

GE
Security

Challenger V8 & V9

Administrator's Manual



Copyright Copyright © 2008, GE Security Pty. Ltd.. All rights reserved.

This document may not be copied or otherwise reproduced, in whole or in part, except as specifically permitted under US and international copyright law, without the prior written consent from GE.

Document number/revision: **1063806 A** (September 2008).

Disclaimer THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. GE ASSUMES NO RESPONSIBILITY FOR INACCURACIES OR OMISSIONS AND SPECIFICALLY DISCLAIMS ANY LIABILITIES, LOSSES, OR RISKS, PERSONAL OR OTHERWISE, INCURRED AS A CONSEQUENCE, DIRECTLY OR INDIRECTLY, OF THE USE OR APPLICATION OF ANY OF THE CONTENTS OF THIS DOCUMENT. FOR THE LATEST DOCUMENTATION, CONTACT YOUR LOCAL SUPPLIER OR VISIT US ONLINE AT WWW.GESECURITY.COM.AU.

We appreciate your input about our product documentation. Please send feedback, or notify us of errors or omissions, by email to GE Security at documentation@gesecurity.com.au.

This publication may contain examples of screen captures and reports used in daily operations. Examples may include fictitious names of individuals and companies. Any similarity to names and addresses of actual businesses or persons is entirely coincidental.

Trademarks and patents GE and the GE monogram are registered trademarks of General Electric. Challenger product and logo are registered trademarks of GE Security Pty. Ltd.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Intended use Use this product only for the purpose it was designed for; refer to the data sheet and user documentation. For the latest product information, contact your local supplier or visit us online at www.gesecurity.com.au.

Contents

	Preface	v
Chapter 1.	Introduction	1
	Welcome to the Challenger system	2
	Testing your system	4
	Challenger user interfaces	5
	Using the keypad	9
	Using cards	11
	What is a user?	11
Chapter 2.	Common tasks	15
	Arming your system	16
	Disarming your system	17
	Dealing with unsealed inputs	19
	Opening doors	20
	Handling alarms	21
	Viewing the quick alarm history	23
	Testing input devices	24
Chapter 3.	User menu reference	27
	1. Panel Status	28
	2. Input Unsealed	28
	3. Input In Alarm	29
	4. Input Isolated	29
	5. History	30
	6. Test Report	30
	7. Service Menu	32
	8. Film Counters	34
	9. Input Text	34
	10. Isolate	35
	11. Deisolate	35
	12. Test Input	36
	13. Start Auto Access Test	37
	14. Program Users	38
	15. Time and Date	46
	16. Isolate/Deisolate RAS/DGP	49
	17. Enable/Disable Service Tech.	50
	18. Reset Cameras	50
	19. Install Menu	50
	20. Door and Floor Groups	51
	21. Holidays	53
	22. Open Door	54
	23. Unlock, Lock, Disable and Enable	54
	24. Print History	55

Appendix A. Programming worksheets

57

User worksheet

58

Door groups worksheet

59

Floor groups worksheet

60

Holidays worksheet

61

Glossary

63

Index

71

Preface

This is the GE Security *Administrator's Manual* for Challenger™ intrusion detection and access control panels. This manual is intended primarily for Challenger system administrators and installers. However, it does contain some detailed information that may be needed by Challenger system operators and users.

Depending on what you need to do, you may need to refer to the other *Challenger V8 & V9* manuals:

- Refer to the *Challenger V8 & V9 User Manual* if you only need to know how to perform everyday operations using an access card or a personal identification number (PIN) on a Challenger system keypad.
- Refer to the *Challenger V8 & V9 Programming Manual* if you are an installer or administrator and you need to know details of Challenger system programming.

This manual describes the tasks that a Challenger system administrator should know how to perform on a Challenger system, using a locally-connected remote arming station (RAS).

Note: A qualified service person, complying with all applicable codes, should perform all required hardware installation.

Conventions used in this document

The following conventions are used in this document:

Bold	Menu items and buttons.
<i>Italic</i>	Emphasis of an instruction or point; special terms.
	File names, path names, windows, panes, tabs, fields, variables, and other GUI elements.
	Titles of books and various documents.
<i>Blue italic</i>	(Electronic version). Hyperlinks to cross-references, related topics, and URL addresses.
Monospace	Text that displays on the computer screen or LCD screen.
	Programming or coding sequences.

Safety terms and symbols

These terms may appear in this manual:



CAUTION: Cautions identify conditions or practices that may result in damage to the equipment or other property.



WARNING: Warnings identify conditions or practices that could result in equipment damage or serious personal injury.

Chapter 1 Introduction

This chapter provides an introduction to the Challenger system.

In this chapter:

<i>Welcome to the Challenger system</i>	2
<i>Testing your system</i>	4
<i>Challenger user interfaces</i>	5
<i>Using the keypad</i>	9
<i>Using cards</i>	11
<i>What is a user?</i>	11

Welcome to the Challenger system

The *Challenger* integrated intrusion detection and access control panel, first released in 1989, is widely accepted as a versatile, high-quality, Australian-made product. Challenger's customisable design makes it the benchmark for intrusion detection (alarm) and access control systems.

The Challenger panel is the heart and soul of the Challenger intrusion detection and access control system. The Challenger 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 following tools:

LCD RAS. Initially the Challenger system must be programmed using a remote arming station (RAS) fitted with a liquid crystal display (LCD) screen and keypad. The RAS's text-based user interface provides a menu that is numbered for rapid access. This manual describes how to program and operate a Challenger system by means of a RAS.

Management software. A Challenger system that is configured and programmed to be accessed via management software (such as TITAN, Ares, or Forcefield) may be programmed and operated via the management software on a graphical interface. Any changes to the Challenger system made via management software must be downloaded to the Challenger panel before they take effect.

If you use management software to administer your Challenger system, use this manual as a reference and refer to the documentation provided with the management software.



CAUTION: If management software is used to program a Challenger panel, to change user data or access control data, or used to upload a panel's programming, the management software becomes the *primary* location for the panel's data, and the panel becomes the secondary location. In other words, keep track of where the 'correct' version of Challenger data is stored. As administrator you are responsible to avoid loss of data, errors in data, or uncertainty about the validity of data.

Challenger systems are modular and they are highly-configurable.

- Being modular means that one Challenger system can be used for basic intrusion detection functionality, and another Challenger system can be used for integrated intrusion detection and access control functionality. A Challenger system can start off simple and be expanded over time with the addition of modules such as Data Gathering Panels (DGPs), Wireless Data Gathering Panels (WDGPs) and Intelligent Access Controllers.
- Being highly-configurable means that the operation of the Challenger system can be tailored by the installer to suit the needs of various customers. For example, a bank may require user PIN codes (alarm codes) to be at least five digits instead of the usual four digits.

A Challenger system might be managed locally from an LCD RAS or via a locally-connected management software computer (Windows computer). Alternatively, the system might be managed remotely via management software computers connected via IP or PSTN (depending on the modules fitted).

In an Enterprise-wide intrusion detection and access control system, thousands of suitably-equipped Challenger systems can be programmed, controlled, and monitored by hundreds of operators working on management software computers in remote locations. Refer to the documentation provided with the management software for details.

Your Challenger system has been programmed to meet your specific requirements. Therefore, not all of the features described in this manual may apply to your system. Also, some of the features described in this manual will not be visible to all users (see *What is a user?* on page 11). Your system may have extra features or equipment installed. The programming instructions for extra equipment are supplied separately.

What's new in this release

This manual describes functionality that is applicable to older Challenger V8 and V9 systems, plus Challenger V8 panel firmware version 8.128 and later. New functionality is identified in the manual, where applicable, and includes the items described in the following sections.

Software IUM

In an Intelligent User Memory (IUM) Challenger system, all users can have PIN codes up to 10 digits long and up to 48 bits of raw card data. Prior to firmware version 8.128, IUM required the use of TS0883 4 MB or TS0884 8 MB memory expansion modules (hardware IUM).

Software IUM is a programmable configuration for Challenger V8 panels that are not fitted with TS0883 4 MB or TS0884 8 MB memory expansion modules, and applies only to Challenger V8 panels using firmware version 8.128 and above.

Learning card data

A card reader RAS can be used to enter a user's card data (card bits) into an IUM Challenger system by presenting (badging) the card at the reader prior to, or during, the user creation process (see [Learning card data](#) on page 43).

Extended capacities

Challenger V8 panels using firmware version 8.128 or later, and fitted with TS0882, TS0883, or TS0884 memory modules have the following increased capacities:

- 255 alarm groups (of which 10 are not editable)
- 255 door groups
- 128 floor groups
- 46 hard time zone numbers in the range 1 to 24 and 42 to 63

Refer to the *Challenger V8 & V9 Programming Manual* for details.

The Challenger family

This manual focuses mainly on the widely-used Challenger V8 system, but also includes the Challenger V8's siblings:

- TS0816P Challenger V9—a variation of Challenger designed to link a number of Challenger V9 panels into a *panel link system*.
- TS0810 Access Manager—a low-cost access control panel that does not have onboard alarm inputs or local reporting functionality.

Refer to the *GE Security Product Catalogue* or our web site at <http://www.gesecurity.com.au> for details of these and other products in the Challenger family.

Testing your system

It is important that you regularly test your Challenger system to ensure that all installed equipment is operating properly.

You may have a technician operate your Challenger system locally or remotely to test and service your intrusion detection system. There are various tests that can be used to ensure your system is working correctly. GE Security recommends you discuss with the technician the testing processes you can perform to check your system, and its ability to report to your remote monitoring company (if applicable).

Routine maintenance on intruder alarm systems installed in a client's premises should be performed in accordance with AS2201.1-1998 SECTION 5. MAINTENANCE, RECORDS AND REPORTS. Note that this standard requires that routine maintenance be performed at least once per year. Refer to *Challenger V8 & V9 Programming Manual* for maintenance recommendations.

See also [Testing input devices](#) on page 24.

Challenger user interfaces

A Challenger system typically has at least one LCD RAS connected to its LAN (RS-485 data bus). The LCD screen plus keypad provides an English-language text-based user interface for programming and operating the Challenger system. Up to 16 RASs may be connected to the Challenger LAN.

Figure 1. LCD keypad remote arming stations



Figure 1 indicates some of the LCD RAS models that may be used in a Challenger system. The latest series CA111x models are used in this manual for illustrations and keypad depictions. The CA1116 model shown here (with cover removed) includes a four-line LCD screen and an integral card reader. Figure 2 on page 5 indicates the locations of various controls on the CA1116 RAS.

Figure 2. Details of CA1116 RAS

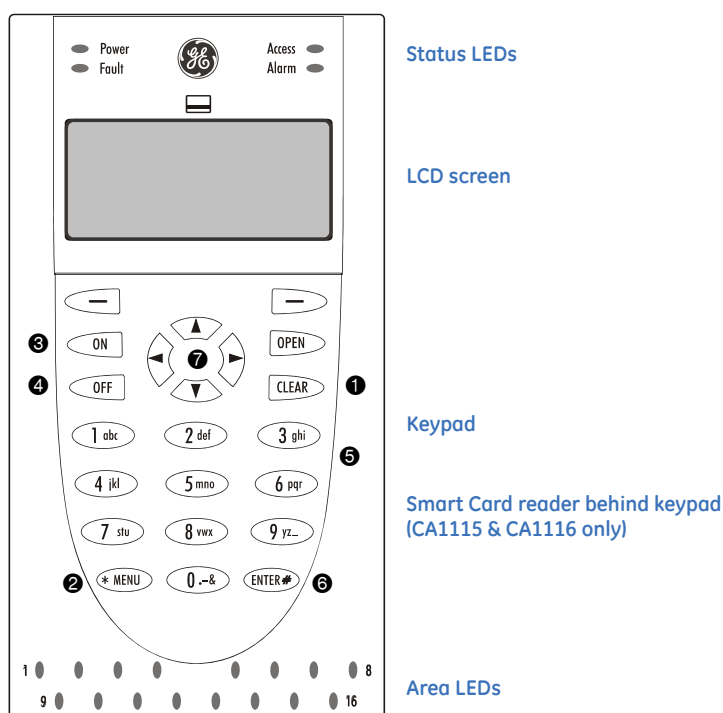


Table 1. Key to Figure 2

Number	Details
❶	Press the Clear key to exit the current function or operation and return to alarm control prompt. (Available on some arming stations only)
❷	Press the Menu* key to: <ul style="list-style-type: none"> • Display the menu login prompt. • Backspace to correct an error. • Scroll backwards in the menu. (Some arming stations may only have a * without the word "menu").
❸	Press the On key after entering your PIN code to tell the Challenger system that you want to arm your areas. (Some arming stations may have a # instead of the ON key).
❹	Press the Off key after entering your PIN to tell the Challenger system that you want to disarm your areas. (Some arming stations may have a * instead of the OFF key).
❺	Press a numeric key to enter numbers, and for entering text when programming user names.
❻	Press the ENTER key: <ul style="list-style-type: none"> • When information is to be processed (similar to the Enter key on a computer). • To scroll forwards in the menu. (Some arming stations may have a # instead of the ENTER key).
❼	Press the up and down keys to scroll through menu options. (Some arming stations may have a NEXT key to display additional text).

The LCD screen

Messages are displayed on the liquid crystal display (LCD) screen on the keypad. These messages guide you through the functions of the Challenger system, such as identifying problems, the procedures necessary to rectify problems, programming functions, and other menu options. The display might also show information you have entered on the keypad.

The first line of the display shows Challenger system information, and scrolls if there are more characters than can be displayed, depending on the arming station type. The second line of the display shows instructions, and the characters you enter on the keypad.


Welcome screen

Your Challenger system may be programmed to display the default message "There Are No Alarms In This Area" (*Figure 3*) when there are no alarms, or it may be programmed to display the time and date (*Figure 4*) or your company name (*Figure 5*). When in alarm, the first line is blank, or it displays "Local Alarm" if there are one or more local alarms active (see [Local alarms](#) on page 22).

Figure 3. Default LCD welcome screen (used in this manual)


There Are No Alarms In This Area
Code:

Figure 4. LCD welcome screen example showing time and date


 A rectangular LCD screen with a black border. The text is white and centered. It displays the time and date on the first line, and a prompt on the second line.

11:19 05/03/2008
Code:

Figure 5. LCD welcome screen example showing custom message


 A rectangular LCD screen with a black border. The text is white and centered. It displays a custom message on the first line, and a prompt on the second line.

GE Security
Code:

Figure 6. LCD welcome screen in alarm state


 A rectangular LCD screen with a black border. The text is white and centered. It displays a single prompt on the first line.

Code:

In some instances there is insufficient space to display all the text being presented (for example, a list of areas in your building). LCD RASs that have small displays (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 text rotation begins after a configurable delay, and scrolls at a configurable speed (this functionality is not applicable to TS0004 or TS0210 LCD RASs).

Displaying input names

Alarm input devices are key components of an intrusion detection system. A Challenger system can have up to 256 inputs per panel (a linked Challenger V9 system can contain up to 16 panels). Inputs are identified by a number and (optionally) a name programmed by the installer.

Note: Using Panel Link (Challenger V9) changes the standard numbering system used in this manual, to reflect that of panel link's system. Refer to *Challenger V9 numbering* in *Challenger V8 & V9 Programming Manual* for details.


Your Challenger system may be programmed to display one input at a time with its name (default setting) or it might be programmed to display a list of input numbers. The following example (from [Dealing with unsealed inputs](#) on page 19) illustrates the difference:

- If *Display one input at a time* is set to YES, each unsealed input's name is displayed.


 A rectangular LCD screen with a black border. The text is white and centered. It displays the name of an unsealed input on the first line, and a prompt on the second line.

Unsealed On 6, Front Door
NEXT or ENTER

- If *Display one input at a time* is set to NO, a list of input numbers is displayed.


 A rectangular LCD screen with a black border. The text is white and centered. It displays a list of input numbers on the first line, and a prompt on the second line.

Unsealed On 6, 7, 9.
NEXT or ENTER

The LCD screen examples used in this manual are based on the default setting where *Display one input at a time* is set to YES. If your Challenger system is programmed to display a list of input numbers, enter an input number and press **[ENTER]** to display the input's name.

Area LEDs

RASs have 1 to 16 area light-emitting diodes (LEDs). The Challenger system can have 16 areas, so a RAS with 16 area LEDs can indicate the status of each area independently.

When the CA111x RAS cover is open or removed, 16 red LEDs are visible at the bottom of the RAS. Each LED represents an area, and the indications are as follows:

- The LED illuminates when its corresponding area is armed (secure).
- The LED flashes slowly when a fault is detected, or when an alarm occurs, in disarm (access).
- The LED flashes quickly when a fault is detected, or when an alarm occurs, in arm (secure).

CA111x status LEDs

CA111x RASs have four status LEDs above the LCD screen. The indications are as follows:

- **Green** — the Power LED is on when the RAS is powered.
- **Yellow** — the Fault LED flashes when there is a system fault (i.e. comms fault, RAS fault, DGP fault, battery test fail, or hardware tamper).
- **Blue** — the Access LED is always off, except for a single flash when a card is badged at CA1115 or CA1116 RASs (subject to Valid Card Flash programming).
- **Red** — the Alarm LED flashes when there is an access alarm, a 24-hour alarm, or a secure alarm.

TS0804 system fault LEDs

TS0804 RASs have system fault LEDs that indicate as follows:

- **Comms** — illuminates if there is a failure in the communications between the Challenger panel and a remote monitoring station.
- **RAS** — illuminates if a remote arming station is offline.
- **DGP** — illuminates if an access controller or data gathering panel is offline.
- **Battery** — illuminates if the auxiliary battery power is found to be low after mains power is lost.

TS0804 system alarm LEDs

TS0804 RASs have system alarm LEDs that indicate as follows:

- **Access** — illuminates if an alarm has occurred in an area that is occupied and the intrusion detection system has been set to allow normal access.
- **24 Hr** — illuminates if an alarm has occurred in an area where an input device has been programmed for 24 hour monitoring.
- **Secure** — illuminates if an alarm has occurred in an area that is secure (armed).
- **Tamper** — illuminates if an alarm has occurred due to tamper.

Internal beeper

The RAS's beeper provides a number of indications:

- A short beep indicates that a valid card is presented at a reader or a key is pressed on a keypad.
- Two short beeps indicate access granted from a card read (may follow one short beep to indicate valid card read).
- Seven short beeps indicates that a PIN or card is not valid at the particular RAS or at the particular time, or that the area you are attempting to arm has an input that is unsealed or in alarm.

- A continuous tone indicates that an input test is being performed.
- Continuous beeping indicates that one or more inputs are in local alarm.
- Your Challenger system may be programmed so that the RAS beeps whilst an entry timer, exit timer, or warning timer is running.

Using the keypad

Use the following steps to access the Challenger user menu when the “Code” prompt is displayed on the bottom line of the LCD screen.

**There Are No Alarms In This Area
Code:**

Your Challenger system might display a custom message instead of the one shown above if it has been programmed to do so. For example it might display your company name or the time and date. See [Welcome screen](#) on page 6.

1. Press **[MENU*]**.

**To Access Menu Enter Code
Code:**

2. Enter **nnnn** (where nnnn is your PIN code), and press **[ENTER]**.

**“0”-Exit “ENTER” -Down “*” -Up
0-Exit, Menu:**

3. You can now select the User menu option you need (see *Table 2* on page 10).

The following keys are used to move between user menu options:

- 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.

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 value, such as a number or amount, enter the value and press **[ENTER]**. The information will be saved and the display will show the next option.

To program a YES/NO option, press **[ENTER]** to accept the display or press **[MENU*]** to toggle between YES and NO. Enter **0** to skip options.

Note: If a value is already programmed and needs to be changed, enter the new value and press **[ENTER]** to change the value.

There are 24 top-level user menus in the Challenger system (see *Table 2* on page 10). Some installations do not need every menu option. Also, access to menus is determined by the alarm groups assigned to the user and to the RAS, so some menus may not be visible to all users or at all RASs.

Table 2. Challenger 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 all unsealed inputs, for example, door open.
3. Input In Alarm	Lists inputs in alarm.
4. Input Isolated	Lists inputs that are isolated.
5. History	Lists events of Challenger system history, including alarms, menu access, etc.
6. Test Report	Displays the current testing status of inputs configured for access or secure testing.
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	Displays input names.
10. Isolate	Isolate inputs.
11. Deisolate	Deisolate inputs.
12. Test Input	Select an individual input and begin the test interval.
13. Start Auto Access Test	Start the auto access test interval for particular inputs.
14. Program Users	Create, modify, or delete user records.
15. Time and Date	Program the panel's time and date and DST settings.
16. Isolate/Deisolate RAS/DGP	Isolate or deisolate RASs or DGPs.
17. Enable/Disable Service Tech	Enable and disable the service technician's PIN code.
18. Reset Cameras	Reset the film frame count on security cameras.
19. Install Menu	Refer to the <i>Challenger V8 & V9 Programming Manual</i> for details.
20. Door and Floor Groups	Program door and floor groups.
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 numbered in the range 17 to 64 (doors controlled by Intelligent Access Controllers).
24. Print History	Print all the Challenger system history contained in memory.

Refer to *Chapter 3, User menu reference* on page 27 for details about these options.

Using cards

A Challenger system may use card reader RAS devices, which may or may not have an LCD screen and keypad. Depending on system programming, a card reader RAS can be used for both alarm control (arming and disarming) and access control (unlocking doors) in the same manner as entering a PIN code on a keypad.

In the Challenger system, the term *cards* includes things like:

- magnetic swipe cards.
- proximity smart cards (including photo ID cards and key fobs).
- Wiegand-format cards.
- Biometric factors (such as fingerprints) read via appropriate biometric readers.

Cards contain data readable by the card reader or Wiegand device, that identifies the user to the Challenger system.

What is a user?

Overview

A user is someone with a PIN code and/or a card who can operate the Challenger system. It helps to think of users as three main types:

Users. Users can typically can arm or disarm the intrusion detection system (called *alarm control*), handle alarms, or open doors (called *access control*). User tasks are described in the *Challenger User Manual*.

Administrators. In addition to a user's role, administrator can also add users and perform other administrative tasks, as described in this manual.

Installers. Installers (or alarm technicians) typically install, program, and maintain the Challenger system. Installer tasks are described in the *Challenger V8 & V9 Programming Manual*. Some tasks (such as testing inputs) may be performed by installers instead of administrators. These tasks are described in this manual.

PIN codes

PIN codes are also known as *alarm codes*. A PIN code is series of four to ten digits. If the Challenger system is also used for access control, the system may be programmed to use a shortened version of the PIN code to open doors or to access lifts (but still must be at least four digits). This shortened version is call a *door code*, and is used to hide the full PIN code from prying eyes. When you enter your code on a keypad, the key presses are displayed as * characters.

Note: Your installer will tell you whether your Challenger system uses door codes in addition to alarm codes.

Challenger systems that use cards for access may or may not also require the user to enter a PIN code, depending on how the system is programmed. In any case, this manual will refer to entering a PIN code as being equivalent to using a card, or using card plus PIN (except where noted).

If the entered PIN code is not valid, or if the time zone is not valid (for example, after hours), or if it is not valid at the particular arming station or reader, the arming station or reader will emit seven quick beeps.

All users have a user record in the Challenger database, and have a PIN code or a card by which they can operate the Challenger system to whatever degree their permissions allow. Permissions to operate the Challenger system are based the user's *alarm group* ([Alarm groups](#) on page 12). Challenger systems that are used for access control also use *door groups* ([Door groups](#) on page 12) and *floor groups* ([Floor groups](#) on page 12).

The Challenger system can be programmed so that a PIN code and/or a card can be used to perform any function or combination of functions during any time period. For example:

- An alarm group for managers may allow access to all Challenger user operations at all times.
- An alarm group for a cleaner may only allow their card to disarm an area for one hour between 5 p.m. and 11 p.m.
- A door group for a night shift worker may allow their PIN to be used to open a door between 11 p.m. and 7 a.m. only.

Alarm groups

The alarm group that is assigned to a user determines whether the user can only arm or disarm the Challenger system, open doors or whether they have administrator or installer privileges. The alarm group is also assigned a time zone that determines the hours that the alarm group can be used.

When an administrator adds a new user (and therefore assigns an alarm group to the new user), the administrator cannot assign more rights to the new user than the administrator has. That is, the administrator can assign their own alarm group to a new user, or they can select from a list of alarm groups with less rights than they have, but they cannot assign an alarm group with installer privileges to a new user (unless the administrator has an alarm group with installer privileges).

Door groups

The door group that is assigned to a user determines which doors (readers) the user can operate, and at what times (via the door group's time zone).

Floor groups

Floor groups are used in Challenger systems that have one or more TS0869 Intelligent 4-Lift Controllers. The floor group that is assigned to a user determines which floors the user can access, and at what times (via the floor group's time zone).

Duress codes

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

The Challenger system will behave as if the user's PIN code was entered (for example, to open a door), and it will initiate a duress alarm to be reported to the monitoring company. The duress alarm can be reset (cancelled) by entering the normal PIN code. Duress codes cannot be used to access a menu (for example, to program the system): a duress code is treated as an invalid code for 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 Challenger LAN, the characters "...," are displayed on the top line of the LCD screen (*Figure 7*).

Figure 7. LCD screen indication of keypad duress alarm

A rectangular box with a black border representing an LCD screen. It contains two lines of text: the first line reads "..., There Are No Alarms In This Area" and the second line reads "Code:". The text is in a bold, sans-serif font.

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

To reset the duress facility (i.e. to turn off the signal), enter a valid PIN code. The ..., will be removed from the LCD screen.

Note: If duress was activated under conditions which are no longer valid (false alarm), and it has been reset, it is important that you contact your monitoring company to ensure that no further action is taken by them.

Chapter 2 Common tasks

This chapter describes tasks typically performed by Challenger system administrators.

In this chapter:

<i>Arming your system</i>	16
<i>Disarming your system</i>	17
<i>Dealing with unsealed inputs</i>	19
<i>Opening doors</i>	20
<i>Handling alarms</i>	21
<i>Viewing the quick alarm history</i>	23
<i>Testing input devices</i>	24

Arming your system

Arming your system is the same as *securing* the areas in your system. When armed, a change in the status of any input from sealed to unsealed typically generates an alarm.

Note: Your system may be programmed to allow you to arm your assigned areas by presenting your card to a reader three times within 10 seconds. This section describes how to arm your system from the RAS keypad.

You arm some or all areas of your premises when the areas are unoccupied. Then, if an input device detects a change (such as someone opening a door), the system can generate an alarm. Once you have armed the system, you must leave the area within a preset exit time to avoid setting off the alarm.

Your ability to arm your premises at a particular RAS depends on the following:

- Each RAS controls 1 to 16 areas. Only the areas controlled by the RAS can be armed at that RAS.
- Your user record (PIN or card) can arm 1 to 16 areas, or no areas. You must know which areas you can and cannot arm.
- Inputs in the areas you need to arm may first need to be sealed (for example, the contacts for all doors and windows must be closed), depending on how your alarm group is programmed. If at any time during the arming process the RAS sounds seven quick beeps and displays the word “unsealed”, you will need to seal or isolate the input (see [Dealing with unsealed inputs](#) on page 19).

The following instructions are based on the system being ready to accept your door code or PIN, as shown below (note the word “Code” on the bottom line).

**There Are No Alarms In This Area
Code:**

The actual steps will vary depending on whether your alarm group has been programmed to prompt with a list of areas. If *prompt with a list of areas* is set to YES, use the following steps to arm one or more areas.

1. Press **nnnn** (where nnnn are your PIN code digits).
2. Press **[ON]**.
3. Any disarmed areas that are assigned to your alarm group are listed.
4. Enter **0** and press **[ENTER]** to arm all disarmed areas. The corresponding RAS area LEDs illuminate.
5. Alternatively, enter one of the displayed area numbers and press **[ENTER]** to arm only that area. Repeat as needed to arm additional areas. The corresponding RAS area LEDs illuminate.
6. When finished arming areas, press **[ENTER]** to exit the display.

If *prompt with a list of areas* is set to NO, use the following steps to arm all unarmed areas that are assigned to your alarm group.

1. Press **nnnn** (where nnnn are your PIN code digits).
2. Press **[ON]**. The corresponding area LEDs illuminate.

Your system may be programmed to automatically go into secure test mode when arming areas that contain inputs configured for secure testing. In such a case, the RAS beeper sounds during the test interval and the LCD screen indicates that the secure test is running.

**Secure test, NEXT For Untested
“0”- Cancel:**

Refer to [Conducting a secure test](#) on page 25 for details.

Disarming your system

Normal disarming

Disarming your system is the same as placing the areas in your system *in access*. When disarmed, a change in the status of an input from sealed to unsealed typically will not generate an alarm.¹

Note: Your system may be programmed to allow you to disarm your assigned areas by presenting your card to a reader. This section describes how to arm your system from the RAS keypad.

You disarm your premises (all areas or selected areas), so that you can enter the premises without setting off the alarm. If you enter before disarming, you typically have a preset entry time to avoid setting off the alarm. The RAS's area LEDs illuminate to indicate which areas are armed.

If there is a current alarm condition when you disarm your system, the alarm will be reset. To determine the cause of the alarm, see [Viewing the quick alarm history](#) on page 23.

Your ability to disarm your premises at a particular RAS depends on the following:

- Each RAS controls 1 to 16 areas. Only the areas controlled by the RAS can be disarmed at that RAS.
- Your user record (PIN or card) can disarm 1 to 16 areas, or no areas. You must know which areas you can and cannot disarm.
- Inputs in the areas you need to disarm may first need to be sealed (for example, the contacts for all doors and windows must be closed), depending on how your alarm group is programmed. If at any time during the disarming process the RAS sounds seven quick beeps and displays the word “unsealed”, refer to [Dealing with unsealed inputs](#) on page 19.

The following instructions are based on the system being ready to accept your door code or PIN, as shown below (note the word “Code” on the bottom line).

There Are No Alarms In This Area
Code:

The actual steps vary depending on whether your alarm group has been programmed to *prompt with a list of areas*.

If *prompt with a list of areas* is set to YES, use the following steps to disarm one or more areas.

1. Press **nnnn** (where nnnn are your PIN code digits).
2. Press **[OFF]**.
3. Any armed areas that are assigned to your alarm group are listed.
4. Enter **0** and press **[ENTER]** to disarm all armed areas. The corresponding RAS area LEDs extinguish.
5. Alternatively, enter one of the displayed area numbers and press **[ENTER]** to disarm only that area. Repeat as needed to disarm additional areas. The corresponding area LEDs extinguish.
6. When finished disarming areas, press **[ENTER]** to exit the display.

1. Certain types of inputs can be programmed to generate an alarm in access (for example, a holdup button) or at any time (for example, a panic button). Input types that can generate alarms regardless of whether the area is armed or disarmed are called *24-hour alarms*.

If *prompt with a list of areas* is set to NO, use the following steps to disarm all armed areas that are assigned to your alarm group.

1. Press **nnnn** (where nnnn are your PIN code digits).
2. Press **[OFF]**. The corresponding RAS area LEDs extinguish.

Your system may be programmed to automatically go into access test mode when disarming areas that contain inputs configured for access testing. In such a case, the RAS beeper sounds during the test interval and the LCD screen indicates that the access test is running.

**Access test, NEXT For Untested
"0"- Cancel:**

Refer to [Conducting an access test](#) on page 24 for details.

Note: If your Challenger system is programmed as a financial institution system, and is programmed to automatically go into access test mode when disarming area 1, that contains camera film count inputs configured for access testing, then you will see the current film counts for cameras 1 to 4. The LCD screen will resemble the example in [8. Film Counters](#) on page 34 until you press [ENTER] or the display times out.

Timed disarming

The alarm group that is assigned to your PIN code might be programmed to temporarily disarm the area that you are going to enter, and then automatically rearm the area after a time so that you don't need to remember to arm it. This is done via a concept called a *user category*.

A user category is programmed with a name to identify the type of user for which it is intended (for example, 'Guard'). When a user category is in effect (the user category timer is running), the LCD screen displays the user category name.

**Guard,
Code:**

When the user category timer expires, the RAS starts beeping for the warning time, and the LCD screen displays 'ending'.

**Guard, ending
Code:**

When the warning timer expires, the area will automatically arm. To avoid setting off an alarm, you need to do one of the following:

- Enter your PIN code before the warning timer expires to reset the user category timer.
- Vacate the area.

Dealing with unsealed inputs

An unsealed input (such as an open door or window contact) can prevent an area from being armed or disarmed, depending on how your system is programmed.

If any input is unsealed when you try to arm or disarm an area, the RAS will sound seven quick beeps and will display the unsealed inputs on the LCD screen.

The display of inputs depends on the programming of system option *Display one input at a time*. This section describes both modes of operation. Later sections describe only the default programming where *Display one input at a time* is set to YES.

If *Display one input at a time* is set to YES, each unsealed input's name is displayed.

Unsealed On 6, Front Door
NEXT or ENTER

Press **[NEXT]** or **[MENU*]** to display additional unsealed input names, if any.

Press **[ENTER]** to exit the display.

If *Display one input at a time* is set to NO, a list of input numbers is displayed.

Unsealed On 6, 7, 9.
NEXT or ENTER

Press **[NEXT]** or **[MENU*]** to display additional unsealed input numbers, if any.

Alternatively, enter the input number and press **[ENTER]** to display the unsealed input's name.

Press **[ENTER]** to exit the display.

After you have determined which inputs are unsealed, you must seal them (for example, close the door) then exit this display and try again to arm or disarm the system.

Note: If you are unable to seal an input, you will need to isolate the input. See [10. Isolate](#) on page 35.

Opening doors

A keypad may be used to unlock a door by entering a door code or PIN code, as applicable (see [PIN codes](#) on page 11). Alternatively, the door may be equipped with a card reader that performs the same function as entering a PIN on a keypad.

Note: If the entered code is not valid, or if the time zone is not valid (for example, after hours), or if it is not valid at the particular arming station or reader, the arming station or reader will emit seven quick beeps. The door must be included in the door group assigned to the user in order for the user to be able to open the door.

The following instructions are based on the system being ready to accept your door code or PIN, as shown below (note the word “Code” on the bottom line).

**There Are No Alarms In This Area
Code:**

Entering a disarmed area

Use the following steps to unlock a door and to enter a disarmed area.

1. Press **nnnn** (where nnn are your door code digits only).
2. Press **[ENTER]**.

Exiting a disarmed area

Use the following steps to unlock a door and to arm an area (i.e. to exit a room that you want to arm after you leave), assuming that your PIN code has permission to arm and disarm.

1. Press **nnnn** (where nnnn are your PIN code digits).
2. Press **[ON]**.

See also User menu option [22. Open Door](#) on page 54.

Entering an armed area

Use the following steps to unlock a door and to disarm an area (i.e. to enter a room without setting off an alarm), assuming that your PIN code has permission to arm and disarm.

1. Press **nnnn** (where nnnn are your PIN code digits).
2. Press **[OFF]**.

Your system may be programmed so that you can enter your PIN to unlock a door and to enter an armed area without setting off an alarm by suppressing (shunting) the relevant inputs (such as door contacts) for a specified time. In such a case the LCD screen would indicate as follows.

**Suppressed
Code:**

If the door is closed prior to the end of the maximum open time, the word “Suppressed” is removed from the LCD screen, and the RAS will sound the warning buzzer for 3 seconds to indicate that the door is no longer suppressed.

If the door is not closed at the end of the suppression time, the display will show “Suppression Ending”, and the RAS will sound the warning buzzer for a preset time to enable you to close the door, or to re-enter your PIN code to extend the suppression time.

Handling alarms

There are three types of alarms used in a Challenger system. They are:

- Alarm. See [Alarms](#) on page 21.
- Local alarm. See [Local alarms](#) on page 22.
- System alarm. See [System alarms](#) on page 23.

If the Challenger system detects an alarm condition, it uses the following indications to notify you of the alarm state:

- The area LED for the area in which the alarm has occurred flashes red on the RAS.
- The message “There are no alarms in this area” (or other text) is no longer displayed on the top line of the LCD screen.
- For local alarms, the message “Local Alarm” is displayed on the top line of the LCD screen and the RAS beeps continuously.

The alarm signal (siren, flashing light, etc.) and the circumstances which cause it depend on the system programming.

An area can have multiple inputs associated with it. When there is an alarm, it is important that you know which input is causing the problem so that you can quickly deal with the alarm. Inputs are identified by a number in the range 1 to 256, and (optionally) a name programmed by the installer.

Note: Using Panel Link (Challenger V9) changes the standard numbering system seen here, to reflect that of Panel Link's system. Refer to *Challenger V9 numbering* in *Challenger V8 & V9 Programming Manual* for details.

Alarms

The Challenger system's input devices may be programmed to generate alarms in a wide range of conditions to suit varying needs. For example, an input that is programmed as:

- An *access alarm* input type will generate an alarm when at least one of its areas are disarmed.
- A *secure alarm* input type will generate an alarm when all of its areas are armed.
- A *access/secure alarm* input type will generate different types of alarms when armed or disarmed.
- A *24-hour alarm* input type will generate an alarm regardless of whether its areas are armed or disarmed.

Also, the system may be programmed to monitor the input's wiring for tamper conditions (open or shorted).

Note: Inputs in alarm are displayed with an A in front of the number. Inputs in tamper are displayed with a T in front of the number.

Determine the cause of the alarm

When there is an alarm, the corresponding area LED on the RAS flashes red. The LCD screen displays the following:

Code:

Press **[ENTER] [ENTER]** to see which inputs are in alarm. If you see only numbers and no names, refer to [Displaying input names](#) on page 7.

**Alarm on A1,
NEXT or ENTER**

Press **[NEXT]** or **[MENU*]** to update the list of inputs and display the next inputs in the list (if any).

Press **[0] [ENTER]** to stop cameras from operating (if applicable) and to exit the display.

Resetting alarms

An authorised user must enter a PIN code at the keypad to reset an alarm. Reset the alarm by disarming the area or all areas. Refer to [Disarming your system](#) on page 17.

If you reset an alarm before determining which input it came from, see [Viewing the quick alarm history](#) on page 23.

If the alarm conditions are no longer valid (false alarm), and the alarm has been reset, it is important that you contact your monitoring company to ensure that no further action is taken by them.

Note: If you are unable to reset an alarm because of a faulty input, you will need to isolate the input. See [10. Isolate](#) on page 35.

Local alarms

Local alarms occur when an area is occupied (that is, disarmed). For example, when an input with 24-hour security has been unsealed (for example, a fire door has been opened).

The circumstances that caused the local alarm need to be checked and rectified by someone on site. Consequently, the alarm does not need to be reported to the remote monitoring company. Certain input types can generate a local alarm during access (disarmed) times, and can report to the remote monitoring company during secure (armed) times.

Responding to a local alarm

When there is a local alarm, the corresponding area LED on the RAS flashes red, and the RAS beeps continuously. The LCD screen displays the following:

**Local Alarm
Code:**

Press **[ENTER] [ENTER]** to see which inputs are in alarm. If you see only numbers and no names, refer to [Displaying input names](#) on page 7.

**Local Alarm on A3,Rear Fire Door 1
NEXT or ENTER**

Note: Inputs in alarm are displayed with an A in front of the number.

Press **[NEXT]** or **[MENU*]** to update the list of inputs and display the next inputs in the list (if any). There may be more than one input in alarm, and if you reset without checking you might not know about the additional inputs.

Press **[0] [ENTER]** to reset all local alarms and to exit the display (unless alarms need to be reset as well).

Note: Your Challenger system may be programmed to require an authorised user to enter their PIN code to reset certain local alarms.

If your system has been programmed with a reminder on local alarms, it will re-alarm after a pre-set time unless the cause has been fixed. It will continue to re-alarm, regardless of resetting each time, unless the alarm cause is fixed. When a re-alarm does occur, the letter preceding the input number will not be shown.

System alarms

System alarms indicate that a Challenger device (control panel, DGP, or RAS) is tampered, stops communicating, or detects a fault condition such as mains fail, low battery, fuse fail, etc. For example:

- Alarm equipment interfered with or covers removed (DGP Tamper).
- Communications cabling cut or shorted (DGP Fail, RAS Fail).
- Connections to siren speakers cut or shorted (Siren Fail).
- Telephone line cut, shorted, or damaged (Report Fail).
- Power supply interrupted or overloaded, or battery problems (Mains Fail, Fuse Fail, Low Battery).

Your system is programmed to handle system alarms in one of two ways:

- *Latching system alarms* set to YES: A valid PIN code that is authorized to reset system alarms must be entered to reset a system alarm. The procedure to identify and reset latching system alarms is the same as the procedure described for [System alarms](#) on page 23.
- *Latching system alarms* set to NO: The system alarm will reset automatically as soon as the condition causing the alarm has been rectified. The procedure to identify latching system alarms is the same as the procedure described for [System alarms](#) on page 23.

If the alarm conditions are no longer valid (problem solved), and the alarm has been reset, it is important that you contact your monitoring company to ensure that no further action is taken by them.

Note: If you are unable to reset a system alarm because the conditions require a service technician to attend, you may need to isolate the RAS or DGP. See [16. Isolate/Deisolate RAS/DGP](#) on page 49.

Viewing the quick alarm history

Quick alarm history is a simple way to determine the location of the input that caused an alarm. This information may be necessary where you have to reset an alarm without first checking the cause.

To display the quick alarm history, there must be no alarms. The LCD screen must show the default message on the top line and the word “Code” on the bottom line.

There Are No Alarms In This Area
Code:

Press **[ENTER] [ENTER]** to display the quick alarm history.

*13:23 31/10 LOCAL ALARM Input 1 Fire D>
1-Scan, 0-Exit

The LCD screen shows the most recent alarm details:

- The time the alarm occurred as hour and minutes (HH:MM).
- The date the alarm occurred as day and month (DD:MM).
- The type or alarm.
- The input number and name of the alarm.

Press **[ENTER]** to display earlier alarms in quick alarm history.

Press **[NEXT]** to display later alarms quick alarm history.

Press **[1]** to shift the text displayed on the top line to reveal any additional characters.

Press **[0]** to exit quick alarm history.

Testing input devices

Testing of input devices may be performed by Challenger system administrators and/or by installers, depending on the situation. In addition, your system may be programmed to initiate tests automatically².

Overview

Input devices are the various items such as PIR detectors, switches, buttons, and so on, that can indicate a change of state in the Challenger system. The system can recognize input states of sealed and unsealed, and optionally open and shorted (when input tamper monitoring is used).

Testing of inputs involves monitoring the state of the input whilst changing its state from sealed to unsealed, and then back to sealed. This is typically done by, for example, opening and closing a door and then checking the Challenger system to verify that the change was correctly reported.

Being highly configurable, the Challenger system contains many testing options to suit a variety of applications. For example:

- You may need to test individual inputs on an ad hoc basis when a device appears to be faulty. See [12. Test Input](#) on page 36.
- The system may need to be tested periodically in accordance with Australian Standard AS2201.1.
- High security applications like banks may require particular inputs (for example, hold up and suspicion buttons) to be tested in access mode at the start of every day.

Each input must be programmed for appropriate testing options and the system must be programmed with an appropriate system test mode. In order to conduct tests and interpret reports, you need to understand how certain terms are used. Refer to [Glossary](#) on page 63.

Conducting an access test

Access testing is typically used for inputs that you need to test as soon as the area is disarmed. For example, to enable you to test a hold-up button immediately after disarming the area. The areas that contain the inputs to be tested must be assigned as vaults.

Your system may be programmed to automatically go into access test mode when disarming areas that contain inputs configured for access testing. In such a case, the RAS beeper sounds during the access test time and the LCD screen indicates that the access test is running (*Figure 8*).

Figure 8. Access test RAS display

**Access test, NEXT For Untested
"0"- Cancel:**

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). The input (for example, a hold-up button) is disabled during any access test on areas assigned to it.

2. "Automatic test" actually means to automatically start a test interval during which you can test inputs by, for example, opening and closing a door to verify that the Challenger system correctly identifies the input's change of state from sealed to unsealed and then back to sealed.

The area is disarmed after one of the following occurs:

- The access test is cancelled by the user.
- The required inputs are tested (toggled from sealed to unsealed and back to sealed).
- The access test time expires.

An input's access test is recorded as completed if the input is toggled from sealed to unsealed and back to sealed (typically by a technician activating a sensor such as a door contact).

Following an access test, you can view the access test report to see if any of the required inputs are untested (see [Access test report](#) on page 31).

See also [13. Start Auto Access Test](#) on page 37 for details of how to manually initiate the access testing interval.

Cancelling an access test

From the access test RAS display (*Figure 8*), press **[0] [ENTER] [ENTER]**. The RAS beeper stops sounding and the selected areas are disarmed.

Conducting a secure test

Secure testing is typically used for inputs that you need to test whilst the area is being armed. For example, to enable you to test a door contact at the end of the day when arming the area.

Your system may be programmed to automatically go into secure test mode when arming areas that contain inputs configured for secure testing. In such a case, the RAS beeper sounds during the test interval and the LCD screen indicates that the secure test is running (*Figure 9*).

Figure 9. Secure test RAS display

Secure test, NEXT For Untested
"0"- Cancel:

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).

The area is armed after one of the following occurs:

- The secure test is cancelled by the user.
- The required inputs are tested (toggled from sealed to unsealed and back to sealed).
- The secure test time expires.

An input's secure test is recorded as completed if the input is toggled from sealed to unsealed and back to sealed.

Following a secure test, you can view the secure test report to see if any of the required inputs are untested (see [Secure test report](#) on page 31).

Cancelling a secure test

From the secure test RAS display (*Figure 9*), press **[0] [ENTER] [ENTER]**. The RAS beeper stops sounding (after the auto test interval expires) and the selected areas are armed.

The secure test takes a little time to finish in order to give the tested inputs time to reseal.

Chapter 3 User menu reference

This chapter is a reference to all the options in the Challenger User menu.

Some options may not apply to your Challenger system, and might not be displayed on the RAS's LCD screen. The programming of your alarm group can limit the options visible to you. Also, the programming of the RAS's alarm group can limit the options visible to any users via the RAS.

Refer to *Using the keypad* on page 9 for details of how to access the User menu.

In this chapter:

<i>1. Panel Status</i>	28
<i>2. Input Unsealed</i>	28
<i>3. Input In Alarm</i>	29
<i>4. Input Isolated</i>	29
<i>5. History</i>	30
<i>6. Test Report</i>	30
<i>7. Service Menu</i>	32
<i>8. Film Counters</i>	34
<i>9. Input Text</i>	34
<i>10. Isolate</i>	35
<i>11. Deisolate</i>	35
<i>12. Test Input</i>	36
<i>13. Start Auto Access Test</i>	37
<i>14. Program Users</i>	38
<i>15. Time and Date</i>	46
<i>16. Isolate/Deisolate RAS/DGP</i>	49
<i>17. Enable/Disable Service Tech</i>	50
<i>18. Reset Cameras</i>	50
<i>20. Door and Floor Groups</i>	51
<i>21. Holidays</i>	53
<i>22. Open Door</i>	54
<i>23. Unlock, Lock, Disable and Enable</i>	54
<i>24. Print History</i>	55

Note: Using Panel Link (Challenger V9) changes the standard numbering system to reflect that of Panel Link's system. Refer to *Challenger V9 numbering* in *Challenger V8 & V9 Programming Manual* for details.

1. Panel Status

Use **Panel Status** to list:

Inputs in alarm. The input number is preceded by “A”. An alarm has occurred at this input and it should be reset. Refer to [System alarms](#) on page 23.

Inputs in tamper alarm. The input number is preceded by “T”. Refer to [System alarms](#) on page 23.

Isolated inputs. The input number is preceded by “i”. Refer to [10. Isolate](#) on page 35.

Unsealed inputs. The input number is preceded by “u”. Refer to [Dealing with unsealed inputs](#) on page 19.

System alarms. For example, DGP Tamper.

The LCD screen displays the following information when no inputs are in alarm, tamper alarm, isolated, or unsealed.

**No Alarms, Tampers, Isolates, Unsealed.
Press ENTER**

Press **[ENTER]** to exit this option.

Press **[NEXT]** to update the display.

When one or more inputs are in alarm, tamper alarm, isolated, or unsealed, the LCD screen displays the most recent alarm. If you see only numbers and no names, refer to [Displaying input names](#) on page 7.

**Summary On u2, Front Door Contact
NEXT or ENTER**

Press **[NEXT]** or **[MENU*]** to display additional inputs, if any.

Press **[ENTER]** to exit the display.

2. Input Unsealed

Use **Input Unsealed** to list all unsealed inputs (for example, a door contact open).

The LCD screen displays the following information when no inputs are unsealed.

**All Inputs are Sealed.
Press ENTER**

Press **[ENTER]** to exit this option.

Press **[NEXT]** to update the display.

When one or more inputs are unsealed, the LCD screen displays the inputs. If you see only numbers and no names, refer to [Displaying input names](#) on page 7.

**Unsealed On 2, Front Door Contact
NEXT or ENTER**

Press **[NEXT]** or **[MENU*]** to display additional input names, if any.

3. Input In Alarm

Use **Input In Alarm** to list all inputs that are in an alarm state (but not in local alarm state). You need to know what inputs are in alarm so that the cause of the alarm can be investigated and the alarm reset (see [System alarms](#) on page 23).

The LCD screen displays the following information when no inputs are in alarm.

**No Alarms.
Press ENTER**

Press **[ENTER]** to exit this option.

Press **[NEXT]** to update the display.

When one or more inputs are in alarm, the LCD screen displays the inputs. If you see only numbers and no names, refer to [Displaying input names](#) on page 7.

**Alarm On 2, Front Door Contact
NEXT or ENTER**

Press **[NEXT]** or **[MENU*]** to display additional inputs in alarm, if any.

Alternatively, enter the input number and press **[ENTER]** to display the name of another input in alarm (if any).

Press **[ENTER]** to exit the display.

4. Input Isolated

Use **Input Isolated** to list all isolated inputs to determine which inputs are not operational and need attention.

An isolated input is one which is excluded from functioning as part of the intrusion detection system. It would typically be isolated because it is faulty, and by isolating it you stop it causing an alarm. See [10. Isolate](#) on page 35 for details.

The LCD screen displays the following information when no inputs are in alarm.

**No Isolated Inputs.
Press ENTER**

Press **[ENTER]** to exit this option.

Press **[NEXT]** to update the display.

When one or more inputs are isolated, the LCD screen displays the inputs. If you see only numbers and no names, refer to [Displaying input names](#) on page 7.

**Isolated On 2, Front Door Contact
NEXT or ENTER**

Press **[NEXT]** or **[MENU*]** to display additional input names, if any.

Alternatively, enter the input number and press **[ENTER]** to display another isolated input's name.

Press **[ENTER]** to exit the display.

5. History

Use **History** to display past events of system history, including alarms, access to the menu, etc. It can help you determine events such as the time that an alarm occurred, the time it was reset and who reset it, the time the system was disarmed in the morning, etc.

1-Alarm Events 2-Log Only Events
Option:

Enter **[1]** and press **[ENTER]** to display events currently held in the panel's memory that are related to the intrusion detection system.

13:49 26/11 Menu Entered at Console 1 >
1-Scan, 0-Exit

The display indicates the most recent event. A > character at the end of the line indicates that the text does not fit on the LCD screen. Press **[1]** to shift the text sideways to see more, and repeat as needed.

Press **[ENTER]** to see earlier events.

The above example shows:

- The time of the event in hours and minutes (HH:MM).
- The date of the event as day and month (DD/MM).
- The type of event, for example, Menu Entered.
- The location of the event, for example, Console (RAS) 1.
- The user's number and name (if applicable). In this case, press **[1]** to shift the text sideways to see the additional text.

Enter **[2]** and press **[ENTER]** to display events currently held in the panel's memory that are not reported to the monitoring station but sent to local printer or computer (for example, access granted at door).

6. Test Report

Inputs can be programmed to be included in either an access test or a secure test. This means that a predefined timer starts running, and during this interval the system looks for the input's state to be toggled from sealed to unsealed and back to sealed (typically by a technician activating a sensor such as a door contact). See *Testing input devices* on page 24.

If an access test or a secure test (interval) has occurred and any inputs that are programmed to be included in the test have not been toggled (i.e. tested), they will be available for viewing via the Test Report option.

Use **Test Report** to display the current testing status of inputs configured for access or secure testing.

Test Report 1-Access 2-Secure
Option:

Enter **[1]** and press **[ENTER]** to display the results of inputs tested during access (disarmed) tests. See *Access test report* on page 31.

Enter **[2]** and press **[ENTER]** to display the results of inputs tested during secure (armed) tests. See *Secure test report* on page 31.

Alternatively, press **[ENTER] [ENTER] [ENTER]** to exit this option.

Access test report

This function displays the results of the access (disarmed) test, which can be performed on specific inputs and cameras to see if they are operating correctly. The inputs must be programmed to be included in access tests (determined by the input's test type). The system must be programmed with an appropriate test mode.

From the Test Report menu option, enter [1] and press [ENTER] to display the results of inputs tested during access tests. If all inputs that are programmed to be tested (including 0 inputs) during an access test have been tested, the LCD screen displays the following.

**No Untested Inputs.
Press ENTER**

Alternatively, when one or more inputs are untested, the LCD screen displays the inputs. If you see only numbers and no names, refer to [Displaying input names](#) on page 7.

**Untested Access On 25, Reception Hold Up
NEXT or ENTER**

Press [NEXT] to update the list of untested inputs and display the remaining inputs in the list (if any).

Press [ENTER] to display the results of camera testing. If all the cameras that are programmed to be tested (including 0 cameras) have been successfully tested the LCD screen displays the following.

**All Cameras Have Tested Successfully
Press ENTER**

Cameras are tested subject to the following:

- The user conducting the access test has been programmed to test cameras.
- Only cameras allocated to area 1 are tested.
- The user has area 1 assigned in their alarm group and is testing area 1.

Press [ENTER] to exit this option.

Use [12. Test Input](#) on page 36 to manually test any untested inputs reported.

Secure test report

This option is used to display the results of the secure (armed) test, which can be performed on specific inputs to see if they are operating correctly. The inputs must be programmed to be included in secure tests (determined by the input's test type). The system must be programmed with an appropriate test mode.

From the Test Report menu option, enter [2] and press [ENTER] to display the results of inputs tested during secure tests. If all inputs that are programmed to be tested (including 0 inputs) have been successfully tested the LCD screen displays the following.

**No Untested Inputs.
Press ENTER**

Alternatively, when one or more inputs are untested, the LCD screen displays the inputs. If you see only numbers and no names, refer to [Displaying input names](#) on page 7.

**Untested Secure On 17. Rear Door Contact
NEXT or ENTER**

Press [NEXT] to update the list of untested inputs and display the remaining inputs in the list (if any).

Press **[ENTER]** to exit this option.

Use [12. Test Input](#) on page 36 to manually test any untested inputs reported.

7. Service Menu

Use **Service Menu** to request a service call or to establish a connection to a remote service centre in order to program the Challenger system over the telephone network.

Code Required
Code:

Enter **nnnn** (where nnnn is your PIN code), and press **[ENTER]**.

1-Request Service Technician
0-Exit, Menu:

Select an option:

- Press **[ENTER]** to scroll through the options.
- Press **[0] [ENTER]** to exit this option.
- Press **[1] [ENTER]** to request service technician. See [Request service technician](#) on page 32.
- Press **[2] [ENTER]** to disconnect management software. See [Disconnect management software](#) on page 32.
- Press **[3] [ENTER]** to dial management software. See [Dial management software](#) on page 33.
- Press **[4] [ENTER]** to dial temporary management software. See [Dial temporary management software](#) on page 33.
- Press **[5] [ENTER]** to direct (via J15) management software. See [Direct \(via J15\) management software](#) on page 33.
- Press **[6] [ENTER]** to answer management software. See [Answer management software](#) on page 34.

Request service technician

Instructs the Challenger panel to send a “Service Requested” message to the Remote Monitoring Station. (Not available in all reporting formats).

Enter **[1]** and press **[ENTER]** to select request service technician.

1-Confirm Request Service Technician
0-Exit, Menu:

Enter **[1]** and press **[ENTER]** to confirm, or enter **[0]** and press **[ENTER]** to exit the menu.

Disconnect management software

Instructs the Challenger panel to terminate the connection to management software.

Enter **[2]** and press **[ENTER]** to select disconnect management software. Challenger disconnects and exits the menu.

Dial management software

Instructs the Challenger panel to dial the pre-programmed service telephone number and attempt to connect to the remote service modem to allow programming changes to be made over the telephone network. If it fails on the first try, it will not redial. The panel will automatically drop the line if there have been no keys pressed by the remote service operator within the last 2 minutes.

Enter **[3]** and press **[ENTER]** to select dial management software.

0-300 baud, 1-2400 baud
300, Menu:

Enter **[0]** and press **[ENTER]** to select 300 baud communication speed. Alternatively, enter **[1]** and press **[ENTER]** to select 2400 baud communication speed (if applicable)³.

1-Confirm Dial
0-Exit, Menu:

Enter **[1]** and press **[ENTER]** to confirm, or enter **[0]** and press **[ENTER]** to exit the menu.

Dial temporary management software

Allows a temporary telephone number to be entered and dialled for the remote computer/RAS connection. The computer operator will not be required to use the security password to gain access to the Challenger.

Enter **[4]** and press **[ENTER]** to select dial temporary management software.

""-Pause, Phone No:
Ser No:

Enter up to 10 digits to program a temporary service telephone number, and then press **[ENTER]**.

Press **[ENTER]** to select the communication speed (if applicable).

0-300 baud, 1-2400 baud
300, Menu:

Enter **[0]** and press **[ENTER]** to select 300 baud communication speed. Alternatively, enter **[1]** and press **[ENTER]** to select 2400 baud communication speed.

1-Confirm Dial
0-Exit, Menu:

Enter **[1]** and press **[ENTER]** to confirm, or enter **[0]** and press **[ENTER]** to exit the menu.

Note: If "Dial Temporary Management Software" is used to make the connection to the remote computer, the computer operator will not be required to use the security password to gain access to the Challenger.

Direct (via J15) management software

Instructs the Challenger panel to establish a temporary direct connection to a computer connected to the Serial Port (J15) on the motherboard (Service Technician option only).

Enter **[5]** and press **[ENTER]** to select direct (J15) management software. Challenger connects via the J15 port and exits the menu.

3. Use of 2400 baud requires panel firmware version 8.105 or later, and suitable PCB hardware.

Answer management software

Instructs the Challenger panel to answer a current dial-in attempt immediately.

Enter **[6]** and press **[ENTER]** to select answer management software. Challenger answers a current dial-in attempt immediately and exits the menu.

8. Film Counters

Use **Film Counters** to display the current frame number position on each of the security camera films.

- If a camera is fitted with a film out detector and that camera does not have a film in it, the frame count will be displayed as OUT (OUT is removed when film is loaded).
- Up to eight cameras can be displayed. A camera position that does not have a camera fitted will display the frame count as '----'.
- A frame count can be from 0 to 9999.

Film Counts 1: 0123 2:1077 3:0056 4:----
Press ENTER

Press **[ENTER]** to see the film counts for cameras 5 to 8.

Press **[ENTER]** a second time to exit this menu.

9. Input Text

Use **Input Text** to display the names assigned to inputs.

Input: 1,Rear Door
Input No:

The LCD screen displays the first input number and its assigned name. If you see only numbers and no names, refer to [Displaying input names](#) on page 7.

Press **[NEXT]** or **[MENU*]** to display subsequent input names.

Alternatively, enter the input number and press **[ENTER]** to display the input's name.

Press **[ENTER]** to exit the display.

10. Isolate

Use **Isolate** to temporarily exclude inputs from functioning as part of the intrusion detection system.

An input would be isolated because it is faulty or broken, and by isolating it, you would stop it causing an alarm. If an input is in an alarm state, then isolating it resets the alarm. After the problem is resolved the input must be deisolated (see [11. Deisolate](#) on page 35).

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.

All Inputs are Sealed.
Isolate No:

Alternatively, if one or more inputs are unsealed the display resembles the following.

Unsealed on 1,Front door
Input No:

If your system is programmed to display one input at a time, press [NEXT] or [MENU*] to display subsequent unsealed input names, and to update the display. If your system is programmed to not display one input at a time, the LCD screen shows only a list of input numbers. However, if there is only a single input, the name is displayed.

From either of the above screens, enter the input number and press [ENTER] to isolate that input. If an attempt is made to isolate an input which is already isolated, the request appears as if it is processed but it is not logged in the history and the input remains isolated.

Press [ENTER] when finished to exit this option. The LCD screen display resembles the following.

Isolated Inputs In This Area
Code:

11. Deisolate

Use **Deisolate** to deisolate inputs (return them to functioning as part of the intrusion detection system). An input would be isolated because it is faulty or broken (see [10. Isolate](#) on page 35). After it is repaired it must be deisolated.

Note: Do not deisolate the input before checking the circumstances, as deisolating an unsealed input may cause an alarm.

The function provides a list of isolated inputs for you to select an input to deisolate. If there are no isolated inputs, the display indicates as follows.

All Inputs are De-Isolated.
Delsolate:

In this case, press [ENTER] to exit this option.

Isolated inputs are displayed. Inputs that are unsealed are indicated with a 'u' in front of the input number.

Isolated on u3, Rear door
Delsolate:

If your system is programmed to display one input at a time, press [NEXT] or [MENU*] to display subsequent input names, and to update the display. If your system is programmed to not display one input at a time, the LCD screen shows only a list of input numbers. However, if there is only a single input, the name is displayed.

From either of the above screens, enter the input number and press **[ENTER]** to deisolate that input. Press **[ENTER]** when finished to exit this option.

12. Test Input

Use **Test Input** to initiate a defined interval during which you can test an individual input (even if the input is isolated) during either access or secure. When you select the Test Input option and enter the input's number, you can then test the input by altering its state and checking the LCD screen to verify that the system correctly identifies the input's state.

Test Individual Input
Input No:

Enter the input number and press **[ENTER]** to display the state of the input.

SEALED on 6,Loading dock
Press ENTER

Unseal the input device and observe the LCD screen. When the input is unsealed or tampered (open or shorted if inputs are monitored for tamper conditions), the display should indicate the change in state, according to *Table 3*.

UNSEALED on 6,Loading dock
Press ENTER

Press **[ENTER]** to return to the previous screen.

Depending on how your system is programmed for input tamper monitoring, the results can indicate the conditions shown in *Table 3*.

Table 3. Input testing results

Input Condition	input tamper monitoring on (default)	Input tamper monitoring off
Sealed (10K Ω resistance)	Sealed	Sealed
Unsealed (5K Ω or 20K Ω resistance)	Unsealed	Unsealed
Open circuit	Open	Unsealed
Short circuit	Short	Unsealed

If the input is not sealed, the RAS emits a continuous tone. When the status of the input is changed to sealed, the display will be updated and the tone will stop. Alternatively, press **[ENTER]** to stop the tone and return to the previous screen.

Press **[ENTER]** when finished to exit this option.

Note: There is a pre-determined time in which to complete the test. If the test is not completed within the programmed time (default is 5 minutes), the option is exited.

13. Start Auto Access Test

Use **Start Auto Access Test** to initiate a defined interval during which specific inputs and cameras (camera input types) may be tested to see if they are operating correctly when the area is in access (disarmed).

The following programming is required:

- The areas that contain the inputs to be tested must be assigned as vaults.
- The inputs to be tested must be included in access tests (input test types 1, 2, 4, or 5).
- Cameras to be tested must be in area 1.
- The access test time programmed by the installer must be sufficient for you to test all the required inputs (default time is 15 minutes).

This option may be used regardless of the programmed Challenger system test mode.

The RAS beeper sounds continuously during the testing time or until you exit this option.

**Access Test, NEXT For Untested
"0"-Cancel:**

From the initial screen, press **[NEXT]** to display an untested input, test the input by unsealing and then sealing it, and press **[NEXT]** to display the next untested input. Repeat until all inputs have been tested. Refer to *Table 3* on page 36 for the results that may be displayed depending on your system's input tamper monitoring programming.

If **[NEXT]** is selected to display any untested inputs, the LCD screen displays the first input number and its assigned name. If you see only numbers and no names, refer to *Displaying input names* on page 7.

**Untested Access On 4, PIR In Office
NEXT or ENTER**

Alternatively, press **[ENTER]** to proceed to the camera test or the Test Completed/Not Completed display (as applicable).

**Untested Access On 2,Camera 1
NEXT or ENTER**

Inputs that are programmed as a camera input types (and assigned to area 1) are also tested.

**All Cameras Have Tested Successfully
Press ENTER**

When all inputs that are programmed to be tested (including 0 inputs) during the access test have been tested, or the time allowed for access test has expired, the test will automatically cease and the display will indicate if the test is completed or not completed.

**Test Completed
Press ENTER**

Or...

**Test Not Completed
Press ENTER**

Press **[ENTER]** to exit this option.

Note: If your Challenger system is programmed as a financial institution system, and is programmed to automatically go into access test mode when disarming area 1, that contains camera film count inputs configured for access testing, then you will see the current film counts for cameras 1 to 4. The LCD screen will resemble the example in [8. Film Counters](#) on page 34 until you press [ENTER] or the display times out.

If there are any tests not completed, you can again select **Start Auto Access Test** to finish the testing.

14. Program Users

Use **Program Users** to manage the user records that are stored in the Challenger panel's memory (see [What is a user?](#) on page 11).

Note: Your Challenger system may be configured for dual custody programming, where any user (other than the master user) requires a second user to enter their PIN code before access is menu option 14.

**Enter Second Code
Code:**

The initial LCD screen, and some of the subsequent screens, will vary depending on the configuration of your Challenger system:

- Non-IUM Challenger systems display the **Program Users** screen shown in *Figure 10*.
- IUM Challenger V8 systems display the **Program Users** screen shown in *Figure 11*.

Figure 10. Program users screen in non-IUM mode

**1-Delete 2-Display 3-Create
Option:**

Figure 11. Program users screen in IUM mode

**1-Delete 2-Display 3-Create 4-Total 5-Card Learn
Option:**

Note: You cannot display, delete, or modify users that have areas in their alarm group that you do not have in your alarm group, or have access to menus that you cannot access.

Refer to the following sections:

- [Option 1—Deleting a user](#) on page 39.
- [Option 2—Displaying a user](#) on page 39.
- [Option 3—Creating or modifying a user](#) on page 40.
- [Option 4—Total users](#) on page 45 (applicable to IUM Challenger systems only).
- [Option 5—Card Learn](#) on page 45 (applicable to IUM Challenger systems only).

Option 1—Deleting a user

From **Program Users**, use the following steps to delete a user.

Note: Do not delete the master user (user number 50).

1. Enter **[1]** and then press **[ENTER]**.

Delete User
User No:

2. Enter the user number and press **[ENTER]** to delete the user record.
3. Repeat to delete another user, or press **[ENTER]** again to exit the delete option.

Option 2—Displaying a user

From **Program Users**, use the following steps to display a user's details.

1. Enter **[2]** and then press **[ENTER]**.

Display User
User No:

2. Enter the user number and press **[ENTER]** to display the user's alarm group.

***-View, Alm Grp:12,Foreman**
Press ENTER

3. Press **[ENTER]** to display the user's door group.

Door Group: 2
Press ENTER

4. Press **[ENTER]** to display the user's floor group.

Floor Group: 1
Press ENTER

5. For Challenger panels programmed to display user flags, press **[ENTER]** to display the user flags, starting with dual custody.

NO - Dual Custody
***-Change 0-Skip**

6. The user flags (see [Glossary](#) on page 63), displayed in sequence are:
 - dual custody
 - guard
 - visitor
 - trace user
 - card only
 - privileged
 - long access
7. In each case, press **[ENTER]** to move to the next user flag, or press **[0]** to exit the user flags (the * option does not apply to display mode).

8. For Challenger panels programmed to allow name files, press [ENTER] to display the user's name.

**Your Name is User Name ,(*)-End
User Name**

9. For Challenger panels programmed to allow you to see PIN codes, press [ENTER] to display the user's PIN code.

**Pin Code: 4346
Press ENTER**

10. For IUM Challenger systems, the user's card bits display.

**Card Bits: 27.0.0.0.25.0.6
*-ID, Bits:**

11. Press [ENTER] again to exit this user record and return to the **Display User** screen.

Option 3—Creating or modifying a user

In any given Challenger panel, the process of using a RAS to create a new user, or to modify an existing user is very similar. You need to:

- Enter the user number that you want to add or modify.
- Step through the LCD screens, adding, skipping, or changing details as you go.
- Press [ENTER] at the end to save the details.

A basic Challenger panel used only for intrusion detection (and not access control) might require only the most basic information such as user number, alarm group, and PIN code. Some Challenger systems allow you to program many other user options, such as:

- The user's name.
- A door group and a floor group defines where the user is allowed to go and at what times of day.
- User flags that further configure how the user's access permissions are handled by the Challenger system.

Some Challenger panels enable you to enter or update a user's card data electronically by presenting the card to the reader (called *learning* the card data), or by manually entering card data.

Determining the user number

If cards are used at readers connected to the Challenger panel, the user number is the same as the card ID number (unless your system uses a card offset). Depending on your Challenger panel's memory configuration, you can program user numbers up to 65,535 in Challenger V8, or 11,466 in Challenger V9.

For a small number of users, you can use the [User worksheet](#) on page 58 to list the Challenger panel's users and to see what the next user number in sequence should be. If the Challenger system contains a large number of users, you may prefer to use management software to program users.

In IUM Challenger systems, you can use [Option 4—Total users](#) on page 45 to see a tally of users.

Creating a user in a non-IUM Challenger system

From **Program Users** (see [14. Program Users](#) on page 38) use the following steps to create a new user or modify a user.

1. Enter **[3]** and then press **[ENTER]**.

Create User
User No:

2. Enter the new or existing user number, and then press **[ENTER]**.

*-View, Alm Grp:1-No Access
Alarm Group:

3. Enter the number of the alarm group to be issued to this user, and then press **[ENTER]**.⁴
Optionally, press **[NEXT]** to display the list of alarm groups that you can issue to a user.
4. Press **[ENTER]** to display the user's door group. Users must have a door group in order to open doors.

Door Group: 0
Door Group:

5. Enter the number of the door group (if applicable) to be issued to this user, and then press **[ENTER]** to display the user's floor group.

Floor Group: 0
Floor Group:

6. Enter the number of the floor group (if applicable) to be issued to this user, and then press **[ENTER]**.
7. For systems programmed to display user flags, press **[ENTER]** to display the user flags, starting with dual custody.

NO - Dual Custody
*-Change 0-Skip

User flags are typically used only for access control at doors 17 to 64 (systems that have Intelligent Access Controllers). The user flags, displayed in sequence, are:

- dual custody
- guard
- visitor
- trace user
- card only
- privileged
- long access

8. For each user flag, press **[MENU*]** to toggle between YES and NO options, press **[ENTER]** to move to the next user flag, or press **[0]** to exit the user flags.

4. You cannot assign an alarm group to a user unless the alarm group has the option "Can this Alarm Group be Assigned to Users" set to YES and your alarm group has all the "Areas" and "User Menu Options" of the alarm group you wish to assign. For example, if the alarm group you wish to assign has "Alarm System Control" and "Modem Access" set to YES, then your alarm group must have these features set to YES also.

9. For Challenger panels programmed to allow name files, press **[ENTER]** to program the user's name (applicable only to user numbers in the range 1 to 200).

Your Name is ,(*)-End

10. Enter up to 16 characters of text for the user's name (see [Entering text](#) on page 42). To enter a letter, press the key the number of times relative to the position of the letter. Both upper and lower case letters are available as well as the numerical values.
11. Press **[MENU*]** to save the name (and to display the new name if programmed). If the name has been changed, only letters preceding the cursor will be saved (the cursor must be to the right of the name when you press **[MENU*]** to save).
12. Press **[MENU*]** to program the user's PIN code.

Pin Code:
Code:

The minimum PIN code length is 4 digits⁵, plus any value programmed for the alarm code prefix. For example, if your system uses an alarm code prefix value of 2 (digits) then you must program PIN codes of at least 6 digits (4 + 2).

In general, every user in a Challenger V8 system can have a PIN code (depending on your system's memory configuration). If using TS0882 MB expanded memory, and the Challenger panel is not configured for software IUM mode, then only the first 1,000 out of 11,466 users can have a PIN code.

Programming or viewing of PIN codes can be prohibited to all users except for the master installer.

13. For Challenger panels programmed to allow you to see PIN codes, enter the PIN code⁶, and then press **[ENTER]** to return to the **Create User** screen, or to the **Waiting For Card** screen (IUM systems only, see [Creating a user in an IUM Challenger system](#) on page 43).

Entering text

Your system may be programmed to allow user numbers in the range 1 to 200 to contain names (up to 16 characters). When entering user names, the keypad automatically changes to text entry mode. In this mode you can use the RAS keypad to enter text, numbers, spaces, or special characters according to [Table 4](#) on page 43.

When each required character is displayed, press **[ENTER]** to move to the next position. When finished, press * to save the name. In this option, **[ENTER]** has no other function than to move the cursor.

5. Minimum PIN code length is 5 digits for systems programmed as "financial institutions".

6. You cannot program a PIN code that already exists, or conflicts with another user's duress code or door code.

Table 4. Key presses to get character

Key	Number of key presses to get character						
	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	.	—	&

Creating a user in an IUM Challenger system

This section describes the *additional* LCD screens that you will see when programming users in IUM Challenger systems. This section is a continuation of the steps in [Creating a user in a non-IUM Challenger system](#) on page 41.

1. For IUM Challenger systems, a “Waiting For Card” message displays.

Waiting For Card
* Hist

2. Do one of the following:
 - Present a card at the designated card learn reader, and then press [ENTER] to save the card bit data in the user record. See [Learning card data](#) on page 43.
 - Press [MENU*] to use card data from the Challenger panel’s history. See [Using data from card history](#) on page 44.
 - Press [ENTER] to manually enter the card data bits or the card ID, depending on panel configuration. See [Manually entering card data](#) on page 44.

Learning card data

Use the following steps to learn card data and save it in a user record, starting at the **Waiting For Card** screen shown on page 43.

1. Present a card at the designated card learn reader. The LCD screen displays the card bit data.

Card Bits: 27.0.0.0.25.0.6
*-ID, Bits:

2. Press [ENTER] to save the card bit data in the user record, and to return to the **Create User** screen.

Using data from card history

When programming a new user for an IUM system, you have the option of using card data that has been previously read and stored in the Challenger panel's card history.

Use the following steps to look up previously-read card data and save it in a user record, starting at the **Waiting For Card** screen shown on page 43.

1. Press **[MENU*]** to display the start of the card history list.

No 1 27.0.0.0.25.0.6
*** Next, # Enrol**

2. Press **[ENTER]** to enrol (save) the displayed card data in the user record, and then to return to the **Create User** screen.

Alternatively, press **[MENU*]** to display the next record in the card history list until you find the one you want. If there are no more records the following screen displays.

End Of History
Press ENTER

3. Press **[ENTER]** to return to the **Create User** screen.

Manually entering card data

If you do not have a designated card learn reader, you can manually enter the card data bits or the card ID, depending on panel configuration.

If the Challenger panel has a site number, then you can enter the card ID number instead of the card bits. The card bits will be calculated automatically from the card ID number and the site number. Site numbers (sometimes referred to as site codes or facility codes) are used when card readers are connected directly to the control panel (RASs 1 to 16).

Use the following steps to enter card data and save it in a user record, starting at the **Waiting For Card** screen shown on page 43.

1. Press **[ENTER]** to display the card bits screen.

Card Bits: 27.0.0.0.25.0.6
***-ID, Bits:**

2. Enter the card bits (raw card data) in format xxx.xxx.xxx.xxx.xxx, where each field is a number from 0 to 255. Press **[ENTER]** after each number to save the data and move to the next field.
3. Press **[ENTER]** to save the card bit data in the user record, and to return to the **Create User** screen.

Alternatively, if the Challenger panel has a site number, you will see a Card ID screen instead of a card bits screen.

Card ID: 0
***-Bits, ID:**

Enter the card ID number and then press **[ENTER]** to save the card bit data in the user record, and to return to the **Create User** screen.

Modifying a user

The process of modifying a user is similar to the process of creating a user, except that each screen will display the previously-programmed values.

In the case of IUM Challenger systems, one difference can be seen where a user already has card data. You have the option of deleting the card data and learning or manually entering new card data, starting at the **Waiting For Card** screen shown on page 43.

1. Press **[ENTER]** to display the user's card bit data.

Card Bits: 27.0.0.0.25.0.6
*-Del

2. Press **[MENU*]** to erase the user's card data and return to the **Waiting For Card** screen. See [Learning card data](#) on page 43.
3. Alternatively, press **[ENTER]** to return to the **Create User** screen.

Option 4—Total users

This option applies to IUM Challenger systems only.

The minimum number of users is 1 (which is user 50, the master user). Use the Total users command to determine how many users have been programmed into the Challenger panel's memory in addition to user 50. For example, if the total users is 21, then 20 users have been programmed, plus the master user.

From **Program Users**, use the following steps to see a tally of users.

1. Enter **[4]** and then press **[ENTER]**.

Total Users 1
Press ENTER

2. Press **[ENTER]** again to exit this screen and return to the Create User screen.

Option 5—Card Learn

This option applies to IUM Challenger systems only.

A card reader RAS can be used to enter a user's card data (card bits) into the Challenger system by presenting (badging) the card at the reader during the user creation process (see [Learning card data](#) on page 43).

By default, the RAS at address 1 is designated the card learn RAS. From **Program Users**, use the following steps to select a new RAS address to be the card learn reader.

1. Enter **[5]** and then press **[ENTER]**.

1
Card RAS:

2. Enter the card reader's RAS address in the range 1 to 16, and then press **[ENTER]**.

16
Card RAS:

3. Press **[ENTER]** again to exit this screen and return to the **Create User** screen.

Special procedures

Programming non-Tecom magnetic card formats

The following procedure must be used to allow non-Tecom format cards such as credit cards, financial institution cards, etc., to be programmed as users. Your system must be equipped with the appropriate card reader in order to perform this function.

Use the following steps to record the non-Tecom format card enrolment number in the user record.

1. Swipe the card in the reader.
2. If the card is not recognized by the system, an event will be logged in history as “Card/Pin” followed by an enrolment number of up to 10 digits (for example, “Card/Pin 1234512345”). Note the enrolment number, which will be recorded as the PIN code when programming the user.
3. Follow the procedure described in [Option 3—Creating or modifying a user](#) on page 40, with the following exceptions:
 - The card number is not the user number, so you must select a user number that can accept a PIN code. In some cases, only the first 1,000 users can have a PIN code (see [14. Program Users](#) on page 38 for details).
 - Enter the enrolment number as the PIN code.

If you want the user to use the card but not the PIN code (enrolment number), the following options must be programmed:

- The system must be programmed to display user flags when programming users.
- Set the user flag “card only” to YES when programming the user.

15. Time and Date

Use **Time and Date** to change the Challenger panel’s time and date settings (for example, to program the daylight savings time start and end dates). The system may be programmed so that the time and date are visible on the LCD display (see [Figure 4, LCD welcome screen example showing time and date](#) on page 7).

Figure 12. Time and date LCD screen

**Time 1-Display, 2-Set, 3-DST, 4-Correct
0-Exit, Menu:**

Select one of the time and date options and press **[ENTER]**. These options are described in the following sections.

Option 1-Display

Use the following steps to see the current settings.

1. From the Time and Date screen ([Figure 12](#)) enter **[1]** and press **[ENTER]**.

**Time 14:33:59 19/03/2008 Wednesday
0-Exit:**

2. Press **[ENTER]** to return to the Time and Date screen.

Option 2-Set

Use the following steps to change the time and date settings.

1. From the Time and Date screen (*Figure 12*) enter [2] and press [ENTER].

Time 14:33:59 19/03/2008 Wednesday
Hours:

2. Enter the correct hours in 24-hour format (or accept the current value) and press [ENTER].

Time 14:33:59 19/03/2008 Wednesday
Minutes:

3. Enter the correct minutes (or accept the current value) and press [ENTER].

Time 14:33:59 19/03/2008 Wednesday
Seconds:

4. Enter the correct seconds (or accept the current value) and press [ENTER].

Time 14:33:59 19/03/2008 Wednesday
Day of Mth:

5. Enter the correct day of month (or accept the current value) and press [ENTER].

Time 14:33:59 19/03/2008 Wednesday
Month:

6. Enter the month (or accept the current value) and press [ENTER].

Time 14:33:59 19/03/2008 Wednesday
Year:

7. Enter the correct year (or accept the current value) and press [ENTER].

Time 14:33:59 19/03/2008 Wednesday
0-Exit, Set-ENTER:

8. Review the displayed settings and press [ENTER] to accept. Alternatively, press [0] [ENTER] to abandon your changes and exit this option.

Option 3-DST

Use the following steps to program the daylight savings time start and end dates.

Program DST start

1. From the Time and Date screen (*Figure 12*) enter [3] and press [ENTER].

0-Disable, Month 00
Start Sunday:

2. Enter a value in the range 1 to 5 and press [ENTER] to indicate which Sunday in the month daylight savings time begins. The following example shows the LCD screen where a value of 1 is entered.

1-First Sunday, Month 00
Start Sunday:

3. If correct press [ENTER] to accept.

1-First Sunday, Month 00
Start Month:

4. Enter a value in the range 1 to 12 and press [ENTER] to indicate which month daylight savings time begins. The following example shows the LCD screen where a value of 10 is entered.

1-First Sunday, Month 10
Start Month:

5. If correct press [ENTER] to accept.

0-Disable, Month 00
End Sunday:

Program DST end

The process for programming the Sunday and month that DST ends is the same as described in [Program DST start](#) on page 48.

Option 4-Correct

Use the following steps to program a time correction for the Challenger panel's internal clock.

1. From the Time and Date screen (*Figure 12*) enter [4] and press [ENTER].

Seconds Correction Per Day: +0
***-Chg, Sec:**

2. Press [0] [ENTER] and then press [MENU*] to toggle the + or – factor for amount of seconds you need to add or subtract each day (the default is +).
3. When the + or – factor is displayed correctly, enter the value in seconds and press [ENTER].

16. Isolate/Deisolate RAS/DGP

Use **Isolate/Deisolate RAS/DGP** to temporarily exclude from the Challenger system fault or tamper messages (system alarms) that are being generated by an arming station (RAS) or data gathering panel (DGP). This would be used if a RAS or DGP has generated a system alarm or is out of service, and needs to be isolated while awaiting service.

Isolating a RAS or DGP will also reset any system alarm generated by the RAS or DGP. Isolating a DGP will not isolate the alarm inputs on that DGP, but will disable DGP's offline and online reporting.

1-RAS, 2-DGP Isolate / Deisolate
0-Exit, Menu:

The following examples are for a RAS: the procedures for isolating a DGP are the same.

Press **[1] [ENTER]** to open the Isolate RAS screen.

No RASs Are Isolated
Isolate RAS:

Alternatively, if RAS 5 has previously been isolated the display would indicate the following.

5,
Isolate RAS:

Enter a RAS number and then press **[ENTER]** to toggle its isolated/deisolated state. For example, press **[5] [ENTER]** to deisolate RAS 5, or press **[6] [ENTER]** to isolate RAS 6 and add it to the top line.

17. Enable/Disable Service Tech

Use **Enable/Disable Service Tech** to enable or disable the service technician.

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

**0-Cancel, 1-Service In
Option:**

Press **[1] [ENTER]** to enable the service technician for the programmed service time period and return to the menu.

If you need to cancel the service technician command before the service time expires, press **[0] [ENTER]**.

18. Reset Cameras

Use **Reset Cameras** to reset the film frame count on all security cameras connected directly to the Challenger panel to zero or to change the frame count number on an individual camera. This would be necessary when you change the film in the camera.

**Reset Camera Counts "0#" -All
Camera No:**

Press **[0] [ENTER]** to reset the film frame count on all security cameras to zero.

Press **[n] [ENTER]** to display the current film frame count on camera *n*. Press **[ENTER]** a second time to return to the Reset Camera screen.

Alternatively, enter a new frame count in the range 0 to 1900 for the selected camera, and then press **[ENTER]** to return to the Reset Camera screen.

19. Install Menu

Access to the Install menu is typically limited to installers or administrators. Refer to the *Challenger V8 & V9 Programming Manual* if you are an installer or administrator and you need to know details of Challenger system programming.

20. Door and Floor Groups

Use **Door and Floor Groups** to program door groups and floor groups.

A door group contains a list of doors and a time zone for each door. A floor group contains a list of floors and a time zone for each floor. The time zone assigned to the door group or floor group restricts user access to the times defined in the time zone. Time zone 0 provides 24-hour access to authorized users.

Groups, 1-Doors 2-Floors
Option:

Select an option:

- Press **[1] [ENTER]** to program a door group.
- Press **[2] [ENTER]** to program a floor group.
- Press **[ENTER]** to exit this option.

Programming a door group

Use the following steps to add doors to a door group or disable doors that have previously been added.

1. From the **Door and Floor Groups** screen, press **[1] [ENTER]** to program a door group.

Door Groups
Group No:

2. Enter a door group number in the range 1 to 255 (the maximum number depends on your system, see [Extended capacities](#) on page 3) and press **[ENTER]**. The LCD screen displays the selected door group number (for example, 1), four of the possible 64 doors, and each door's assigned time zone (** indicates that the door number is disabled).

Door Grp 1 D1- D2-** D3-** D4-****
Enter Door:

3. Enter a door number in the range 1 to 64 and press **[ENTER]**.

Door Grp 1 D1- D2-** D3-** D4-****
***-Dis, Tz-D1:**

4. Enter a hard time zone number in the range 1 to 24 (and 42 to 63 if your system permits, see [Extended capacities](#) on page 3) or enter a soft time zone number in the range 26 to 41 (for doors 1 to 16 only) and press **[ENTER]**. Alternatively, if you need to disable a door, enter **[MENU*]** as the time zone and then press **[ENTER]**.

Door Grp 1 D1-01 D2- D3-** D4-****
Enter Door:

In the above example, we've programmed door group 1 with door 1, where door 1 can be accessed during time zone 1. The LCD screen is ready for you to add another door number and time zone to door group 1.

We suggest that each time you program or change a door group, you record the details on a page printed from [Door groups worksheet](#) on page 59.

Programming a floor group

Use the following steps to add floors to a floor group or disable floors that have previously been added.

1. From the **Door and Floor Groups** screen, press [2] [ENTER] to program a floor group.

Floor Groups
Group No:

2. Enter a floor group number in the range 1 to 128 (the maximum number depends on your system, see *Extended capacities* on page 3) and press [ENTER]. The LCD screen displays the selected floor group number (for example, 1), four of the possible 64 floors, and each floor's assigned time zone (** indicates that the floor number is disabled).

Floor Grp 1 F1- F2-** F3-** F4-****
Enter Floor:

3. Enter a floor number in the range 1 to 64 and press [ENTER].

Floor Grp 1 F1- F2-** F3-** F4-****
***-Dis, Tz-F1:**

4. Enter a time zone number in the range 0 to 46 (the maximum number depends on your system, see *Extended capacities* on page 3) and press [ENTER]. Alternatively, if you need to disable a floor, enter [MENU*] as the time zone and then press [ENTER].

Floor Grp 1 F1-01 F2- F3-** F4-****
Enter Floor:

In the above example, we've programmed floor group 1 with floor 1, where floor 1 can be accessed during time zone 1. The LCD screen is ready for you to add another floor number and time zone to floor group 1.

We suggest that each time you program or change a floor group, you record the details on a page printed from *Floor groups worksheet* on page 60.

21. Holidays

Use **Holidays** to 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 that are declared a holiday.

Holidays
Holiday No:

Enter a holiday number in the range 1 to 24 and then press **[ENTER]**. The Holiday programming screen displays.

Holiday 1:00/00/00
Day of Mth:

From the Holiday programming screen you can:

- Program the selected holiday.
- View the details of a previously programmed holiday.
- Press **[MENU*]** to display the next of the 12 holiday records in sequence.

Programming a holiday

Use the following steps to program a holiday.

1. From the Holiday programming screen, enter the day that the holiday falls on and then press **[ENTER]**. For example, for ANZAC Day 25 April 2008, press **[2] [5] [ENTER]**. The LCD screen displays the day and prompts you to enter the month.

Holiday 1:25/00/00
Month:

2. Enter the month that the holiday falls on and then press **[ENTER]**. For example, for ANZAC Day 25 April 2008, press **[4] [ENTER]**. The LCD screen displays the day and month and prompts you to enter the year.

Holiday 1:25/04/00
Year:

3. Enter the year that the holiday falls on and then press **[ENTER]**. For example, for ANZAC Day 25 April 2008, press **[8] [ENTER]**. The date is programmed and the LCD screen returns to the Holidays screen for you to program another holiday.

Holidays
Holiday No:

We suggest that each time you program or change a holiday, you record the details on a page printed from [Holidays worksheet](#) on page 61.

22. Open Door

Use **Open Door** to unlock a door that you are authorized (via the door group assigned to your PIN code) to unlock.

The Open Door command would typically be used at a RAS that's at a different location from the door (for example, from a security desk), otherwise the commands described in *Opening doors* on page 20 could be used.

Open Door
Door No:

Enter the door number and then press **[ENTER]**. Alternatively, press **[ENTER]** to return to the User menu.

23. Unlock, Lock, Disable and Enable

Use **Unlock, Lock, Disable and Enable** to unlock, lock, disable or enable a door controlled by an Intelligent Access Controller (doors numbered in the range 17 to 64).

The door will remain in the state selected until an opposite event occurs in the system that will change the state of that door. For example, door 21 automatically unlocks at 8 a.m. and relocks at 5 p.m. by using an override time zone. If the user wishes to secure the premises and leave at 4 p.m., the door can be locked using the lock option, but will still automatically unlock at 8 a.m. again the following morning.

1-Unlock 2-Lock 3-Disable 4-Enable
Option:

Select an option:

- Press **[1] [ENTER]** to unlock a door.
- Press **[2] [ENTER]** to lock a door.
- Press **[3] [ENTER]** to disable a door.
- Press **[4] [ENTER]** to enable a door.
- Press **[ENTER]** to exit this option.

The following example uses option 1. The other options are similar.

Use **1-Unlock** to unlock a door that you are authorized (via the door group assigned to your PIN code) to unlock.

Unlock Door
Door No:

Enter the door number and then press **[ENTER]**. Alternatively, press **[ENTER]** to return to the User menu.

24. Print History

Use **Print History** to send events contained in the alarm events buffer and access events buffer to a printer connected to the Challenger panel. Events are listed in chronological order.

Print History back To 00/00/00
Enter Day:

The history that is available for printing depends on the following:

- The alarm events buffer and access events buffer can each contain only 100 events (standard memory) or 1,000 events (expanded memory). When a buffer is full, the oldest events are discarded.
- The printer must be ready (not offline or out of paper).
- In a panel link system, events are sorted across all panels in chronological order.

The print history option can be used in two ways:

- If you specify a 'back to' date, events starting from the specified date to the present are printed regardless of whether they have been previously printed.
- If you enter 00/00/00 as a 'back to' date, any events that have been previously printed (either from this command or from real time printing) will not be printed.

Use the following steps to print all history events from a specified date to the present.

1. From the Print History screen, enter the first day that you want to see history from and then press **[ENTER]**. For example, for 20 March 2008, press **[2] [0] [ENTER]**. The LCD screen displays the day and prompts you to enter the month.

Print History back To 20/00/00
Enter Month:

2. Enter the month and then press **[ENTER]**. For example, for 20 March 2008, press **[3] [ENTER]**. The LCD screen displays the day and month and prompts you to enter the year.

Print History back To 25/04/00
Enter Year:

3. Enter the year and then press **[ENTER]**. For example, for 20 March 2008, press **[8] [ENTER]**. The events are sent to the printer and the LCD screen returns to the User menu.

Appendix A Programming worksheets

Use the worksheets on the following pages to record details of:

<i>User worksheet</i>	58
<i>Door groups worksheet</i>	59
<i>Floor groups worksheet</i>	60
<i>Holidays worksheet</i>	61

In addition, your installer should provide you with worksheets or programming details for your system's:

- Alarm groups
- Time zones

Programming worksheets for these items are provided in the *Challenger V8 & V9 Programming Manual*.

User worksheet

User records are programmed in User menu option [14. Program Users](#) on page 38.

Copy this page as needed to record the programming details of the panel's users (in addition to user 50 "TECOM Master").

Figure 13. User worksheet

Site	Challenger		Users
User number	<input type="text"/>	PIN	<input type="text"/> Name (optional) <input type="text"/>
Alarm group	<input type="text"/>	Door group	<input type="text"/> Floor group <input type="text"/>
User flags (optional), mark a check box to indicate YES <input checked="" type="checkbox"/>			
Dual custody	<input type="checkbox"/>	Visitor	<input type="checkbox"/> Card only <input type="checkbox"/> Long access <input type="checkbox"/>
Guard	<input type="checkbox"/>	Trace user	<input type="checkbox"/> Privileged <input type="checkbox"/>
User number	<input type="text"/>	PIN	<input type="text"/> Name (optional) <input type="text"/>
Alarm group	<input type="text"/>	Door group	<input type="text"/> Floor group <input type="text"/>
User flags (optional), mark a check box to indicate YES <input checked="" type="checkbox"/>			
Dual custody	<input type="checkbox"/>	Visitor	<input type="checkbox"/> Card only <input type="checkbox"/> Long access <input type="checkbox"/>
Guard	<input type="checkbox"/>	Trace user	<input type="checkbox"/> Privileged <input type="checkbox"/>
User number	<input type="text"/>	PIN	<input type="text"/> Name (optional) <input type="text"/>
Alarm group	<input type="text"/>	Door group	<input type="text"/> Floor group <input type="text"/>
User flags (optional), mark a check box to indicate YES <input checked="" type="checkbox"/>			
Dual custody	<input type="checkbox"/>	Visitor	<input type="checkbox"/> Card only <input type="checkbox"/> Long access <input type="checkbox"/>
Guard	<input type="checkbox"/>	Trace user	<input type="checkbox"/> Privileged <input type="checkbox"/>
User number	<input type="text"/>	PIN	<input type="text"/> Name (optional) <input type="text"/>
Alarm group	<input type="text"/>	Door group	<input type="text"/> Floor group <input type="text"/>
User flags (optional), mark a check box to indicate YES <input checked="" type="checkbox"/>			
Dual custody	<input type="checkbox"/>	Visitor	<input type="checkbox"/> Card only <input type="checkbox"/> Long access <input type="checkbox"/>
Guard	<input type="checkbox"/>	Trace user	<input type="checkbox"/> Privileged <input type="checkbox"/>

Door groups worksheet

Door groups are programmed in User menu option [20. Door and Floor Groups](#) on page 51.

Copy this page as needed to record the programming details of the panel's door groups. There can be up to 255 door groups for a Challenger V8 (requires panel firmware version 8.128 or later) or for a Challenger V9.

Figure 14. Door groups worksheet

Site		Challenger		Door groups			
Door group number		Description (optional)					
Door	Time zone	Door	Time zone	Door	Time zone	Door	Time zone
1		17		33		49	
2		18		34		50	
3		19		35		51	
4		20		36		52	
5		21		37		53	
6		22		38		54	
7		23		39		55	
8		24		40		56	
9		25		41		57	
10		26		42		58	
11		27		43		59	
12		28		44		60	
13		29		45		61	
14		30		46		62	
15		31		47		63	
16		32		48		64	

Hard time zones can be assigned to any door.
Soft time zones (26 to 41) may be assigned only to doors 1 to 16.

Floor groups worksheet

Floor groups are programmed in User menu option [20. Door and Floor Groups](#) on page 51.

Copy this page as needed to record the programming details of the panel's floor groups. There can be up to 128 floor groups for a Challenger V8 (requires panel firmware version 8.128 or later) and 255 door groups for a Challenger V9.

Figure 15. Floor groups worksheet

Site		Challenger		Floor groups			
Floor group number		Description (optional)					
Floor	Time zone	Floor	Time zone	Floor	Time zone	Floor	Time zone
1		17		33		49	
2		18		34		50	
3		19		35		51	
4		20		36		52	
5		21		37		53	
6		22		38		54	
7		23		39		55	
8		24		40		56	
9		25		41		57	
10		26		42		58	
11		27		43		59	
12		28		44		60	
13		29		45		61	
14		30		46		62	
15		31		47		63	
16		32		48		64	

Hard time zones can be assigned to any floor.

Holidays worksheet

Holidays are programmed in User menu option [21. Holidays](#) on page 53.

Copy this page as needed to record the programming details of the panel's holiday records.

Figure 16. Holidays worksheet

Site			Challenger			Holidays
1	Name (optional)		Date (dd/mm/yy)			
2	Name (optional)		Date (dd/mm/yy)			
3	Name (optional)		Date (dd/mm/yy)			
4	Name (optional)		Date (dd/mm/yy)			
5	Name (optional)		Date (dd/mm/yy)			
6	Name (optional)		Date (dd/mm/yy)			
7	Name (optional)		Date (dd/mm/yy)			
8	Name (optional)		Date (dd/mm/yy)			
9	Name (optional)		Date (dd/mm/yy)			
10	Name (optional)		Date (dd/mm/yy)			
11	Name (optional)		Date (dd/mm/yy)			
12	Name (optional)		Date (dd/mm/yy)			
13	Name (optional)		Date (dd/mm/yy)			
14	Name (optional)		Date (dd/mm/yy)			
15	Name (optional)		Date (dd/mm/yy)			
16	Name (optional)		Date (dd/mm/yy)			
17	Name (optional)		Date (dd/mm/yy)			
18	Name (optional)		Date (dd/mm/yy)			
19	Name (optional)		Date (dd/mm/yy)			
20	Name (optional)		Date (dd/mm/yy)			
21	Name (optional)		Date (dd/mm/yy)			
22	Name (optional)		Date (dd/mm/yy)			
23	Name (optional)		Date (dd/mm/yy)			
24	Name (optional)		Date (dd/mm/yy)			

Glossary

Table 5. Challenger V8 & V9 terms

Term	Definition
24-hour alarm	Input types (5, 29, 33, and 59) that will generate an alarm regardless of area status (armed or disarmed).
4-Door/Lift DGP	See “Intelligent Access Controller”.
access	The condition of an area when it is occupied and when the intrusion detection system has been set so that normal activity does not set off an alarm. Opposite of “secure”.
access control	The control of entry to, or exit from, a security area.
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. Inputs in vault areas may be tested from User menu option 13. Start Auto Access Test on page 37.
access time	For doors 1 to 16 (connected to a control panel), the door event flag will unlock the door for the time programmed in door(s) unlock time. For doors 17 and higher (connected to an Intelligent Controller), the door will unlock for the time programmed in door or lift access time.
alarm	The state of a 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.
alarm code	The user’s full PIN code (used for alarm control). See also “door code”.
alarm code prefix	The alarm code prefix value in the range one to four enables users to enter a door code (a shorter PIN code) for access control. For example, if a user’s full PIN code 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 code (for example, 3456). The PIN code must be at least five digits in length in order to use a door code. The smallest alarm code prefix value is one (the resulting door code must be at least four digits). See also “door code”.
alarm control	The control over alarm functions.
alarm group	A panel programming concept that defines a group of areas, functions and menu options. Alarm groups are assigned to users, arming stations, 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 alarm events or other events to a remote monitoring company by means of a dialler and 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). Global anti-passback communicates reader information to all controllers on a Challenger LAN to ensure tracking of movements. Note: This functionality requires the use of an Intelligent Access Controller.
area	A logical grouping of input devices that are armed and disarmed simultaneously. Each area is identified by a number and name. for example, 1. Office, 2. Workshop, 3. Boardroom.
Ares	Ares management software. QNX-based software running on multiple nodes (workstations), capable of controlling enterprise-scale Challenger installations. See also Forcefield.
arm	See <i>secure</i> .

Table 5. Challenger V8 & V9 terms (continued)

Term	Definition
arming station (RAS)	A device that provides a user interface for security functions for areas or for access points (doors). The arming station may be an LCD keypad, or any other device which can be used to perform security functions such as arm or disarm, open doors, etc.
authorised RAS	This function gives the user the ability to badge their card on a reader-equipped RAS on the Intelligent Controller sub-LAN in order to selectively arm or disarm area(s) normally controlled via the system LAN. Specifically, badging at the door's reader simulates the user entering their PIN at the authorised system RAS and provides a means of selecting areas. Selection of areas is not otherwise available from a RAS on the sub-LAN. Note: This functionality requires the use of an Intelligent Access Controller.
burglar alarm	An alarm triggered by a security device like a PIR or door contact, indicating someone has entered without authorised access.
card	A portable device (card or fob) that holds information to identify a user. The information to identify a user can be available on a magnetic strip, a bar-code, a Wiegand card, or in a chip (smart card).
card only	If the user flag "card only" is set to YES the user will not be able to use the PIN code. This allows the PIN code field to be used to program cards on formats not normally compatible with the Challenger system when a special reader is used.
card offset	A card offset value is added or subtracted from the actual card ID number to adjust the user number.
cardholder	See <i>user</i> .
central station	See " <i>remote monitoring company</i> ".
Challenger panel	Control panel: the key component of the modular Challenger system. It may be used as a stand-alone alarm panel with LAN, intrusion detection system inputs, relays (outputs), siren, strobe, onboard dialler and STU port for reporting. An LCD keypad arming station provides a text-base user interface for controlling the system. A Challenger panel may be expanded with the addition of Intelligent Access Controllers and other devices to provide greater system capacity, advanced access control functionality, connection to management software computers, and interfaces to a wide range of devices via IP or RS-232.
CID	Ademco Contact ID reporting format.
console	See "arming station".
console warning	Programming option in the Input database (keypad buzzer).
control panel	An electronic device that is used to gather data from inputs on the premises. Depending on programming and status of areas, it will generate alarm signals. If required, alarms and other events can be reported to a remote monitoring company.
DGP	Data Gathering Panel—A device that collects data from other security devices within an area, and transfers it to the control panel or a 4-door or 4-lift DGP.
dialler	An electronic device that allows the intrusion detection system to transmit alarms and other events to a remote monitoring company. Can also be used to perform upload and download of access control data with management software.
disarm	See <i>access</i> .
door code	An optional version of the user's PIN code 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 potentially revealing the entire PIN code 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.

Table 5. Challenger V8 & V9 terms (continued)

Term	Definition
door group	A panel programming concept that assigns a group of doors or lifts to a user, in order to allow access at those doors or lifts. Access to each door in a group may be restricted via a time zone.
DOTL	Door open too long. Note: This functionality requires the use of an Intelligent Access Controller.
download	The transfer of records from a management software computer to a control panel.
dual custody	When the Challenger system option "dual custody" is enabled, two users must enter their codes before access is granted to user programming. If the user flag "dual custody" is set to YES the user will always require a second valid user code or card to be entered to perform any alarm or access control function at doors 17 to 64.
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 activate a door event flag. For example, an egress button provided inside a door to allow users to exit without using a door reader. Note: This functionality requires the use of an Intelligent 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 Intelligent Access Controller.
event flag	A signal activated by an input condition, area condition, system status, or fault condition, door command (on doors 1 to 16), or shunt condition. The main purpose of an event flag is to activate a relay.
extended access time	The time for the door to unlock when a user, with the "LONG ACCESS" flag enabled, presents a valid card or PIN at the door reader. Note: This functionality requires the use of an Intelligent Access Controller.
fire alarm	An alarm triggered by fire or smoke detectors indicating a fire.
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 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 requires the use of an Intelligent Access Controller.
Forcefield	Forcefield management software. QNX-based software running on single or multiple nodes with Windows client computers providing the user interface. Depending on hardware and license modules purchased, Forcefield is capable of controlling Challenger installations ranging from small to enterprise scale (in the range of 5,000 panels and 1,000,000 users).
global anti-passback	See <i>anti-passback</i> .
guard status	If the user flag "guard status" is set to YES the user can accompany a visitor type user at doors 17 to 64.
guard tour	A defined series of checkpoints at which a security guard must check in, within specified time intervals. Failure to check in on time triggers an alarm or other event. Note: This functionality requires Ares or Forcefield management software.

Table 5. Challenger V8 & V9 terms (continued)

Term	Definition
hardware IUM	Challenger V8 systems fitted with TS0883 4 MB or TS0884 8 MB memory expansion modules (the panel and all Intelligent Access Controllers must use matching modules). See also "IUM".
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 uploaded 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.
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 requires the use of an Intelligent Access Controller.
in reader region	When a valid card or PIN is entered at the door In reader, the number of the region that the user is entering into is recorded against the user code. Note: This functionality requires the use of an Intelligent Access Controller.
input	An electrical signal from a security device (input device) to the intrusion detection system. Each input device is identified by a number and text, for example, 14. Reception Holdup Button, 6. Fire Exit Door. Challenger input conditions are: sealed, unsealed, tamper, inhibited.
input type	The input type determines exactly how an input will function in given circumstances. Most input types require an area, but input types that affect the status of areas (types 6, 31, 34, 35) need alarm groups.
installer	A company that installs and services security equipment.
Intelligent Access Controller	4-door or 4-lift DGP. Intelligent Access Controllers expand the Challenger system providing door relays, interlocking door functionality, greater system capacity, and advanced access control functionality such as anti-passback, DOTL, extended access time, and more.
isolate	The input device is inhibited from indicating sealed or unsealed status. It is excluded from functioning as part of the system.
IUM	Intelligent User Memory. In an IUM system, all users can have 10-digit PIN codes and up to 48 bits of raw card data. See also "hardware IUM" and "software IUM".
key switch	A device using a key-operated switch to arm or disarm areas.
keypad	An arming station with keys to input data. Used to program the control panel, perform user functions, view alarms, etc.
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. Keypad duress can be enabled or disabled for individual keypads connected to an Intelligent Access Controller.
LAN	The system's RS-485 data bus. Also, sub-LAN for the Intelligent Access Controller's RS-485 data bus.
local alarm	An alarm which is transmitted only within a building, and occurs when an area is occupied. The circumstances which 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 is called a macro output.

Table 5. Challenger V8 & V9 terms (continued)

Term	Definition
long access	If the user flag "long access" is set to YES the user will be allowed extended door access times at doors 17 to 64 (for example, to allow the door to remain open longer for disabled access).
low security time zone	When the time zone is valid, a valid card or a PIN code is required to open a door. When the time zone is not valid and "Card and PIN code reader" is set to YES, both a valid card and PIN code are required to open a door. Note: This functionality requires the use of an Intelligent 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 Challenger system may be programmed and operated TITAN, Ares, or Forcefield management software on a graphical interface.
mode time	For a RAS connected to a control panel, the mode time is fixed at 10 seconds for 3 badge arming. For a RAS connected to an Intelligent Access Controller, the mode time is programmable.
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 requires the use of an Intelligent 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 user code. Note: This functionality requires the use of an Intelligent Access Controller.
override time zone	The programmed time zone will automatically unlock the door for the programmed time periods. Free access is allowed when the time zone is valid. Note: This functionality requires the use of an Intelligent Access Controller.
PIN	Personal Identification Number—A number given to, or selected by, a user. It is necessary to enter a PIN on an LCD RAS to perform most functions. The PIN is associated with a user number which identifies the PIN holder to the system. PINs range in length from 4 to 10 digits. See also "door code".
PIR	Passive Infrared detector. A security device used to detect intruders in a certain part of an area or premise.
poll	An inquiry message continually sent by the control panel to DGPs and arming stations. Polling allows the remote unit to transfer data to the control panel.
privileged	If the user flag "privileged" is set to YES the user's code or card will override any anti-passback restrictions or reader disabled functions in place on doors 17 to 64.
RAS	See "arming station".
reader	A device (arming station) used for access control that can read magnetic strip reader or proximity cards to allow access.
region	A defined access control area having 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. Regions are numbered from 0 to 254. Region 0 acts as 'Off premises'. Region 255 is used for 'Region disabled'. Note: This functionality requires the use of an Intelligent Access Controller.

Table 5. Challenger V8 & V9 terms (continued)

Term	Definition
relay	Relay or open collector output from the panel or a relay controller. The numbering system can support 255 relays, however, this is subject to practical limitations. For example, relays can be added to a panel or Intelligent controller by connecting a series of relay controllers. The numbering system allows for 32 relay controllers, but the <i>recommended</i> maximum number of relay controllers to be connected in series is 19 (152 relays). If more than 152 relays are required, it's best to connect the additional relays via DGPs.
relay control group	A relay control group is a predefined set of eight consecutive relay numbers (starting at 1). The first relay control group uses relay number 1, the second relay control group uses relay number 9 (1 + 8), the third relay control group uses relay number 17 (9 + 8) and so on.
relay controller	A PCB module which connects to the panel or a DGP to provide additional relay or open collector outputs.
remote monitoring company	A company which monitors whether an alarm has occurred in a 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".
RTE	Request to exit, egress.
sealed	The input is not activated, for example, door closed.
secure	The condition of an area where a change in the status of any input (from sealed to unsealed) causes an alarm (armed). 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.
shunt	A procedure which 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".
software IUM	A programmable configuration for Challenger V8 panels that are not fitted with TS0883 4 MB or TS0884 8 MB memory expansion modules. Software IUM applies only to Challenger V8 panels using firmware version 8.128 and above. See also "IUM".
STU	Subscriber Terminal Unit
STU port	The Challenger PCB's serial (J15) port.
tamper	The input is open or short-circuited. Someone may have tried to tamper with the security device. Your Challenger system may be programmed to monitor tamper indications on input devices (input tamper monitoring).
test (manual)	Use Test Input to test individual inputs (even if the input is isolated) during either access or secure, to determine if it is operating correctly. See 12. Test Input on page 36. See also <i>access test</i> and <i>secure test</i> .
test report	If an access test or a secure test (interval) has occurred and any inputs that are programmed to be included in the test have not been toggled (i.e. tested), they will be reported as untested via the Test Report option. See 6. Test Report on page 30.
time & attendance	An LCD RAS can be used as a time and attendance reader, when used with TS9010 TITAN Time & Attendance Utility.

Table 5. Challenger V8 & V9 terms (continued)

Term	Definition
time zone, timezone	A time zone is a means of making certain Challenger functionality conditional. There are two types of time zones: <ul style="list-style-type: none"> • 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.
TITAN	Acronym for Tecom Integrated Total Alarm Network, TITAN management software. Windows-based software running on single or multiple computers providing the user interface. Capable of controlling small Challenger installations. TITAN (single user) is typically used by installers to program Challenger panels.
trace user	If the user flag “trace user” is set to YES all alarm and access functions performed by the user at doors 17 to 64 will cause a trace message to be sent to the management computer.
unsealed	The input is unsealed, for example, door open.
upload	The transfer of records from a control panel to a management software computer.
user	A record containing (at least) a user’s PIN or card number to identify the user to the Challenger system. Also called ‘card holder’.
user category	A user category can be assigned to an alarm group to restrict or enable special functionality or access by a user.
user flags	Additional data entered in user records to enable advanced access control functionality for systems containing Intelligent Access Controllers. The user flags are dual custody, guard, visitor, trace user, card only, privileged, and long access.
vault area	A vault area is armed and disarmed by being linked to a controlling area instead of being armed and disarmed directly from a RAS.
visitor status	If the user flag “visitor status” is set to YES the user must be accompanied by a guard type user at doors 17 to 64.

Index

A

access control	2
access test	24, 30
<i>automatic</i>	24
<i>cancelling</i>	25
<i>completing</i>	25
<i>manually starting</i>	37
<i>report</i>	31
alarm	
<i>code</i>	11
<i>group</i>	12
<i>LEDs</i>	8
alarms	21
<i>cause</i>	21
<i>history</i>	23
<i>local</i>	22
<i>reminder</i>	22
<i>resetting</i>	22
<i>system</i>	23
answer management software	34
area LEDs	8
Ares management software	2
arming your system	16

B

beeper	8
--------------	---

C

camera test	37
Challenger system	2
Challenger V9	3, 7
code	
<i>alarm</i>	11
<i>door</i>	11
<i>duress</i>	13
<i>PIN</i>	11
code prompt	6
conventions	v
custom message	9

D

daylight savings time	48
-----------------------------	----

dealing with unsealed inputs	19
DGP	2
dial management software	33
dial temporary management software	33
direct (via J15) management software	33
disarming your system	17
disconnect management software	32
door and floor groups	51
door code	11
door group	12, 51
door groups worksheet	59
door opening	21
door shunting	21
duress alarm	13
<i>code</i>	13
<i>indication</i>	13
<i>reset</i>	13
duress code	13

E

enable/disable service tech	50
extended	
<i>door groups</i>	59
<i>floor groups</i>	60

F

fault LEDs	8
financial institution option	42
firmware version	
8.105	33
8.128	3, 59, 60, 68
floor groups	12, 52, 60
Forcefield management software	2

G

glossary	63
----------------	----

H

handling alarms	21
history	30
holidays	53
holidays worksheet	61

I

iDGP	
<i>See Intelligent Access Controller.</i>	
input name	7
input tamper monitoring	36
inputs	
<i>deisolate</i>	35
<i>in alarm</i>	28, 29
<i>in tamper alarm</i>	28
<i>isolate</i>	35
<i>isolated</i>	28, 29
<i>monitoring</i>	36
<i>names</i>	34
<i>testing</i>	36
<i>unsealed</i>	28
install menu	50
Intelligent Access Controller	2, 54, 63, 64, 65, 67
intrusion detection	2
isolate/deisolate RAS/DGP	49
IUM	
<i>software</i>	3

J

J15 port	33
----------------	----

L

LCD screen	6
LED	
<i>alarm</i>	8
<i>area</i>	8
<i>status</i>	8
<i>system alarm</i>	8
<i>system fault</i>	8
local alarms	22

M

magnetic swipe cards	11
management software	32
<i>Ares</i>	2
<i>Forcefield</i>	2
<i>TITAN</i>	2

Menu option

01. Panel Status	28
02. Input Unsealed	28
03. Input In Alarm	29
04. Input Isolated	29
05. History	30
06. Test Report	30
07. Service Menu	32
08. Film Counters	34
09. Input Text	34
10. Isolate	35
11. Deisolate	35
12. Test Input	36
13. Start Auto Access Test	37
14. Program Users	38
15. Time and Date	46
16. Isolate/Deisolate RAS/DGP	49
17. Enable/Disable Service Tech	50
18. Reset Cameras	50
19. Install Menu	50
20. Door and Floor Groups	51
21. Holidays	53
22. Open Door	54
23. Unlock, Lock, Disable and Enable	54
24. Print History	55

N

non-Tecom magnetic cards	46
--------------------------------	----

O

open door	54
opening door	20

P

panel link	7
panel link system	3
panel status	28
PIN code	11
<i>length</i>	2
preface	v
print history	55
program users	38, 39, 41, 45
prompt with a list of areas	16

Q

quick alarm history	23
---------------------------	----

R

RAS	
<i>beeper</i>	8
<i>details</i>	5
<i>keypad</i>	9
<i>LCD screen</i>	6
<i>LEDs</i>	8
<i>models</i>	5
RAS keypad	6
remote arming station (RAS)	2
request service technician	32
reset cameras	50
routine maintenance	4

S

safety terms and symbols	v
secure test	30
<i>automatic</i>	25
<i>cancelling</i>	25
<i>completing</i>	25
<i>report</i>	31
security camera	34
service technician	32, 50
shunted door	21
smart cards	11
software IUM	3
start auto access test	37
status LEDs	8
suppressed door	21
suppressed input	20
suppression time	20
system alarms	23

T

test	
<i>input</i>	36
<i>report</i>	30
testing	
<i>inputs</i>	36
<i>system</i>	4
testing inputs	24
time and attendance	68
time and date	46
time correction	48

time zone	11
timed disarming	18
TITAN management software	2
TS0810 Access Manager	3
TS0816 Challenger	2
TS0816P Challenger	3

U

unlock, lock, disable and enable	54
unsealed input	19
user category	18
user flags	39
user menu	10, 27
user menu options	10
users	
<i>card data</i>	44
<i>card history</i>	44
<i>card ID</i>	44
<i>card learn reader</i>	43
<i>creating</i>	40
<i>deleting</i>	39
<i>displaying</i>	39
<i>modifying</i>	40, 45
<i>name files</i>	42
<i>non-Tecom format cards</i>	46
<i>PIN code</i>	42
<i>programming</i>	40
<i>programming names</i>	42
<i>total</i>	45
<i>worksheet</i>	58

V

vault area	37, 69
V9	3, 7

W

WDGP	2
web site	3
Wiegand-format cards	11
worksheet	
<i>door groups</i>	59
<i>floor groups</i>	60
<i>holidays</i>	61
<i>users</i>	58

