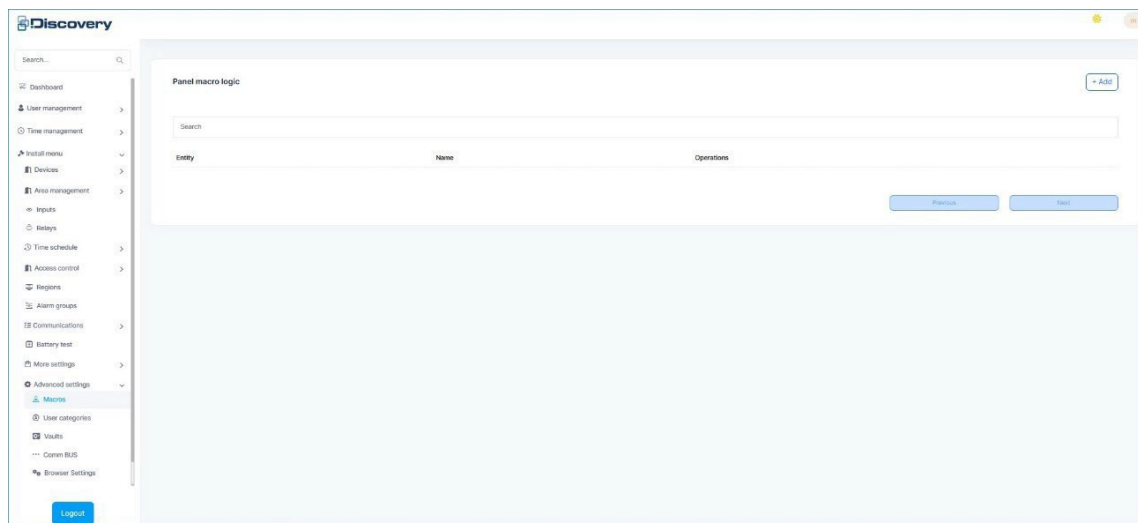
When the latched function is used, the fourth macro input resets the output and does not use the AND/OR selections.

Figure 26: Overview of macro logic



Note: It is very important to plan the macro logic carefully, noting all details and the origin of every input and event flag, before attempting to program.

A worksheet is provided to record programming details and to further describe this option. See "[Macro logic worksheet](#)" on page 255. See also "[Programming macros](#)" on page 41.



To program a new Panel macro logic, click the **+ Add** button to bring up the Setup page.

Macro number

Enter the number of the Panel macro logic (Entity).

Macro name

Enter the Macro name in. The name may contain up to 30 characters (including spaces).

Macro type

Click on the Macro type drop down arrow to reveal the following options listed in Table 18 below. Click on the desired option.

See also “[Examples of macro function selections](#)” on page 43.

Table 18: Macro output options

Option	Function
Disabled	This macro logic program is disabled.
Nontimed	Follows the result of the logic equation only. If an event flag or output for this macro changes, the logic equation will be calculated again.
On pulse	Activates for the programmed time or the active period of the logic result, whichever is shortest. This option is either On Pulse – seconds, or On – Pulse minutes.
On timed	Activates for the programmed time regardless of the macro output changing. This option is either On Timed – seconds, or On – Timed minutes.
On delay	Activates after the programmed time unless the result of the logic equation is no longer valid. This option is either On Delay – seconds, or On – Delay minutes.
Off delay	Follows the result of the logic equation, but remains active for the time programmed after the result of the logic equation is no longer active. This option is either Off Delay – seconds, or Off – Delay minutes.
Latched	Activates on any of the first three macro inputs in the logic equation and is only reset by the fourth macro input. Any programmed AND / OR function is not used.

Macro Duration (sec/min)

Enter the time period (0 to 255 seconds or minutes) that is used when any of the timed macro output functions are selected (on pulse, on timed, on delay, or off delay).

When

Enables programming of up to four logic inputs, which can be event flags or relays. For each logic input, select the logic input type (Event flag or Relay), then select the specific event flag or relay by clicking the Browse button or entering the event flag number or relay number directly into the field.

The logic connecting the four logic inputs can be programmed for AND or OR functions. A NAND or NOR function can be achieved by inverting the logic of the particular logic input with the Not check box.

Input 1 - 4

Type

Specify whether the macro output should trigger an **Event flag** or a **Relay**, and then specify which event flag or relay depending on choice.

Press the dropdown arrow to toggle between “Event Flag” and “Relay”.

Enter the event flag or input number from either typing it in or clicking on the **Open** Button and choosing your entry.

Enter the same number twice to invert the macro output. It will now trigger the event flag or output if the result of the equation is not true. An inverted macro output is indicated by the exclamation mark (!) preceding the number.

When the display shows the correct number, press OK to save the display and move to the next option.

Macro inputs

Program up to four macro inputs (event flag or relay numbers).

When all conditions of the logic equation are met, the macro output is active and the event flag or relay programmed in the previous step is activated (depending on any timing function programmed on the macro output).

Press the drop down arrow to toggle between Event Flag and Relay.

Select the Event flag / Relay field or the **Open** button next to it to display a list of Event flags / Relays that may be used with this input. Select or create the Event flag / Relay to be used, then press the **OK** button to save. The Event flag / Relay may be cleared from this entity by selecting the  trash icon next to the Event flag / Relay field.

Macro logic equation

Specify the logical operators that create the macro logic equation. Two operators are available, as follows:

- AND — Result is true only if both inputs are active.
- OR — Result is true if one of the inputs is active. Click the drop down arrow to toggle between AND or OR.

Press **Save** to save the displayed information and to return to the original macro logic display.

Note: NAND and NOR functions can be made by inverting the logic of the particular input. Any unused macro inputs must be tick as “NOT”.

If any macro entry needs to be deleted select the  trash icon next to the corresponding Macro entry.

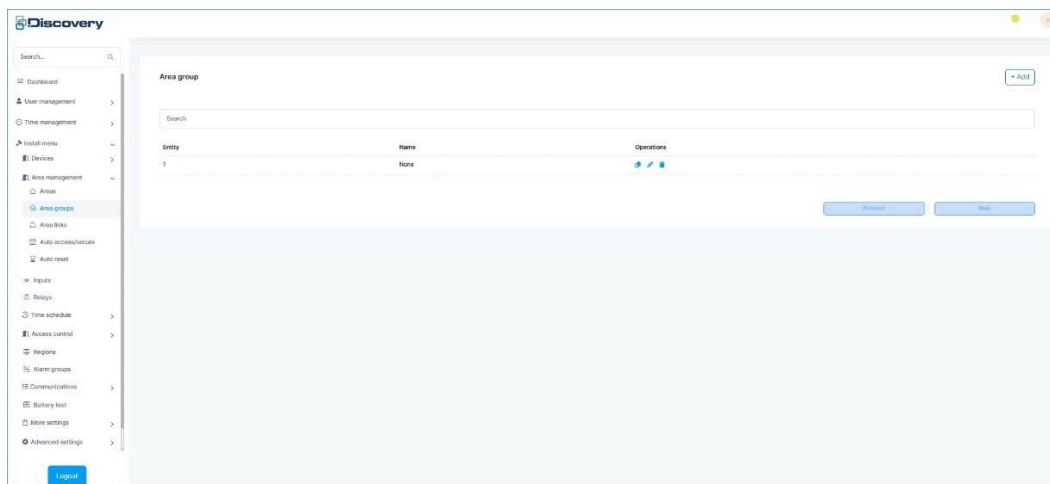
Area group

INSTALL MENU > AREA MANAGEMENT > AREA GROUP

A Discovery system can have 99 areas. To help manage areas, one or more areas can be incorporated into area groups. There can be 255 area groups.

Note: Area Group 1 contains all areas by default. If the Discovery panel does not need all areas, we recommend removing unneeded areas from Area Group 1.

Each area in an area group must be configured to allow certain users (as specified by the user's alarm group) to have permissions for arming, disarming, alarm reset, and for timing.



Programming

To program a new Area group, click the **+ Add** button to bring up the Setup page.

Setup

Area group number

Must be between 1 and 255.

Area group name

Area

Add area

Area

Arm

Disarm

Reset

Time

Save

Cancel

Area group number

Enter an area group number.

Area group name

Type the Area group name. The name may contain up to 30 characters (including spaces).

Area

To add the first area to the group, click the **Add area** and tick the area number in the range from 1 to 99.

Tick the required **Area properties**

Arm area - area to be armed.

Disarm – area to be disarmed

Reset – allows alarms in this area to be reset.

Time – allows this area to be time disarmed.

Note: After you add the first area to the group and scroll through the options, you can continue adding areas by enabling them as you come to them, or by returning to the area group later and adding the next area by number.

In each of these Areas, once entered press **OK** save.

Automation zone

INSTALL MENU > MORE SETTINGS > AUTOMATION ZONE

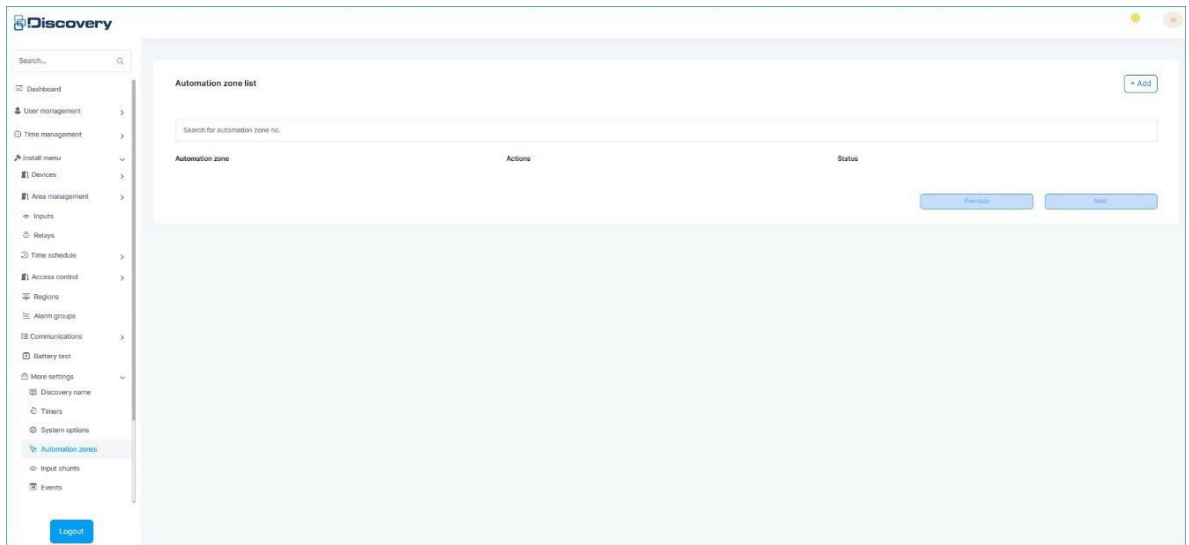
Use the Automation menu to configure automation zones.

An automation zone is one or more building devices (including C-Bus® devices) that can be controlled via the Discovery panel.

The automation zone record enables control to (and optionally feedback from) one or more devices in a C-Bus group. This section refers to such devices as an 'automation zone' even if it applies to a C-Bus group.

Refer to "[Controlling automation zones via RAS](#)" on page 56 for details about manually turning automation zones on and off via an LCD RAS.

A worksheet is provided to record programming details and to further describe this option. See "[Automation zones worksheet](#)" on page 262.



Programming

To program a new Automation zone, click the **+ Add** button to bring up the Setup page.

Automation zone number

The record number identifies an automation zone.

Automation zone name

The first 30 character of the description (including spaces) are sent to the panel as the automation zone name.

Enable (Checkbox)

When the automation zone is enabled, the Discovery panel can interact with it.

- Ticked Enables the automation zone.
- Unticked Disables the automation zone.

Trigger level (%)

This option determines the automation zone's maximum value (such as the brightness of lights) when triggered (turned on) by the Challenger panel.

The range of allowed values is 0 to 100%.

Reset level (%)

This option determines the automation time zone's maximum value (such as the brightness of lights) when triggered (turned on) by the Discovery panel.

Enter a value in the range 0 (off) to 100 (on).

Trigger time (sec)

This option determines the duration (in seconds) that the automation zone will be at active (including ramp time) when triggered by the Challenger panel.

The range of allowed values is from 0 to 65,535 seconds.

Ramp rate

This option determines the rate (speed) which is the time interval at which the automation zone will change between the Reset level (above) and the Trigger level (above). The options are:

- Instantaneously.
- 4 seconds.
- 8 seconds.
- 12 seconds.
- 20 seconds.
- 30 seconds.
- 40 seconds.
- 60 seconds.
- 90 seconds.
- 2 minutes.
- 3 minutes.
- 5 minutes.

- 7 minutes.
- 10 minutes.
- 15 minutes.
- 17 minutes.

To save all of these entries for the Automation zone click **Save** or to cancel click **Cancel**.

Trigger time zone

An event flag is used to trigger the automation zone.

Enter the event flag number, by clicking in the field and selecting from the list. Or create a new one by clicking on the **Add panel time zone**, or **Add soft time zone** and fill the Setup form out.

The Trigger time zone may be cleared from this entity by selecting the  trash icon next to the Trigger time zone field.

Disable trigger TZ (Time zone)

Nominate a hard or soft time zone in which the event flag cannot trigger the automation zone.

Select trigger time zone event setup. Or create a new one by clicking on the **Add panel time zone**, or **Add soft time zone** and fill the Setup form out.

The Disable trigger time zone may be cleared from this entity by selecting the  trash icon next to the Disable trigger time zone field.

Event to trigger time zone

This option can trigger the automation zone when the nominated event flag is inactive.

Select Event to trigger time zone. Or click on the **+ Add event flag** to create a new one.

The Event to trigger time zone may be cleared from this entity by selecting the  trash icon next to the Event to trigger time zone field.

Tick boxes to enable:

Invert trigger

Use this option to Invert the automation zone trigger event flag

- Ticked Inverts the automation zone trigger event flag.
- Unticked Triggers the automation zone normally.

Enable logging

Use this option to log the automation zone's C-Bus events to the panel's history.

- Ticked Logging of C-Bus events is enabled. C-Bus events will be recorded in the Challenger panel

history and communicated to management software.

- Unticked Logging of C-Bus events is disabled.

Automation only on for mask

Use this option to enable automation only on for masking effect

- Ticked Automation only on for masking effect enabled
- Unticked Automation only on for masking effect disabled

Enable quick control

Use this option to enable quick control via supported RAS models.

- Ticked Enables quick control via supported RAS modules (the CA111x RAS's left hand "-" key).
- Unticked Disables quick control.

Note: Quick control does not require user authentication via PIN. We recommend that control be assigned to a specific RAS (in a secure area) in "Control zone on RAS" in order to prevent unauthorised use.

Enable manual control

Use this option to enable control via User menu 24–Automation Control and to allow users to activate (trigger) the automation zone (installers can manually activate the automation zone via Install menu option 43– Automation Status without this option being enabled).

- Ticked Allow operators to activate the automation zone via management software, or users via RAS menu 24.
- Unticked Does not allow operators or users to activate the automation zone.

Manual on control

Use this option to enable installers and users to turn the automation zone on immediately at 100% until turned off or triggered (in which case the zone's programming will turn it off).

- Ticked Allow operators to activate the automation zone to 100% On immediately via management software, or users via RAS menu 24, or RAS quick control (see Enable quick control above).
- Unticked Does not allow operators or users to activate the automation zone.

Manual off control

Use this option to enable installers and users to turn the automation zone off (reset) immediately.

Nominate a hard or soft time zone to trigger the automation zone (regardless of an event flag). Enter the time zone number in the range 0 to 63, and then press [ENTER].

- Ticked Allow operators to activate the automation zone to Off immediately via management software, or users via RAS menu 24, or RAS quick control (see Enable quick control above).
- Unticked Does not allow operators or users to activate the automation zone to Off immediately.

RAS number

Select a RAS number, or click on the **+ Add ras** to create a new one. The RAS number may be cleared from this entity by selecting the  trash icon next to the RAS number field.

Protocol type

Select the Protocol type from the drop down list:

- Internal
- TECOM
- TECOM with feedback
- CBUS
- CBUS with feedback

Activates event flag

This option activates an event flag when triggered.

Select an Activates event flag event. Or click on the **+ Add event flag** to create a new one. The Activates event flag may be cleared from this entity by selecting the  trash icon next to the Activates event flag field.

Set event flag level (%)

This option applies only if the automation zone Type (above) is set to C-Bus with feedback. When the automation zone reaches a specified brightness level, the associated Challenger event flag is set (activated). For example, set the event flag when the automation zone reaches 90% brightness.

Enter a value in the range 0 (off) to 100 (on).

Reset event flag level (%)

This option applies only if the automation zone Type (above) is set to C-Bus with feedback.

When the C-Bus zone reaches a specified brightness level, the associated Challenger event flag is reset (deactivated). For example, reset the event flag when the automation zone reaches 30% brightness.

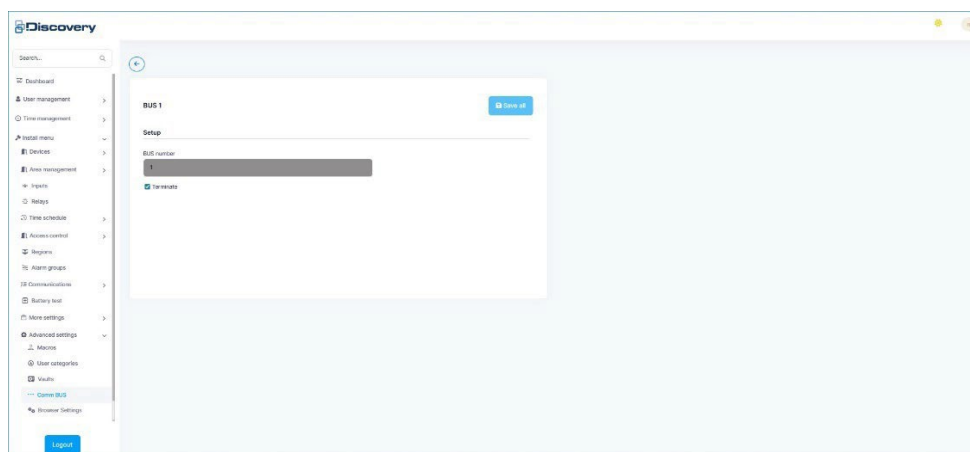
BUS number

RAS menu name: Network number. Bus number tells the Challenger panel what C-Bus network the zone uses. The bus number ranges from 0 to 255.

The location for setting the "Electronic LAN termination" on the Discovery

Web Interface is:

Install menu > Advanced settings > Comm BUS > Select a Comm BUS > Tick or Un-tick the "Terminate" button



Group number

Group number associates this automation zone record with a C-Bus group for monitoring and controlling.

The group number ranges from 0 to 255.

App number

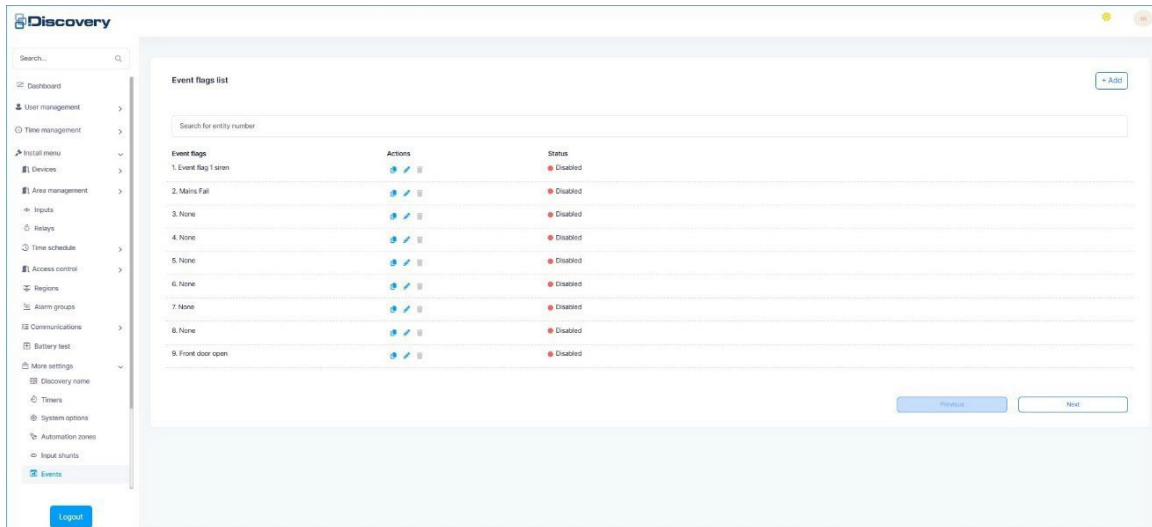
The devices in the C-Bus group may be filtered via C-Bus application address designations. If applicable, enter the C-Bus application address.

The App number ranges from 0 to 255.

Event flag

INSTALL MENU > MORE SETTINGS > EVENTS

A Discovery panel's event flags can be assigned names. Use this option to assign or change an event flag's name.



Programming

To program a new Event flag, click the **+ Add** button to bring up the Setup page.

The 'Setup' page for an event flag. It has a title 'Setup' and a search bar. Below is a form with two fields: 'Event flag number' with a dropdown menu showing '1' and a red error message 'Must be between 1 and 255.'; and 'Event flag name' with a text input field containing 'DEFAULT'. At the bottom right are 'Save' and 'Cancel' buttons.

Setup

Event flag number

1

Must be between 1 and 255.

Event flag name

DEFAULT

Save Cancel

Event flag number

Enter the event flag number.

Event flag name

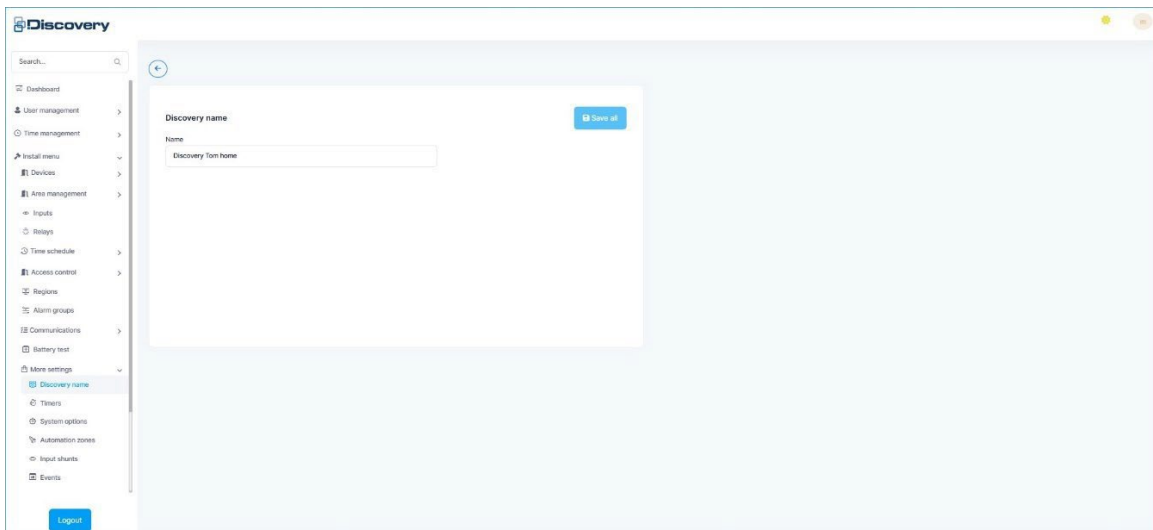
Enter the name by typing it in. The name may contain up to 30 characters (including spaces).

To save the entry click on the **Save** button. To cancel click on the **Cancel** button.

Discovery name

[INSTALL MENU](#) > [MORE SETTINGS](#) > [DISCOVERY NAME](#)

This feature allows you to name the Discovery panel. This is useful when there are multiple panels on a site.



Enter a name to describe (name) the Discovery panel. The name may contain up to 30 characters (including spaces).

Click the **Save all** button to save it.

Standard lifts

[INSTALL MENU](#) > [ACCESS CONTROL](#) > [LIFTS](#) > [STANDARD LIFTS](#)

Discovery panels can support two lifts with up to ten floors each, without requiring a Four-Lift Controller.

Each lift may have up to two reader interfaces:

- The **local reader** is the standard lift reader where a user can badge a card or enter a PIN to activate their desired floor.
- The **remote reader** enables the user to remotely activate the floor to allow a visitor to access the lift and select the desired floor.

Each reader has an access timer. This allows the remote reader to be configured with an extended access time compared to the local reader. For example, the remote reader can be configured with enough time for a visitor to cross an apartment building's foyer to get to the lift and select the desired floor.

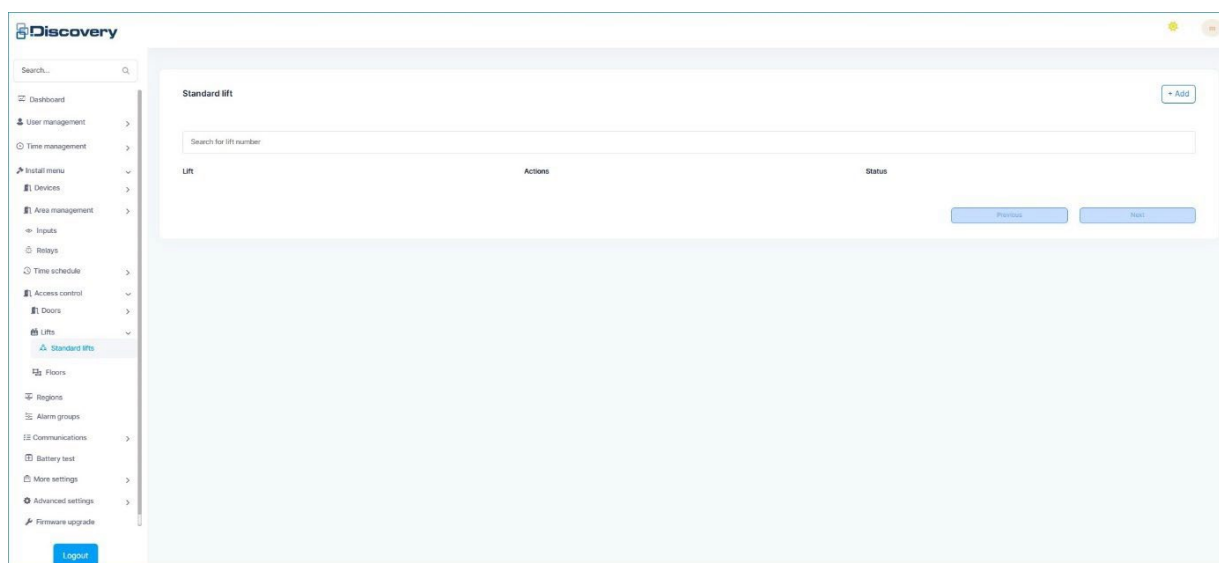
An override floor group can be configured for each lift so that certain floors can be accessed at certain times of the day, without requiring a valid card or PIN at the lift reader.

A security event flag and security floor group can be configured for each lift. When the security event flag is activated, the security floor group is activated. The security floor group allows certain floors to be accessed at certain times of the day, without requiring a valid card or PIN at the lift reader, provided the security event flag is activated.

The time that a floor will be active for will be determined based on which reader has activated it. For example, if a floor relay has been activated via a remote reader, and another floor relay has been activated by the local reader, then each floor relay will be active for the appropriate amount of time. This allows multiple remote readers to activate multiple floor relays.

See the *Discovery Administrators Manual* for more information on programming floor groups.

A worksheet is provided to record programming details and to further describe this option. See "[Standard lifts worksheet](#)" on page 264.



Programming

To program a new Lift, click the **+ Add** button to bring up the Setup page.

Setup

Lift number
0
Must be between 1 and 128.

Lift name

☒ Enabled

Local reader location
Default (local lift no) ▼

Remote reader location
Default (remote RAS no) ▼

Remote RAS
Open

Local RAS access time (sec)

Save Cancel

Lift number

Enter a Lift number in the range 1 to 128.

Lift name

Enter a name to identify the lift. The name may contain up to 30 characters (including spaces).

Enabled (checkbox)

Tick the checkbox to enable the lift.

Local reader location

From the drop down menu choices are:

- Default (local lift no)
- Onboard Wiegand 1 – Use onboard Reader ports 1 or 2
- Onboard Wiegand 2 – Use onboard Reader ports 1 or 2

Remote reader location

From the drop down menu choices are:

- Default (remote RAS no)
- Onboard Wiegand 1 – Use onboard Reader ports 1 or 2
- Onboard Wiegand 2 – Use onboard Reader ports 1 or 2

Remote RAS

Search, Choose or **+ Add ras** from the RAS setup screen.

Local RAS access time (sec)

Enter a value (1 to 255 seconds) for the lift access time from the local reader. This will determine how long the relay(s) are accessed for when a valid user accesses the Lift reader. The default value is 5 seconds.

Enter the number of seconds required.

Remote RAS access time (sec)

Enter a value (1 to 255 seconds) for the lift access time from the remote RAS. This will determine how long the relay(s) are accessed for when a valid user accesses the remote reader (if used) for this lift. The default value is 10 seconds.

Enter the number of seconds required.

Security event

Search, Choose or **+ Add event flag** from the Security Event Flag setup screen.

Override floor group

Enter the number of a designated floor group (1 to 128) that determines the floors that may be freely accessed in the lift controls.

Click the **Open** button to select the Override floor group. To create one use the menu options to add floor group. The Override floor group may be cleared from this entity by selecting the  trash icon next to the Override floor group number field.

Security floor group

Enter the number of a floor group (1 to 128) that determines the floors that may be freely accessed in the lift controls, without using a valid card or PIN at the lift reader, provided that the security trigger event flag is activated.

Click the **Open** button to select the Security floor group. To create one use the menu options to add floor group.

The Security floor group may be cleared from this entity by selecting the  trash icon next to the Security floor group number field.

Floor 1 Relay – Floor 10 Relay

A relay can be set for each of the ten floors for the lift.

Enter a relay number (from 1 to 512) for the floor

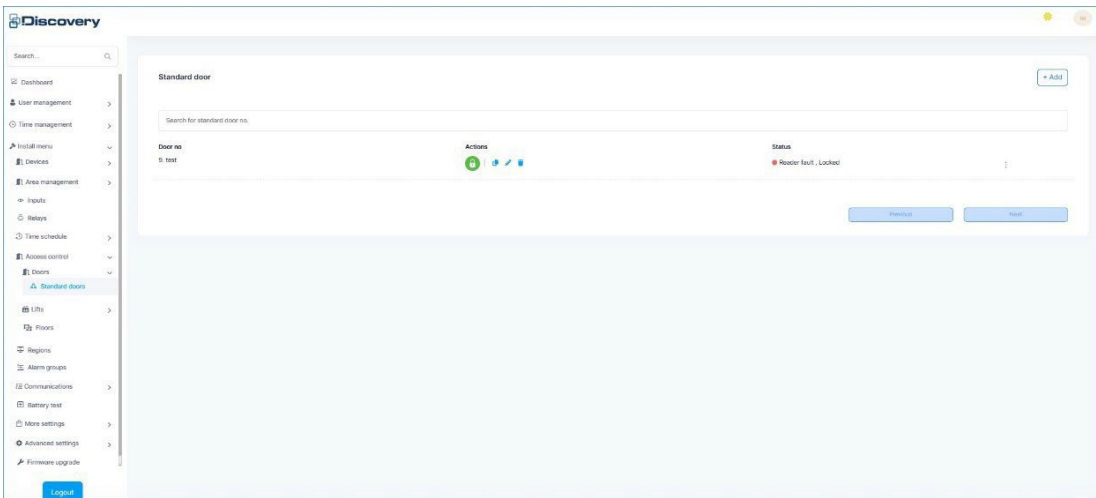
Click the **Open** button to select the floor group. To create one use the menu options to add a Relay.

The Floor # Relay may be cleared from this entity by selecting the  trash icon next to the Floor # Relay number field.

Standard doors

INSTALL MENU > ACCESS CONTROL > DOORS > STANDARD DOORS

Discovery panels can support 32 doors, without requiring a Four-Door Controller or Network Access Controller.



A worksheet is provided to record programming details and to further describe this option. See “[Standard doors worksheet](#)” on page 265.

To program a new Door, click the **+ Add** button to bring up the Setup page.

Setup

Door number

0

Must be between 1 and 128.

Door name

☒ Enabled

Reader location

Default (door number)

☒ Override after entry

☒ Report DOTL

☒ Report open close

☒ Report forced

☒ Report secure/unsecure

Access time (sec)

5

Save

Cancel

Door number

Enter a Door number in the range 1 to 128.

Door name

If the door does not exist, the RAS will prompt you to create it. Name the door. A maximum of 30 characters including spaces.

Enabled

Tick the checkbox to enable the Door.

Reader location

From the drop down menu choices are:

- Default (door number)
- Onboard Wiegand 1 – Use onboard Reader ports 1 or 2
- Onboard Wiegand 2 – Use onboard Reader ports 1 or 2

Override after entry

This option determines whether the override time zone (see [“Override time zone”](#) section on page 186) takes effect immediately when the time zone commences or after a user enters.

When set to Enabled, the override time zone takes cannot unlock the door for the programmed times unless a user has entered.

Toggle this option to enable Override after entry

- Ticked Override after entry enabled
- Unticked Override after entry disabled

Report DOTL

The door can send a report to the printer/computer when a DOTL (Door Open Too Long) condition is detected.

Toggle this option to enable a report to be sent to a printer/computer when the door is open too long.

- Ticked Report door DOTL enabled
- Unticked Report door DOTL disabled

Report open close

The door can send a report to the printer/computer when the input assigned to the door is unsealed and resealed.

Toggle this option to enable a report to be sent to a printer/computer when a door is open or closed (Sealed or unsealed)

- Ticked Report open close enabled
- Unticked Report open close disabled

Report forced

The door can send a report to the printer/computer when the door is forced (i.e. input unsealed while the door is locked).

Toggle this option to enable a report to be sent when a door is forced.

- Ticked Report forced enabled
- Unticked Report forced disabled

Report secure/unsecure

The door can report secured and accessed (unsecured) events. This option only functions when the hardware type is set to Maglock. It is intended to specifically report when a door is secured (closed, locked, and not shunted), as opposed to simply locked/unlocked, or opened/closed.

When this option is set to Enabled, whenever a user badges their card and/or access is granted on a door, the door lock will unlock and send an "unsecured" message to the management software. When the door is locked, the door input is sealed, and shunting has expired (if configured), a "secured" message will be sent to the management software.

Toggle this option to enable a report when a door is secure / unsecure.

- Ticked Report door secure / unsecure enabled
- Unticked Report door secure / unsecure disabled

Access time (sec)

Program the amount of time for the door to unlock when a user enters a valid card or PIN at the door reader. The user is then able to open the unlocked door during the access time. Enter the number of seconds required.

Pre-lock time (sec)

Once the door input has been sealed, the Discovery panel waits for the pre lock time to expire before locking the door. If the door opens input unseals during the pre-lock time, the door is deemed open and the pre lock timer is cancelled. The shunt continues during the pre-lock time. Enter the number of seconds required.

Post-lock time (sec)

The post-lock time allows time for a lock to fully engage. After the post lock time has expired, the door is deemed secure, and the shunt is cancelled. If the door input unseals during the post lock time, the door is deemed open and the post lock timer is cancelled. The shunt continues during the post lock time. Enter the number of seconds required.

Multi badge time

The multi badge time is the amount of time allowed between the first and last presentation of the card. If the card is not presented within this time, then the user will need to commence the function again.

The value can be specified in seconds or minutes.

Override time zone

The override time zone controls the times when the door can be opened without the need to use a valid card or PIN. Free access is allowed when the time zone is valid.

Select the Override time zone field or the **Open** button next to it to display a list of time zones that may be used with this Door. Select or create the time zone to be used, then press the **OK** button to save. The time zone may be cleared from this entity by selecting the  trash icon next to the Override time zone field.

Door event flag

This event flag triggers when a user opens the door and remains active for the Trigger duration.

Select the Door event flag field or the **Open** button next to it to display a list of events that may be used with this door. Select or create the event to be used, then press the **OK** button to save. The event may be cleared from this entity by selecting the  trash icon next to the Door event flag field.

Event flag active time (sec)

Defines the time for the Door event flag (above) to remain active. The range is 0 to 65,535 (0 means that it is not timed).

Preferred camera

Select the preferred camera number from the list.

Shunt options

Shunting is a procedure that stops an open door causing an alarm for a set time.

Shunt type

This field defines shunt conditions. The options are:

Options	Function
No shunting	The door is not shunted.
Input shunting	The door is shunted. Generates an alarm, based on the input type settings, if left open longer than the programmed shunt time.
Input shunting & DOTL	The door is shunted as with option 1, and additionally generates a DOTL (Door Open Too Long) alarm if it is left open longer than the programmed shunt time.
Auto shunting & DOTL	The door is shunted as with option 1, and additionally generates a DOTL (Door Open Too Long) alarm if it is left open longer than the programmed shunt time.

Choose the shunt option from the drop down.

Shunt time (sec)

Program the amount of time that the door may be opened for without causing an alarm (shunted). This allows time for a user to pass through the door and shut it again. Enter the number of seconds required.

Warning time (sec)

Program the amount of time for a relay to activate, to sound a warning device, before the shunt time expires. Enter the number of seconds required.

Cancel shunt when door is secured

For security reasons, it may be required to limit the shunt period as much as possible in order to detect the door being opened again during the shunt time (after the debounce time of approximately 2 seconds).

Select this option to use the programmed shunt time to shunt the door input and then to cancel the shunt when the door closes (i.e. the door input is resealed).

Toggle the Cancel shunt when door is secured to enable it.

- Ticked Enable cancel shunt when door is secured
- Unticked Disable cancel shunt when door is secured

Alarm

Alarm control

Select the type of alarm control that can be used by the door from the drop down.

Option	Function
0 No alarm control	It is not possible to arm/disarm using the reader.
1 1 badge to disarm, 3 to arm	Presentation of a valid card at the reader will disarm the areas in the alarm group on first badge. Badging three times will arm the areas.

Deny if area secured

Deny access to the door if any area in the alarm group assigned to this door is secured/armed.

Toggle this option to enable deny access to the door if any area in the alarm group assigned to this door is secured/armed.

- Ticked Enable deny access to the door if any area in the alarm group assigned to this door is secured/armed.
- Unticked Disable deny access to the door if any area in the alarm group assigned to this door is secured/armed.

Alarm group

Alarm groups may be assigned to doors to restrict alarm control from that door to the areas assigned to the alarm group.

Restrictions on the level of alarm control available (for example Disarm Only), and the time period (time zone) when the alarm control functions can be performed, may also be specified in the alarm group.

See "[Alarm groups](#)" on page 90 for details.

Select the Alarm group field or the **Open** button next to it to display a list of Alarm groups that may be used with this Door. Select or create the Alarm group to be used, then press the **OK** button to save. The Alarm group may be cleared from this entity by selecting the  trash icon next to the Alarm group field.

Egress

Egress time zone

The egress time zone controls the times when an egress button will unlock a door to allow

exit. When the time zone is valid, a user can press the egress button and the door will unlock.

Select the Egress time zone field or the **Open** button next to it to display a list of time zones that may be used with this Door. Select or create the time zone to be used, then press the **OK** button to save. The time zone may be cleared from this entity by selecting the  trash icon next to the Egress time zone field.

Egress reporting

When selected, a report is sent to management software when the egress function is used. This is only a reporting function.

- Ticked Egress reporting enabled
- Unticked Egress reporting disabled

Hardware

Lock type

To support simple programming of complex door operation, the Challenger has various lock types, with associated inputs, relays and timers. The lock type determines which inputs and relays are used and how they are used. The lock types are:

- Strike
- Maglock

Lock relay

Specify the relay number to be activated to unlock the door.

Select the Lock Relay field or the **Open** button next to it to display a list of Relays that may be used with this Door. Select or create the Relay to be used, then press the **OK** button to save. The Relay may be cleared from this entity by selecting the  trash icon next to the Lock Relay field.

Door input 1

Specify the input number used to indicate if the door is open or closed. This is usually the reed switch. Select the Door input 1 field or the **Open** button next to it to display a list of Door inputs that may be used with this Door. Select or create the Door input to be used, then press the **OK** button to save. The Door input may be cleared from this entity by selecting the  trash icon next to the Door input 1 field.

Warning relay

Specify the relay to be activated during the “Warning time” when the shunt timer is about to expire, e.g. may be used to activate a buzzer above a door to indicate the door needs to be closed.

Select the Warning Relay field or the **Open** button next to it to display a list of Relays that may be used with this door. Select or create the Relay to be used, then press the **OK** button to save. The Relay may be cleared from this entity by selecting the  trash icon next to the Warning Relay field.

DOTL input

This option specifies the input number that reports the DOTL (door open to long) alarm condition for the door being programmed (if DOTL is enabled in the shunting options for the door).

DOTL inputs must not have any alarm devices connected to them, and must be sealed with EOL resistors.

Select the DOTL Input field or the **Open** button next to it to display a list of Inputs that may be used with this door. Select or create the Input to be used, then press the **OK** button to save. The Input may be cleared from this entity by selecting the  trash icon next to the DOTL Input field.

Egress input

Specify the input number that activates the egress function for the door being programmed. Egress functionality is programmed on the door's Alarm/Egress tab.

Select the Egress Input field or the **Open** button next to it to display a list of Inputs that may be used with this door. Select or create the Input to be used, then press the **OK** button to save. The Input may be cleared from this entity by selecting the  trash icon next to the Egress Input field.

Chapter 6

Maintenance

Summary

This section provides information to help you diagnose and solve various problems that may arise while configuring or using your KGS Fire & Security Australia Pty Ltd product and offers technical support contacts in case you need assistance.

Content

Troubleshooting	192
Maintenance	196
Introduction	196
Standards	196
Peripheral devices	197
Automated testing	197
Recommended routine maintenance procedures	198
Contacting technical support	201

Troubleshooting

Refer to the following tables:

- Table 19: Discovery panel help below
- [Table 20](#): RAS and Card Reader help on page 194
- [Table 21](#): TS0820, TS0824, and TS1020 DGP help on page 195
- [Table 22](#): TS0840 to TS0842 Relay Card help on page 196

Onboard status LEDs indicates the live status of power, inputs and outputs, communications, and various connected devices.

Note: When tamper is sealed, only the **DC in** and **Batt** Power LEDs will operate. For full operation of onboard LEDs, tamper must be unsealed.

See the *Discovery Installation and Quick Programming Manual* for more information on the explanations on LEDs status.

Table 19: Discovery panel help

Condition	Possible causes
Master LCD Arming Station has all LEDs flashing and displays "Service" message.	The RAS programming option "LCD arming station" might be set to NO. The panel's LANs may be connected incorrectly. The address on the RAS may be incorrectly set.
Panel is not communicating with RASs and/or DGPs.	The panel's LANs may be connected incorrectly, or the wrong cable type may have been used. RAS and/or DGP numbers to be polled may not be programmed correctly or the device's LAN address may be incorrectly set.
RASs and/or DGPs appear to be going offline and online. (Indicated by RAS/DGP fail LEDs on 16-area RAS, by LCD "RAS Fail" message, or by excessive poll errors reported).	The panel's LANs may be connected incorrectly, or the wrong cable type may have been used. LAN termination may be incorrect. Short circuit on LAN.
Input going into alarm while area disarmed.	The programmed input type may be a 24-hr alarm or access alarm type. Input wired incorrectly causing tamper condition (open circuit or short circuit) instead of unsealed condition. EOL resistors may be installed incorrectly.
Unable to assign alarm groups when programming users.	No alarm groups have been programmed with the option "Can This Alarm Group be Assigned to Users" enabled. If a code other than the Master code (User 50) is being used to access "Program Users", the Alarm Group assigned to it may not allow the function (you can't assign an alarm group that has areas or menus that you don't have).

Panel not reporting to Monitoring Station.	Communications path may be configured incorrectly. In dialler panels, the path's account code may be programmed incorrectly. In dialler panels, the path's phone no. 1 must be programmed.
Inputs indicating unsealed when they are sealed.	The 2K2/6K8 end-of-line resistor option is not compatible with alarm devices using normally open (NO) alarm contacts, and will result in the input indicating unsealed when it is sealed.

Table 20: RAS and Card Reader help

Condition	Possible causes
All the LEDs on the RAS are flashing.	The address recorded on the RAS may be incorrect and polling to the RAS is not being acknowledged. The LAN may be connected incorrectly. The RAS is not being polled.
LEDs are not operating.	No power or low power.
LEDs do not appear to be indicating the correct condition.	Area LEDs may be incorrectly mapped. The RAS programming option “LCD arming station” might be set incorrectly for the particular RAS. The “Disable LEDs that don’t report” option may be set incorrectly.
An error is indicated (7 beeps) when a code is entered on the keypad.	An invalid PIN may have been used. The RAS may not have been programmed with an alarm group. The alarm group of the PIN may not permit access at this RAS.
A code or card is valid, but the door doesn’t unlock.	If the RAS is used to unlock a door, assign a door event flag to the RAS.
A code or card is valid, but the area doesn’t arm or disarm as expected.	The RAS’s options for “Cards auto disarm” or “Cards always disarm/arms” are set incorrectly.
A RAS has been replaced with a different model and it won’t go online.	If you disconnect an encrypted RAS and replace it with a non-encrypted RAS, the RAS will not work until you depoll and repoll it.
The RAS appears to lock up when the relay which it controls via the OUT terminal, activates.	The relay probably does not have a reverse diode across it to protect against back EMF.
When you touch a TS0004 or TS0210 RAS it seems to lock up due to static.	The RAS may not have been earthed. The star washers on the cover screws may not be in place. These are used to provide an electrical connection between the cover and the base.
TS1001 RAS displays unexpected results.	Base assembly not earthed as described in <i>TS1001 Touch Screen Arming Station Installation Manual</i> , REV 03 (or later).

Table 21: TS0820, TS0824, and TS1020 DGP help

Condition	Possible causes
The “Tx” LED on the DGP is not flashing.	The links may be incorrectly set. (The address recorded on the DGP may be incorrect and polling to the DGP is not being acknowledged). The LAN cable may be connected incorrectly. The DGP is not being polled. (It may not have been included in Data Gathering Panels to be polled when programming DGPs).
“Tx” and “Rx” LEDs are not operating.	No power or low power. The LAN cable may be connected incorrectly.
The DGP appears to be going offline and online. (Indicated by “DGPFail” on an LCD RAS or by the “DGP” LED on a TS0804 RAS).	LAN termination may be incorrect.
Some or all DGP inputs are permanently in tamper. (Or permanently in alarm if “Input Tamper Monitoring” in Install menu option 7 is set to NO).	The input numbers for the DGP have been calculated incorrectly, and input type numbers have therefore been assigned to the wrong inputs in the Input Database. The 8-Input Expansion module (if fitted) has the DIP switches incorrectly set. Additional items for TS1020 DGP: The EOL resistor setting may be incorrect. The expander type setting may be incorrect (you need to specify whether TS0021 or TS1021 modules are used). The 2K0, 1K5, and 1K0 options are not compatible with inputs connected via TS0021 Eight-Input Expansion Modules. The 2K2/6K8 option is not compatible with alarm devices using normally open (NO) alarm contacts.
Two or three Eight-Input expansion modules are fitted to increase the DGP to 24 or 32 inputs, but the 17 th to 32 nd inputs on the DGP do not seem to function.	DIP switch 5 on the DGP has not been set to ON. The expansion modules’ DIP switches may be set incorrectly.
4-Way Relay modules (TS0840) being used with the DGP do not function, but some of the LEDs on the module appear to be permanently on.	DIP switch 6 on the DGP is set to ON. (DIP switch 6 should only be on if 8-Way Relay modules or 16-Way Open Collector modules are being used).
8-Way Relay modules or 16-Way Open Collector modules connected to the DGP do not function.	DIP switch 6 on the DGP is set to OFF.
The siren output (with 8 ohm siren speaker connected) does not operate when it is meant to.	The 16th (last) relay number associated with the DGP address has not been mapped to a siren event flag number. The TS1020 DGP’s siren mode setting may be incorrect.

Table 22: TS0840 to TS0842 Relay Card help

Condition	Possible causes
8-Way Relay card (TS0841) won't function when connected to the Discovery panel.	The Number of Relay Controllers has not been set in Install menu System options.
8-Way Relay card (TS0841) won't function when connected to a DGP.	DIP switch 6 has been set to OFF.
16-Way Open Collector card (TS0842) won't function when connected to the Discovery panel.	The Number of Relay Controllers has not been set in Install menu System options.
16-Way Open Collector card (TS0842) won't function when connected to a DGP.	DIP switch 6 has been set to OFF.
4-Way Relay card (TS0840) won't function when connected to the Discovery panel.	The number of relay controllers has not been set to 0 in Install menu System options.
4-Way Relay card (TS0840) won't function when connected to a DGP.	The card's DIP switch 6 has been set to ON.
Relays will not function after being enabled as above.	The relay has not been mapped to an Event Flag or the relay number has been calculated incorrectly and therefore not programmed as the correct relay number. The relay is being held inactive during a time zone. The cable has been connected incorrectly, or is the wrong cable for the application. There are too many relay boards being powered from the Discovery panel's J14 connector (the panel can power one relay board only). The relay board's LED will appear dim or off if relays are drawing too much power. You will need to turn all relays off before you can recover from fuse fail condition.

Maintenance

Introduction

This section outlines the KGS Fire & Security Australia Pty Ltd recommended maintenance for Discovery panels.

Standards

Routine maintenance on intruder alarm systems installed in a client's premises should be performed in accordance with AS/NZS 2201.1-2007 SECTION 5 MAINTENANCE AND SERVICE, and SECTION 6 RECORDS AND REPORT.

Copies of this standard are available from Standards Australia and can be purchased online (Standards Australia web site: <http://www.standards.org.au/>).

Peripheral devices

Specific routine maintenance procedures for individual items of peripheral devices connected to the KGS Fire & Security Australia Pty Ltd equipment are not included in this procedure. “Peripheral devices” include, but are not limited to, movement detectors, smoke detectors, warning devices, batteries, and access readers.

Note that operation of most peripheral devices will be performed as part of the test procedures required in this maintenance procedure. However, this may or may not meet the routine maintenance procedures recommended by the suppliers or manufacturers of those devices.

If required, obtain routine maintenance procedures for peripheral devices from the suppliers or manufacturers of those devices. As a minimum, follow the procedure described in AS/NZS 2201.1-2007 relating to:

- Detection devices
- Audible and visible alarm and warning devices

Automated testing

Refer to the following sections for details of system features that can be used to provide some automated system testing:

- Input Test Type — See “[Input database](#)” on page 64.
- Siren Output Test — See “[System options](#)” on page 103.
- Periodic Dialler Test Reports — See “Communications” on page 121.
- Dynamic Battery Testing — See “[Battery testing](#)” on page 160.

These automated functions are not designed to replace any of the routine maintenance procedures, but will further enhance the integrity of the system during normal day-to-day operation.

Recommended routine maintenance procedures

Table 23: Discovery system routine maintenance schedule

Task	Frequency	Description
Notify the monitoring company	As required	If the system is monitored, the central monitoring station (CMS) staff must be notified before any tests are made. To perform testing and/or maintenance work on monitored systems, you must be authorised to do so. Central stations have procedures for identifying authorised personnel.
Notify personnel on the premises	As required	Prior to any test that will impact on any personnel, ensure that all affected personnel and appropriate supervisory and/or management staff are given any necessary notification, warning or instructions (for example, testing of zone inputs and warning devices).
Check the equipment schedule	Once per year	Check the installation, location and siting of all equipment and devices against the records supplied by the installation company. Record and report any discrepancy.
Check the wiring and conduits	Once per year	Inspect all visible wiring and conduits.
Check for dust, moisture and vermin	Once per year	Check for ingress of dust, moisture, condensation and vermin into all equipment enclosures. If excessive moisture or foreign matter is present, check enclosure location, environment, mounting method and cable entry points for sources of entry, and take steps to rectify.
Check the power supply	Once per year	Check that all mains operated modules and power supplies are connected to a mains outlet and are operational.
Check the Discovery 2 A power supply output voltage $13.8\text{ V} \pm 2\%$	Once per year	Test DC voltage across the “+” and “-” output terminals on all power supplies, with battery disconnected.
Check the detector supply voltage $13.8\text{ V} \pm 2\%$	Once per year	Test DC voltage across the “Auxiliary Power Output” terminals on the following equipment: • Discovery panel • Standard input data gathering panels • Intelligent 4-Door/4-Lift Controllers
Check batteries	Once per year	Check that all battery-backed panels and power supplies have the battery fitted and connected to the “Batt +” and “Batt -” terminals. • Discovery panel • Standard input DGPs • Intelligent 4-Door/4-Lift Controllers • Power supplies (battery backed)

Task	Frequency	Description
Test battery charge voltage 13.8 V $\pm$ 2%	Once per year	Test DC voltage on the “Batt +” and “Batt -” terminals. • Discovery panel • Standard input DGPs • Intelligent 4-Door/4-Lift Controllers • Power supplies (battery backed) NOTE: When mains power is restored following an AC fail condition, the battery charge voltage may range from 11 V to 13.8 V while the battery is recharging.
Replace battery	As specified by the battery manufacturer — OR — no more than 3 years	Replace the sealed lead-acid battery with a battery of the same specifications. Record the installation date of the new battery where it is clearly visible on the battery itself, or on a label clearly visible within the equipment enclosure and in the system maintenance records.
Check LCD/LED RAS keypad keys	Once per year	Check operation of every key on the keypad. Observe that labelling on all keys is clearly legible. Observe that keypad backlighting is operational on supported keypads.
Check LCD/LED RAS keypad displays	Once per year	Observe all LCD characters are operational. Observe LCD backlight is operational. Test operation of each LED on RAS terminals. See “Lamp test” on page 159.
Check LCD/LED RAS egress and output	Once per year	If the RAS egress or output is used then test their operation. The egress should open the door and the output should activate when required.
Test operation of access reader inputs and outputs	Once per year	Test the operation of all access readers using appropriate user ID tokens, including card, key fob, PIN, and so on. Results of reader operation and response of reader LEDs and beeper will depend on system programming. The required operation and test method should be recorded in the system maintenance records.
Test the secondary (backup) communications format (if provided)	As agreed between the alarm company and the client, but not less than once per year. Also see “Notes” on page 200.	NOTE: Must be pre-arranged in consultation with the CMS staff. • Disconnect the primary (main) communications format. • Perform an operation that triggers reporting. • Check that, after attempting to communicate via the primary format, the system reports successfully via the secondary format. • Re-connect the primary communications format.

Task	Frequency	Description
Test the primary (main) communications format. (May be performed in conjunction with zone input testing).	As agreed between the alarm company and the client, but not less than once per year. Also see "Notes" on page 200.	NOTE: Must be pre-arranged in consultation with the CMS staff. • Perform an operation that triggers reporting. • Check that the system reports successfully.
Test system inputs (detection devices). Test areas programmed to Report. NOTE: Special testing devices or procedures may be required if testing of smoke, heat, seismic glass-break detectors, and so on, is required.	As agreed between the alarm company and the client, but not less than once per year. Also see "Notes" on page 200.	• Obtain a list of all inputs to be tested. • Test each input by causing it to switch from the sealed state to un-sealed (alarm) and back to sealed. • The Test Input user menu can be used to monitor the zone activity. • Check-off each input on the list as it is successfully tested. • Record and report any discrepancy. Many alarm companies recommend that input testing includes reporting the zone input alarms to the central station to fully test the alarm system operation. When this type of testing is required, the following points must be noted: • The testing must be pre-arranged in consultation with the CMS staff. • All the relevant areas must be turned on. • After testing, turn the relevant Areas off again. • Obtain the central station report of all input alarms/restores and area opens/closes reported during the testing procedure. • Compare the input/area list and central station report to ensure that all tested inputs reported alarm and restore, and all tested areas reported close and open as required. • Record and report any discrepancy.
Test warning device outputs. (May be performed in conjunction with zone input testing).	As agreed between the alarm company and the client, but not less than once per year. Also see "Notes" on page 200.	NOTE: The CMS staff may need to be notified before these tests are made. Test the operation of each audible and visible warning device. • Turn on the appropriate area. • Activate a detection device or user operation that is programmed to trigger the warning device. • Check that the warning device operates as specified. • Record and report any discrepancy.
Backup history files for management software (for example, CTPlus or Forcefield).	Recommended monthly	Backups should be performed on a regular basis depending on the number of events. The backup file should be verified and then the same data should be purged or deleted from the database.

Task	Frequency	Description
Backup or export database for management software (forexample, CTPlus or Forcefield).	Recommended monthly	Database backups or exports should be performed on a regular basis. Verify that the backup file has been created.
Perform modifications	As required	Any modifications to the system as a result of the maintenance procedure must be recorded and reported. Technician to program next service date. See "Option 33: Program next service" on page 181.
Obtain client approval	At the conclusion of every routine maintenance visit	Obtain the signature of the client or the client's representative on the maintenance record.

Notes

The frequency for testing the operation of all detection devices, audible and visible alarm warning devices and remote signaling (reporting) operations should be determined according to the needs of the particular installation.

AS/NZS 2201.1-2007 specifies that these tests must be carried out at least once per year (depending on site), however some central stations and clients prefer more frequent testing to ensure the integrity of the system. For example:

- Sites requiring a higher level of security monitoring, or that are prone to interference of harsh environmental conditions, may choose to have these tests carried out quarterly or more frequently.
- Very large sites with hundreds of detection devices may choose to do testing every 6 months with 50% of the detection devices tested on each visit.

Sites where the automated testing functions in the product have been enabled and properly implemented may find that annual routine maintenance is adequate.

Contacting technical support

For assistance installing, operating, maintaining, and troubleshooting this product, refer to this document and any other documentation provided.

If you still have questions, please contact your Installation Company or distributor, as applicable.

Note: Be ready with the equipment before calling for technical support.

Appendix A Reference materials

Content

System numbering.....	203
Overview	203
Zone input numbering	203
Relay and output numbering	205
Siren output numbering	206
Door and lift numbering	206
Time zone numbering	207
Input types.....	209
Input tamper monitoring.....	209
Application notes	209
List of input types	209
Alarm group default settings	219
Event flags	222
Reporting	224
CID reporting codes for input events	224
CID reporting codes for system events	225
STU serial reporting formats	225
Programming map.....	225

System numbering

Overview

All DGPs, zone inputs, relays (outputs), doors, and lifts are numbered according to a set formula. This is used when determining the physical numbers and locations when programming.

Zone input numbering

A Discovery system can receive alarm signals from up to 1008 zone inputs. The Discovery panel itself has 16 zone input connections. Additional zone inputs may be provided by Data Gathering Panels (DGPs), Wireless Data Gathering Panels (WDGPs) and Network Access Controllers on the system LAN. This section will refer to all of these devices as DGPs, unless otherwise noted.

Every DGP is assigned a DGP address in the range 1 to 15 (on COMM 1) and 17 to 32 (on COMM 2). Network Access Controllers may use the first 12 addresses on each LAN.

The Discovery numbering scheme allocates 32 zone inputs per DGP address for a theoretical total of 1008 zone inputs (including the panel's 16 zone inputs).

Note: Network Access Controllers can use 16 zone input connections; the TS0827 Four-Input DGP can use 4 zone input connections. The system total of 1008 zone inputs is reduced accordingly when these products are used.

Table 24 below lists the standard and expanded input capacities for various DGPs.

Table 24: Input connection options for DGP devices

DGP Model	Type	Onboard inputs	Expanded inputs
TS1020	8-input analogue DGP	8	32 (using 3 x TS1021)
TS0820, TS0824	8-input standard DGP	8	32 (using 3 x TS0021)
TS0827	4-input DGP	4	N/A
TS0825E	Inovonics Wireless DGP	16 wireless inputs	32 wireless inputs

The Discovery panel has inputs and relays numbered 1 to 16. DGP input and relay numbers are assigned according to Table 25 below.

Table 25: DGP addressing, DPG DIP switches, and input and relay numbering

LAN	Address	Polled as	SW1	SW2	SW3	SW4	Inputs	Relays
COMM 1	DGP 1	DGP 1	I	O	O	O	17 to 48	17 to 32
COMM 1	DGP 2	DGP 2	O	I	O	O	49 to 80	33 to 48
COMM 1	DGP 3	DGP 3	I	I	O	O	81 to 112	49 to 64
COMM 1	DGP 4	DGP 4	O	O	I	O	113 to 144	65 to 80
COMM 1	DGP 5	DGP 5	I	O	I	O	145 to 176	81 to 96
COMM 1	DGP 6	DGP 6	O	I	I	O	177 to 208	97 to 112
COMM 1	DGP 7	DGP 7	I	I	I	O	209 to 240	113 to 128
COMM 1	DGP 8	DGP 8	O	O	O	I	241 to 272	129 to 144
COMM 1	DGP 9	DGP 9	I	O	O	I	273 to 304	145 to 160
COMM 1	DGP 10	DGP 10	O	I	O	I	305 to 336	161 to 176
COMM 1	DGP 11	DGP 11	I	I	O	I	337 to 368	177 to 192
COMM 1	DGP 12	DGP 12	O	O	I	I	369 to 400	193 to 208
COMM 1	DGP 13	DGP 13	I	O	I	I	401 to 432	209 to 224
COMM 1	DGP 14	DGP 14	O	I	I	I	433 to 464	225 to 240
COMM 1	DGP 15	DGP 15	I	I	I	I	465 to 496	241 to 256
COMM 2	DGP 1	DGP 17	I	O	O	O	497 to 528	257 to 272
COMM 2	DGP 2	DGP 18	O	I	O	O	529 to 560	273 to 288
COMM 2	DGP 3	DGP 19	I	I	O	O	561 to 592	289 to 304
COMM 2	DGP 4	DGP 20	O	O	I	O	593 to 624	305 to 320
COMM 2	DGP 5	DGP 21	I	O	I	O	625 to 656	321 to 336
COMM 2	DGP 6	DGP 22	O	I	I	O	657 to 688	337 to 352
COMM 2	DGP 7	DGP 23	I	I	I	O	689 to 720	353 to 368
COMM 2	DGP 8	DGP 24	O	O	O	I	721 to 752	369 to 384
COMM 2	DGP 9	DGP 25	I	O	O	I	753 to 784	385 to 400
COMM 2	DGP 10	DGP 26	O	I	O	I	785 to 816	401 to 416
COMM 2	DGP 11	DGP 27	I	I	O	I	817 to 848	417 to 432
COMM 2	DGP 12	DGP 28	O	O	I	I	849 to 880	433 to 448
COMM 2	DGP 13	DGP 29	I	O	I	I	881 to 912	449 to 464
COMM 2	DGP 14	DGP 30	O	I	I	I	913 to 944	465 to 480
COMM 2	DGP 15	DGP 31	I	I	I	I	945 to 976	481 to 496
COMM 2	DGP 16	DGP 32	O	O	O	O	977 to 1008	497 to 512

Legend: I = ON, O = OFF

Notes:

- Input numbers in the range 1000 to 1008 will not report CID alarms.
 - The Discovery panel is assigned input numbers 1 to 16.
 - The Discovery panel is assigned relay numbers 1 to 16 (more with potential duplication). Relay 15 is assigned to the panel's strobe.
 - The siren output is the highest relay number assigned to the DGP address.
 - DGP installation instructions may say "Set the first four segments to OFF to disable the DGP". This does not apply to DGPs used on COMM 2, where you set the first four segments to OFF for DGP 16.
-

Relay and output numbering

Relay numbers are used for physical relays, for logical outputs such as used in macros, and for open collector outputs and LEDs.

Discovery panels support 512 relays:

- Panel relays numbered 1 to 16 (relay 15 operates the strobe). Higher relay numbers can be used at the risk of duplication (for example, relay 17 on both the panel and DGP 1 can activate simultaneously).
- COMM 1 can have 15 DGPs with relays numbered 17 to 256.
- COMM 2 can have 16 DGPs with relays numbered 257 to 512.
- Each DGP address uses the 16th relay number for the siren output. In Discovery, the number that a relay uses depends on where it is used:
- When programming the relay in the Discovery panel, the DGP address must be considered (for example, the first relay on DGP 1 is relay 17).
- When programming an Network Access Controller's physical relays, the DGP address is already known, so the relays for any address are numbered from 1.

Note: If you want to control a Network Access Controller's physical relay from the Discovery panel, you need to use the relay's macro event number as an input for a DGP macro logic program (refer to the Network Access Controller's programming manual for details).

Relay numbers are assigned according to [Table 25](#) on page 204.

If the Discovery panel has more than 16 relays, then the numbering system allows for duplication between the Discovery panel's relays and a DGP's relays.

Example:

- The Discovery panel has three TS0841 8-way relay controllers, so it has 23 relays numbered 1 to 24 (relay 15 is assigned to the panel's strobe).

- DGP 1 (TS0820) has one TS0841 8-way relay controller, so it has 16 relays numbered 17 to 32.
- The relay numbers 17 to 24 apply to both the panel and the DGP. The result of this duplication is that any relays that share a number will both be active (or inactive) simultaneously.

Siren output numbering

The siren output is the highest relay number assigned to the DGP address.

The internal and external siren speaker outputs on Discovery panels are always treated as relay 16. On DGPs with siren speaker outputs, the last of the 16 relay numbers associated with that DGP address is the siren output. For example, on COMM 1, DGP 3, the siren speaker output is relay 64.

To enable the siren speaker output, the relay number representing the siren output must be mapped to the required siren event flag number. The default mapping is event flag 1. Siren event flag numbers are programmed in "[Area database](#)" on page 71.

Door and lift numbering

Door and lift numbers are determined by:

- The RAS or reader address when connected to the Discovery system LANs (doors 1 to 16 and 65 to 80). These doors and lifts are reserved for RASs 1 to 16 and 65 to 80, and provide only basic access control (door opening) except where used as standard doors / lifts.
 - The DGP or NAC / DWI address when connected to the local LAN (doors 17 to 64 and 81 to 128). These door and lift numbers are controlled by Network Access Controllers, except where used as standard doors / lifts, and provide enhanced access control functions such as anti-passback.
-
- **Note:** When using DWIs, only the first 2 doors / lifts can be used in the assigned DGP address. E.g. using a DWI as DGP 1 you can only use door / lift number 17 and 18 (reader 1 and reader 2 respectively), the other door / lift number allocations (19 and 20) cannot be used. This limitation does not apply to NACs.
-

Refer to Table 26 below for details of door and lift numbering.

Table 26: Door and lift numbers allocated per DGP

Device and address	First door or lift	Second door or lift	Third door or lift	Fourth door or lift
COMM 1, RAS 1 to 16			Doors 1 to 16	
COMM 1, DGP 1	17	18	19	20

COMM 1, DGP 2	21	22	23	24
COMM 1, DGP 3	25	26	27	28
COMM 1, DGP 4	29	30	31	32
COMM 1, DGP 5	33	34	35	36
COMM 1, DGP 6	37	38	39	40
COMM 1, DGP 7	41	42	43	44

Device and address	First door or lift	Second door or lift	Third door or lift	Fourth door or lift
COMM 1, DGP 8	45	46	47	48
COMM 1, DGP 9	49	50	51	52
COMM 1, DGP 10	53	54	55	56
COMM 1, DGP 11	57	58	59	60
COMM 1, DGP 12	61	62	63	64
COMM 2, RAS 65 to 80		Doors 65 to 80		
COMM 2, DGP 17	81	82	83	84
COMM 2, DGP 18	85	86	87	88
COMM 2, DGP 19	89	90	91	92
COMM 2, DGP 20	93	94	95	96
COMM 2, DGP 21	97	98	99	100
COMM 2, DGP 22	101	102	103	104
COMM 2, DGP 23	105	106	107	108
COMM 2, DGP 24	109	110	111	112
COMM 2, DGP 25	113	114	115	116
COMM 2, DGP 26	117	118	119	120
COMM 2, DGP 27	121	122	123	124
COMM 2, DGP 28	125	126	127	128

Although standard DGPs are numbered 1 to 16, Network Access Controllers and Dual Wiegand Interfaces are numbered from 1 to 12, therefore a Discovery system can only have 12 NACs / DWIs on each LAN (24 in total).

Time zone numbering

A time zone ('hard' time zone) is a program setting that identifies specific time periods on specific days. Time zones are allocated to security system functions to control the activity of that function by time and day and are primarily used to restrict access.

Time zones are numbered 1 to 24 and 42 to 63, and are programmed for specific time periods. Each time zone is made up of one to eight sub-time zones.

Soft time zones are numbered 26 to 41 and are active only when a relay is active (they are based on events instead of on time). [Table 27](#) on page 208 lists the hard

and soft time zones that can be used in a Discovery system.

Table 27: Time zone application

Number	Type	Application
0	24-hour	Always valid, cannot be edited.
1 to 24, 42 to 63	Hard	Use wherever you need to define up to eight sub-time zones containing a start time, an end time, the weekdays that the sub-time zone is valid, and an option to make the sub-time zone valid on specified holiday types. See “Time zones” on page 144.
25	Service	Use to enable the service technician’s PIN or card, and can also be used to enable or disable any other system functions such as relays that are required while the service technician is in attendance. See “Programming service technician access” on page 47.
26 to 41	Soft	Soft time zones are active only when a relay or output is active. See “Soft time zones” on page 158.

Input types

Input types may be grouped by their basic functionality as follows:

- Access alarms—Inputs that will only generate an alarm when one or more of the areas assigned are in access (disarmed). Refer to input types 1 and 11.
- Secure alarms – Inputs that will only generate an alarm when all of the areas assigned are in secure (armed). Refer to input types 2, 3, 4, 13, 14, 28, 60, 61, and 62.
- 24-hour alarms—Inputs that will generate the same alarm regardless of area status. Refer to input types 5, 29, 33, and 59.
- Access/secure alarms—Inputs that will generate different types of alarms when in access and secure. Refer to input types 8, 15, 21, 22, 30, 40, 41, 42, 44, 45, 46, 47, and 56.
- Area control—Inputs that turn areas on and off. Refer to input type numbers 6, 31, 34, and 35. These inputs do not have areas assigned to them. Their functions are determined by assigning an alarm group to them.
- Activate event flag only—Inputs that activate event flags but do not generate alarms. Refer to input types 7, 20, 32, and 43.
- Activate report only—Inputs that activate reports but do not generate alarms. Refer to input types 27 and 57.
- Special purpose—Special input types for system functions. Refer to input types 9, 12, 16, 18, 19, and 58.
- Camera monitoring—Panel inputs 1 to 16 only (not DGP inputs) that

monitor camera film levels. Refer to input types 23, 24, 25, 26, 36, 37, 38, 39, 48, 49, 50, 51, 52, 53, 54, and 55

Input tamper monitoring

The system option “Input tamper monitoring” determines whether the Discovery panel can detect two input states (sealed and unsealed) or four input states (sealed, unsealed, open, and short), as follows:

- When input tamper monitoring is enabled, open or short conditions are both reported as an input tamper alarm (subject to input type).
- When input tamper monitoring is disabled, then an open or short circuit will be treated as unsealed.

Certain input types use the open and short conditions for their functions, in which case input tamper monitoring may not be possible (or is limited). Input types 7, 12, 20, 27, 23, 24, 25, 26, 36, 37, 38, 39, 48, 49, 50, 51, 52, 53, 54, 55, 57, 58, are affected.

Application notes

- Do not use input type 17.
- Input type 10 is designated ‘spare’ and has no functionality.
- An input is in access when any of the areas assigned to it are disarmed.
- An input is in secure when all of the areas assigned to it are armed.
- Disarming a total disarm area (or area group) prevents alarm input types from generating alarms (except to indicate input tamper, if input tamper monitoring is used).
- The exit timer suppresses alarms from entry/exit input types (3, 4, 13, 14, 41, 42, 61, and 62) but does not suppress alarms from other inputs. See “[Enable exit fault reporting](#)” on page 111 to report alarms from non-entry/exit type inputs as “exit error alarms”.
- The input type can affect the input’s programmed event flag and event selections. For example, input types that activate event flags only (7, 20, 32, and 43) do not generate alarms, so alarm-based event flags won’t work. Camera count input types do not activate event flags, but camera film out input types will activate a programmed event flag. Refer to “Programming input event flags” on page 67 for more details.
- There are three twin trip input types (60, 61, and 62). See “[Programming twin trip inputs](#)” on page 58 for more information.

List of input types

Table 28 below lists the input types grouped by basic functionality. Refer to the Index for a list of input types by number.

The column *Name* is an expanded version of what is displayed on an LCD RAS.

For example, the name of input type 44 on a RAS is “(Acc.Loc/Sec.Alm) Dis Cln.Tr”. This name is shown here as “Access local/secure alarm disabled by cleaners or trades”.

Table 28: Input types

Input type	Name	Description
0	none	No input type programmed. The physical input does not exist. Note: This is the default type for inputs 17 to 1008. Input type 0 is not retrieved to management software.
Access alarms —Inputs that will only generate an alarm when one or more of the areas assigned are in access (disarmed). Refer to input types 1 and 11.		
1	Access alarm	In access an unsealed input generates an alarm. <i>Example:</i> Hold-up button
11	Delayed access alarm	In access an unsealed input starts the delay holdup timer and the RAS indicates alarm condition (but the alarm is not reported). An alarm is reported if a second delayed access alarm is unsealed (in any area) or if the delayed holdup timer expires. <i>Example:</i> Hold-up button to report after a delay. <i>Programming:</i> Delay holdup time.
Secure alarms – Inputs that will only generate an alarm when all of the areas assigned are in secure (armed). Refer to input types 2, 3, 4, 13, 14, 28, 60, 61, and 62.		
2	Secure alarm	In secure an unsealed input generates an alarm. <i>Example:</i> Internal door, PIR (motion detector). Note: This is the default type for inputs 1 to 16.
3	Entry/exit alarm	In secure an unsealed input generates an alarm when the entry and exit timers for the areas assigned to the input have expired. When the area changes to secure the exit timer starts. Unsealing the input during the exit time will not generate an alarm. If the input is unsealed after the exit time has expired, then the entry timer starts. Unsealing the input during the entry time will not generate an alarm. An alarm is generated if the input is still unsealed when the entry time expires. <i>Example:</i> Front door. <i>Programming:</i> Area entry and exit times.
4	Entry/exit handover alarm	In secure an unsealed input generates an alarm when the exit timer for the input has expired and the entry timer is not running. <i>Example:</i> PIR at entrance. <i>Programming:</i> Area entry and exit times.
13	Entry/exit no seal check	In secure an unsealed input generates an alarm when entry/exit timers have expired. The input does not need to be sealed when turning the area to secure. <i>Programming:</i> Area entry and exit times.

14	Entry exit handover alarm no seal check	In secure an unsealed input generates an alarm when the exit timer has expired and the entry timer is not running. The input does not need to be sealed when turning the area to secure. <i>Programming:</i> Area entry and exit times.
----	--	--

Input type	Name	Description
28	Non-latching secure alarm	In secure an unsealed input generates an alarm. The alarm resets automatically when the input seals. <i>Example:</i> PIR Note: Unlike previous Discovery versions, the input must be sealed (or isolated) before the area can be armed.
60	Twin trip secure alarm	In secure, generates an alarm if input unsealed a second time within the maximum twin trip time. <i>Example:</i> PIR (motion detector). <i>Programming:</i> Maximum twin trip time.
61	Twin trip entry exit handover	In secure, generates an alarm if input unsealed a second time within the maximum twin trip time, provided the exit timer for the input has expired and the entry timer is not running. <i>Example:</i> PIR at entrance. <i>Programming:</i> Area entry and exit times, and maximum twin trip time.
62	Twin trip handover no seal check	In secure, generates an alarm if input unsealed a second time within the maximum twin trip time, provided the exit timer has expired and the entry timer is not running. The input does not need to be sealed when setting the area to secure. <i>Programming:</i> Area entry and exit times, and maximum twin trip time.
24-hour alarms —Inputs that will generate the same alarm regardless of area status. Refer to input types 5, 29, 33, and 59.		
5	24-hour alarm	In access or secure, an unsealed input generates an alarm. <i>Example:</i> Panel tampers, panic alarm.
29	24-hour non-latching alarm	In access or secure, an unsealed input generates an alarm. The alarm resets automatically when the input seals.
33	24-hour alarm & isolate input	In access or secure, an input can report an alarm, a tamper condition, or be isolated: • Shorted – generates an alarm • Sealed – no alarm generated • Unsealed – isolate (no alarm generated) • Open – generates a tamper alarm <i>Example:</i> A key switch is used to isolate the input in shopping centres where only one input is available for each shop. Note: The input's "Activate Selected Event on Unseal" option does not apply to this input type.
59	24-hour alarm disabled by time zone 41	An input with this type is disabled when soft time zone 41 is activated by a relay (no local alarm, alarm or tamper can be generated). If the input is still unsealed when time zone 41 becomes invalid an alarm will not be generated unless the input seals and is unsealed again. In access or secure (when time zone 41 is not valid) an unsealed input generates an alarm. <i>Programming:</i> Link soft time zone 41 to a relay.

Input type	Name	Description
Access/secure alarms —Inputs that will generate different types of alarms when in access and secure. Refer to input types 8, 15, 21, 22, 30, 40, 41, 42, 44, 45, 46, 47, and 56.		
8	Delayed access/secure alarm	In access an unsealed input starts the delay holdup timer and the RAS indicates alarm condition (but the alarm is not reported). An alarm is reported if a second delayed access alarm is unsealed (in any area) or if the delayed holdup timer expires. In secure an unsealed input generates an alarm. <i>Example:</i> Hold-up button on a counter where more than one hold-up button is used. <i>Programming:</i> Delay holdup time.
15	Access local/secure alarm	In access an unsealed input generates a local alarm (“Local Alarm” is displayed and the beeper sounds on RASs assigned to the same areas). The local alarm can be reset via RAS by pressing [ENTER] [ENTER] 0 [ENTER], or USER CODE [OFF] AREA [ENTER] to stop the audible alert and cancel the event. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. In secure an unsealed input generates an alarm. <i>Example:</i> Emergency exit. <i>Programming:</i> Local alarm reminder time.
21	Access local (code to reset)/secure alarm	In access an unsealed input generates a silent local alarm (the area LED flashes, but there is no other indication). An authorised user code is required to reset the silent local alarm via RAS by pressing USER CODE [OFF] AREA [ENTER]. If the input remains unsealed, it will re-alarm after the programmed local alarm reminder time. In secure an unsealed input generates an alarm. <i>Example:</i> Emergency door. <i>Programming:</i> Local alarm reminder time.
22	Access delayed non-latching/secure alarm	In access an unsealed input starts the delay holdup timer and the RAS indicates alarm condition (but the alarm is not reported). If the input reseals before the delay holdup timer expires, then the alarm automatically resets. An alarm is reported if a second delayed access alarm is unsealed (in any area) or if the delayed holdup timer expires. In secure an unsealed input generates an alarm. <i>Example:</i> Hold-up button. <i>Programming:</i> Delay holdup time.
30	Access local non-latching/secure alarm	In access an unsealed input generates a silent local alarm (the area LED flashes, but there is no other indication). The alarm automatically resets when the input seals. In secure an unsealed input generates an alarm. The alarm does not automatically reset when the input seals. <i>Example:</i> Emergency door.

Input type	Name	Description
40	Access suspicion or delayed holdup/secure alarm	In access an unsealed input starts the delay holdup timer and the RAS indicates alarm condition (but the alarm is not reported). An alarm is reported if a second delayed access alarm is unsealed (in any area) or if the delayed holdup timer expires. A shorted input activates cameras in the areas that are assigned to the input. When the input switches back to sealed, the cameras continue to operate for the suspicion time. An open input reports a tamper. In secure an unsealed input generates an alarm. <i>Programming:</i> Delay holdup time, suspicion time.
41	Accesslocal/entry exit alarm	In access an unsealed input generates a local alarm ("Local Alarm" is displayed and the beeper sounds on RASs assigned to the same areas). The local alarm can be reset via RAS by pressing [ENTER] 0 [ENTER], or USER CODE [OFF] AREA [ENTER] to stop the audible alert and cancel the event. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. In secure an unsealed input generates an alarm when the entry/exit timers for the areas assigned to the input have expired. <i>Example:</i> Emergency door that is also used to enter the premises. <i>Programming:</i> Area entry and exit times, local alarm reminder time.
42	Accesslocal (code to reset)/entry exit alarm	In access an unsealed input generates a silent local alarm (the area LED flashes, but there is no other indication). The silent local alarm can be reset via RAS by pressing USER CODE [OFF] AREA [ENTER]. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. In secure an unsealed input generates an alarm when the entry/exit timers for the areas assigned to the input have expired. <i>Example:</i> Emergency door that is also used to enter the premises. <i>Programming:</i> Local alarm reminder time, area entry and exit times.
44	Access local/secure alarm disabled by cleaners or trades	In access an unsealed input generates a silent local alarm (the area LED flashes, but there is no other indication). The silent local alarm can be reset via RAS by pressing USER CODE [OFF] AREA [ENTER]. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. If a user with user category 2 or user category 6 in their alarm groups enters their code to put the area in access, then an unsealed input does not generate a silent local alarm. In secure an unsealed input generates an alarm. <i>Example:</i> Emergency door. <i>Programming:</i> Local alarm reminder time. If you want to disable the silent local alarm in access (for certain users), then program a user category (2 or 6), the user category time, and the user's alarm group.

Input type	Name	Description
45	Access event flag/secure alarm disabled by cleaners or trades	In access an unsealed input activates the input's event flag. If a user with user category 2 or user category 6 in their alarm groups enters their code to put the area in access, then an unsealed input does not activate the input's event flag. In secure an unsealed input generates an alarm. <i>Example:</i> Emergency door. <i>Programming:</i> Input event flag number. If you want to disable the event flag in access (for certain users), then program a user category (2 or 6), the user category time, and the user's alarm group.
46	Access alarm/secure alarm	In access an unsealed input generates an alarm (this is normal functionality where the alarm is determined by the input's programmed report ID number). In secure an unsealed input reports a general alarm (CID 140) regardless of the input's programmed report ID number.
47	Suspicion holdup/secure alarm	In access an unsealed input generates an alarm (this is normal functionality where the alarm is determined by the input's programmed report ID number). A shorted input activates cameras in the areas that are assigned to the input. When the input switches back to sealed, the cameras continue to operate for the suspicion time. An open input reports a tamper. In secure an unsealed input reports a general alarm (CID 140) regardless of the input's programmed report ID number. <i>Programming:</i> Suspicion time.
56	Access local (code to reset)/secure alarm, disabled by time zone 41	An input with this type is disabled when soft time zone 41 is activated by a relay (no local alarm, alarm or tamper can be generated). If the input is still unsealed when time zone 41 becomes invalid an alarm will not be generated unless the input seals and is unsealed again. In access (when time zone 41 is not valid) an unsealed input generates a silent local alarm (the area LED flashes, but there is no other indication). The silent local alarm can be reset via RAS by pressing USER CODE [OFF] AREA [ENTER]. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. In secure (when time zone 41 is not valid) an unsealed input generates an alarm. <i>Example:</i> Emergency door. <i>Programming:</i> Local alarm reminder time, and link soft time zone 41 to a relay.
Area control —Inputs that turn areas on and off. Refer to input type numbers 6, 31, 34, and 35. These inputs do not have areas assigned to them. Their functions are determined by assigning an alarm group to them.		
6	Area control input	An unsealed (momentary) input performs the programmed alarm group functions, such as arming an area. <i>Example:</i> Push button for quick arming on exit (the alarm group should allow arm but not disarm). <i>Programming:</i> Alarm group.

Input type	Name	Description
31	Area control on-off	An unsealed input secures the area. A sealed input puts the area in access. This input type uses an alarm group to perform the arm/disarm functions. <i>Example:</i> Latching key switch to arm and disarm areas. <i>Programming:</i> Alarm group.
34	Area disarm/user category arm	When disarmed, switching from sealed to unsealed starts the warning time. As long as the input remains unsealed, the RAS beeps and displays the user category name followed by “ending”. The area arms when the warning time expires. When armed, switching from unsealed to sealed disarms the area. <i>Example:</i> Latching key switch used to arm and disarm. <i>Programming:</i> Warning time, a user category, and the input’s alarm group.
35	Area user category arm only	When disarmed, unsealing the input starts the warning time. The RAS beeps and displays the user category name followed by “ending”. The area arms when the warning time expires. <i>Example:</i> Push button used to arm but not disarm. <i>Programming:</i> Warning time, a user category, and the input’s alarm group.
Activate event flag only —Inputs that activate event flags but do not generate alarms. Refer to input types 7, 20, 32, and 43.		
7	Camera suspicion input	An unsealed input activates the film cameras in the areas assigned to the input. When the input reseals, the cameras continue to operate for the suspicion time. <i>Example:</i> Suspicion button. <i>Programming:</i> Suspicion time. Note: This input type cannot indicate tamper.
20	Input to activate event flag 24-hour	In access or secure an unsealed, opened, or shorted input activates the input’s event flag. <i>Example:</i> Doorbell. <i>Programming:</i> Input event flag number. Note: This input type cannot indicate tamper.
32	Input to activate event flag in secure	In secure an unsealed input activates the input’s event flag. <i>Example:</i> Temperature alarm on freezer activates buzzers. <i>Programming:</i> Input event flag number. Note: This input type can indicate tamper on open or short when its area is disarmed (access).
43	Input to activate event flag in access	In access an unsealed, opened, or shorted input activates the input’s event flag. <i>Example:</i> Buzzer to indicate that a closet door is open. <i>Programming:</i> Input event flag number. Note: This input type can indicate tamper on open or short when its area is armed (secure).

Input type	Name	Description
Activate report only —Inputs that activate reports but do not generate alarms. Refer to input types 27 and 57.		
27	Input to activate report	In access or secure an unsealed, open, or shorted input reports an alarm to management software and central station, but does not indicate an alarm condition on the RAS. The alarm automatically resets when the input reseals. <i>Example:</i> Temperature alarm on freezer. Note: This input type cannot indicate tamper.
57	Input to report and screen	In access or secure an unsealed, open, or shorted input reports an alarm to management software and central station, but does not indicate an alarm condition on the RAS (however, it displays the system's event text via LCD RAS). The alarm automatically resets when the input reseals. <i>Example:</i> Temperature alarm on freezer. <i>Programming:</i> Event text. Note: This input type cannot indicate tamper.
Special purpose —Special input types for system functions. Refer to input types 9, 12, 16, 18, 19, and 58.		
9	Reset delayed input	When unsealed this input type resets a delayed alarm from input types (8, 11, 22, and 40) where the input has been resealed or the delay timer is still running (a full alarm has not been generated). If the delayed input is still unsealed, then it stops the cameras from operating but the delayed time continues to run. <i>Example:</i> Reset button for quick cancellation of alarm.
12	Courier restart	This is a pulsed key switch that resets the entry timers and restarts the exit timers for all areas assigned to the input. <i>Example:</i> Key switch next to door.
16	24-hour local mains fail	In access or secure, an unsealed input generates a local alarm ("Local Alarm" is displayed and the beeper sounds on RASs assigned to the same areas). The local alarm can be reset via RAS by pressing [ENTER] [ENTER] 0 [ENTER], or USER CODE [OFF] AREA [ENTER] to stop the audible alert and cancel the event. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. Note: This input type is not used in standard commercial versions of Discovery systems.
18	24-hour local comms fail	In access or secure, an unsealed input generates a local alarm ("Report Fail: Local Alarm" is displayed and the beeper sounds on RASs assigned to the same areas). The Comms Fail LED is activated on applicable RAS models. The local alarm can be reset via RAS by pressing [ENTER] [ENTER] 0 [ENTER], or USER CODE [OFF] AREA [ENTER] to stop the audible alert and cancel the event. If the input remains unsealed, it generates a new local alarm after the programmed local alarm reminder time. <i>Programming:</i> Local alarm reminder time.
19	Comms fail LED	In access or secure, an unsealed input displays "Report Fail" on RASs assigned to the same area, and the Comms Fail LED is activated on applicable RAS models.

Input type	Name	Description
58	Input to screen text	In access or secure, an unsealed, open, or shorted input displays the system's event text via LCD RAS. <i>Example:</i> Temperature alarm on freezer. <i>Programming:</i> Event text. Note: This input type cannot indicate tamper.
Camera monitoring —Panel inputs 1 to 16 only (not DGP inputs) that monitor camera film levels. Refer to input types 23, 24, 25, 26, 36, 37, 38, 39, 48, 49, 50, 51, 52, 53, 54, and 55.		
23	Camera 1 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 1. Note: This input type cannot indicate tamper.
24	Camera 2 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 2. Note: This input type cannot indicate tamper.
25	Camera 3 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 3. Note: This input type cannot indicate tamper.
26	Camera 4 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 4. Note: This input type cannot indicate tamper.
36	Camera 5 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 5. Note: This input type cannot indicate tamper.
37	Camera 6 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 6. Note: This input type cannot indicate tamper.
38	Camera 7 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 7. Note: This input type cannot indicate tamper.
39	Camera 8 count	In access or secure, a transition from open to short across normally open contacts increments the film counter for camera 8. Note: This input type cannot indicate tamper.
48	Camera 1 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 1. Note: This input type cannot indicate tamper.
49	Camera 2 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 2. Note: This input type cannot indicate tamper.
50	Camera 3 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 3. Note: This input type cannot indicate tamper.
51	Camera 4 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 4. Note: This input type cannot indicate tamper.

Input type	Name	Description
52	Camera 5 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 5. Note: This input type cannot indicate tamper.
53	Camera 6 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 6. Note: This input type cannot indicate tamper.
54	Camera 7 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 7. Note: This input type cannot indicate tamper.
55	Camera 8 film out	In access or secure, an open, shorted, or unsealed input generates a "Film Out" alarm for camera 8. Note: This input type cannot indicate tamper.

Alarm group default settings

Table 29: Discovery user menus and options provided for alarm groups

AG number	Name	Editable?	Discovery user menus and options (defaults)
1	No Access	No	User menus: None Areas: None Option: User Alarm Group
2	Master RAS or Door	No	User menus: All Areas: Defined by Area Group 1 Options: • Alarm System Control • List of Areas • Keypad Duress • Reset System Alarms • Remote Access • User Categories: All • Disable auto-deisolate • Auto isolate unsealed inputs • Forced arming • Prevent forced disarming

AG number	Name	Editable?	Discovery user menus and options (defaults)
3	Master Code	No	User menus: All Areas: Defined by Area Group 1 Options: • Alarm System Control • List of Areas • Keypad Duress • Reset System Alarms • Remote Access
4 to 10	Spare	No	User menus: None Areas: None Options: None
11	High Level User Master	Yes	User menus: All except 19 Areas: Defined by Area Group 1 Options: • Alarm System Control • List of Areas • Keypad Duress • Reset System Alarms • Remote Access
12	Low Level User Master	Yes	User menus: 1, 5, 9, 10, 11, 14, 15, 16 Areas: Defined by Area Group 1 Options: • Alarm System Control • List of Areas • Keypad Duress
13	All Area UserCode	Yes	User menus: 1, 5, 9, 10, 11 Areas: Defined by Area Group 1 Options: • Alarm System Control • List of Areas • Keypad Duress
14	Area 1	Yes	User menus: 1, 5, 9, 10, 11 Area: 1 Options: • Alarm System Control • Keypad Duress
15	Area 2	Yes	User menus: 1, 5, 9, 10, 11 Area: 2 Options: • Alarm System Control • Keypad Duress

AG number	Name	Editable?	Discoveryuser menus and options (defaults)
16	Area 3	Yes	User menus: 1, 5, 9, 10, 11 Area: 3 Options: • Alarm System Control • Keypad Duress
17	Area 4	Yes	User menus: 1, 5, 9, 10, 11 Area: 4 Options: • Alarm System Control • Keypad Duress
18	Area 5	Yes	User menus: 1, 5, 9, 10, 11 Area: 5 Options: • Alarm System Control • Keypad Duress
19	Area 6	Yes	User menus: 1, 5, 9, 10, 11 Area: 6 Options: • Alarm System Control • Keypad Duress
20	Area 7	Yes	User menus: 1, 5, 9, 10, 11 Area: 7 Options: • Alarm System Control • Keypad Duress
21	Area 8	Yes	User menus: 1, 5, 9, 10, 11 Area: 8 Options: • Alarm System Control • Keypad Duress
22	Area 9	Yes	User menus: 1, 5, 9, 10, 11 Area: 9 Options: • Alarm System Control • Keypad Duress
23	Area 10	Yes	User menus: 1, 5, 9, 10, 11 Area: 10 Options: • Alarm System Control • Keypad Duress

AG number	Name	Editable?	Discovery user menus and options (defaults)
24	Area 11	Yes	User menus: 1, 5, 9, 10, 11 Area: 11 Options: - Alarm System Control - Keypad Duress
25	Area 12	Yes	User menus: 1, 5, 9, 10, 11 Area: 12 Options: - Alarm System Control - Keypad Duress
26	Area 13	Yes	User menus: 1, 5, 9, 10, 11 Area: 13 Options: - Alarm System Control - Keypad Duress
27	Area 14	Yes	User menus: 1, 5, 9, 10, 11 Area: 14 Options: - Alarm System Control - Keypad Duress
28	Area 15	Yes	User menus: 1, 5, 9, 10, 11 Area: 15 Options: - Alarm System Control - Keypad Duress
29	Area 16	Yes	User menus: 1, 5, 9, 10, 11 Area: 16 Options: - Alarm System Control - Keypad Duress
30 to 255	<i>Programas needed</i>	Yes	<i>Program as needed</i>

Event flags

An event flag is a signal that is activated by a condition in an input, an area, a RAS, a macro, an input shunt, or the system. Event flags can be:

- Predefined (numbered in the range 1 to 16). See [Table 30](#) on page 223.
- Custom (numbered in the range 17 to 255).
- Summary (system event flags, numbered in the range 17 to 255).

Event flags enable the installer to map events to physical relays or to other functions, as required. Event flags may be linked to:

- A relay, see “[Map relays](#)” on page 147. In the case of relays, you would typically use the relay number as the event flag number.
- A macro, see “[Program macro logic](#)” on page 165 (a macro can trigger an event flag, which can in turn trigger another macro).
- A shunt timer or a shunt warning timer, see “[Input shunts](#)” on page 153.

Each event flag can be assigned a name. Refer to “[Event flag names](#)” on page 179.

Copy the worksheets in “[Event flags worksheets](#)” on page 252 to record the details of all user-defined event flags.

An event flag can be used to accomplish more than one task. For example, an event flag can be assigned to an input and to the area containing the input. This enables one event flag to do two things in response to the input’s alarm condition. For example:

- The siren can sound when any of the area’s inputs are in alarm.
- A light can flash above a door (the particular input’s location). Event flags are programmed in a number of databases, including:
- Input database, see “[Input database](#)” on page 63 for details.
- Area database, see “[Area database](#)” on page 71 for details.
- RAS database, see “[RAS database](#)” on page 158 for details.
- Input shunts, see “[Input shunts](#)” on page 153 for details.
- System, see “[Program summary event flags](#)” on page 163 for details.
- Macro logic, see “[Program macro logic](#)” on page 41 for details.
- DGP database Network Access Controller DGPs can trigger event flags internally. (Refer to the DGP’s programming manual for details).

Table 30: Predefined event flags

Number	Functionality	Description
0	Disabled	Use to disable an event flag.
1	Siren	Default siren event flag (assigned in area database). If set to YES in the input database, activates when any siren activates in any area.
2, 3, 4, 5, 9, 10, 11	Secure Alarm	If set to YES on the input database, activates when an alarm is generated by the input and all the areas assigned to the input are secure. It is typically used to activate the system strobe output.

Number	Functionality	Description
6, 7, 13	Access Alarm	If set to YES in the input database, activates when an alarm is generated by the input and one or more of the areas assigned to the input are in access.
8	24-Hour Alarm	If set to YES in the input database, activates at any time an alarm is generated by the input.
16	Tester	Activates during the secure test. A tester event is used to activate a device that allows the testing of other devices. The tester event flag activates for half the tester event flag time programmed in "Timers" on page 100. The remaining period of the secure test time is settling time to allow the tested device to switch back to sealed state (make sure that the secure test time is longer than the tester event flag time).

Reporting

A Discovery panel can report (send messages) to a remote monitoring company in a variety of formats.

This section provides details of the following reporting types:

- "CID reporting codes for input events" below
- "CID reporting codes for system events" on page 212

-
- "STU serial reporting formats" on page 212

Note: Refer to the "Discovery Event Codes" document for the CID codes and descriptions.

CID reporting codes for input events

For each input that you need to send Ademco Contact ID (CID) event messages to a remote monitoring company, you need to program a report ID type. When selecting report ID types on an LCD RAS, only the Contact ID code and classification are displayed (the sub-classification is not displayed on the RAS).

These CID codes are used for reporting input events:

- From Discovery to the remote monitoring company where the reporting format is Contact ID.
- From a TS2000 Network Master Receiver when receiving events from

a Discovery panel where the reporting format is Contact ID.

Note: Refer to the "CID Codes via RAS / Keypad entry" section of the "Discovery10 Discovery Event Codes" document to view Report Type details and descriptions.

In each case, the area number (01 to 99) is reported in decimal via the group byte.

CID reporting codes for system events

CID codes are used for reporting system events via:

- Discovery panel to a remote monitoring company.
- TS2000 Network Master Receiver when receiving events from a Discovery panel where the reporting format is a Contact ID format or sub-format.

Contact ID formats or sub-formats are used where a communication path's reporting format is Contact ID Modem, IP Receiver, or a Contact ID sub format of Securitel STU.

Contact ID messages typically contain only decimal values, except where a Contact ID Hex sub-format is specified. In Contact ID Hex reporting the CID message's group number and point ID are offset by 2000 and reported in "hex" to a monitoring station (hex format in this instance is based on Ademco Contact ID Protocol (0 to 9 and B to F)).

Note: Refer to the "Decimal to CID Hex cross-reference" section of the "Discovery10 Discovery Event Codes" document to view a conversion table showing Contact ID Hex values used in the Discovery system.

STU serial reporting formats

The hex values in this section are true hexadecimal (base 16) and not the CID hex (0-9, B-F).

Note: Refer to the "STU serial reporting formats" section of the "Discovery10 Discovery Event Codes" document to view STU reporting codes used in the Discovery system.

Programming map

The Discovery menu is divided into two main functional areas:

- User menu
 - RAS user menu (see "[User menu structure](#)" on page 11).
 - WebUI main menu
- Install menu
 - RAS install menu (see "[Install menu structure](#)" on page 12).
 - WebUI Install Menu

The Install menus depicted on the following pages display unrestricted user access and contain options that do not apply to every Discovery system.

Access to the Install menu is typically limited to trained Discovery system installers and

other service technicians to program the Discovery system. Some of the options contained in the Install menu can adversely affect the operation of the system if used incorrectly.

Appendix B Programming worksheets

Print these worksheets as needed to record the system's programming details.

Content

Input worksheet.....	228
Area worksheet.....	229
Area group worksheet	230
RAS worksheet.....	231
DGPs worksheet.....	233
Alarm group worksheet.....	234
Timers worksheet	235
System options worksheet.....	236
Auto reset worksheet.....	238
Communications worksheets.....	239
Time zones worksheet.....	245
User categories worksheet	246
Relay mapping worksheet	247
Arm or disarm via time zone worksheet	248
Vaults worksheet	249
Area linking worksheet	249
Input shunt worksheet.....	250
Soft time zones worksheet.....	251
Battery testing worksheet	251
Custom message worksheet	252
Next service date worksheet.....	252
Event flags worksheets.....	252
Macro logic worksheet.....	255
Users worksheet.....	256
Door groups worksheet	257
Floor groups worksheet	259
Holidays worksheet	260
Automation zones worksheet.....	262
Doors & lifts worksheet	263
Standard lifts worksheet.....	264
Standard doors worksheet.....	265

Input worksheet

For programming details see “[Input database](#)” on page 63.

Figure 30: Input worksheet

Site		Discovery	
Input no.		Input name	
Input type		Type desc.	
Report ID		CID code and description	
Area		or area group	or alarm group
Test option		0 No Testing Required 1 Test During Access Test 2 Tested in Secure Test & Access 3 Test During Secure Test 4 Set Event Flag 13 During Access Test 5 Set Pre-Alarm During Access Test	
Test input within		days	
Selected event flag		Second event flag	
Mark check boxes to indicate YES ☒			
☐ Siren event	☐ Event flag 6, access alarm	☐ Activate selected event on unseal	
☐ Console warning	☐ Event flag 7, access alarm	☐ Camera event	
☐ Make all events 24-hour	☐ Event flag 8, 24-hr alarm	☐ Print when input is unsealed	
☐ Event flag 2, secure alarm	☐ Event flag 9, secure alarm	☐ Unsealed triggers second E/F	
☐ Event flag 3, secure alarm	☐ Event flag 10, secure alarm	☐ Isolate triggers second E/F	
☐ Event flag 4, secure alarm	☐ Event flag 11, secure alarm	☐ Alarm triggers second E/F	
☐ Event flag 5, secure alarm	☐ Event flag 13, secure alarm		

Input no.		Input name	
Input type		Type desc.	
Report ID		CID code and description	
Area		or area group	or alarm group
Test option		0 No Testing Required 1 Test During Access Test 2 Tested in Secure Test & Access 3 Test During Secure Test 4 Set Event Flag 13 During Access Test 5 Set Pre-Alarm During Access Test	
Test input within		days	
Selected event flag		Second event flag	
Mark check boxes to indicate YES ☒			
☐ Siren event	☐ Event flag 6, access alarm	☐ Activate selected event on unseal	
☐ Console warning	☐ Event flag 7, access alarm	☐ Camera event	
☐ Make all events 24-hour	☐ Event flag 8, 24-hr alarm	☐ Print when input is unsealed	
☐ Event flag 2, secure alarm	☐ Event flag 9, secure alarm	☐ Unsealed triggers second E/F	
☐ Event flag 3, secure alarm	☐ Event flag 10, secure alarm	☐ Isolate triggers second E/F	
☐ Event flag 4, secure alarm	☐ Event flag 11, secure alarm	☐ Alarm triggers second E/F	
☐ Event flag 5, secure alarm	☐ Event flag 13, secure alarm		

Area worksheet

For programming details see “[Area database](#)” on page 71.

Figure 31: Area worksheet

Site			Discovery				
Area no.		Area name					
Exit time (s)		Entry time (s)		Area account			
Siren event		Isolate		Local alarm		Warning timer	
Area accessed		Secure alarm		Exit timer		Camera event	
Unsealed		Access alarm		Entry timer		Pre-alarm timer	
Out-of-hours TZ		Area disarm time (m)			Perimeter area		

Area no.		Area name					
Exit time (s)		Entry time (s)		Area account			
Siren event		Isolate		Local alarm		Warning timer	
Area accessed		Secure alarm		Exit timer		Camera event	
Unsealed		Access alarm		Entry timer		Pre-alarm timer	
Out-of-hours TZ		Area disarm time (m)			Perimeter area		

Area no.		Area name					
Exit time (s)		Entry time (s)		Area account			
Siren event		Isolate		Local alarm		Warning timer	
Area accessed		Secure alarm		Exit timer		Camera event	
Unsealed		Access alarm		Entry timer		Pre-alarm timer	
Out-of-hours TZ		Area disarm time (m)			Perimeter area		

Area no.		Area name					
Exit time (s)		Entry time (s)		Area account			
Siren event		Isolate		Local alarm		Warning timer	
Area accessed		Secure alarm		Exit timer		Camera event	
Unsealed		Access alarm		Entry timer		Pre-alarm timer	
Out-of-hours TZ		Area disarm time (m)			Perimeter area		

Area group worksheet

For programming details see “[Area groups](#)” on page 170.

Figure 32: Area group worksheet

Site

Discovery

Area group no.

Description

Permissions: mark check boxes to indicate YES ☒

Area	Arm	Disarm	Reset	Timed
1	☐	☐	☐	☐
2	☐	☐	☐	☐
3	☐	☐	☐	☐
4	☐	☐	☐	☐
5	☐	☐	☐	☐
6	☐	☐	☐	☐
7	☐	☐	☐	☐
8	☐	☐	☐	☐
9	☐	☐	☐	☐
10	☐	☐	☐	☐
11	☐	☐	☐	☐
12	☐	☐	☐	☐
13	☐	☐	☐	☐
14	☐	☐	☐	☐
15	☐	☐	☐	☐
16	☐	☐	☐	☐
17	☐	☐	☐	☐
18	☐	☐	☐	☐
19	☐	☐	☐	☐
20	☐	☐	☐	☐
21	☐	☐	☐	☐
22	☐	☐	☐	☐
23	☐	☐	☐	☐
24	☐	☐	☐	☐
25	☐	☐	☐	☐
26	☐	☐	☐	☐
27	☐	☐	☐	☐
28	☐	☐	☐	☐
29	☐	☐	☐	☐
30	☐	☐	☐	☐
31	☐	☐	☐	☐
32	☐	☐	☐	☐
33	☐	☐	☐	☐
34	☐	☐	☐	☐
35	☐	☐	☐	☐
36	☐	☐	☐	☐
37	☐	☐	☐	☐
38	☐	☐	☐	☐
39	☐	☐	☐	☐
40	☐	☐	☐	☐
41	☐	☐	☐	☐
42	☐	☐	☐	☐
43	☐	☐	☐	☐
44	☐	☐	☐	☐
45	☐	☐	☐	☐
46	☐	☐	☐	☐
47	☐	☐	☐	☐
48	☐	☐	☐	☐
49	☐	☐	☐	☐
50	☐	☐	☐	☐
51	☐	☐	☐	☐
52	☐	☐	☐	☐
53	☐	☐	☐	☐
54	☐	☐	☐	☐
55	☐	☐	☐	☐
56	☐	☐	☐	☐
57	☐	☐	☐	☐
58	☐	☐	☐	☐
59	☐	☐	☐	☐
60	☐	☐	☐	☐
61	☐	☐	☐	☐
62	☐	☐	☐	☐
63	☐	☐	☐	☐
64	☐	☐	☐	☐
65	☐	☐	☐	☐
66	☐	☐	☐	☐
67	☐	☐	☐	☐
68	☐	☐	☐	☐
69	☐	☐	☐	☐
70	☐	☐	☐	☐
71	☐	☐	☐	☐
72	☐	☐	☐	☐
73	☐	☐	☐	☐
74	☐	☐	☐	☐
75	☐	☐	☐	☐
76	☐	☐	☐	☐
77	☐	☐	☐	☐
78	☐	☐	☐	☐
79	☐	☐	☐	☐
80	☐	☐	☐	☐
81	☐	☐	☐	☐
82	☐	☐	☐	☐
83	☐	☐	☐	☐
84	☐	☐	☐	☐
85	☐	☐	☐	☐
86	☐	☐	☐	☐
87	☐	☐	☐	☐
88	☐	☐	☐	☐
89	☐	☐	☐	☐
90	☐	☐	☐	☐
91	☐	☐	☐	☐
92	☐	☐	☐	☐
93	☐	☐	☐	☐
94	☐	☐	☐	☐
95	☐	☐	☐	☐
96	☐	☐	☐	☐
97	☐	☐	☐	☐
98	☐	☐	☐	☐
99	☐	☐	☐	☐

RAS worksheet

For programming details see “[RAS database](#)” on page 158.

Figure 33: RAS worksheet

Site				Discovery											
RAS number				Area alarm group				Menu alarm group							
Model (optional)				Door event flag				Relay number							
Mark check boxes to indicate YES ☒															
☐ Poll RAS				☐ Door event flag on alarm codes				☐ Reset from RAS without code							
☐ LCD arming station				☐ Display shunting on LCD				☐ Restricted user category to disarm							
☐ Toggle keyboard control				☐ Disarm/arm using one key				☐ Cards arm after three badges							
☐ ENTER key opens door only				☐ Cards auto disarm											
☐ Card and Code				☐ Cards always disarm/arms											
Area LED mapping (each LED can indicate an area from 1 to 99)															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

RAS number				Area alarm group				Menu alarm group							
Model (optional)				Door event flag				Relay number							
Mark check boxes to indicate YES ☒															
☐ Poll RAS				☐ Door event flag on alarm codes				☐ Reset from RAS without code							
☐ LCD arming station				☐ Display shunting on LCD				☐ Restricted user category to disarm							
☐ Toggle keyboard control				☐ Disarm/arm using one key				☐ Cards arm after three badges							
☐ ENTER key opens door only				☐ Cards auto disarm											
☐ Card and Code				☐ Cards always disarm/arms											
Area LED mapping (each LED can indicate an area from 1 to 99)															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

RAS number				Area alarm group				Menu alarm group							
Model (optional)				Door event flag				Relay number							
Mark check boxes to indicate YES ☒															
☐ Poll RAS				☐ Door event flag on alarm codes				☐ Reset from RAS without code							
☐ LCD arming station				☐ Display shunting on LCD				☐ Restricted user category to disarm							
☐ Toggle keyboard control				☐ Disarm/arm using one key				☐ Cards arm after three badges							
☐ ENTER key opens door only				☐ Cards auto disarm											
☐ Card and Code				☐ Cards always disarm/arms											
Area LED mapping (each LED can indicate an area from 1 to 99)															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Site			Discovery		
RAS number		RAS name			
Area alarm group		Door event flag		Model (optional)	
Menu alarm group		Relay number			
Mark check boxes to indicate YES ☒					
☐ Poll RAS	☐ Display shunting on LCD	☐ Restricted user category to disarm			
☐ LCD arming station	☐ Disarm/arm using one key	☐ Cards arm after three badges			
☐ Toggle keyboard control	☐ Cards auto disarm	☐ Card and code			
☐ ENTER key opens door only	☐ Cards always disarm/arms	☐ Entry and exit console warning			
☐ Door event flag on alarm codes	☐ Reset from RAS without code				
Area LED mapping (each LED can indicate an area from 1 to 99)					
1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16		

RAS number		RAS name			
Area alarm group		Door event flag		Model (optional)	
Menu alarm group		Relay number			
Mark check boxes to indicate YES ☒					
☐ Poll RAS	☐ Display shunting on LCD	☐ Restricted user category to disarm			
☐ LCD arming station	☐ Disarm/arm using one key	☐ Cards arm after three badges			
☐ Toggle keyboard control	☐ Cards auto disarm	☐ Card and code			
☐ ENTER key opens door only	☐ Cards always disarm/arms	☐ Entry and exit console warning			
☐ Door event flag on alarm codes	☐ Reset from RAS without code				
Area LED mapping (each LED can indicate an area from 1 to 99)					
1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16		

DGPs worksheet

For programming details see “[DGP database](#)” on page 87.

Figure 34: DGP worksheet

Site

Discovery

Mark check boxes to indicate YES ☒

LAN 1 DGPs

Address 1 — DGP type:		☐ Poll DGP	Address 9 — DGP type:		☐ Poll DGP
Address 2 — DGP type:		☐ Poll DGP	Address 10 — DGP type:		☐ Poll DGP
Address 3 — DGP type:		☐ Poll DGP	Address 11 — DGP type:		☐ Poll DGP
Address 4 — DGP type:		☐ Poll DGP	Address 12 — DGP type:		☐ Poll DGP
Address 5 — DGP type:		☐ Poll DGP	<i>4-Door and 4-Lift DGPs end here</i>		
Address 6 — DGP type:		☐ Poll DGP	Address 13 — DGP type:	0	☐ Poll DGP
Address 7 — DGP type:		☐ Poll DGP	Address 14 — DGP type:	0	☐ Poll DGP
Address 8 — DGP type:		☐ Poll DGP	Address 15 — DGP type:	0	☐ Poll DGP

LAN 1 DGPs

Address 17 — DGP type:		☐ Poll DGP	Address 25 — DGP type:		☐ Poll DGP
Address 18 — DGP type:		☐ Poll DGP	Address 26 — DGP type:		☐ Poll DGP
Address 19 — DGP type:		☐ Poll DGP	Address 27 — DGP type:		☐ Poll DGP
Address 20 — DGP type:		☐ Poll DGP	Address 28 — DGP type:		☐ Poll DGP
Address 21 — DGP type:		☐ Poll DGP	<i>4-Door and 4-Lift DGPs end here</i>		
Address 22 — DGP type:		☐ Poll DGP	Address 29 — DGP type:	0	☐ Poll DGP
Address 23 — DGP type:		☐ Poll DGP	Address 30 — DGP type:	0	☐ Poll DGP
Address 24 — DGP type:		☐ Poll DGP	Address 31 — DGP type:	0	☐ Poll DGP
			Address 32 — DGP type:	0	☐ Poll DGP

DGP type codes:

- 0—Standard DGP (TS0820, TS0824, TS-827) or Wireless DGP (TS0825, TS0825E, CA1230)
- 1—Intelligent 4-Door Controller DGP (TS0866, TS0867)
- 2—Intelligent 4-Lift Controller DGP (TS0869)
- 3—C10 Door Controller DGP (TS1066)
- 4—C10 Door Controller Alarm mode

Alarm group worksheet

For programming details see “[Alarm groups](#)” on page 90.

Figure 35: Alarm Group worksheet

Site		Discovery	
Alarm group no.		Alarm group name	
Area* / area group		Time zone	
		Alternate alarm group	

Mark check boxes to indicate YES ☒

Alarm group YES/NO options (items marked * display only when an area is assigned)

☐ User alarm group	☐ Prevent forced disarming
☐ Alarm system control	☒ Can user access via remote
☐ Prompt with list of areas	☐ Link user to category 1
☐ Keypad duress	☐ Link user to category 2
☐ Reset system alarms	☐ Link user to category 3
☐ Can area be armed*	☐ Link user to category 4
☐ Can area be disarmed*	☐ Link user to category 5
☐ Can area be reset*	☐ Link user to category 6
☐ Can area be timed*	☐ Link user to category 7
☐ Disable auto-deisolate	☐ Link user to category 8
☐ Auto isolate unsealed inputs	☐ No arming if user category not timing
☐ Forced arming unsealed inputs	☐ Enable area search

User menu YES/NO options

☐ 1. Panel Status	☐ 13. Start Auto Access Test
☐ 2. Input Unsealed	☐ 14. Program Users
☐ 3. Input in Alarm	☐ 15. Time & Date
☐ 4. Input Isolated	☐ 16. Isolate/Deisolate RAS/DGP
☐ 5. History	☐ 17. Enable/Disable Service Tech
☐ 6. Test Report	☐ 18. Reset Cameras
☐ 7. Service Menu	☐ 19. Install Menu
☐ 8. Film Counters	☐ 20. Door and Floor Groups
☐ 9. Input Text	☐ 21. Holidays
☐ 10. Isolate	☐ 22. Open Door
☐ 11. Deisolate	☐ 23. Unlock, Lock, Disable and Enable
☐ 12. Test Input	☐ 24. Automation Control

Timers worksheet

For programming details see “[Timers](#)” on page 100.

Figure 36: Timers worksheet

Site				Discovery			
User category 1 (m)		User category 8 (m)		Local alarm reminder (m)			
User category 2 (m)		Access test (m)		Individual testmode (m)			
User category 3 (m)		Secure test (m)		Door(s) unlock (s)			
User category 4 (m)		Warning (m)		Tester event flag (s)			
User category 5 (m)		Delay holdup (s)		Siren (m)			
User category 6 (m)		Suspicion (s)		Mains fail (m)			
User category 7 (m)		Service (m)		Card to code (s)			
Min area search (m)		Max area search (m)					

Site				Discovery			
User category 1 (m)		Access test (m)		Door(s) unlock (s)			
User category 2 (m)		Secure test (m)		Tester event flag (s)			
User category 3 (m)		Warning (m)		Siren (m)			
User category 4 (m)		Delay holdup (s)		Mains fail (m)			
User category 5 (m)		Suspicion (s)		Card to code (s)			
User category 6 (m)		Service (m)		Min area search time (m)			
User category 7 (m)		Local alarm reminder (m)		Max area search time (m)			
User category 8 (m)		Individual input test (m)		Max twin trip (s)			

System options worksheet

For programming details see “[System options](#)” on page 104.

Figure 37: System options worksheet

System Options Part 1			
Discovery Number			
Total disarm area/area group		Event text	
Film low		Number of prefix digits	
Film out		Time before Rotate	
Test mode		Rotate speed	
No. of relay controllers		User Offset	
EOL resistor	☐ 10K ☐ 4K7 ☐ 2K2 ☐ 6K8 ☐ 5K6 ☐ 3K7 ☐ 3K3 ☐ 2K0 ☐ 1K5 ☐ 1K0 ☐ 2K2/6K8		
Time zone	☐ No time zone ☐ Lord Howe Island ☐ Hobart Tas ☐ Melbourne Vic ☐ Sydney NSW ☐ Broken Hill NSW ☐ Brisbane Qld ☐ Adelaide SA ☐ Darwin NT ☐ Perth WA ☐ Eucla WA ☐ New Zealand		
Area search time zone		Decrement test days during TZ	
System Options Part 2			
System YES/NO options Mark check box to indicate YES ☒			
☐ Input tamper monitoring	☐ Dual custody code programming		
☐ Automatic deisolate when Accessed	☐ Display alarms instant on LCD		
☐ Display one input at a time	☐ Sirens only after report fail		
☐ Name file	☐ Financial options		
☐ System alarms set siren and strobe	☐ Display user flags		
☐ System alarms latch	☐ Delay holdup lockout		
☐ Siren testing	☐ Skip access check for service tech		
☐ Disable 0 ENTER camera reset	☐ Enable expanded test reporting		
☐ Disable auto insert of user cat.	☐ Expanded test success reporting		
☐ Disable LEDs that don't report	☐ Enable exit fault reporting		
☐ Disable code from displaying	☐ Enable V8 Multibreak		
☐ Disable flashing area LEDs	☐ Enable V8 Numbering		
System Options Part 3			
Site Code A		Offset A	
Site Code B		Offset B	
		Card learn RAS	

Site		Discovery	
------	--	-----------	--

System Options Part 1

Total disarm area/area group		Event text	
Film low		Number of prefix digits	
Film out		Time before rotate	
Test mode		Rotate speed	
No. of relay controllers		User offset	

EOL resistor ☐ 10K ☐ 4K7 ☐ 2K2 ☐ 6K8 ☐ 6K6 ☐ 3K7 ☐ 3K3 ☐ 2K0 ☐ 1K5 ☐ 1K0 ☐ 2K2/6K8

Time zone ☐ No time zone ☐ Lord Howe Island ☐ Hobart Tas ☐ Melbourne Vic
☐ Sydney NSW ☐ Broken Hill NSW ☐ Brisbane Qld ☐ Adelaide SA
☐ Darwin NT ☐ Perth WA ☐ Eucla WA ☐ New Zealand

Area search time zone Decrement test days during TZ

System Options Part 2

System YES/NO options Mark check boxes to indicate YES ☒

☐ Input tamper monitoring	☐ Dual custody code programming
☐ Automatic deisolate when accessed	☐ Display alarms instant on LCD
☐ Display one input at a time	☐ Sirens only after report fail
☐ Name file	☐ Financial options
☐ System alarms set siren and strobe	☐ Display user flags
☐ System alarms latch	☐ Delay holdup lockout
☐ Siren testing	☐ Skip access check for service tech
☐ Disable 0 ENTER camera reset	☐ Enable expanded test reporting
☐ Disable auto insert of user category	☐ Expanded test success reporting
☐ Disable LEDs that don't report	☐ Enable exit fault recording
☐ Disable code from displaying	☐ Enable V8 multibreak
☐ Disable flashing area LEDs	☐ Enable V8 numbering

System Options Part 3

Site Code A		Card learn RAS	
Offset A		External siren mode	
Site Code B		Internal siren mode	
Offset B			

Auto reset worksheet

For programming details see “[Auto reset](#)” on page 116.

Figure 38: Auto reset worksheet

Site		Discovery	
Alarm group no.		Alarm group name	
Auto reset time (m)			

Communications worksheets

For programming details see “[Communications](#)” on page 117.

Figure 39: Communications devices worksheet

Site		Discovery	
------	----------------------	-----------	----------------------

Comm. Devices

Location

Expander Type

Modem Options

☐ Monitor Ring	☐ Line Fault Monitoring
☐ Enable Blind Dial	☐ Enable New Zealand Dialing

Ethernet

☐ Enable Ethernet ☐ Enable Ping

IP Address

Subnet Mask

Gateway IP Address

WiFi

Network Name (SSID)

☐ Enable WiFi ☐

IP Address

Subnet Mask

Gateway IP Address

Pass Phrase

GSM

SIM 1	SIM 2
SIM PIN	SIM PIN
SIM APN	SIM APN
APN Username	APN Username
APN Password	APN Password
SIM APN Authentication	SIM APN Authentication

Serial

BAUD Rate Parity Stop Bits

USB

USB Options

☐ Host	☐ Slave
-------------------------------	--------------------------------

Figure 40: Communications devices worksheet (onboard hardware)

Site

Discovery

Onboard devices

Mark check boxes to indicate YES ☒

Modem

☐ Monitor ring

☐ Blind dial

☐ PSTN line fault monitor

☐ New Zealand dialling

Serial

BAUD rate

Parity

Stop bits

USB

USB option

☐ Host

☐ Slave

Ethernet

☐ Enable Ethernet

☐ Enable ping

IP address

Subnet mask

Gateway address

DNS server 1

DNS server 2

Figure 41: Communications devices worksheet (external hardware)

Site		Discovery	
------	----------------------	-----------	----------------------

External device Mark check boxes to indicate YES ☒

Location

Board type

Serial

BAUD rate Parity Stop bits

Ethernet

☐ Enable Ethernet ☐ Enable ping

IP address . . .

Subnet mask . . .

Gateway address . . .

WiFi

☐ Enable WiFi ☐ Enable ping

IP address . . .

Subnet mask . . .

Gateway address . . .

Network name (SSID)

Passphrase 1

Passphrase 2

Figure 42: Communications paths worksheet

Site	Discovery		
Main			
Path no.	Format	Sub-format	
Name			
Location	Port	Account code	
Priority	Backup for path no.	Computer password	
Connection control			
☐ Always connect	☐ Connect on event	☐ Connect on service	
☐ Connect on buffer at 80%	☐ Isolated inputs trigger path	☐ Stay connected on empty buffer	
☐ Control command	☐ Trigger comms fail event	☐ Area account codes	
☐ Heartbeat fail triggers path			
Filter			
By area	By area group	By time zone	Multi-break alarm timer
☐ Report alarm events	☐ Report access events	☐ Send events out of TZ	
☐ Remove unsent events	☐ System alarm report	☐ Multi break alarms	
☐ Multi break restores	☐ Report open/close	☐ Common open/close	
☐ Report computer connected			
Test calls			
Test call option (0-8)	Hours	Minutes	Day
Dial settings			
PABX no.	Phone 1	Phone 2	
Number of redials	Number of calls to answer	Number of rings to answer	
☐ Auto answer	☐ Call back	☐ DTMF dial	
IP settings			
IP address (remote computer)	Send IP port	Listen IP port	
IP mode (UDP/IP or TCP/IP)	Server/client mode		
☐ Dynamic computer IP address			
Encryption settings			
Encryption type	☐ None	☐ Twofish	☐ AES 128-bit ☐ AES 256-bit
Key 16			
— or —			
Key 32			
Advanced settings			
Computer attempts	Message ACK timeout	Message retries	
Connect timeout	Connect retries	Wait time between connections	
Heartbeat timeout			

Sic

Discovery

Mllh

D

E"llh

Sub ronn.rt

Interface location

Bai: 'lar lhoo

Interface port

.im:ciuJ"ll;jc

Priority

O!lmutllr ii

at.m: an <i11ntd

☐ Always conn
☐ Conner 111111H1 ll:-8lllJ;
☐ Cblitrd ixnt,mnd
☐ caunu :c.r:oo ,r:wnl li"t!: no pil

D a:.oncDi oo -r:m:

DZ;: led j?UIS. lrl(19U" itah

D, room nag

CIIIUK:I:I IM1 g-JV!m

D 8lwj on ttll'ar

l.f.s;c: ll'tell ll:.'CNJnl <Jdll

Filter

Of.11'11.1 JIU.

zone D

M I ?rcllli:'

☐ Report alarm events
☐ Remove unsent events
☐ Multi break restores
☐ Report connection events

O z.c ts;

DRI!Ki'I ;ram-;

D Rcpal'l

DRI:!!YSloo

&Joo-1: ts: wterTI

J..b.u11 bra.iii: lilnrt.

O ctrnmlllll:lf=.:ln.l:bl:t

Ilo nn dmis. pr:lidng JTTK.

Test calls

Test call option (0-8)

Dial settings

E"AEiC mll.

1

E=txmc 2

umber of redials

Auto answer

Ji

Nu

C'Hnb ,afmq;

IP

8cn

Pllf

D

lcn pari

.S.:r.mdkiP III -::;sD.

IPM:dl: 0T0P1P0

UEE'

S flr:ll"a m!4l-

o ro

""O

IIORISS

E:na,-ptoo J. ng;

E:nrr;ptm 'tp'pe

(

Twofish

AES 128-bit

AES256!1:11

.....

lll!

T""H I

Ad trn

Connect timeout (s)

CIMlIPta"lll Is.

PJJ'lhaiik 1111

Name

Message ACK timeout (ms)

D

Message retries

D

Wait time between connections (s) -

Heartbeat timeout (s)

D

Password

Time zones worksheet

For programming details see “[Time zones](#)” on page 146.

Figure 43: Time zones worksheet

Site

Discovery

Time zone no.

Time zone name

Sub-time zones

Start

End

Days

S

M

T

W

T

F

S

Holiday types

1

2

3

4

5

6

7

8

Mark check boxes to indicate YES

☒

Time zone no.

Time zone name

Sub-time zones

Start

End

Days

S

M

T

W

T

F

S

Holiday types

1

2

3

4

5

6

7

8

Mark check boxes to indicate YES

☒

User categories worksheet

For programming details see “[User category](#)” on page 5.

Figure 44: User categories worksheet

Site		Discovery	
User category names			
User category 1			
User category 2			
User category 3			
User category 4			
User category 5			
User category 6			
User category 7			
User category 8			

Relay mapping worksheet

For programming details see “[Map relays](#)” on page 147.

Figure 45: Relay mapping worksheet

Site

Discovery

Mark check boxes to indicate YES ☒

Relay no.		Application		
Event flag		Time zone		☐ Inactive during time zone ☐ Relay inverted
Relay no.		Application		
Event flag		Time zone		☐ Inactive during time zone ☐ Relay inverted
Relay no.		Application		
Event flag		Time zone		☐ Inactive during time zone ☐ Relay inverted
Relay no.		Application		
Event flag		Time zone		☐ Inactive during time zone ☐ Relay inverted
Relay no.		Application		
Event flag		Time zone		☐ Inactive during time zone ☐ Relay inverted
Relay no.		Application		
Event flag		Time zone		☐ Inactive during time zone ☐ Relay inverted
Relay no.		Application		
Event flag		Time zone		☐ Inactive during time zone ☐ Relay inverted
Relay no.		Application		
Event flag		Time zone		☐ Inactive during time zone ☐ Relay inverted
Relay no.		Application		
Event flag		Time zone		☐ Inactive during time zone ☐ Relay inverted

Arm or disarm via time zone worksheet

For programming details see “[Arm/disarm via TZ](#)”. On page 146.

Figure 46: Arm or disarm via time zone worksheet

Site		Discovery	
Arm/disarm no.		Application	
Time zone no.		Alarm group no.	
Arm/disarm no.		Application	
Time zone no.		Alarm group no.	
Arm/disarm no.		Application	
Time zone no.		Alarm group no.	
Arm/disarm no.		Application	
Time zone no.		Alarm group no.	
Arm/disarm no.		Application	
Time zone no.		Alarm group no.	
Arm/disarm no.		Application	
Time zone no.		Alarm group no.	
Arm/disarm no.		Application	
Time zone no.		Alarm group no.	
Arm/disarm no.		Application	
Time zone no.		Alarm group no.	

Vaults worksheet

For programming details see “[Vaults](#)” on page 151.

Figure 47: Vaults programming worksheet

Site

Discovery

Vault area

or area group

Area linking worksheet

For programming details see “[Area linking](#)” on page 153.

Figure 48: Area linking worksheet

Site

Discovery

Area

Linked to area

or area group

Input shunt worksheet

For programming details see “[Input shunts](#)” on page 153.

Figure 49: Input shunt worksheet

Site

Discovery

Shunt timer no.

Application

Input number

Relay number

Shunt time

Warning time

Event flag

Warning event flag

Shunt RAS

Input shunt YES/NO options

Mark check boxes to indicate YES ☒

☐ Door open command starts shunt

☐ Door shunted in access

☐ Door shunted in secure

☐ Cancel door event flag

☐ Input holds event flag at 2 seconds

☐ Entry/exit shunting

☐ Report door open/close

Shunt timer no.

Application

Input number

Relay number

Shunt time

Warning time

Event flag

Warning event flag

Shunt RAS

Input shunt YES/NO options

Mark check boxes to indicate YES ☒

☐ Door open command starts shunt

☐ Door shunted in access

☐ Door shunted in secure

☐ Cancel door event flag

☐ Input holds event flag at 2 seconds

☐ Entry/exit shunting

☐ Report door open/close

Shunt timer no.

Application

Input number

Relay number

Shunt time

Warning time

Event flag

Warning event flag

Shunt RAS

Input shunt YES/NO options

Mark check boxes to indicate YES ☒

☐ Door open command starts shunt

☐ Door shunted in access

☐ Door shunted in secure

☐ Cancel door event flag

☐ Input holds event flag at 2 seconds

☐ Entry/exit shunting

☐ Report door open/close

Shunt timer no.

Application

Input number

Relay number

Shunt time

Warning time

Event flag

Warning event flag

Shunt RAS

Input shunt YES/NO options

Mark check boxes to indicate YES ☒

☐ Door open command starts shunt

☐ Door shunted in access

☐ Door shunted in secure

☐ Cancel door event flag

☐ Input holds event flag at 2 seconds

☐ Entry/exit shunting

☐ Report door open/close

Soft time zones worksheet

For programming details see “[Soft time zones](#)” on page 160.

Figure 50: Time zone to follow relay worksheet

Site		Discovery	
Soft time zone	Relay	Description	
26	☐		
27	☐		
28	☐		
29	☐		
30	☐		
31	☐		
32	☐		
33	☐		
34	☐		
35	☐		
36	☐		
37	☐		
38	☐		
39	☐		
40	☐		
41	☐		

Battery testing worksheet

For programming details see “[Battery testing](#)” on page 161.

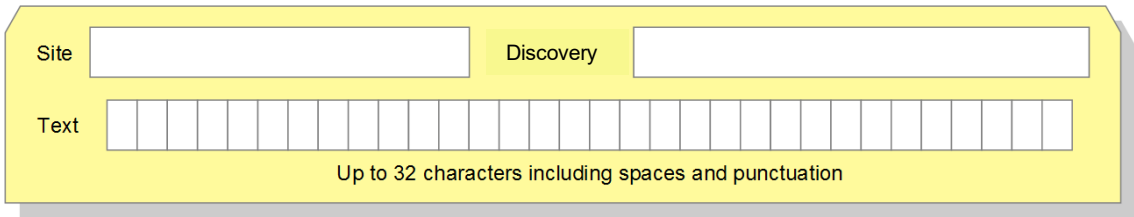
Figure 51: Batterytesting worksheet

Site		Discovery	
☐ Disabled	☐ Every working day	☐ Every Monday	☐ First Monday of month
Mark check boxes to indicate YES ☒			
Start		hh	mm
Duration (m)			

Custom message worksheet

For programming details see “[Custom message](#)” on page 161.

Figure 52: Custom message worksheet

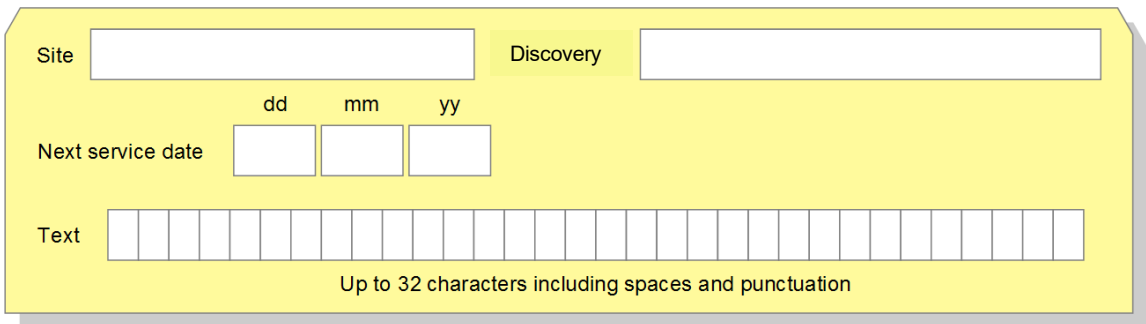


A yellow rectangular form with a 3D effect. It contains two text input fields at the top: 'Site' on the left and 'Discovery' on the right. Below these is a 'Text' field consisting of 32 individual character boxes. A label 'Up to 32 characters including spaces and punctuation' is centered below the character boxes.

Next service date worksheet

For programming details see “[Program next service](#)” on page 163.

Figure 53: Next service date worksheet



A yellow rectangular form with a 3D effect. It contains two text input fields at the top: 'Site' on the left and 'Discovery' on the right. Below these is a 'Next service date' section with three boxes labeled 'dd', 'mm', and 'yy'. At the bottom is a 'Text' field consisting of 32 individual character boxes. A label 'Up to 32 characters including spaces and punctuation' is centered below the character boxes.

Event flags worksheets

Event flags 1 to 16 have pre-defined functionality as shown in [Table 30](#) on page 223. The functionality is indicated when programming inputs (for example “Event Flag 2, Secure Alarm”). However, they can also be assigned names. Any of the 255 event flags can be assigned names to describe their particular application via “[Event flag names](#)” on page 163.

Event flags 17 to 255, and some predefined event flags can be used to define either summary (system) events or for outputs to relays or macros.

- Use [Figure 54](#) on page 253 to record the numbers of summary event flags. See “[Program summary event flags](#)” on page 165 for details.
- Use [Figure 55](#) on page 254 to record the numbers (typically using the same number as the physical relay) and names (or application) of event flags.

Figure 54: Summary event flags worksheet

Site		Discovery	
Mains fail	☐	Duress	☐
Low battery	☐	Film out	☐
Fuse fail	☐	Report fail	☐
Tamper	☐	Test mode	☐
Siren fail	☐	All secured	☐
DGP isolate	☐	Console trigger	☐
DGP offline	☐	Area search running	☐
RAS offline	☐	Area search done	☐

Figure 55: Event flag names worksheet

[illegible]

Macro logic worksheet

For programming details see “[Program macro logic](#)” on page 167.

Figure 56: Macro logic worksheet

Site

Discovery

Mark check boxes to indicate YES ☒

Macro number

Description

Macro function:

Disabled ☐

On pulse ☐

Non-timed ☐

On timed ☐

Latched ☐

On delay ☐

Off delay ☐

Time

Seconds

Minutes

Macro output activates:

Event flag ☐

Number

Input ☐

Invert ☐

Macro output is generated subject to the following inputs:

Macro input 1

Event flag ☐

Number

Relay ☐

Invert ☐

and ☐

or ☐

Macro input 2

Event flag ☐

Number

Relay ☐

Invert ☐

and ☐

or ☐

Macro input 3

Event flag ☐

Number

Relay ☐

Invert ☐

Macro input 4

Event flag ☐

Number

Relay ☐

Invert ☐

Notes:

“Invert” indicates an inactive input or a deactivated output.

Macro input 4 resets the output for latched functionality. The and/or selection does not apply.

Macro number

Description

Macro function:

Disabled ☐

On pulse ☐

Non-timed ☐

On timed ☐

Latched ☐

On delay ☐

Off delay ☐

Time

Seconds

Minutes

Macro output activates:

Event flag ☐

Number

Input ☐

Invert ☐

Macro output is generated subject to the following inputs:

Macro input 1

Event flag ☐

Number

Relay ☐

Invert ☐

and ☐

or ☐

Macro input 2

Event flag ☐

Number

Relay ☐

Invert ☐

and ☐

or ☐

Macro input 3

Event flag ☐

Number

Relay ☐

Invert ☐

Macro input 4

Event flag ☐

Number

Relay ☐

Invert ☐

Notes:

“Invert” indicates an inactive input or a deactivated output.

Macro input 4 resets the output for latched functionality. The and/or selection does not apply.

Users worksheet

User records are programmed in user menu “[Program Users](#)” on page 23.

Figure 57: Users worksheet

Site		Discovery	
Mark check boxes to indicate YES ☒			
User number	PIN	Name	
Start date		End date	
hh:mm dd/mm/yyyy		hh:mm dd/mm/yyyy	
Alarm group	Door group	Floor group	
☐ Dual custody	☐ Guard	☐ Visitor	☐ Trace
☐ Card only	☐ Privileged	☐ Long access	
User number	PIN	Name	
Start date		End date	
hh:mm dd/mm/yyyy		hh:mm dd/mm/yyyy	
Alarm group	Door group	Floor group	
☐ Dual custody	☐ Guard	☐ Visitor	☐ Trace
☐ Card only	☐ Privileged	☐ Long access	
User number	PIN	Name	
Start date		End date	
hh:mm dd/mm/yyyy		hh:mm dd/mm/yyyy	
Alarm group	Door group	Floor group	
☐ Dual custody	☐ Guard	☐ Visitor	☐ Trace
☐ Card only	☐ Privileged	☐ Long access	
User number	PIN	Name	
Start date		End date	
hh:mm dd/mm/yyyy		hh:mm dd/mm/yyyy	
Alarm group	Door group	Floor group	
☐ Dual custody	☐ Guard	☐ Visitor	☐ Trace
☐ Card only	☐ Privileged	☐ Long access	
User number	PIN	Name	
Start date		End date	
hh:mm dd/mm/yyyy		hh:mm dd/mm/yyyy	
Alarm group	Door group	Floor group	
☐ Dual custody	☐ Guard	☐ Visitor	☐ Trace
☐ Card only	☐ Privileged	☐ Long access	

Door groups worksheet

Door groups are programmed in user menu Door and Floor Groups. Discovery panels support 255 door groups.

Figure 58: Door groups 1 to 128 worksheet

Site

Discovery

Door group no.

Description

Door	TZ	Door	TZ	Door	TZ	Door	TZ
1		33		65		97	
2		34		66		98	
3		35		67		99	
4		36		68		100	
5		37		69		101	
6		38		70		102	
7		39		71		103	
8		40		72		104	
9		41		73		105	
10		42		74		106	
11		43		75		107	
12		44		76		108	
13		45		77		109	
14		46		78		110	
15		47		79		111	
16		48		80		112	
17		49		81		113	
18		50		82		114	
19		51		83		115	
20		52		84		116	
21		53		85		117	
22		54		86		118	
23		55		87		119	
24		56		88		120	
25		57		89		121	
26		58		90		122	
27		59		91		123	
28		60		92		124	
29		61		93		125	
30		62		94		126	
31		63		95		127	
32		64		96		128	

Figure 59: Door groups 129 to 255 worksheet

Site		Discovery					
Door group no.		Description					
Door	TZ	Door	TZ	Door	TZ	Door	TZ
129		161		193		225	
130		162		194		226	
131		163		195		227	
132		164		196		228	
133		165		197		229	
134		166		198		230	
135		167		199		231	
136		168		200		232	
137		169		201		233	
138		170		202		234	
139		171		203		235	
140		172		204		236	
141		173		205		237	
142		174		206		238	
143		175		207		239	
144		176		208		240	
145		177		209		241	
146		178		210		242	
147		179		211		243	
148		180		212		244	
149		181		213		245	
150		182		214		246	
151		183		215		247	
152		184		216		248	
153		185		217		249	
154		186		218		250	
155		187		219		251	
156		188		220		252	
157		189		221		253	
158		190		222		254	
159		191		223		255	
160		192		224			

Floor groups worksheet

Floor groups are programmed in user menu Door and Floor Groups. Discovery panels support 128 floor groups.

Figure 60: Floorgroups worksheet

Site

Discovery

Floor group no.

Description

Floor	TZ	Floor	TZ	Floor	TZ	Floor	TZ
1		33		65		97	
2		34		66		98	
3		35		67		99	
4		36		68		100	
5		37		69		101	
6		38		70		102	
7		39		71		103	
8		40		72		104	
9		41		73		105	
10		42		74		106	
11		43		75		107	
12		44		76		108	
13		45		77		109	
14		46		78		110	
15		47		79		111	
16		48		80		112	
17		49		81		113	
18		50		82		114	
19		51		83		115	
20		52		84		116	
21		53		85		117	
22		54		86		118	
23		55		87		119	
24		56		88		120	
25		57		89		121	
26		58		90		122	
27		59		91		123	
28		60		92		124	
29		61		93		125	
30		62		94		126	
31		63		95		127	
32		64		96		128	

Holidays worksheet

Holiday records are programmed in user menu [Holidays](#).

Figure 61: Holidays worksheet

Site

Discovery

Mark check boxes to indicate YES ☒

Holiday	Description	Start	End	Recur	Holiday types							
					1	2	3	4	5	6	7	8
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐	☐	☐	☐	☐

Figure 62: Holiday types worksheet

Site		Discovery	
Holiday type	Description		
1			
1			
3			
4			
5			
6			
7			
8			

Automation zones worksheet

Automation zones are programmed in “[Automation](#)” on page 171.

Figure 63: Automation zones worksheet

Site

Discovery

Automation zone no.

Name

Mark check boxes to indicate YES

☒

☐ Enable zone

Event flag to trigger zone

☐ Invert trigger

TZ to disable E/F trigger

TZ to trigger zone

Trigger (on) level %

Reset (off) level %

Trigger (on) for (s)

Ramp rate

☐ Instant

☐ 20 seconds

☐ 90 seconds

☐ 7 minutes

☐ 4 seconds

☐ 30 seconds

☐ 2 minutes

☐ 10 minutes

☐ 8 seconds

☐ 40 seconds

☐ 3 minutes

☐ 15 minutes

☐ 12 seconds

☐ 60 seconds

☐ 5 minutes

☐ 17 minutes

Control

Control on RAS no.

☐ Enable quick control

☐ Enable manual control

☐ Manual On control

☐ Manual Off control

Zone type

☒ Internal

☐ Tecom

☐ Tecom with feedback

☐ C-Bus

☐ C-Bus with feedback

C-Bus options

☐ Enable logging of C-Bus events

Zone activates E/F

Set E/F at level (%)

Reset E/F at level (%)

Group number

Network number

Application number

Doors & lifts worksheet

Doors are programmed in “Door/lift names and E/F trigger”.

Figure 64: Doors & lifts worksheet

[illegible]

Standard lifts worksheet

Standard lifts are programmed in “[Standard lifts](#)” on page 179.

Figure 65: Standard lifts worksheet

Site		Discovery			
Lift number		Lift name			
Remote reader		Floor 1 relay		Floor 6 relay	
Lift access time (s)		Floor 2 relay		Floor 7 relay	
Remote reader access time (s)		Floor 3 relay		Floor 8 relay	
Override floor group		Floor 4 relay		Floor 9 relay	
Security floor group		Floor 5 relay		Floor 10 relay	
Security trigger E/F					
Lift number		Lift name			
Remote reader		Floor 1 relay		Floor 6 relay	
Lift access time (s)		Floor 2 relay		Floor 7 relay	
Remote reader access time (s)		Floor 3 relay		Floor 8 relay	
Override floor group		Floor 4 relay		Floor 9 relay	
Security floor group		Floor 5 relay		Floor 10 relay	
Security trigger E/F					

Standard doors worksheet

Standard lifts are programmed in “[Standard doors](#)” on page 183.

Figure 66: Standard doors worksheet

Site

Discovery

Door number

Door name

Door access options

Access time (s)

Pre lock time (s)

Post lock time (s)

Override time zone

☐ Override after entry

Shunting/Passback/Egress

Shunt type

☐ No shunting

☐ Input shunting

☐ Input shunting & DOTL

Shunt time (s)

Warning time (s)

☐ Cancel shunt when door secures

Egress time zone

☐ Egress reporting

Alarm control

Alarm group

Alarm control

☐ No alarm control

☐ 1 badge to disarm, 3 to arm

☐ 3 badge to disarm, 3 to arm

Multi badge time (s)

☐ No access if area armed

Hardware

Lock type

☐ Strike

☐ Maglock/dropbolt

Door input

Egress input

DOTL input

Lock relay

Warning relay

Glossary

2-state monitoring	The system's input circuits are monitored for sealed and unsealed conditions.
4-state monitoring	The system's input circuits are monitored for sealed, unsealed, open, and short conditions. 4-state monitoring (also called input tamper monitoring) is used in Discovery systems by default. See "input tamper".
24-hour alarm	Input types that will generate an alarm regardless of area status (armed or disarmed).
4-Door/Lift DGP	See "Network Access Controller".
Access	The state of an area when it's disarmed. The condition of an area when it is occupied and when the intrusion detection system has been set so that normal activity does not generate an alarm. Opposite of "secure".
Access control	Control of entry to, or exit from, a security area. The Discovery system typically controls access by allowing only authorised users to unlock a door or to enter a lift.
Access test	The access (disarmed) test is a defined interval during which specific inputs may be tested to see if they are operating correctly when the area is occupied. The input must be programmed to be included in access tests (determined by the input's test type).
Access time	The time that a door will remain unlocked after a user has been granted access.
Acknowledge	See "reset".
Alarm	The state of an intrusion detection system when an input is unsealed and the condition of the area is such that state should be signalled, for example, a door is opened when its area is armed.
Alarm code	The user's full PIN (used for alarm control and optionally for door control). See also "door code".
Alarm code prefix digits	The alarm code prefix value in the range one to four enables users to enter a door code (a shorter PIN) for access control. For example, if a user's full PIN is six digits long (for example, 123456), and the alarm code prefix value is two, then the first two digits are removed for access control, and the user can operate doors by entering only the last four digits of the PIN (for example, 3456).
Alarm control	The control over alarm (arm and disarm) functions.

Alarm group	A panel programming concept that defines a group of areas, functions and menu options. Alarm groups are assigned to users, RASs, or door readers, to define what areas can be controlled and what functions can be performed by that user, or from that device. An alarm group can also be assigned to certain input types such as key switches.
Alarm reporting	A procedure to transmit (via Ethernet, dialler, or other means) alarm events or other events to a remote monitoring company by means of a set of rules called a protocol.
Anti-passback	Anti-passback affects the ability of users to move from one region to another. Entering a region twice in succession is either not possible (hard anti-passback), or will only result in an event being logged in the history log, reported to the printer and to management software (soft anti-passback). Also see “Privileged”. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Area	A logical grouping of input devices that are armed and disarmed simultaneously.
Area group	A Discovery system can have 99 areas, so area groups are used to help manage them. There can be 255 area groups.
Area search	Area search is a process by which a person must ensure that a facility is safe as part of the disarming process.
Armed	See “secure”.
Arming station (RAS)	A remote arming station (RAS) is a device that provides a user interface for security functions for areas or for access points (doors). The RAS may be an LCD keypad, or any other device that can be used to perform security functions such as arm or disarm, open doors, and so on.
Card	A portable device (card or fob) that holds information to identify a user to the Discovery system. The information to identify a user can be stored in a chip (smart card), on a magnetic strip, a bar-code, a Wiegand card, or in biometric data such as a fingerprint.
Card only	The “card only” user flag is enabled for users when you want non-Tecom format cards such as credit cards, financial institution cards, and so on, to be programmed as users, and you want to use only the card and not the PIN. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Central station	See “remote monitoring company”.
CID	Ademco Contact ID alarm reporting format.
Computer event	Event-driven mode of IP connection (UDP/IP) to a management software computer. In event-driven mode, the Discovery panel reports events only as they occur in order to minimise network bandwidth requirements.

Computer polled	Polled mode is typically used for RS-232 or USB connection to a management software computer. It can also be used for IP connection (TCP/IP). Polled mode typically consumes greater bandwidth than event-driven mode. However this can be useful for panels that deliver little event-driven activity. Some networks require a certain amount of activity in order to maintain an active communications path.
Console	See "arming station".
Console warning	Same as keypad buzzer.
DGP	Data Gathering Panel. A DGP expands the capacity of the Discovery system.
Dialler	An electronic device that allows the intrusion detection system to transmit alarms and other events to a remote monitoring company via telephone lines. Can also be used to perform sending and retrieval of access control data with management software.
Disarmed	See "access".
Door code	An optional version of the user's PIN shortened by the number of digits specified in the alarm code prefix. The door code is used for access control (for example, to open a door) without revealing the entire PIN used for alarm control.
Door contact	A magnetic contact used to detect if a door or window is opened.
Door control	The control over door functions.
Door group	A panel programming concept that assigns a group of doors to a user in order to allow access at those doors. Access to each door in a group may be restricted via a time zone.
DOTL	Door open too long. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Dual custody	The term "dual custody" is used in the following ways: • If the Discovery system option "Dual Custody Code Programming" is enabled, then two users are required to authenticate before access is granted to menu, Program Users. • If the "dual custody" user flag is enabled for a user, the user will always require a second valid user authentication in order to perform an alarm or access control function at a door or lift connected to an Network Access Controller (doors or lifts 17 to 64 and 81 to 128). • If a RAS connected to an Network Access Controller (doors or lifts 17 to 64 and 81 to 128) is designated as either an "IN reader dual custody" or "OUT reader dual custody", then two users are required to authenticate in succession in order to unlock the door.

Duress	A situation where a user is being forced to breach the system security (for example, forced at gunpoint to open a door). The duress facility allows a signal to be activated (for example, notification to a remote monitoring company) by the user. See also “keypad duress”.
Egress	Exit, or request to exit (RTE)
Egress input	An input that is programmed to request that a door be briefly unlocked. For example, an egress button is provided inside a doorway to allow users to exit without using a door reader. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Egress time zone	When the egress time zone is valid, a user may press the egress button and the door will unlock. Note: This functionality requires the use of an Network Access Controller.
End-of-line resistor	See EOL resistor
EOL resistor	End-of-line resistor used to detect the electrical state of zone input circuits.
Event flag	A signal activated by an input condition, area condition, system status, or fault condition, door command (on doors 1 to 16 on LAN1 and doors 65 to 80 on LAN2), or shunt condition. Event flags are typically used to activate relays or as macro inputs.
Extended access time	A programming option in Network Access Controllers that provides a user with the “long access” user flag enabled to have longer than normal time for a door to unlock. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Extended shunt time	A programming option in Network Access Controllers that provides a user with the “long access” user flag enabled to have longer than normal time for a door to be shunted. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Floor group	A panel programming concept that assigns a group of floors to a user in order to allow selection of those floors when accessing a lift reader. Access to each floor in a group may be restricted via a time zone.
Fob	A type of smart card. See “card”.
Forced arming	Allows areas to arm regardless of any unsealed inputs that may subsequently cause an alarm.
Forced door debounce time	Forced door debounce time delays the generation of a forced door alarm for the specified interval. It caters for certain locks that may cause erroneous forced door reporting. Note: This functionality applies only to doors or readers connected to an Network Access Controller.

Guard	The term “guard” is used in the following ways: • If the “guard” user flag is enabled for a user, the guard cannot unlock a door without being accompanied by another valid user. Note: This functionality applies only to doors or readers connected to an Network Access Controller. • The term “guard” is also used in reference to “guard failed to check in” alarms, which can be generated by means of user category 7.
Hard time zone	See time zone
History	A list of past intrusion detection and access control events stored in memory which can be viewed on an LCD RAS, sent to a printer, or retrieved to a management software computer.
Hold-up alarm	A (silent) alarm that is triggered by a hold-up button. Normally it will not trigger any siren, only send a message to a remote monitoring company.
Holiday	A specified date (or range of dates) during which typical users are denied access during times that they would normally be permitted access.
Holiday type	Functionality to enable access to be granted to certain users during one holiday type, but not necessarily to another holiday type. Each holiday must have at least one type assigned.
In reader	A reader (RAS) that provides entry to a region through a door. The in reader is accompanied by an out reader that provides exit from the region through the door. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
In reader region	When a valid card or PIN is entered at the door’s in reader, the number of the region that the user is entering into is recorded against the PIN. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Input	Also called zone input. An electrical signal from a security device (input device) to the intrusion detectionsystem. Each input device is identified by a system name (for example “INPUT1”), and optionally by a custom name (for example “Reception Holdup Button”).
Input tamper	The Discovery system is typically configured to monitor the state of its zone input circuits (4-state monitoring). Input tamper alarms are generated when the circuit indicates an open-circuit or a short-circuit condition.
Input test	Input test is a defined interval during which a selected input can be tested (toggled from sealed to unsealed and then back to sealed) to verify that the panel correctly identifies the states.
Input type	The input type determines exactly how an input will function when its area is armed or disarmed. Most inputtypes require an area, but some input types that affect the status of areas need alarm groups.
Installer	A person who installs and services security equipment.
Network Access Controller	Four-door or Four-lift DGPs.

Intrusion detection	Electrical detection devices (called inputs) are connected to the Discovery panel or a DGP. Based on the type of device and whether the device's location (called area) is armed or disarmed, the device triggers an alarm when something activates it. For example, the device might be a reed switch that detects a door being opened when the area is armed. An alarm typically triggers a siren and flashing light to operate, and sends a message to a remote monitoring company.
Isolate	The device is inhibited from reporting alarms. It is excluded from functioning as part of the system.
IUM	Intelligent User Memory. IUM users can have 10-digit PINs and up to 48 bits of raw card data). All Discovery users are IUM users.
Key switch	A device using a key-operated switch to arm or disarm areas.
Keypad	A RAS with buttons to input data.
Keypad duress	When enabled, a duress code (user's alarm code + 1) can be entered on a keypad to activate a duress alarm. Keypad duress is enabled or disabled in Alarm Groups.
LAN	The term "LAN" is used in the following ways: • The system's two RS-485 data busses (COMM 1 and COMM 2). • The Discovery panel may be connected to a computer via LAN (local area network) or WAN (wide area network).
Local alarm	An alarm that is reported only within a building, and typically occurs when an area is disarmed (occupied). The circumstances that cause a local alarm can be checked and rectified by personnel on site and it is therefore unnecessary for the alarm to be relayed to a remote monitoring company. Certain input types can generate a local alarm during access (disarmed) times, and can report to remote monitoring company during secure (armed) times.
Logic equation	A logic expression that combines macro inputs in a specific manner. The result of a logic equation produces the macro action.
Long access	The "long access" user flag is enabled for users who need to have longer than normal time for an Network Access Controller's door to unlock. See "Extended access time". Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Low security time zone	When a RAS's low security time zone is valid, then either a card or a PIN can be used to open a door. When the time zone is not valid and "Card and Code" is set to YES, then both card and PIN are required to open a door. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Macro input	An event flag or an output that is used in a logic equation. Each macro input is an event flag or output.
Macro logic program	A set of rules that is created by macro inputs, logic equations, and macro outputs.

Macro output	A macro output holds the result of a logic equation. The macro output can have a timing element. Macro outputs trigger event flags or inputs.
Management software	A Discovery system may be programmed and operated via Security Commander management software on a graphical interface.
Operator	Customer staff member or installer who has login rights to system management software.
Out reader	A reader (RAS) that provides exit from a region through a door. The out reader is accompanied by an in reader that provides entry to the region through the door. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Out reader region	When a valid card or PIN is entered at the door out reader, the number of the region that the user is exiting from into is recorded against the PIN. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Override time zone	A door can be programmed with an override time zone that, when valid, automatically keeps the door unlocked. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Perimeter area	An area that contains entry/exit inputs on the perimeter of the premises.
PIN	Personal Identification Number—A number given to, or selected by, a user that identifies the user to the Discovery system.
PIR	Passive Infrared detector. A security device used to detect intruders in a certain part of an area or premises.
Poll	An inquiry message continually sent by the control panel to DGPs and RASs. Polling allows the remote unit to transfer data to the control panel.
Prefix digits	See “Alarm code prefix digits”
Privileged	If the “privileged” user flag is enabled for a user, then anti-passback functionality does not apply to the user (for regions 0 to 199). Note: This functionality applies only to doors or readers connected to an Network Access Controller.
RAS	Remote arming station. See “arming station”.
Reader	A device (RAS) used for access control that can read magnetic stripe or proximity cards to authenticate the user.
Region	A defined access control area having intelligent doors acting as boundaries. Regions are used by the anti-passback functions to keep track of users. The system can deny access to a card or PIN belonging to a user when the user is already assigned to the region. A region can also keep a count of users in order to activate a macro logic program when a certain value is reached. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Relay	Relay or output from the panel or a relay controller.

Relay controller	A PCB module that connects to the panel or a DGP to provide additional relay or open collector outputs.
Remote monitoring company	A company that monitors whether an alarm has occurred in an intrusion detection system. A remote monitoring company is located away from the building or area it monitors. Also known as “central station.”
Reporting	See “alarm reporting.”
Reset	An authorised user typically must enter a PIN at the keypad to reset (acknowledge) an alarm.
Retrieve	To transfer records from a control panel to a management software computer.
RTE	Request to exit, egress.
Sealed	The input is not activated, for example when a door is closed.
Secure	The state of an area when it's armed. The condition of an area when it should be vacant and the intrusion detection system has been set so that detected activity generates an alarm. Opposite of “access”.
Secure test	The secure (armed) test is a defined interval during which specific inputs may be tested to see if they are operating correctly when the area is unoccupied. The inputs must be programmed to be included in secure tests (determined by the input's test type).
SecureStream	Short for SecureStream IP Receiver, an Internet protocol (IP) alarm receiver designed for the Discovery panel alarm network.
Send	To transfer records from a management software computer to a control panel.
Shunt	A procedure that inhibits an input from generating an alarm when unsealed. For example, shunts stops a door generating an alarm when opened for a short time.
Smart card	See “card”.
Soft time zone	A time zone that is active when a relay is active
STU	Subscriber Terminal Unit
STU port	The Discovery PCB's serial (J15) port.
Tamper	Indication that a security device may have been interfered with. Some devices such as panels and DGPs have tamper switches to detect if they have been opened or removed from their mounting. See “input tamper”.
Tecom IP Receiver	An Internet protocol (IP) alarm receiver designed for the Discovery panel alarm network.
Time and attendance	An LCD RAS connected to an intelligent controller can be used as a time and attendance reader (it generated time and attendance transactions).

Time zone	A time zone is a means of making certain Discovery functionality conditional. 'Hard' time zones are valid between defined start and end times on selected days. Soft time zones are valid when a relay (output) is active.
Time zone	See time zone
Total disarm area	The system can be programmed so that one or more areas can have overriding control over the alarm functionality for designated inputs in another area. This functionality is used, for example, to prevent a 24-hour input type from going into alarm when it's not needed.
Trace user	The "trace user" user flag is enabled for users when you want to be able to trace the user's operation of an Network Access Controller's doors or lifts. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Unsealed	The input is activated, for example, when a door is opened.
User	Someone with a PIN and/or a card who can operate the Discovery system (for example, to unlock a door).
User category	User categories provide timing functionality for specific areas.
User flag	Options on a user record that controls how the system operates with respect to the user. User flags are dual custody, guard, visitor, trace user, card only, privileged, and long access. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
User record	A record containing (at least) a user's PIN or card number to identify the user to the Discovery system.
Vault	An area or area group that, when armed, will automatically arm other areas after a specified time.
Visitor	If the user flag "visitor status" is set to YES the user must be accompanied by a non-visitor user. Note: This functionality applies only to doors or readers connected to an Network Access Controller.
Zone input	See "input".

Index

2

- 24-hour alarm event flag, 74
- 24-hour alarm inputs, 232
- 2-state monitoring, 114

4

- 4-state monitoring, 114

A

- access alarm event flag, 73, 79
- access alarm inputs, 231
- access event reporting, 137
- access test time, 104
- access/secure alarm inputs, 233
- accessed event flag, 78
- account code, 132
- acknowledgement timeout, 146
- activate event flag only inputs, 236
- activate report only inputs, 237
- alarm code prefix, 111
- alarm control with key switches, 38
- alarm event reporting, 136
- alarm group
 - alarm system control, 98
 - alternate alarm group, 103
 - area search, 102
 - assigning to new users, 28, 98
 - auto isolate unsealed inputs, 101
 - can area be armed, 99
 - can area be disarmed, 99
 - can area be reset, 100
 - can area be timed, 100
 - defaults, 96, 239
 - disable auto-deisolate, 100
 - forced arming when inputs unsealed, 101
 - keypad duress, 99
 - name, 97
 - no arming if user category not timing, 102
 - number, 97
 - prevent forced disarming, 101
 - prompt with list of areas, 98
 - reset latching system alarms, 99
 - time zone, 103
 - user alarm group, 98
 - user categories, 101
 - user menu options, 102
- alarm group programming, 95
- alarm groups overview, 95
- alarm reporting, 69
- alternate alarm group, 103
- always connect, 134
- area
 - access alarm event flag, 79
 - accessed event flag, 78
 - area account, 77
 - cameraeventflag, 80
 - disarm time, 81
 - entry time, 77
 - entry timer eventflag, 80
 - exit time, 77
 - exit timer event flag, 79
 - isolate event flag, 79
 - local alarm event flag, 79
 - name, 77
 - number, 76
 - out-of-hours' time zone, 81
 - perimeter area, 81
 - pre-alarm timer eventflag, 81
 - programming, 76
 - secure alarm event flag, 79
 - siren event flag, 78
 - unsealed event flag, 78
 - warning timer event flag, 80
- area accessed event flag, 30, 78
- area account, 77, 135
- area alarm group, 86
- area control inputs, 235
- area disarm time, 81
- area groups, 189
- area linking, 55, 169
- area permissions, 99, 100, 189
- area search, 20, 55, 102
 - enable, 102
 - maximum time, 107
 - minimum time, 107
 - time zone, 113
- arm or disarm via time zone, 166, 167
- arming station
 - card reader, 36
 - card readers, 37
 - keypad, 34
 - programming, 34

- authentication, 148
- auto access test only, 110
- auto answer, 142
- auto isolate unsealed inputs, 101
- auto reset, 120
 - alarm group, 121
 - time, 121
- automatic arming and disarming, 43
- automatic deisolate when area accessed, 115
- automatic input testing, 72
- automation, 192
- automation zones, 7

B

- backup for path, 133
- backup programming, 190
- basic alarm system, 23
- battery testing, 178
- baud rate, 123
- blind dialling, 122
- bootloader, 158

C

- call back, 142
- camera control and monitoring, 39
- camera event flag, 39, 40, 74, 80
- camera monitoring inputs, 238
- camera testing, 118
- card learn RAS, 120
- card to code time, 106
- cards auto disarm, 89
- C-Bus, 7, 192
- CID codes, 69, 244
 - inputs, 245
 - system events, 245
- CID hex, 245
- CID via satellite, 146
- cleaners or trades, 162
- common areas, 46, 55
- common open/close, 138
- communications
 - Ethernet status, 150
 - path status, 149
- communications path
 - account code, 132
 - always connect, 134
 - area account, 135
 - authentication, 148
 - auto answer, 142
 - backup for path, 133
 - call back, 142
 - common open/close, 138
 - computer attempts, 145
 - computer password, 133
 - connect on buffer at 80%, 134
 - connect on event, 134
 - connect on service, 134
 - connect retries, 147

- connect timeout, 147
- control command, 135
- dial settings, 140
- DTMF dialling, 143
- dynamic computer IP address, 144
- enable, 131
- event time zone, 136
- filter event to area, 136
- format, 129
- heartbeat, 147
- heartbeat fail triggers path, 136
- IP address, 143
- IP mode, 144
- IP port, 144
- isolates trigger path, 135
- location, 131
- message ACK timeout, 146
- message retries, 146
- multi break alarm timer, 136
- multi break alarms, 137
- multi break restorals, 138
- name, 131
- number of calls, 142
- number of redials, 142
- number of rings, 142
- PABX, 141
- priority, 132
- remove unsent events, 137
- report access events, 137
- report alarm events, 136
- report computer connected, 139
- report open/close, 138
- reset queues, 148, 149
- setup, 128
- slot, 132
- status, 149
- stay connected on empty, 135
- system alarm report, 137
- telephone number, 141
- test calls, 139
- trigger comms fail event, 135
- wait time between connections, 147
- computer attempts, 145
- computer connected, 139
- computer password, 133
- connect on buffer at 80%, 134
- connect on event, 134
- connect on service, 134
- connect retries, 147
- connect timeout, 147
- connecting to a printer via IP, 33
- connecting to a printer via J15, 32
- connecting to a printer via RS-232, 32
- connecting to management software, 34
- console warning event flag, 73
- control command, 135
- custom RAS message, 181

D

- decrement testdays during TZ, 113
- defaults, 162
 - areas, 26
 - inputs, 26
 - RAS, 26
 - relay mapping, 27
 - system options, 27
 - timers, 27
 - users, 28
- delay holdup time, 104
- delayed holdup input types, 118
- delayed holdup lockout, 118
- DGP
 - battery test, 180
 - polling, 92
 - programming, 92
- dial settings, 140
- disable 0 ENTER for camera reset, 116
- disable auto insert of user category, 116
- disable auto-deisolate, 100
- disable code from displaying, 117
- disable flashing area LEDs, 117
- disarm time, 81
- display alarms instantly, 117
- display last card, 176
- display one input at a time, 115
- display user flags, 118
- door code, 111
- door event flag, 35, 36
- doors unlock time, 105
- DTMF dialling, 143
- dual custody, 289
- dual custody programming, 117
- duress, 53, 99, 184
- dynamic computer IP address, 144

E

- enable area search, 102
- enable auto test, 109
- enable/disable service technician, 52
- entering characters via RAS, 61
- entity names, 7
- entry time, 77
- entry timer event flag, 80
- EOL resistor, 112
- EOL resistors, 114
- Ethernet
 - enable, 124
 - gateway address, 126
 - IP address, 125
 - ping, 125
 - subnet mask, 125
- Ethernet status, 150
- event flag
 - 24-hour alarm, 74, 244
 - access alarm, 73, 79, 244
 - accessed, 78

- all secured, 185
- camera, 80
- camera event, 74
- console trigger, 185
- console warning, 73
- custom, 242
- DGP isolated, 183
- DGP offline, 184
- door, 105
- duress, 184
- entry timer, 80
- example, 243
- exit timer, 79
- film out, 184
- fuse fail, 183
- input, 72, 75
- isolate, 79
- local alarm, 79
- low battery, 182
- mains fail, 182
- make all events 24-hour, 73
- number, 165
- overview, 242
- panel tamper, 183
- pre-alarm, 72
- pre-alarm timer, 81
- predefined, 242, 243
- print input when unsealed, 74
- RAS offline, 184
- report fail, 185
- second, 75
- secure alarm, 73, 79, 243
- shunt, 171
- shunt warning, 171
- siren, 73, 78, 227, 243
- siren fail, 183
- summary, 242
- test mode, 185
- tester, 72, 244
- unsealed, 78
- user-defined, 242
- warning timer, 80

- event flag 13, 72
- event flags, 30
- event text, 111
- event time zone, 136
- exit fault reporting, 119
- exit time, 77
- exit timer event flag, 79
- expanded test reporting, 119
- expanded test success reporting, 119

F

- factory defaults, 26
- film count input types, 238
- film counters, 118
- film low level, 109
- film out level, 109

- filter event to area, 136
- financial institutions, 56, 118
- forced arming when inputs unsealed, 101
- four-state monitoring, 114

H

- heartbeat fail triggerspath, 136
- heartbeat timeout, 147
- holiday types, 6, 161
- holidays, 6
- how to
 - add users, 28
 - basic setup, 23
 - configure alarm reporting, 69
 - connect a printer, 32
 - connect to software, 34
 - control cameras, 39
 - print via IP, 33
 - program a card reader, 36
 - program a RAS, 34
 - program automatic arm/disarm, 43
 - program common areas, 55
 - program delayed alarms, 42
 - program input testing, 71
 - program IP connections, 57
 - program keypad duress, 53
 - program macros, 47
 - program RAS beepers, 53
 - program relays, 29
 - program service tech access, 52
 - upgrade to Discovery, 58 use
 - area search, 55
 - use key switches, 38
 - use timed input testing, 60

I

- individual input test time, 105
- input
 - 24-hour alarm event flag, 74
 - access alarm event flag, 73
 - alarm group, 71
 - camera event flag, 74
 - console warning event flag, 73
 - event flags, 72
 - make all events 24-hour event flag, 73
 - name, 69
 - number, 69
 - print input when unsealed, 74
 - reporting, 69
 - secure alarm eventflag, 73
 - siren event flag, 73
 - test input within, 74
 - test options, 71
 - types, 69, 229
- input eventflag, 72, 75
- input event flags, 43
- input programming, 69
- input shunt, 170

- input tamper monitoring, 114
- input test type
 - no testing required, 71
 - set event flag 13 during access test, 72
 - set pre-alarm during access test, 72
 - test during access test, 72
 - test during secure test, 72
 - tested in secure test & access, 72
- input testing, 60
- input type
 - 00, no input programmed, 231
 - 01, access alarm, 231
 - 02, secure alarm, 231
 - 03, entry exit alarm, 231
 - 04, entry exit handover alarm, 231
 - 05, 24-hour alarm, 232
 - 06, area control input, 235
 - 07, camera suspicion input, 236
 - 08, delayed access/secure alarm, 233
 - 09, reset delayed input, 237
 - 10, spare, 230
 - 11, delayed access alarm, 231
 - 12, courier restart, 237
 - 13, entry exit no seal check, 231
 - 14, entry exit handover alarm no seal check, 231
 - 15, access local/secure alarm, 233
 - 16, 24-hour local mains fail, 237
 - 17, do not use, 230
 - 18, 24-hour local comms fail, 237
 - 19, comms fail LED, 237
 - 20, input to activate event flag 24-hour, 236
 - 21, access local (code to reset)/secure alarm, 233
 - 22, access delayed non-latching/secure alarm, 233
 - 23, camera 1 count, 238
 - 24, camera 2 count, 238
 - 25, camera 3 count, 238
 - 26, camera 4 count, 238
 - 28, non-latching secure alarm, 232
 - 29, 24-hour non-latching alarm, 232
 - 30, access local non-latching/secure alarm, 233
 - 31, area control on-off, 236
 - 32, input to activate event flag in secure, 236
 - 33, 24-hour alarm & isolate inputs, 232
 - 34, area disarm/user category arm, 236
 - 35, area user category arm only, 236
 - 36, camera 5 count, 238
 - 37, camera 6 count, 238
 - 38, camera 7 count, 238
 - 39, camera 8 count, 238
 - 40, access suspicion or delayed holdup/secure alarm, 234
 - 41, access local/entry exit alarm, 234
 - 42, access local (code to reset)/entry exit alarm, 234

- 43, input to activate event flag in access, 236
- 44, access local/secure alarm disabled by TZ 41, 234
- 45, access event flag/secure alarm disabled by cleaners or trades, 235
- 46, access alarm/secure alarm, 235
- 47, suspicion holdup/secure alarm, 235
- 48, camera 1 film out, 238
- 49, camera 2 film out, 238
- 50, camera 3 film out, 238
- 51, camera 4 film out, 238
- 52, camera 5 film out, 239
- 53, camera 6 film out, 239
- 54, camera 7 film out, 239
- 55, camera 8 film out, 239
- 56, access local(code to reset)/secure alarm disabled by TZ 41, 235
- 58, input to screen text, 238
- 59, 24-hour alarm disabled by TZ 41, 232
- Network Access Controllers, 175, 177, 227, 228, 243
- IP address, 143
- IP port, 144
- isolate event flag, 79
- isolates trigger path, 135
- IUM, 4

K

- key presses for characters, 61
- key switch, 38
- keypad duress, 53, 184

L

- lamp test, 159
- latching system alarms, 116
- LCD custom text, 181
- LCD text rotation speed, 112
- listen IP port, 59
- LIUM, 158
- local alarm event flag, 79
- local alarm reminder time, 105

M

- macro
 - event flag or input, 188
 - inputs, 188
 - logic, 47, 186
 - logic equation, 189
 - number, 187
 - output function, 187
 - programming, 47
 - timed, 188
- mains fail time, 106
- maintenance, 217
- maintenance date, 181
- maintenance message, 181

- make all events 24-hour, 73
- management software, 10
- manual access test/auto secure test, 110
- map relays, 164
 - active or inactive during time zone, 165
 - invert relay, 166
- maximum area search time, 107
- menu
 - install, 15
 - user, 14
- menu alarm group, 86
- message ACK timeout, 146
- message retries, 146
- migrating from Discovery V8, 58
- minimum area search time, 107
- MIUM, 158
- monitor ring, 122
- morning check, 56
- multi break alarm timer, 136
- multi break alarms, 137
- multi break restorals, 138

N

- New Zealand dialling, 123
- New Zealand requirements, v
- next service, 181
 - date, 181
 - message, 181
- no arming if user category not timing, 102
- number of calls, 142
- number of redials, 142
- number of rings, 142
- numbering
 - conventions, 224
 - doors and lifts, 227
 - inputs, 224
 - Network Access Controllers, 228 relays, 226
 - siren outputs, 227
 - time zones, 228

O

- open/close, 138
- out-of-hours' time zone, 81

P

- PABX, 141
- parity, 123
- password, 133
- path authentication, 148
- path enable, 131
- path format, 129
- path location, 131
- path name, 131
- path priority, 132
- path slot, 132
- path status, 149

- perimeter area, 81
- PIN display, 117
- PIN length, 111, 118
- poll errors, 175
 - device type, 175
- poll RAS, 83
- power consumption, 178
- pre-alarm timer event flag, 42, 81
- prevent forced disarming, 101
- print input when unsealed, 74
- printing, 32
- programming
 - alarm groups, 95
 - areas, 76
 - arming stations, 34
 - automatic arming and disarming, 43
 - delayed holdup inputs, 42
 - DGPs, 92
 - inputs, 69
 - IP connections, 57
 - macros, 47
 - RASs, 82
 - relays, 29
 - remote controllers, 177
 - service technician access, 52
 - users, 28
- programming map, 245
- PSTN line fault monitor, 123

R

RAS

- area alarm group, 86
- buzzer, 185
- cards always disarm/arm, 89
- cards arm after three badges, 90
- cards auto disarm, 89
- console trigger event flag, 185
- disarm/arm using one key, 89
- display shunting on LCD, 89
- door event flag, 87
- door event flag on alarm codes, 88
- ENTER key opens door only, 88
- LCD, 88
- LEDs, 159
- menu alarm group, 86
- options, 88
- polling, 83
- programming, 82
- reset from RAS without code, 90
- restricted user category to disarm, 90
- toggle keyboard control, 88
- relay controllers, 110
- relay programming, 29
- remote controllers, 177
- remove unsent events, 137
- report
 - access events, 137
 - alarm events, 136

- battery test, 180
- report open/close, 138
- reset input test days, 192
- reset path queues, 148, 149
- restore programming, 190

S

SD Card

- backup, 190
- restore, 190
- second eventflag, 75
- secure alarm event flag, 73, 79
- secure alarm inputs, 231
- secure test time, 104
- selected event flag, 72
- send access control data, 175
- send IP port, 59
- service time, 105
- shunt
 - cancel door event flag, 173
 - door open command, 172
 - entry/exit, 173
 - event flag, 171
 - in access, 172
 - in secure, 172
 - input, 170
 - input holds eventflag, 173
 - number, 170
 - report door open/close, 173
 - time, 171
 - warning event flag, 171
 - warning time, 171
- siren event flag, 73, 78
- siren testing, 116
- siren time, 106
- sirens only after report fail, 117
- skip access check, 118
- soft time zone
 - number, 174
 - relay, 174
- softtime zones, 174
- source ports, 59
- special purpose inputs, 237
- stay connected on empty buffer, 135
- stop bits, 124
- STU reporting, 245
- sub-time zones, 160
- summary event flags, 182
- suspicion time, 105
- system alarm report, 137
- system alarms set siren and strobe, 116
- system event flags, 182
- system options, 107
- system test mode, 109
 - auto access test only, 110
 - enable auto test, 109
 - manual access test/auto secure test, 110
 - no test, 109

T

- TCP/IP mode, 144
- technical support, 222
- telephone number, 141
- test calls, 139
- test input within, 74
- test mode, 109
- tester eventflag, 72
- tester eventflag time, 106
- testing batteries, 178
- text entry, 61
- text words, 7, 157, 170, 177, 178
- time before LCD text rotation, 111
- time zone, 103, 113
- time zone number, 160
- time zones, 160
 - holiday types, 161
- time zones to control relay, 165
- time zones to follow relay, 174
- timed input testing, 60, 113, 192
- timers, 103
 - access test time, 104
 - card to code time, 106
 - delay holdup time, 104
 - doors unlock time, 105
 - individual input test time, 105
 - local alarm reminder time, 105
 - mains fail time, 106
 - maximum area search time, 107
 - minimum area search time, 107
 - secure test time, 104
 - service time, 105
 - siren time, 106
 - suspicion time, 105
 - tester eventflag time, 106
 - user category time, 103
 - warning time, 104
- TIUM, 158
- total disarm area, 71, 107
- trigger comms fail event, 135
- triggering RAS beepers, 53
- troubleshooting, 214
- two-state monitoring, 114

U

- UDP/IP mode, 144
- unsealed eventflag, 78
- USB device, 124
- USB host, 124
 - user category, 44, 80, 81, 90, 100, 101, 102, 104, 116, 162, 167, 168, 234, 235, 236
 - name, 164
 - number, 163
 - programming, 163

- user category time, 103
- user flags, 118
- user menu options, 14, 102
- user name file, 115
- users, 28
 - alarm group, 28
 - name, 28
 - PIN, 29
 - user number, 28
- using area search, 55

V

- V8 multibreak, 119
- vault area, 110
- vault areas, 168
- version information, 157

W

- wait time between connections, 147
- warning time, 104
- warning timer event flag, 80
- worksheet
 - alarm groups, 256
 - area groups, 252
 - area linking, 270
 - areas, 251
 - arm/disarm via time zone, 269
 - auto reset, 260
 - battery testing, 272
 - communications devices, 261
 - communications paths, 264
 - custom message, 273
 - DGPs, 255
 - door groups, 278
 - floor groups, 280
 - holiday types, 282
 - holidays, 281
 - input shunts, 271
 - inputs, 250
 - macro logic, 276
 - nextservice date, 273
 - RASs, 253
 - relay mapping, 268
 - soft time zone, 272
 - summary event flags, 273
 - time zone to follow relay, 272
 - time zones, 266
 - timers, 257
 - user categories, 267
 - user-defined event flags, 275
 - users, 277
 - vaults, 270