GE
Security

TITAN System Management Software
User Manual

P/N 1064080 • REV B • 27MAY09

Document number: **1064080** Revision B

5. Limited Warranty. GE Security Pty. Ltd. warrants that:

(a) that the Software is properly recorded on the hardware;

(b) that the accompanying text is a complete copy and contains all material reasonably appropriate for the installation and use of the Software; and

GE Security Pty. Ltd. makes no representations or warranties of any kind that this software is error free, that all defects, if any, can be corrected or that the software is fit for any particular purpose. As a condition of this license agreement you accept all risks arising out of the use of this software including loss of data.

GE Security Pty. Ltd.'s and its suppliers' entire liability and your exclusive remedy shall be repair or replacement of the Software or hardware that does not meet GE Security Pty. Ltd.'s Limited Warranty and which is returned to GE Security Pty. Ltd. with a copy of your receipt within 30 days of the date of delivery to you. Any replacement Software or hardware is warranted for the remainder of the original warranty period or 30 days, whichever is longer.

This Limited Warranty is void if failure of the Software or hardware has resulted from accident, abuse, or misapplication. Further, you agree to indemnify and hold harmless GE Security Pty. Ltd., its subsidiaries, employees, suppliers and agents from and against all loss, costs, damages, liability or expense by reason of any liability imposed by law upon GE Security Pty. Ltd., its subsidiaries, employees, suppliers or agents resulting from any such unauthorised use of the Software or hardware.

GE Security Pty. Ltd. and its suppliers make no representation or warranty that the Software or hardware are error-free, or that any defects can be corrected, and disclaim all other warranties, either express or implied, including, but not limited to, implied warranties or merchantability and fitness for a particular purpose, with regard to the Software, the accompanying written materials, and any accompanying hardware.

You assume responsibility for the Software's selection to achieve your required purpose and for the installation, use and results of the Software and hardware.

In no event shall GE Security Pty. Ltd. or its suppliers be liable for any damages whatsoever (including without limitation, damages for loss of business profits or information, business interruption or any other incidental or consequential loss or other pecuniary loss) arising out of the use of or inability to use the Software or hardware, even if GE Security Pty. Ltd. has been advised of the possibility of such damages.

The limitations and exclusions of liability set out above are subject to any overriding statutory provisions to the contrary and so may not apply to you.

6. Indemnification. You agree to indemnify and hold harmless GE Security Pty. Ltd., its employees, agents and suppliers from and against all loss, cost, damage, liability or expense by reason of any liability imposed by law upon GE Security Pty. Ltd., its subsidiaries, employees, agents and suppliers resulting from an unauthorised use of software.

7. General. This is not a sale of the Software and title to this software and the copyrights, patent and other intellectual property rights in the software are retained by GE Security Pty. Ltd.

This agreement is the entire agreement between us and supersedes any prior communications between us relating to the subject matter of this agreement. You acknowledge that you have read this agreement, understand it and agree to be bound by its terms and conditions.

If any provision of this agreement is unenforceable all others will remain in effect.

This agreement is governed by the laws of the Australian Capital Territory.

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

This is the GE Security *TITAN User Manual* for the following products:

- TS9002 TITAN single-user
- TS9011 TITAN multi-user server
- TS9008 TITAN multi-user client

The screen images used and commands described in this manual are based primarily on TITAN single-user 1.09.00. TITAN multi-user 2.07.11 examples are used only where needed to illustrate a particular item in TITAN multi-user. This manual will be revised to describe other software versions only as GE deems necessary.

This document includes an overview of the product, as well as detailed instructions explaining:

- how to manage user records;
- how to create and issue ID cards;
- how to generate reports; and
- how to acknowledge and respond to alarms.

There is also information describing how to operate and maintain your Challenger system. To use this document effectively, you should meet the following minimum qualifications:

- a basic knowledge of management software; and
- a basic knowledge of security systems and components.

Read these instructions and all ancillary documentation entirely *before* installing or operating this product. Refer to *Chapter 8*, *Troubleshooting, Support* on page 117 for instructions on obtaining support.

This manual, as with the *TITAN online help*, may describe features that do not affect you as an operator because of the menu permissions allocated to your operator record.

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

Conventions used in this document

The following conventions are used in this document:

Bold	Menu items and buttons.
Italic	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.
Blue italic	(Electronic version). Hyperlinks to cross-references, related topics, and URL addresses.
`Monospace`	Text that displays on the computer 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 overview of TITAN (Tecom Integrated Total Alarm Network) and instructions for getting started using the software.

In this chapter:

Product overview

GE's Challenger platform unites alarm and access control with smart card operations and remote communications. All of its functions work together from a single Challenger panel or from multiple Challenger panels. Challenger is built using modular components, so you can grow the system and its capabilities to match your changing security needs.

With Challenger you can:

- Use cards (including smart cards or key fobs) to lock or unlock doors, arm or disarm areas, and perform other operations.
- Select who goes where and when, with flexible access control.
- Issue ID cards and assign user privileges individually or by groups of employees.
- Assign alarm inputs to specific areas or groups of areas.
- Virtually eliminate false alarms with all-in-one security control. Users no longer need to remember a PIN code to disarm a security system after unlocking a door.
- Manage your security operations onsite or from remote locations.

It is assumed that your security dealer has designed and configured your Challenger security system, and that items such as doors have already been programmed. This document focuses on TITAN, the tool you use to manage your Challenger security system.

After you learn the basics of TITAN operation, you will be able to create user records, create photo ID cards, issue user cards or fobs, and respond to security alarms. But Challenger lets you reach far beyond the basics. Take time to explore Challenger's capabilities with your dealer so that you can put intelligent security to work for you.

The scope of this manual is day-to-day operation of a Challenger system after it has been installed and configured.

System requirements

TITAN Single User and TITAN Multi User are supported for use on Microsoft Windows XP SP2.

Product contents

The TITAN system consists of the following:

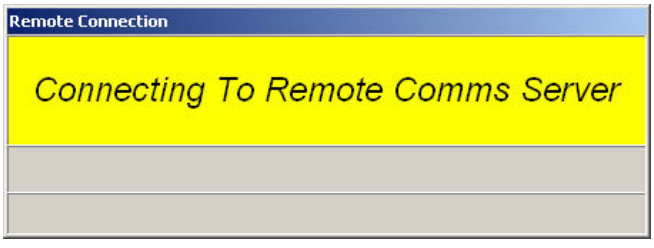
- a CD-ROM with the following software components:
  - TITAN software;
  - PDF files of the latest release notes and this user manual
- a paper copy of this user manual.

Getting started

TITAN may be launched from the **TITAN Security System** program group or from the TITAN desktop shortcut (if using a shortcut, see also *Troubleshooting* on page 118).

In TITAN multi-user, the Remote Connection window briefly displays (*Figure 1*).

Figure 1. Connecting to TITAN multi-user server

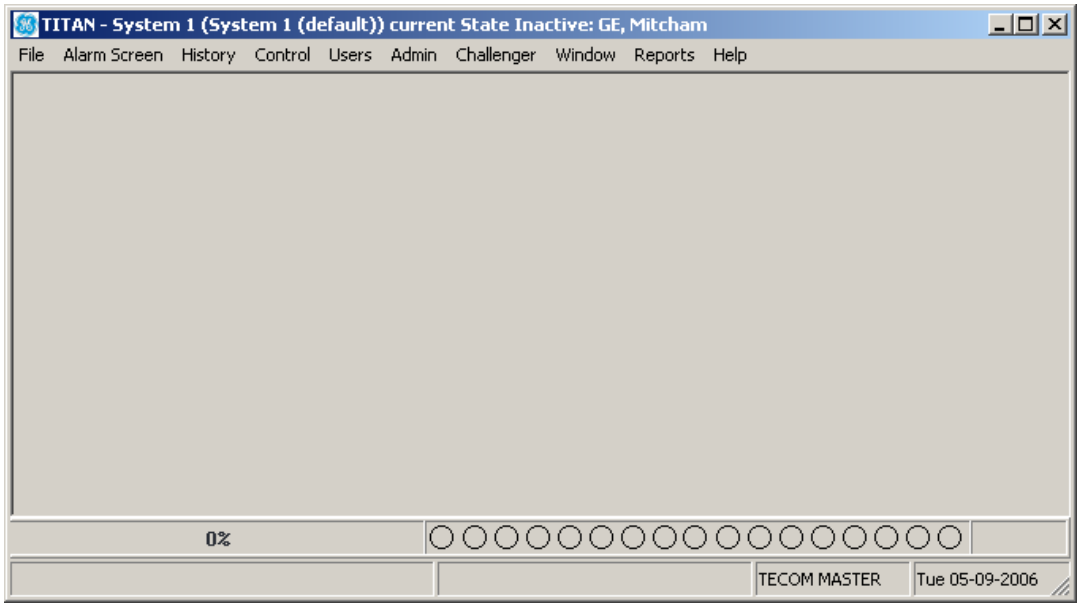


After the TITAN multi-user client computer connects with the TITAN multi-user server, or in the case of TITAN single-user, the TITAN login window appears (*Figure 2*).

Figure 2. Login window

TECOM MASTER is the default operator ID, and is not intended for normal use (the default password should be changed to protect the system). Your installer or administrator should have created an operator name and password for you already. If you do not know your operator and password information, contact your installation company; otherwise, enter your login information and click **OK**. The TITAN work area opens (*Figure 3* on page 5).

Figure 3. Work area for TITAN single-user



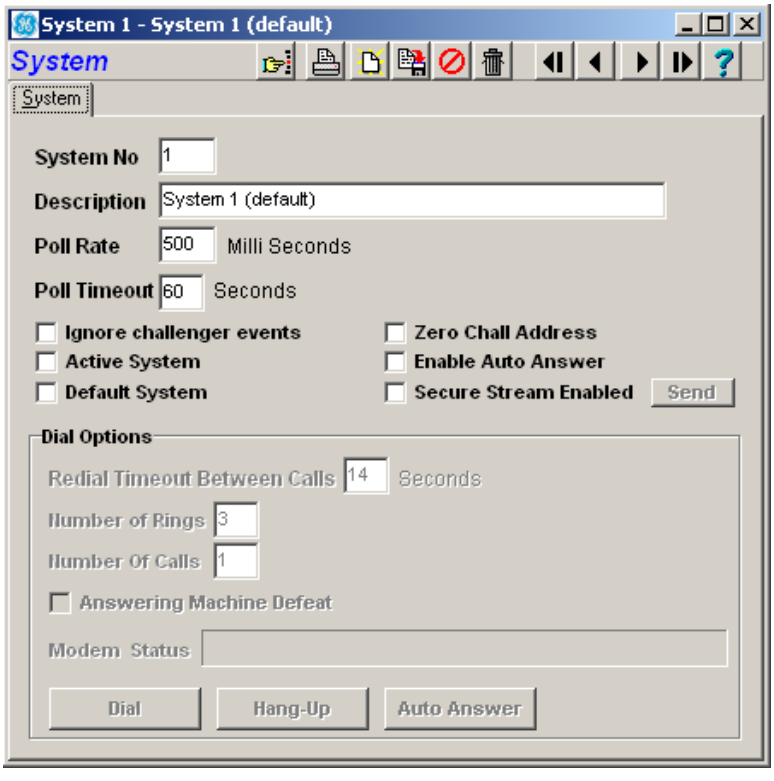
After login the menus and commands available to you as a TITAN operator depend on the menu permissions allocated to your operator record (see *Managing operator records* on page 78). Menus that are not included in an operator's permissions are grayed and unavailable when the operator logs in.

This manual, as with the *TITAN online help*, may describe features that do not affect you as an operator because of the menu permissions allocated to your operator record.

System selection

After you log on to TITAN, select the system you want to manage (*Figure 4*). Skip this step if you have only one system or if you are working on a multi-user client workstation.

Figure 4. System window for TITAN single-user



To activate a system and connect to a Challenger, do the following:

1. Go to **File > Open System** to open the *System* window, and use the toolbar buttons (see *Figure 6* on page 9) to select the system you want to work with. If there are multiple systems and you are unsure which system to use, contact your installation company.
2. Click the **Active System** check box to place a check mark in it.

3. Click **Save** to activate the system and connect to the system's Challenger panels.

For TITAN single-user, the state of the system's port connections display at the bottom of the TITAN work area (*Figure 5*).

Figure 5. Connection indicators for TITAN single-user

Connection indicators display the state of the system's port connections (direct, modem, card programmer, and TCP/IP). Each LED-like indicator corresponds with a TITAN port record, counting from left to right.

The colour-coded indications are as follows:

- Green—TITAN is communicating with the panel or card programmer.
- Red—TITAN has issued a command, and the panel or card programmer has not yet responded (rarely seen, usually only if an error exists). Prolonged display indicates a comms error.
- Yellow—The panel has transmitted an event. Prolonged display indicates a comms error.
- Blue—The panel has acknowledged a TITAN message.
- Grey—The corresponding port connection is unassigned.

Main menu

There are several menus in the TITAN application, many with submenus that display separate dialogue boxes with even more tabs. A brief summary of the functions available within each menu is listed below.

File. The File menu allows you to perform general system activities, such as perform system maintenance, upload from or download to Challenger panels, print all reports, configure user preferences, log off, and exit.

Alarm screen. The Alarm screen menu open the *Alarms* window, which displays a list of all alarms that were received by the computer. Use this menu to acknowledge alarms.

History. The History menu provides a live history log and history reports. The Challenger live history log is a record of events reported by Challenger panels, alarm acknowledgments, Challenger panel programming changes, and events manually added by operators, and updated in real time. History reports allow you to restrict history log data to certain types of events, which can then be generated into a printable report. The Full Log Upload option enables a technician to upload (without removing) alarm events and/or access events from one or more Challenger panels (available on TITAN single-user only).

Control. The Control menu is used to perform a variety of control functions for the many elements of the Challenger system. Use the control menu for such activities as locking/unlocking doors, setting or recalling the date/time from a Challenger panel, arming/disarming a floor, and isolating/deisolating an input.

Users. The Users menu contains data for all Challenger panel users, or cardholders, and is used to manage those users. This menu also allows you to edit door groups, floor groups, and holidays, and design card layouts using the *Card layout editor*.

Admin. The Admin menu lets you perform high-level administrative functions, such as configuring Challenger panel options or connection links, viewing/managing the Challenger command and timed command queues, creating and editing the system operators, setting alarms, user-defined fields, create departments, and displaying/editing system maps.

Challenger. The Challenger menu is used to program and manage the settings of the Challenger panels in your system. See *Challenger panel programming* on page 112 for details.

Window. The Window menu controls the way windows display within the TITAN software. You can use this menu to cascade or tile windows, arrange windows according to your own preference, or to minimize all windows.

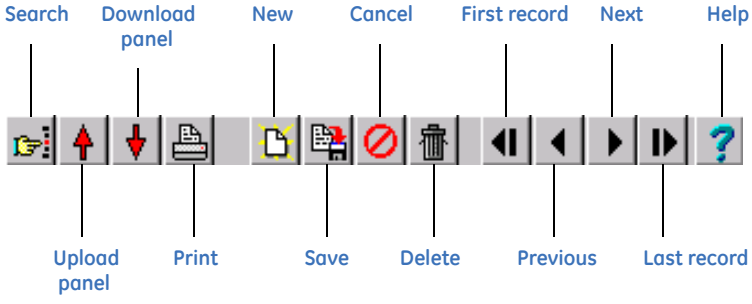
Reports. The Reports menu allows you to generate a variety of reports, including user reports that provide information about your cardholders, admin reports that display detailed system data, and Challenger reports that print programming details of a single panel. You can also view users by region and an event tree that displays a list of all event flags programmed in the Challenger panels.

Help. The Help menu can be used to open the TITAN help files. This menu also displays the version of your TITAN software.

Standard toolbar

Most windows in the TITAN software contain a standard toolbar used to perform basic functions (*Figure 6*).

Figure 6. Standard TITAN toolbar



Search. The Search button brings up a window that allows you to scroll through a list of records and select the one you want or type the record name and perform a search.

Upload from Challenger panel. The Upload button loads information from the Challenger panels in your system into your computer.

Download to Challenger panel. The Download button sends information from your computer to the Challenger panels in your system.

Print. The Print button prints the current record.

New. The New button creates a new record.

Save. The Save button saves the current record information.

Cancel. The Cancel button clears all changes made to the current record and resets any unsaved fields.

Delete. The Delete button deletes the current record.

First, previous, next, and last. These buttons are used to scroll through records.

Help. The Help button launches the online help information for the current window.

Chapter 2 Control system setup

This chapter explains how to set up your access and alarm control system, including how to set time zones and create door groups, floor groups, alarm groups, regions, and holidays.

In this chapter:

Access control

One of the key elements of the Challenger system is access control. Before you create users and issue cards, you need to determine which people need access to the various locations throughout the building during what times. Defining time zones allows you to determine the days and hours of access, while creating door and floor groups determines which people can access those doors/floors during those times. You can also define holidays and, if using a 4 Door/Lift Controller DGP, create regions for a higher degree of access control.

Creating time zones

The Challenger system uses two types of time zones: time zones based on specific time periods, and soft time zones based on events. This section describes how to program time zones.

Time zones are used to create time slots in which certain events can take place. For example, times to automatically arm areas, disable users or to activate relays to open a door. Time zones are assigned to alarm groups, door groups, floor groups, relays, arm and disarm timers, and out of hours access reporting to restrict or enable some Challenger panel operations during specific time periods.

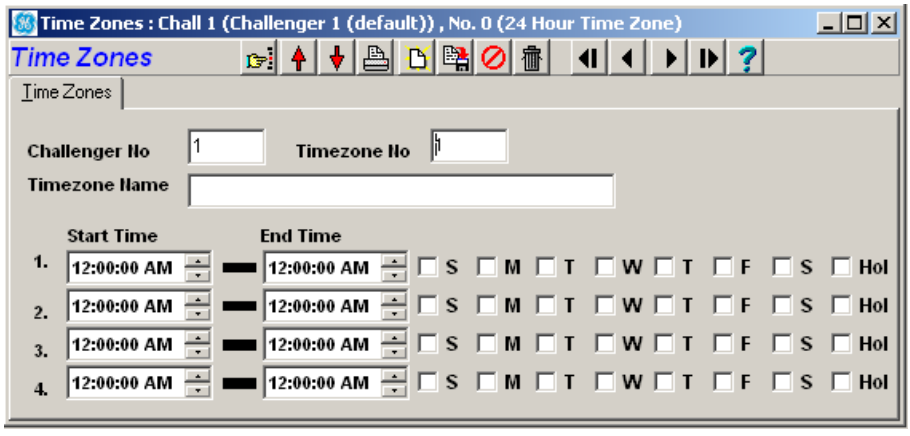
Time zone 0 is a 24-hour time zone (always valid) and is not programmable. Time zones 1 to 24 and are programmed for specific time periods. Each time zone is made up of one to four subtime zones containing: a start time, an end time, the weekdays that the subtime zone is valid, and an option to make the subtime zone valid on programmed holidays.

Challenger V8 panels using firmware version 8.128 or later, and fitted with TS0882, TS0883, or TS0884 memory modules, can have 46 time zones numbered 1 to 24 and 42 to 63.

To set up a time zone, do the following:

1. Go to **Challenger > Time Zones**.
2. In the *Time Zones* window (*Figure 7* on page 13), click **New**.

Figure 7. Time zones window



3. Double-click the *Challenger no.* field to select the Challenger panel you want to work with.
4. Enter a name for the time zone in the *Time zone name* field.
5. Edit the Start Time and End Time fields by clicking in each numerical field and over typing the entry or by using the up and down arrows to change the value. The Time Zones window displays a 12-hour clock with AM and PM fields.
   - A start time must be earlier than the end time.
   - There are four lines (subtime zones), the first of which must be completed.
   - The three additional subtime zones are used for time zones with multiple times or days.
   - Use consecutive subtime zones where the start time and end time are on different days. For example, to create a time zone that continues past midnight, you must define one subtime zone that ends at 11:59 PM, and a following subtime zone that begins at 12:00 AM on the next day.
6. Populate the check boxes for the days of the week on which you want the subtime zone to be valid.
7. Populate the **Hol** check box if you want the subtime zone to be valid on defined holidays (see *Creating holidays* on page 17). Leave the **Hol** check boxes blank if you do not want the subtime zone to be valid on a holiday.

8. Click **Save**.

Creating door groups

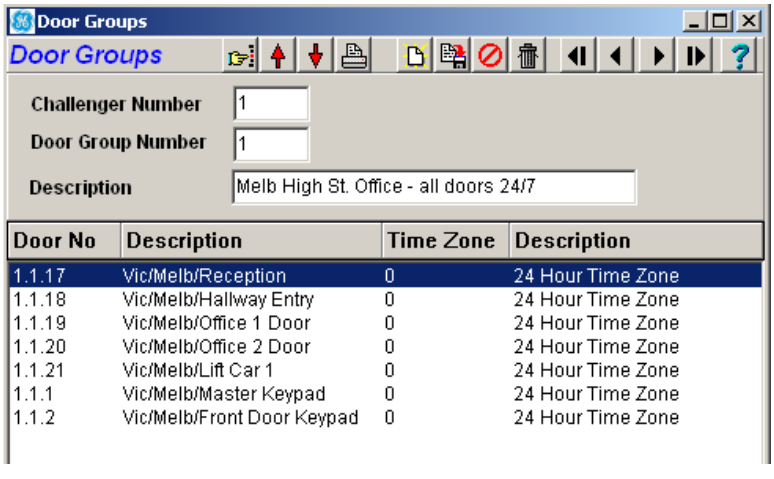
Door groups are used to specify when access to specific doors or lifts will be granted. After creating door groups, you can assign them to users. (For more information on assigning door groups to users, see *Chapter 3*, *Users* on page 23).

Challenger V8 panels using firmware version 8.128 or later, and fitted with TS0882, TS0883, or TS0884 memory modules, can have 255 door groups.

To create a door group, do the following:

1. Go to **Users > Door groups**.
2. In the *Door groups* window (*Figure 8*), click **New**.

Figure 8. Door groups window



3. Double-click the *Challenger Number* field to select the Challenger panel you want to work with.
4. Enter a name for the door group in the *Description* field.
5. From the list, select a door you want to add to the door group.
6. Right-click and select **Add time zone**.

7. From the *Time zone list*, select the time zone that corresponds to when the door group needs to access the door, then click **OK**.
8. Repeat steps four and five for each additional door you want to add to the door group.
9. Click **Save**.

Creating floor groups

Floor groups are used to specify when access to specific floors will be granted. After creating floor groups, you can assign them to users. (For more information on assigning floor groups to users, see *Chapter 3, Users* on page 23).

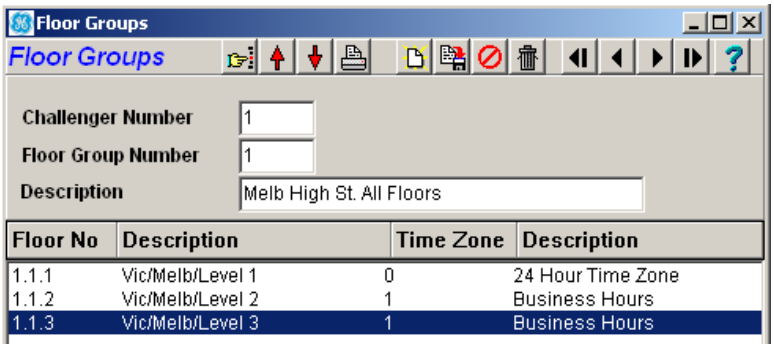
For a user to be given access to a floor, you must assign both a floor group and a door group. The floor group determines access to floors, and the door group determines access to lifts.

Challenger V8 panels using firmware version 8.128 or later, and fitted with TS0882, TS0883, or TS0884 memory modules, can have 128 floor groups.

To create a floor group, do the following:

1. Go to **Users > Floor groups**.
2. In the *Floor groups* window (*Figure 9*), click **New**.

Figure 9. Floor groups window



3. Double-click the *Challenger Number* field to select the Challenger panel you want to work with.
4. Enter a name for the floor group in the *Description* field.

5. From the list, select a floor you want to add to the floor group.
6. Right-click and select **Add time zone**.
7. From the *Time zone list*, select the time zone that corresponds to when the floor group needs to access the floor, then click **OK**.
8. Repeat steps four and five for each additional floor you want to add to the floor group.
9. Click **Save**.

Creating regions

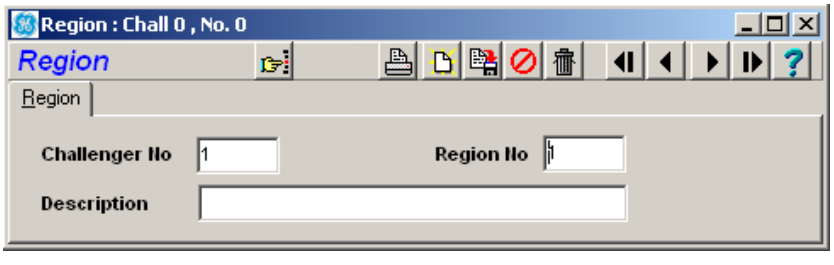
Regions are used by 4-Door/Lift Controller DGPs in combination with antipassback and also allow Challengers to report where users can be found. (See *Chapter 5, Reports* on page 57 for more information on the *Users by region* report).

Regions are assigned to individual doors in the 4 Door/Lift Controller DGP's doors menu.

To create regions, do the following:

1. Go to **Challenger > Intelligent Access Controller > Regions**.
2. In the *Regions* window (*Figure 10*), click **New**.

Figure 10. Regions window



3. Double-click the *Challenger No* field to select the Challenger panel you want to work with.
4. Enter a name for the region in the *Description* field.
5. Click **Save**.

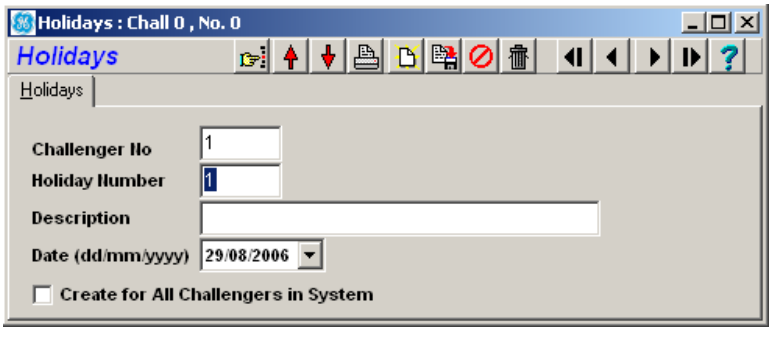
Creating holidays

You can create up to 24 different holidays for Challenger panels. Holidays can be used in conjunction with time zones to control access or alarm functions. For example, staff that are allowed access during normal weekdays can be denied access on weekdays that are holidays.

To create holidays, do the following:

1. Go to **Users > Holidays**.
2. In the *Holidays* window (*Figure 11* on page 17), click **New**.

Figure 11. Holiday window



3. Double-click the *Challenger No* field to select the Challenger panel you want to work with.
4. Enter the name of the holiday in the *Description* field.
5. From the drop-down list, select the date of the holiday from the calendar.
6. To create the holiday for all panels, check *Create for all Challengers in system*.
7. Click **Save**.

Alarm control

Alarm control in the Challenger system is managed by alarm groups. Alarm groups are usually programmed by the installer and allow users, inputs, and arming stations to control the Challenger panel system alarm functions.

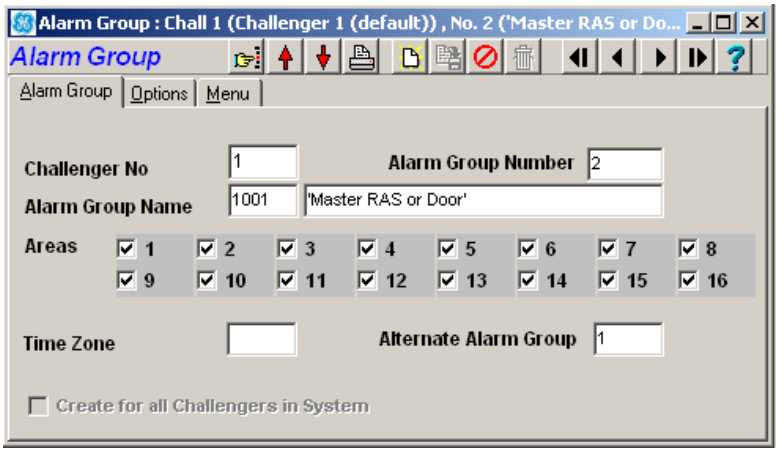
What is an alarm group?

An alarm group consists of specific areas, keypad menu options, panel options, and time zones that dictate a user's alarm control authorisation level. Alarm groups are assigned to users (see *Chapter 3*, *Users* on page 23 for more information) and to any equipment where users perform system functions, such as arming stations and doors.

Note: Any changes made to alarm groups will affect both the functions performed by users in that alarm group and the functions available at remote arming stations or door readers.

Go to **Challenger > Alarm groups** to open the *Alarm group* window (*Figure 12*).

Figure 12. Alarm group window



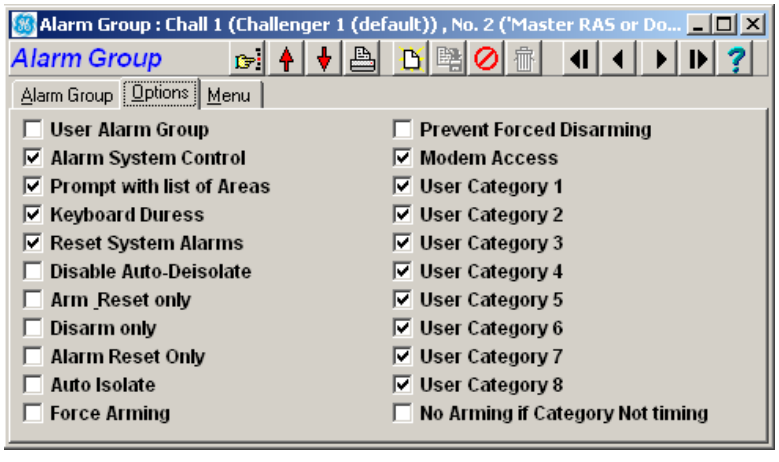
Double-click the *Challenger No* field to select the Challenger panel you want to work with.

There are three tabs in the *Alarm group* window.

Alarm group. This tab contains the general alarm group information, including the Challenger panel number, the alarm group number, name, and description, the areas and time zone assigned to the group, and the alternate alarm group number (*Figure 12* on page 18).

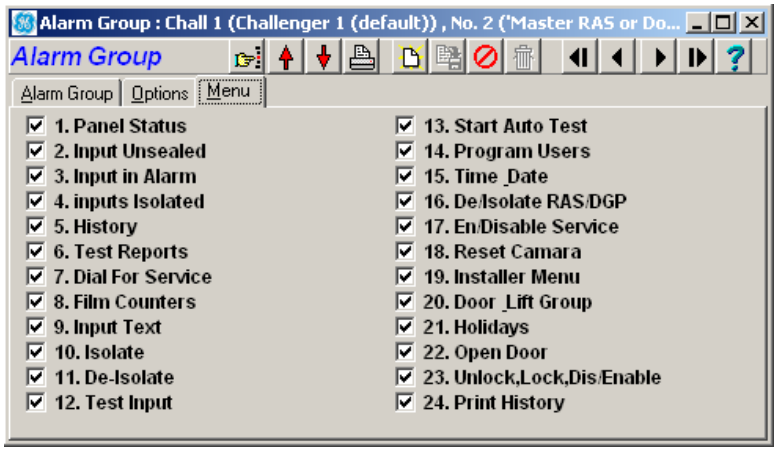
Options. This tab displays the panel options assigned to the alarm group (*Figure 13*).

Figure 13. Alarm group options



Menu. The *Menu* tab displays the keypad menu options assigned to the alarm group (see *Figure 14* on page 20). Menu options are assigned in accordance with the authorisation level of the alarm group; only installers should be assigned option 19, *Installer Menu*.

Figure 14. Alarm group menu options



Alarm group programming

Alarm groups 1 to 10 are hard-coded into the Challenger system and contain master control and default settings. They cannot be changed but can be viewed in the *Alarm group* window. Alarm groups 11 to 29 are preprogrammed with standard settings but can be changed if required.

Alarm groups 14 to 29 are preset for individual areas:

Alarm group	Area	Alarm group	Area	Alarm group	Area	Alarm group	Area
14	1	18	5	22	9	26	13
15	2	19	6	23	10	27	14
16	3	20	7	24	11	28	15
17	4	21	8	25	12	29	16

Alarm groups 30 to 138 (or 30 to 255, see below) are programmable to suit individual system requirements.

Challenger V8 panels using firmware version 8.128 or later, and fitted with TS0882, TS0883, or TS0884 memory modules, can have 255 alarm groups.

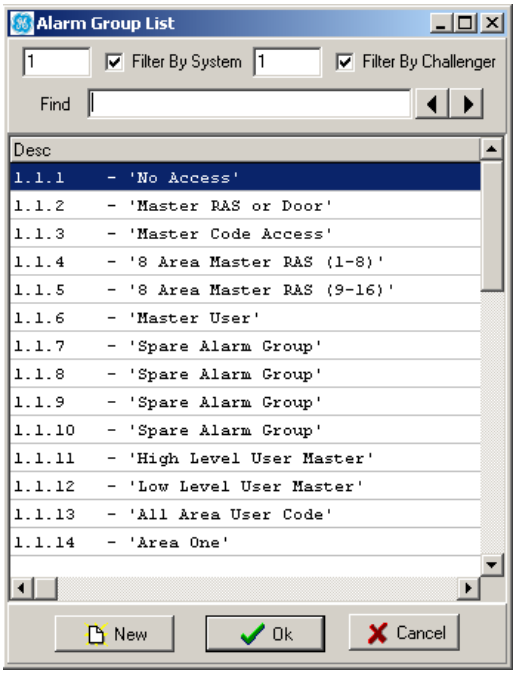
Managing alarm groups

In most cases, alarm groups will be configured and programmed by the Challenger installer. Because alarm groups are the key component of the entire alarm system, you must be careful when making changes to them. As noted above, any changes made to alarm groups affects not only the users assigned to the group, but also the corresponding remote arming stations or door readers. Check with your security installer before changing an alarm group.

To create an alarm group, click the **New** button at the top of the *Alarm group* window. Go through each of the three tabs to configure the settings for the alarm group, clicking the **Save** button before moving to the next tab.

To edit an existing alarm group, scroll through the alarm groups to find the one you want to change. You may also click the **Search** button to bring up the *Alarm group list* window (*Figure 15*). When you locate the alarm group you want to edit, select the alarm group name and click **OK** to display the alarm group in the *Alarm group* window. Make the desired changes and click the **Save** button for each tab.

Figure 15. Alarm group list



Chapter 3 Users

This chapter provides information about managing user records including how to create departments, create and edit users, and create user-defined titles.

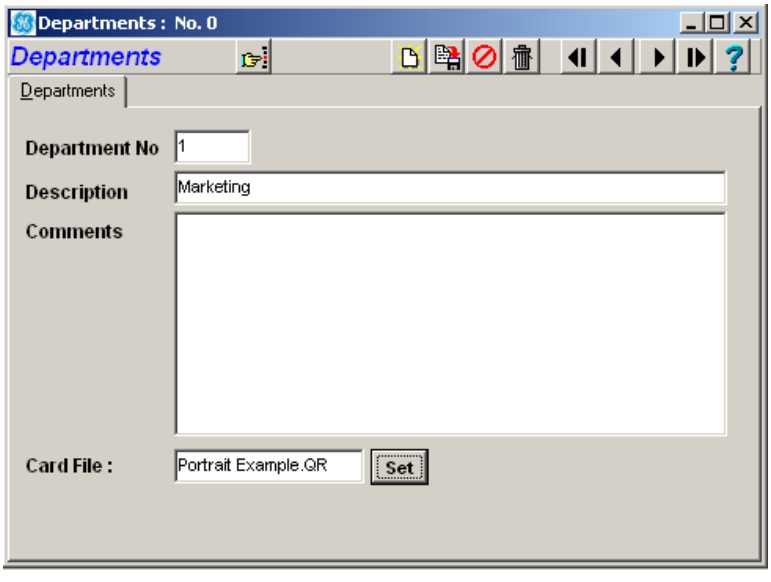
In this chapter:

Creating departments

Departments are used to associate users with photo ID card layouts. You need to define at least one department before you can issue security cards.

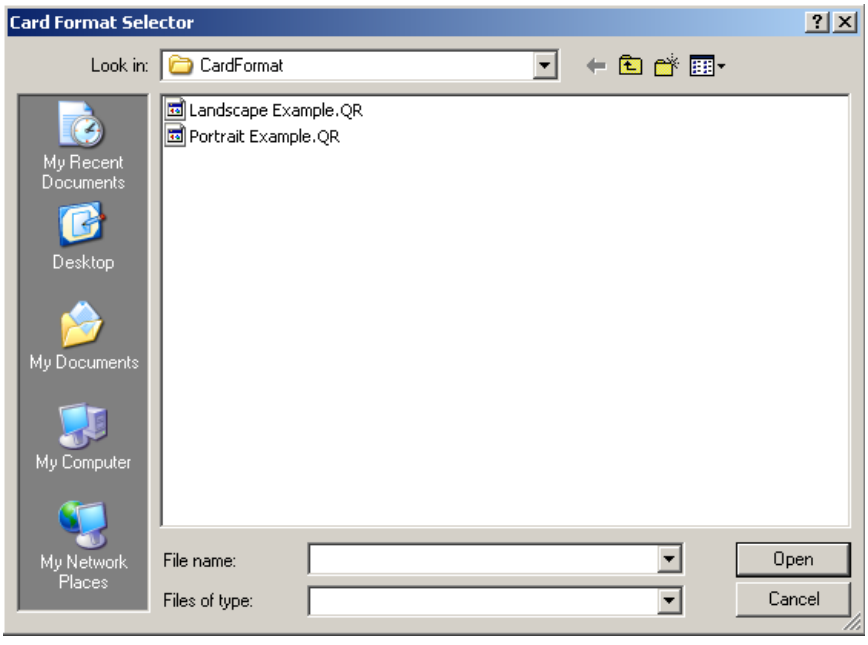
To create departments, select **Admin > Department** to open the *Departments* dialogue box (*Figure 16*).

Figure 16. Departments dialogue box



Click **New** to add a department. Enter the department name in the Description field and include any notes about the department under the Comments field. To link the department to a specific card layout, click **Set**. Select the card layout file from the *Card format selector* dialogue box. (*Figure 17* on page 25).

Figure 17. Card format selector



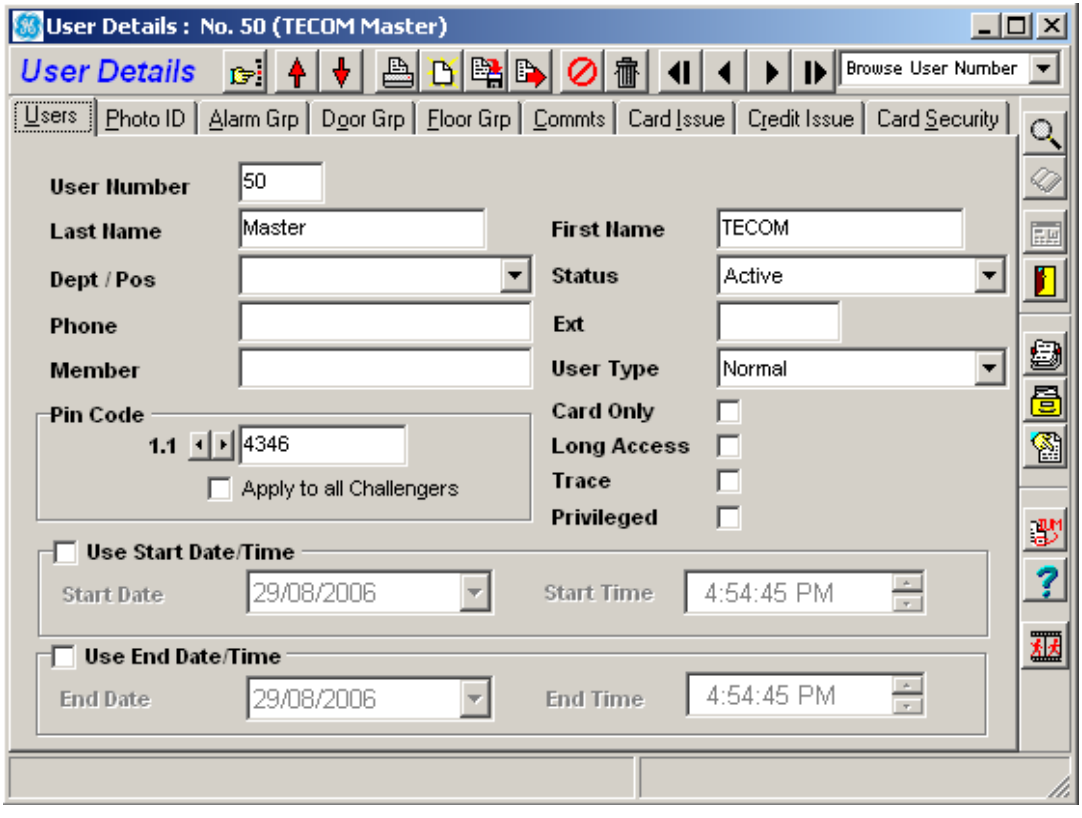
See *Designing a card layout* on page 44 for details about creating card formats.

Managing user records

One of the primary functions of TITAN is to manage user records. To do so, bring up the *User Details* window (*Figure 18*) by selecting **Users > Users**.

Note: The terms *operator* and *user* are not interchangeable for this application. *Operator* refers to system-level operation of the TITAN software; *user* refers to anyone issued a badge or allowed access in or out of the facility.

Figure 18. User details window

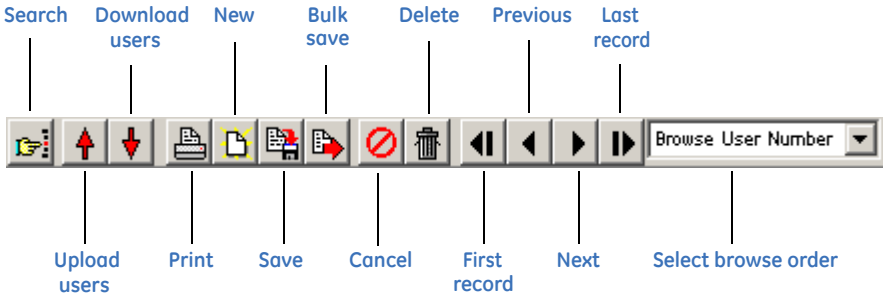


Let’s look at the buttons and tabs in the user details window.

Quick access buttons

The *User details* window has quick access buttons on the top (*Figure 19*) and right-hand sides (*Figure 20* on page 28) for common tasks. These quick access buttons are functional regardless of which window tab is displayed.

Figure 19. User details quick access buttons (horizontal)



Search. The search button at the far left brings up the *User list* window. This is equivalent to double-clicking the *User number* field on the *Users* tab.

Upload/download user data. The upload/download buttons are equivalent to **File > Upload... > Users** and **File > Download... > Users**.

Print. Prints the current user record information.

New. Creates a new user record.

Save. After making changes to a user's record, you must click this icon before moving to another tab or your changes will be lost.

Bulk save. Saves the current user and displays a *Bulk User Save* dialogue box. The *Bulk User Save* dialogue box enable you to:

- Apply the changes to all of the system's users or a range of user numbers.
- Create new user records based on the saved values (you will need to specify a range of user numbers).
- Generate card data for the new user records.

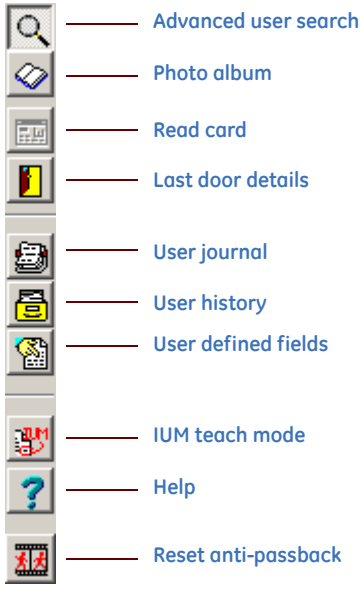
Cancel. Clears all changes made to the current tab of information. Resets changed but unsaved fields.

Delete. Deletes the current user record.

First, previous, next, last and browse selection. Unlike the browse buttons on most windows, the first record, previous, next, and last record buttons function according to the browse selection, as follows:

- When *Browse User Number* is selected, the records are ordered by the user number in the TITAN database.
- When *Browse Last name* is selected, the records are ordered by the user's last name.

Figure 20. User details quick access buttons (vertical)



Advanced user search. Click to open the *User search* window (*Figure 21* on page 29). This is different from the search button shown in *Figure 19* on page 27 in that it allows you to search for users based on any number of criteria (first name, last name, department, etc.). Refer to *TITAN online help* for details.

Figure 21. User search window

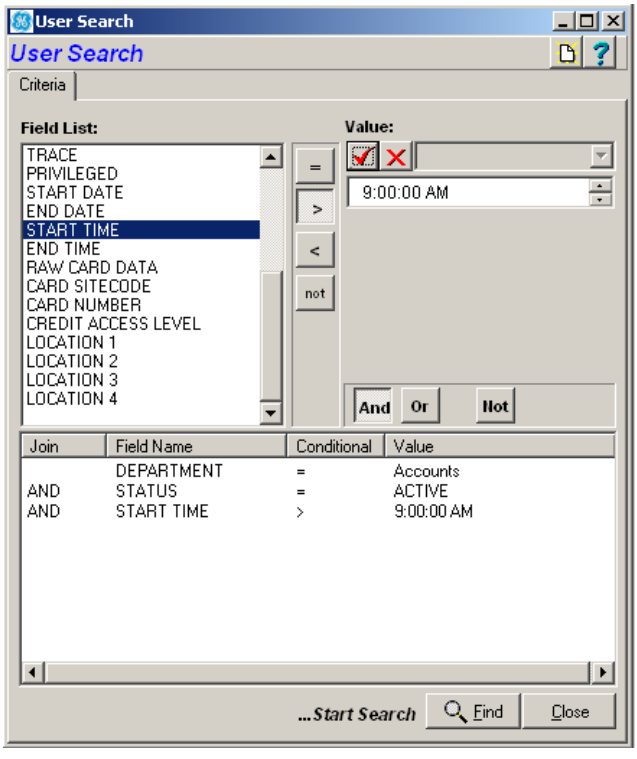


Photo album. The photo album is a collection of photos, user numbers and names for a group of users. The photo album allows you to preview or print a user photo album. This button is active after you find users via the *User search* window (*Figure 21*).

Read card. Reads the card on the card programmer and displays the card status.

Last door details. This button shows the last door the user passed through to exit the premises.

User journal. This brings up the *User journal* window, a history of all programming changes for the selected user. The user journal cannot be edited; it is a permanent record for that user number. If a user is deleted and later created again, the journal entries for that user number will remain intact.

User history. This button executes a powerful search that displays the current user's activities.

User-defined fields. User-defined fields allow you to append information—such as a second telephone number, car registration number, etc.—to an employee's record. (For information on adding titles to user-defined fields, see *Creating user-defined titles* on page 35).

IUM teach mode. Quick method of collecting a card's raw card data, see *Collecting raw card data in IUM teach mode* on page 38.

Help. Launches the *TITAN online help* for the Users window.

Reset anti-passback. Click to reset the user's region record when you need to clear an antipassback violation, see *Clearing an antipassback violation* on page 41. After resetting, the user record must be downloaded to the 4-Door/Lift Controller DGP.

User detail tabs

This section describes the tabs on the *User details* window.

Users tab. This tab lets you select from your list of existing users to make edits to their records or create new user records. Double-click the user number field to bring up the user list (*Figure 22* on page 34). Select the user you want to edit from the list or click **New** to create a new user record.

The following fields are located in the Users tab:

- **User number:** Identifies the user within the Challenger panel as a number. Used by the system to link a PIN or card to the functions it will perform and the doors it can enter.
- **User name:** Last name and first name of the user, with each field containing up to 20 characters (only 16 characters in total can be downloaded to a Challenger panel).
- **Dept/Pos:** Users can be assigned to departments to indicate the area where they work, and for assigning photo ID card layouts. (For information on creating departments, see *Creating departments* on page 24. For information on selecting an image for a photo ID card, see *Using a photo or captured image* on page 51).

- **Status:** Select the current status of the user record (active, void, lost, or expired). Only users with a status of active will be granted access through readers. If the user's start time is in the future, the status will be automatically set to void when the record is saved.
- **Phone, Ext,** and **Member** fields**.** Optional.
- **User type:** Defines the type of user for enhanced security. There are four user types:
  - *Normal*: Normal operation.
  - *Dual custody*: Requires two valid user codes/cards to perform any alarm or access control functions.
  - *Guard*: The user's code/card can only perform functions when performed in conjunction with a visitor's code/card.
  - *Visitor*: Requires a code/card from a Guard user type. See above.
- **PIN code:** A four to ten digit number assigned to users who need to operate arming stations (keypads). Challenger panels with expanded memory can have user-defined PIN codes for the first 1,000 users. Challenger panels with IUM can have user-defined PIN codes for all users (see *Table 2* on page 113 for details). Alternatively, this field may be used to record a non-Tecom magnetic swipe card enrolment number, read by the appropriate non-Tecom magnetic swipe reader.
- **Card only:** When checked, the user will not be able to use a PIN code. This allows the PIN code field to be used to program cards on formats not normally compatible with the Challenger panel, when a special reader is used.
- **Long access:** Allows extended door unlock times to provide disabled users a longer door opening time.

Note: Long access is only available on 4-Door/Lift Controller DGP readers.

- **Trace:** Causes a "trace" message to be sent to the Challenger system when alarm and access functions are performed by the user.

Note: Trace is only available on 4 Door/Lift Controller DGP readers.

- **Privileged:** If this box is checked, the user's card or PIN will override any "antipassback" restrictions.

Note: Privileged is only available on 4 Door/Lift Controller DGP readers.

Photo ID tab. Use this tab to create and issue a security card for your employee. (See *Creating and issuing cards* on page 51 for more details).

Alarm grp tab. The user's alarm group is used to assign alarm control and menu functions to the user. To select an alarm group, click **Add/edit** to open a list of available alarm groups. Select the required alarm group and click **OK**.

Door grp tab. This tab lists all the doors the user may access. Each door group may have a different time period (time zone) when access to the door will be granted. The user's door group determines which doors the user has access to and at what times. To select a door group, click **Add/edit** to open a list of available door groups. Select the required door group and click **OK**. Access to each door in a group may be restricted by a time zone.

Floor grp tab. This tab lists all the floors the user may access. Each floor group may have a different time period (time zone) when access to the floor will be granted. The user's floor group determines which floors the user has access to and at what times. To select a floor group, click **Add/edit** to open a list of available floor groups. Select the required floor group and click **OK**.

For a user to be given access to a floor, you must assign both a floor group and a door group. The floor group determines access to floors, and the door group determines access to lifts.

Commts tab. Use this field to keep a log of comments about the user (optional).

Card issue tab. This tab will only be of use when using card readers in combination with IUM modules installed, or the use of smart card being programmed with a smart card programmer. All details for the card can be edited.

From left to right, the columns show:

Challenger	The Challenger number
Status	The current status of the card (Active, Disabled, Void, Reassigned or Lost)
Raw card data	Shows a special number when an IUM is installed. Holds seven numbers, of which the highest gives the number of bits used. The others hold the card information (card number, site or facility code).
Card number	Holds the card number.
Site code	Holds the site or facility code.
PIN code	Holds the PIN code.
Status changed	Holds the date and time when the last status change has been made to this card user.
Programmed	Indicates if the card has been programmed (only valid for Smart Cards).

Buttons let you write card data to a smart card, cancel the changes, or erase the current card. (See *Writing smart cards or fobs* on page 55 for details).

Credit issue. Add credits to a user's account, if smart cards are used for credit purposes. Every user can have credits for up to four different accounts. (See *Using smart cards for credit* on page 52 for details).

Card security. Set the access level and the locations where the credits can be used. (See *Card security (location/access rights)* on page 54 for details).

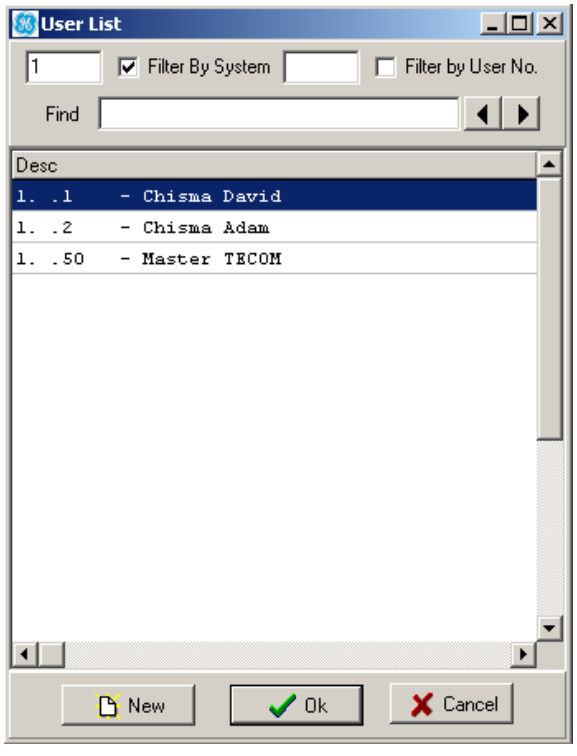
Managing user records

To create a new user record, click the **New** button at the top of the *User details* window. Follow through the tabs on the *User details* window and configure the settings in each field for that user.

To edit an existing record, scroll to the user record you want to change. You may also click either the **Search** button, which will bring up the *User list* window (*Figure 22* on page 34), or the **User search** button to search for the user's name or a part of the name.

When you locate the record you want to edit with either search method, double-click the user record or highlight the user record and click **OK** to display the record in the *User details* window. Make the desired changes and click the save icon to save the information.

Figure 22. User list

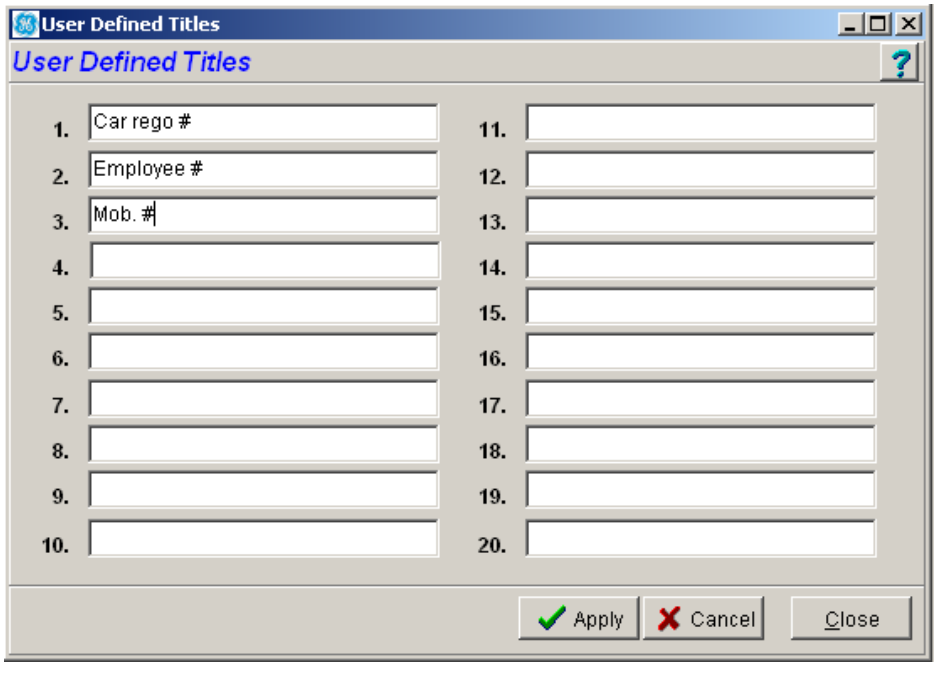


To delete a user record, locate the user record you want to delete (as explained above) and click the **Delete** button at the top of the *User details* window.

Creating user-defined titles

User-defined titles allow extra fields to be added to a user record, such as a second telephone number, license plate number, or employee number. To create titles for user-defined fields, click **Admin > User defined titles**. In the *User defined titles* dialogue box, enter the user-defined titles in the blank fields and click **Apply** (*Figure 23* on page 35).

Figure 23. User-defined titles



After the user-defined titles have been applied, they can be accessed in the *User details* window by clicking the **User defined fields** button. (See *Quick access buttons* on page 27*)*. Enter the information for each user-defined title, then click the **Save** button (*Figure 24* on page 36). The **User defined fields** button is also used to view user information that has previously been saved in the user-defined fields.

Figure 24. User-defined fields in User details record

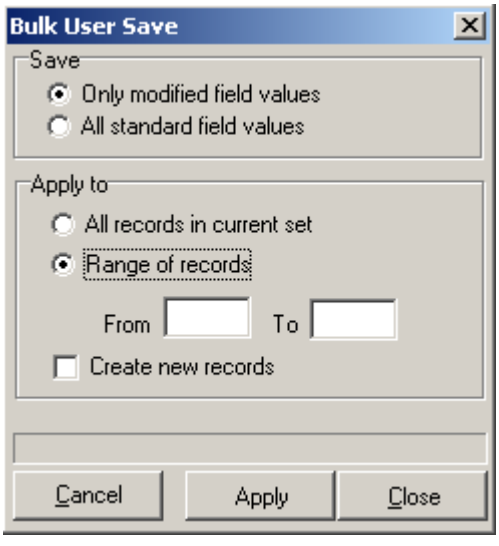
Managing user records in bulk

TITAN enables you to change details over a range of user records, or to create a range of new user records based on the currently-displayed user. For example, you can assign a door group to user number one, and by bulk saving, you can apply the door group to users from 1 to 1000 without having to add the door group to each user's details individually.

Bring up the *User Details* window (*Figure 18* on page 26) by selecting **Users > Users**, and then select (or create) the user record that you want to base the bulk operation upon.

Make the required changes and then click the **Bulk Save** quick access button (*Figure 19* on page 27) to open the *Bulk User Save* dialogue box.

Figure 25. Bulk User Save dialogue box for bulk save



The *Bulk User Save* dialogue box enables you to:

- Apply the changes just made to the specified users.
- Apply all the current user programming to the specified users.
- Apply the changes to all of the users, or a range of user numbers, in the current set. The current set may be the results of an advanced user search, for example, all users belonging to a specific department.
- Create new user records based on the saved values (you will need to specify a range of user numbers).

Click **Apply** to perform the selected bulk function.

New user records will not overwrite existing user records. For example, if you attempt to create users 1 through 10 and users 1, 2, and 3 already exist, new records will be created for only users 4 through 10.

Advanced user procedures

The following sections describe how to perform some of the more advanced operator tasks involving user records.

Collecting raw card data in IUM teach mode

The IUM teach device allows you to collect raw card data from cards with a known or unknown format, simply by badging the card at a RAS or door you choose. This method is much faster than copying the raw card data from the event history file and pasting it into the the *Raw Card Data* field in the *User Details* window (Card Issue tab).

To collect raw card data in IUM teach mode, do the following:

1. Go to **Admin > Challenger > Options tab** for an IUM Challenger.
2. In the **IUM Teach Device** field, type the number of the RAS or door you want to use to extract the raw card data from the card.
3. Click the **IUM format** arrow and select the format that suits the card. If you don't know the card format, select **User Defined**.
4. Click **Save**.
5. Go to **Users > Users** and navigate to the user record to be assigned the card.
6. Click the **Card Issue** tab and select the Challenger that controls the RAS or door that you specified as the IUM teach device. Press the CTRL key and select any additional Challengers that will need to use the card.
7. Click the **IUM Teach Mode** button (see *Figure 20* on page 28).
8. Badge the card at the IUM teach device. The raw card data displays in the *Raw Card Data* field in the *User Details* window (Card Issue tab).
9. Click **Save**.

Adding a set of cards with a different site code

The Challenger panel will accept smart cards that use two different site codes. The initial site code is called A and the second site code is called B.

The second batch of cards will likely use a range of card ID numbers that aren't consecutive with the first batch, or that overlap. A site offset is used to adjust the card ID numbers in order to make the user numbers consecutive and to avoid overlaps. Site offset numbers may range from -32,767 to +32,767. The site code values (supplied with the cards) and site offsets are programmed in the Challenger's system options.

In order to know what offset number to use, you need to know what the next user number should be and what card ID number the site B cards begins with. Expressed as a formula, the calculation is

First card ID number + (or -) site offset number = next user number

For example:

- If you want the next user number to be 101, and the second batch starts at card number 1, you need an offset of 100 (1 + 100 = 101). In this case, you would enter 100 in the **Offset B** field (as shown in *Figure 26* on page 40).
- If you want the next user number to be 101, and the second batch starts at card number 1001, you need an offset of -900 (1001 - 900 = 101). In this case, you would enter -900 in the **Offset B** field.

The Challenger panel will calculate the user number from:

Card ID number + (or -) site offset value = user number

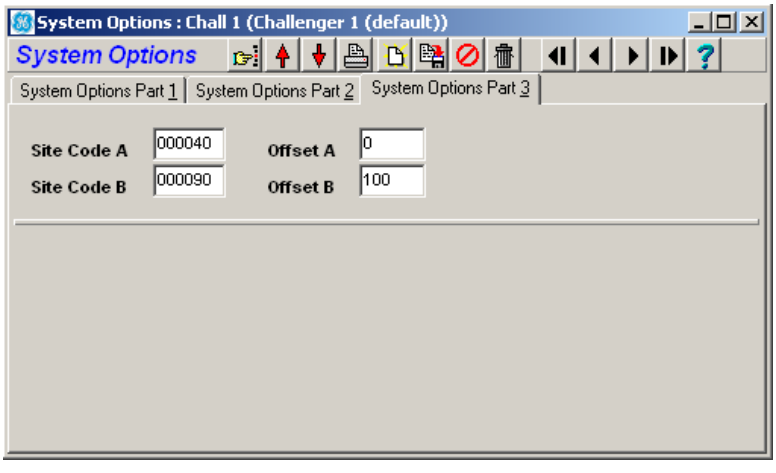
If the required offset is outside of the range -32,767 to +32,767, TITAN automatically adjusts the offset value when the record is saved. For example:

- a (within range) value of 32,767 is saved as 32,767
- an outside range value of 32,768 is saved as 0
- an outside range value of 32,769 is saved as -32,767
- an outside range value of 32,770 is saved as -32,766

To use the a batch of cards with a different site code, do the following:

1. Go to **Challenger > System Options > System Options > System Options Part 3 tab**.
2. If not already programmed, type the old cards' site code in **Site Code A** using leading zeros if necessary so that the number is six digits (for example, 000040).
3. Type the new cards' site code in **Site Code B** using leading zeros if necessary so that the number is six digits (for example, 000090).
4. Type the offset value to use for site B the **Offset B** field (for example, 100). See *Figure 26* on page 40.
5. Save the record.

Figure 26. Site codes and offsets



Clearing an antipassback violation

Antipassback controls the operation of a reader if a card or PIN is used to attempt to enter a region that the user is currently assigned to.

Entering a region twice in succession may be prevented if hard antipassback is programmed for the door. For example, if a user leaves a building without using their card at the reader, when they return they may be denied access because the system still has the user assigned to the region inside the building.

In such a case, it will be necessary to reset the user's region code. The user may do so themselves by using the card at a different reader that resets their region code (for example, the user could enter the premises via a different external door that is not programmed for antipassback).

Alternatively, the operator can click **Reset anti-passback** in the *User Details* window (*Figure 20* on page 28), and then download the user record to the Challenger panel (and therefore to the 4-Door/Lift Controller DGP connected to the reader).

Updating raw card data

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. As of panel firmware version 8.128, Challenger panels that are not fitted with TS0883 or TS0884 hardware IUM modules can be programmed to use software IUM.

Use the *Update Raw Card Data* command to create or update raw card data for all user records or a defined range of user records for one or more Challenger panels.

Use the following steps to update or generate IUM data:

1. Select **Users > Update Raw Card Data**.
2. In the list of Challenger panels, select *all panels* or a particular panel, as required.
3. Select either *All records in current set*, or *Range of records in current set*, as required.
4. If you select *Range of records in current set*, specify the range of records in the **From** and **To** fields.

5. A Challenger panel that has card readers connected directly to it (via RAS numbers 1 to 16), will have at least one site code (called site number when programming via a RAS). If applicable, select either *Site Code A* or *Site Code B*, which will be used to generate the raw card data.
6. Alternatively, select the **Update using** radio button, and then:
   - Click the Card Type arrow and select the required card format.
   - Type the Site Code value (the acceptable range of values depends on the selected card type).
7. Check the **Overwrite Raw Card Data** selection box to create raw card data, replacing any exiting raw card data. Alternatively, if the selection box is cleared, raw card data will be created only for cards that do not already have raw card data.
8. Click **Update** to execute.

Chapter 4 Security cards

A *security card* is typically a smart card with a user's details (such as name and photograph) printed on it. However, that is not always the case: a "smart card" might be in the form of a key fob, and a "security card" might be an ID card without a photo or smart card functionality.

In this chapter:

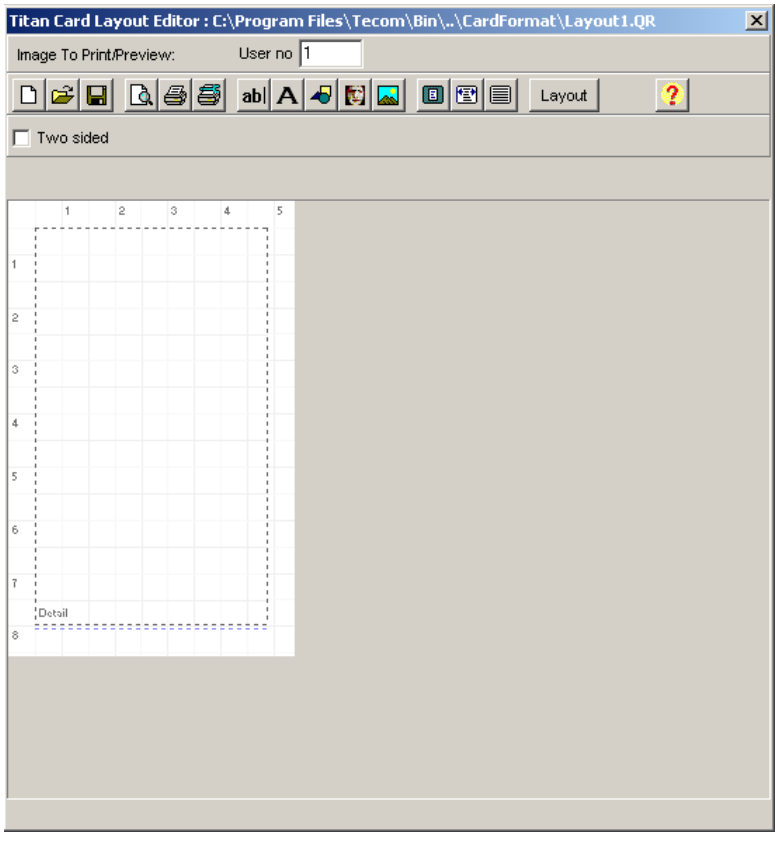
Designing a card layout

TITAN has a layout tool option (TS9006 Photo ID) that allows you to create your own card design for your photo ID cards. When licensed, the Card Layout Editor allows you to:

- Automatically add user details to each card from the users database.
- Add text labels.
- Add shapes, database images, backgrounds and graphics, and format these shapes.
- Save the card layout.
- Print photo ID cards on a card printer.

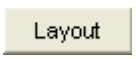
Select **Admin > Card layout editor** to bring up the *Card layout editor* window (*Figure 27*).

Figure 27. Card layout editor



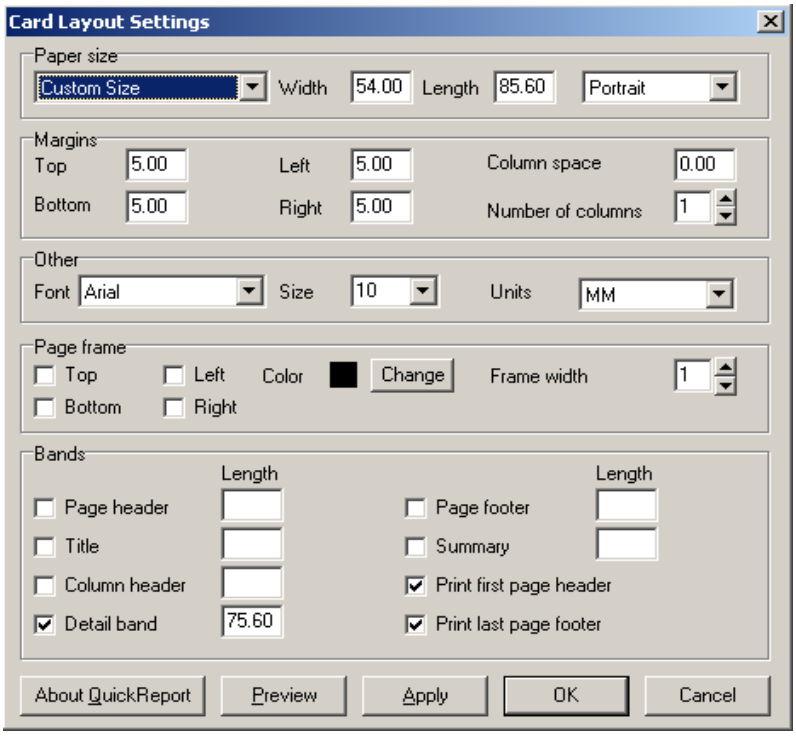
The *Card layout editor* has buttons that are used to create or edit card designs (*Table 1*).

Table 1. Card layout editor buttons

Button	Function
 New	Creates a new card layout
 Open	Opens a previously saved card layout
 Save	Saves the current card layout
 Print preview	Previews the current card layout before printing
 Print	Prints the current card layout
 Print setup	Configures printer settings
 Add db field	Adds a database field or function to the card layout
 Add label	Adds normal text to create labels in the card layout
 Add shape	Adds a shape to the card layout (circle, rectangle, lines)
 Add db image	Defines an area on the layout to place the user's image
 Add image/background	Adds an image or background to the card layout
 Fit height	Fits card layout view to window height
 Fit width	Fits card layout to window width
 No scaling	Displays card layout at full size
 Layout	Opens the card layout settings dialogue box (*Figure 28* on page 46)
 Help	Opens the Card layout help topic.

Click **Layout** to open the card layout settings dialogue box that allows you to configure the card layout settings, including the card size, margins, fonts, and orientation. (*Figure 28*).

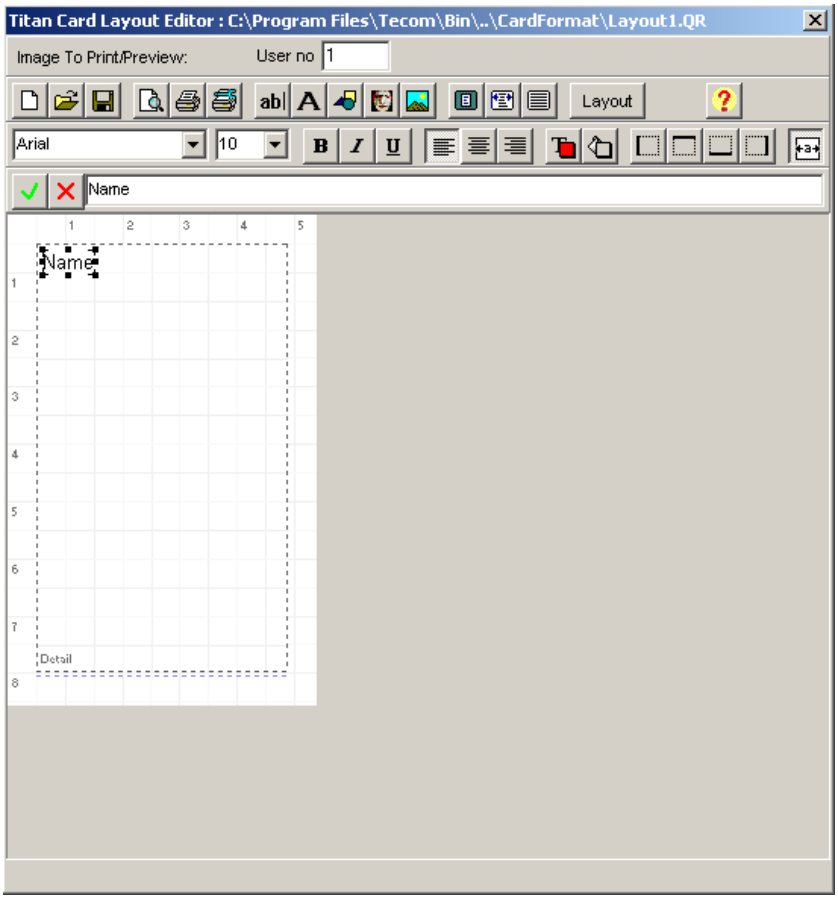
Figure 28. Card layout settings window



To design a card layout, do the following:

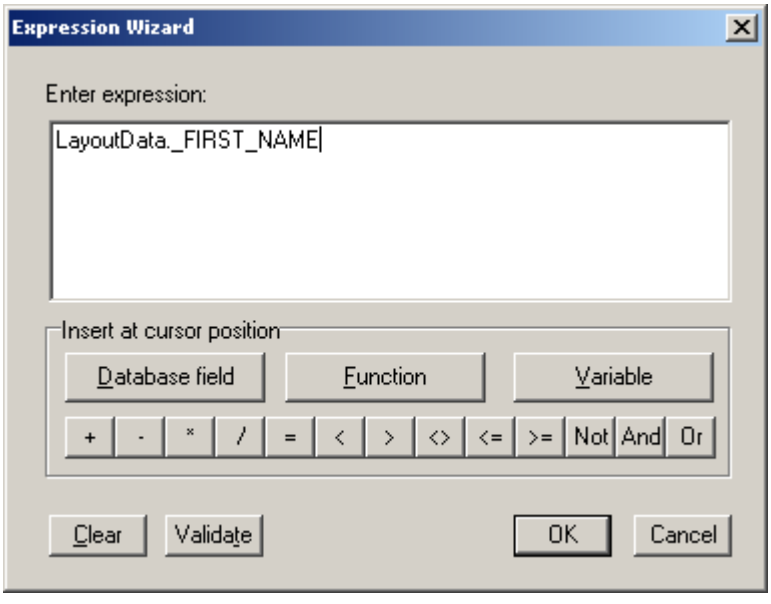
1. Click the **New** button to create a new layout, or click the **Open** button to open and edit an existing card layout.
2. Click the **Layout** button to bring up the card layout window. Use this dialog to configure the card size and settings, then click **Apply**. Click **OK** to close this window.
3. Click the **Add image/background** button to add a background or an image to the card layout, such as the company logo. New options appear under the main toolbar. Click the **Load image...** button to browse for and load the image. Check the boxes next to *Autosize*, *Center*, and *Stretch* to format the image.
4. Click the **Add label** button to add a text label, such as “Name” or “Department.” Click in the card layout where you want to place the label, using the grid for alignment. After you insert the label, new options appear in the *Card layout editor* that allow you to format the text (*Figure 29* on page 48). Click in the blank field in between the main toolbar and the text formatting toolbar and highlight the word “none.” Replace the text with your own label, then click the green check button to activate the change. Use the text formatting toolbar to format your new label.

Figure 29. Add label window



5. Click the **Add db field** button to add corresponding database fields next to the labels you created. This loads the user data directly from the user database. Click in the card layout where you want to place the database field, using the grid for alignment. New options appear in the *Card layout editor*, similar to the Add label options. Click the ***fx*** button above the card layout to open the *Expression Wizard* window (see *Figure 30* on page 49).

Figure 30. Expression wizard



6. In the *Expression Wizard* window, click **Database field** to access the user database. From the list of available fields on the right, select the database field that corresponds to the label you created, then click **OK**.
7. Use the *Expression Wizard* buttons to refine the database fields. For example, *Figure 30* contains the simple expression `LayoutData._FIRST_NAME`, which would print a users' first names on cards. If you want to add to the expression, click + to add another field, function, variable, or fixed text (fixed text must be enclosed in a pair of single quote marks).

   Any text characters that are not contained in the database fields are considered as fixed text, even a space character. So if you wanted to print users' first names followed by their last names, and separated by a space, the expression would be

   ```
   LayoutData._FIRST_NAME + ' ' + LayoutData._LAST_NAME
   ```

8. After you've built your expression, click **Validate** to check it.

9. Click **OK** again to close the *Expression Wizard*. The field now appears in the card layout. Use the formatting toolbar to format the field, then click the green check button to activate the changes.
10. To add a place for user photos in the card layout, click the **Add db image** button. Click in the card layout where you want to place the photo, then use the grid to align it.
11. Click the **Print preview** button to preview the current card layout for the selected user number.
12. Click **Close** and change the user number field to preview another user.
13. When you are satisfied with the layout, click **Save**.

When you issue cards, you can specify different designs for different users and different privileges.

Creating and issuing cards

This section describes how to set up and print a layout on a user card. See *Writing smart cards or fobs* on page 55 for details about programming smart cards.

Using a photo or captured image

To create and issue security cards containing a user's photo, select **Users > Users** and then click the *Photo ID* tab in the *User details* window (*Figure 31*).

Figure 31. Photo ID tab

The first step is to acquire a digital image of the user—either in JPEG or BMP format—and store it in a central location. By default TITAN looks for user photographs in:

```
C:\Program Files\Tecom\PhotoID
```

However, you can save your employee photos anywhere that you can browse to.

If you have a video camera connected to your computer, click **Capture** to view, freeze, and then save an image file of the user. Alternatively, click **Load** to use a previously-saved image file. Use the cropping square to center the image then click **Accept**.

Clicking **Issue** will show a print preview for the user's security card. You must have the card printer set as your Windows default printer, and the user must be assigned to a department that has a designated card file (layout). If you are content with the preview, make sure your card printer is ready and click the **Print** button to produce the security card.

Using smart cards for credit

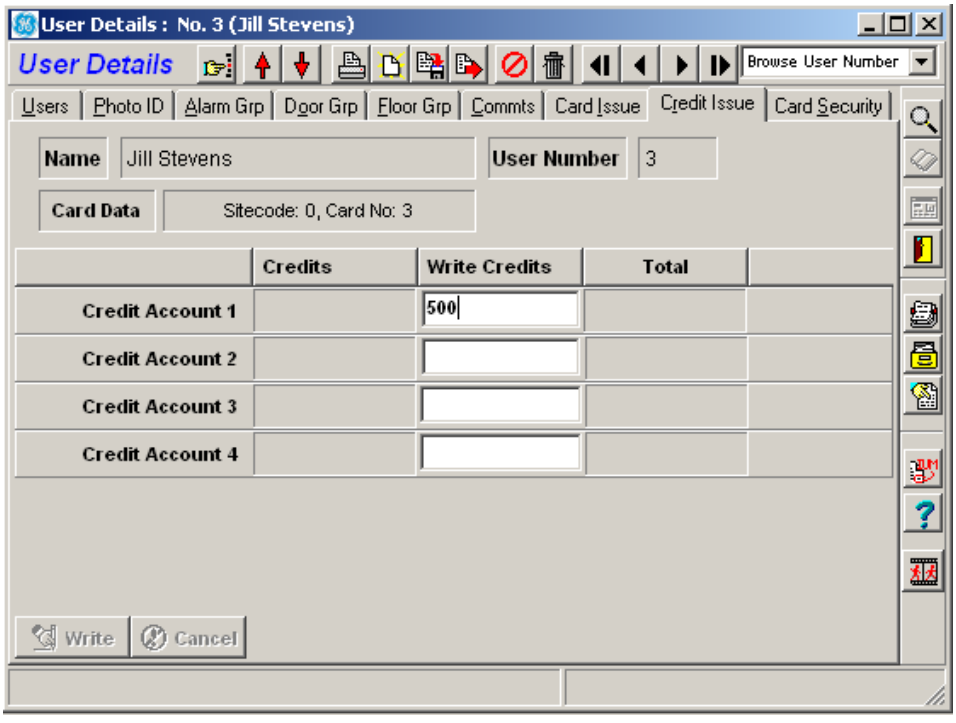
Smart cards or fobs may be used for resource control (credit use). For example, a tennis court may issue smart cards to members in order to operate lighting at night. The credit functionality could, for example, provide 10 hours of lighting before the card would have to be 'recharged'.

Note: Smart cards do not offer the same functionality as genuine credit cards (such as Visa, Mastercard, American Express, etc.). In the context of smart cards, 'credit' refers to token values allocated to a card and 'credit accounts' refers to groups of credits. GE recommends that smart card credit functionality is not used for high-value transactions, and not used simultaneously with access control functionality.

Your installer may help you set up Challenger smart card readers to work with credits programmed into your users' smart cards. Users can use these cards to "purchase" items or services—such as copies on an office copier, vending machine items, prepaid meal tickets, parking meter time, and after-hours time extensions for extra HVAC and lighting. Challenger administers these services through the users' smart card credit accounts.

To change a user's smart card credits, select the user in the *User details* window and click the *Credit issue* tab (*Figure 32*).

Figure 32. Credit issue tab



Type the required number of credits into the appropriate credit accounts fields (up to 65,534 in total). You can change the four credit account names from the defaults (Credit account 1 through Credit account 4) to something more representative of your site, such as Photocopier and Drinks Machine. Go to **Admin > Card programmer > Define credit units** to change the credit account names.

When you are sure of the values in each account, click the **Write** button at the bottom left of the window to write the new values to the smart card or click **Cancel** to cancel the action. If a card's credit is depleted or if a user wants to purchase additional credits, you must rewrite the cards through the same process. (See *Writing smart cards or fobs* on page 55 for details on writing cards).

Note: Placing a total of 65,535 credits on a card will turn the card into a "master" card that may be used without credits being deducted.

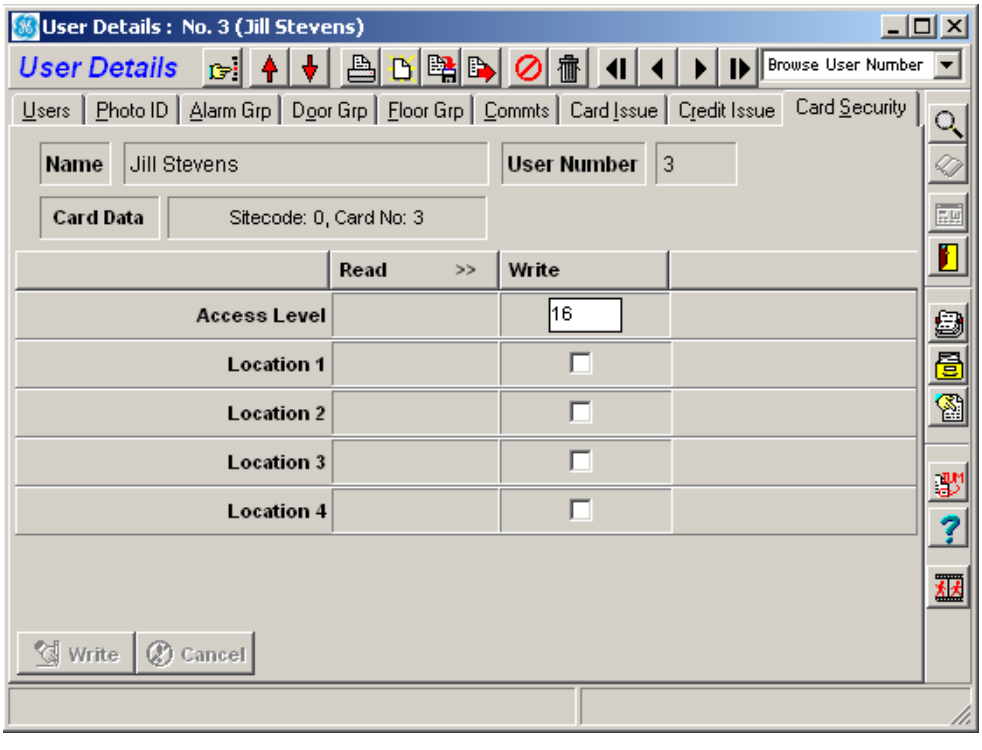
Card security (location/access rights)

For credit use, Challenger uses a location name and an access level of 1 to 16 to determine whether a card can perform a transaction at a particular reader.

- First, the location name designated for the card must match the location name designated for the reader.
- Second, the access level designated for the card must equal or exceed the access level designated for the reader.
- Third, the number of credits available on the card must equal or exceed the number of credits required by the reader's programmed token value as the ‘cost’ of the transaction.

To set location and access rights for a user, select the *Card security* tab (*Figure 33*).

Figure 33. Card security tab



You can change the four location names from the defaults (*Location 1* through *Location 4*) to something more representative of your site, such as *Front Office*, *Factory*, *Store Room*, and *Executive Suite*. Go to **Admin > Card programmer > Define location rights** to change the location names.

Determine the location and access for each user, then check the appropriate boxes and enter the access level value in the *Write* column. When you are sure of the values in each account, click the **Write** button at the bottom left of the window to write the new values to the smart card or click **Cancel** to cancel the action.

Writing smart cards or fobs

Use a TS0870P smart card programmer connected to the TITAN computer to program (write to) smart cards or fobs.

The smart card programmer must be correctly installed, configured, and activated. Refer to the *TS0870P Installation Guide* or *TITAN online help* for details.

To write a card (for example, to program a photo ID smart card, or to add account credits, reduce hours, move to a different area, etc.), do the following:

1. Lay the card on the smart card programmer.
2. Click the **Write** button in the *Card issue* tab, the *Credit issue* tab, or the *Card security* tab.

Chapter 5 Reports

This chapter provides an overview of TITAN reports, including user, admin, Challenger, users in regions, and the event tree reports, and provides instructions for using the *Print all reports* feature.

In this chapter:

Reports menu

There are over 40 different reports you can generate through TITAN. Each one provides you with a hard copy record of your system's settings and events. You can also save reports in electronic format by clicking **Print** and then clicking the **Save Report** button in the print preview window.

The report generator is preformatted, so you don't have to worry about creating a report template. All you need to do is select the data you want to print. The headers will list the date and time of the printing.

User reports

User reports display Challenger panel user information and are accessed by selecting **Reports > Users**. The following user reports can be run:

- **Users:** Displays details, including photos, for a range of users or all users. Check *Sort Alphabetically* to display users sorted by name or click *Sort by Department* to sort by all or by a selected department. Select *New Page* to start each department's users on a new page (see *Figure 34* on page 59).
- **User summary:** Displays summary data for a range of users or all users of a specified Challenger (see *Figure 35* on page 59). The selection options are similar to the Users report.
- **Door groups:** Lists door groups, including the door group name, the doors included in the group, and the corresponding time zones.
- **Floor groups:** Lists floor groups, including the floor group name, the areas included in the group, and the corresponding time zones.
- **Holidays:** Displays holiday details, including the holiday name, number, and date.
- **In Group:** Displays users according to the alarm group, floor group or door group they belong to.

See also *User history by department* on page 66.

Figure 34. User report window

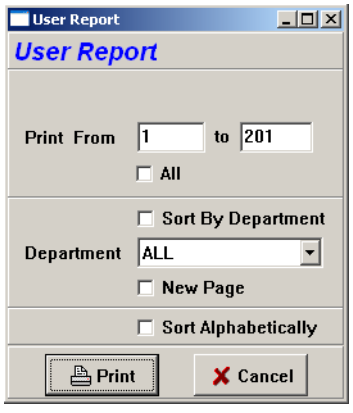
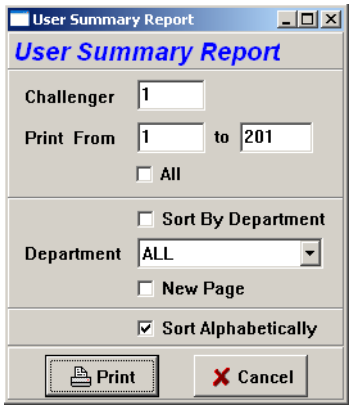


Figure 35. User summary report window



Admin reports

Admin reports display Challenger system details and are accessed by selecting **Reports > Admin**. The following Admin reports can be run:

- **System:** Lists data about each system defined in TITAN, including system number and description, polling details, and whether Challenger events are being ignored.
- **Challenger:** Displays details for Challenger panels, including the panel description, location, and communication mode.
- **Ports:** Displays port details, including system, port, and comms port numbers, description, baud rate, and communication mode.

Challenger reports

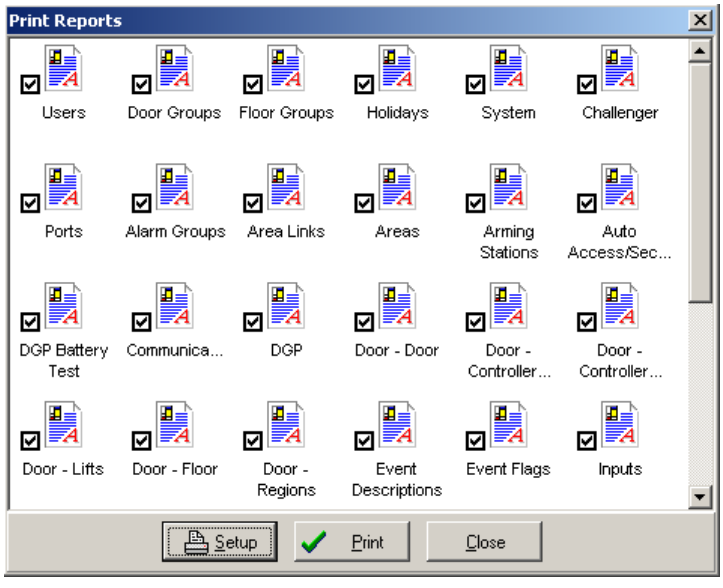
Challenger reports print programming details of a single Challenger panel and are accessed by selecting **Reports > Challenger**.

Some examples of Challenger panel reports are: Alarm groups, Area links, Areas, Arming Stations, Communications, DGP, and so on.

Print all reports

If you need to print and archive all your settings, or you want to print several reports at once, select **Reports > Print all...**. This will bring up the print reports window (*Figure 36*).

Figure 36. Print all reports window



Uncheck the reports you don't want and click **Print**. Click **Setup** to configure the printer or **Cancel** to exit the print routine without printing.

Users by region

The Users by region report lists all regions used in 4-Door/Lift Controller DGPs and displays a list of users currently in each region. Check *Sort by Department* to sort by all or by a selected department. Select *New Page* to start each department's users on a new page.

To access this report, select **Reports > Users by Region**.

Note: Doors on the 4-Door/Lift Controller DGP must be programmed with in/out regions for this report to function correctly.

Muster

Generates a report based on a region, showing users inside or outside a given region. To access this report, select **Reports > Muster**.

Event tree

The Event tree report displays a list of all event flags programmed into the Challenger panels and where they are used. To access this report, select **Reports > Event tree**.

History menu

Custom history reports

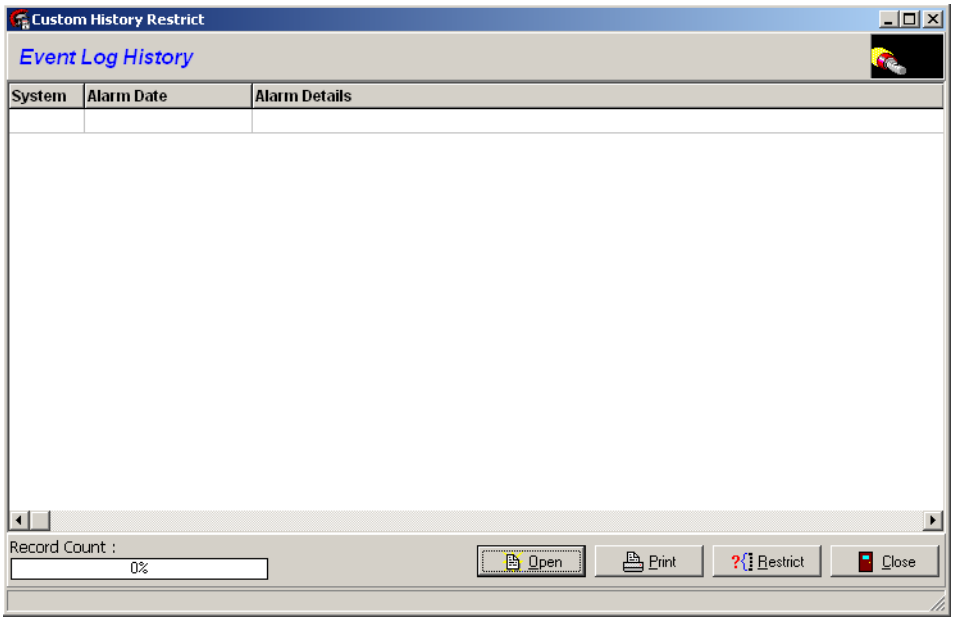
You can view or print a custom history report from either:

- Data contained in the live event log
- Saved data.

To create a custom history report, do the following:

1. Go to **History** > **Reports** > **Custom**. The *Custom History Restrict* window displays (*Figure 39*).

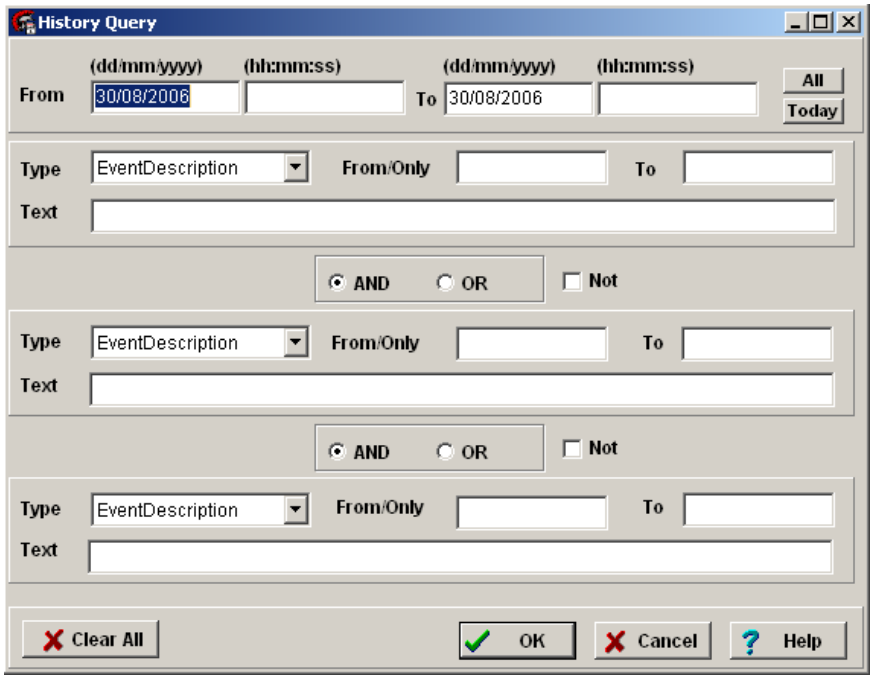
Figure 37. Custom History Restrict window (initial state)



2. If you want a report based on data contained in the live event log, click **Restrict** to open the history query window (*Figure 38* on page 64).

3. Alternatively, if you want a report based on previously saved data, click **Open** to select the history file. The path and filename of the open file displays below the record count display. Click **Restrict** to open the history query window.

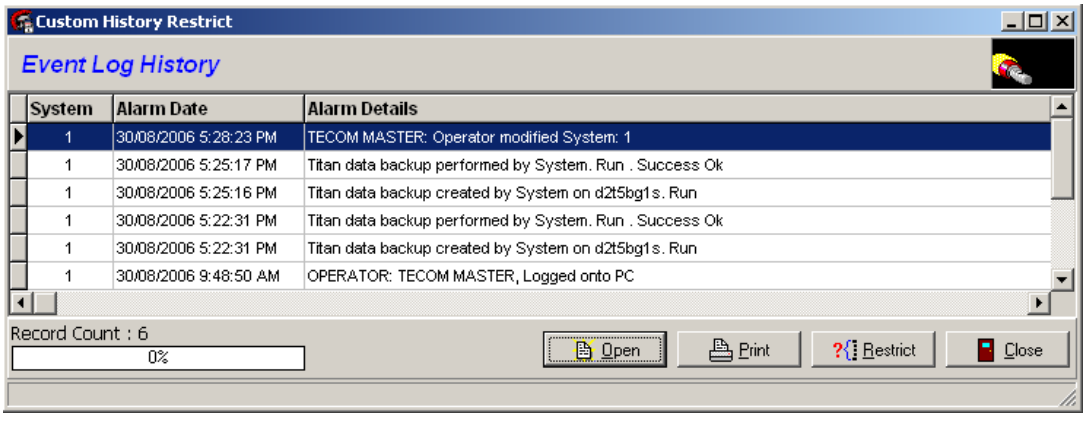
Figure 38. History query window



4. Enter the time period that you're interested in. Alternatively, click **All** or **Today**.
5. In the *Type* field, select *User* if you want to track a particular user or group of users, *Door* to check on a specific door, or any of the other selections.
6. Right-click the *From/Only* fields to select the required item or to begin a range of items.

7. If you want to limit your search more precisely, use one or both of the boolean (AND, OR, NOT) selectors on the lower half of the window.
8. When you're finished defining the report click **OK**.
9. The results display in the custom history restrict window (*Figure 39* on page 65). Double-clicking any of these entries will bring up a window explaining the details of the event.

Figure 39. Custom history restrict window (populated)



10. Click **Print** to see a print preview for the report (if *Print Preview Reports* is selected in *User Preferences*).
11. If you are content with the preview, make sure your printer is ready and click the **Print** button in the preview window, or click the **Save** button to save the report.

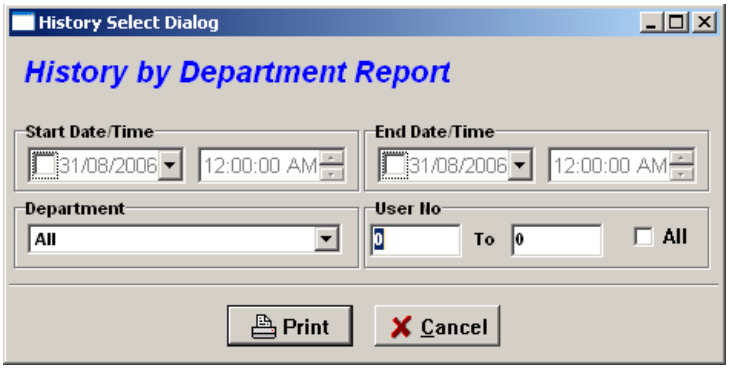
User history by department

Generates a report of user history events over a defined time span, and sorted by:

- Department, or for all departments
- User number, or for all users

To access this report, select **History > Reports > User History by Department** (*Figure 40*).

Figure 40. User history by department report window



Chapter 6 Operation

This chapter explains how to run some common tasks, such as controlling the system, responding to alarms, and accessing TITAN alarm and event records via the History menu.

In this chapter:

Operating TITAN

This section explains how to perform common tasks in TITAN, such as arming an area, isolating an input, responding to alarms, and accessing alarm and event records.

Using the Control menu

Most of the options in this menu allow you to send commands to your Challenger or groups of Challengers. You can choose which items to send commands to, pick from a variety of everyday security commands, and you can even check the status of each item to make sure they have been updated.

A TITAN operator may have permissions to control the system, including, for example, arming an area, isolating an input, or opening a door (operators without control permission will not have access to the Control menu).

The Control menu has many options. We'll describe only a couple here to show you how it works. Control options can also be accessed via map icons (see *Managing system maps* on page 80).

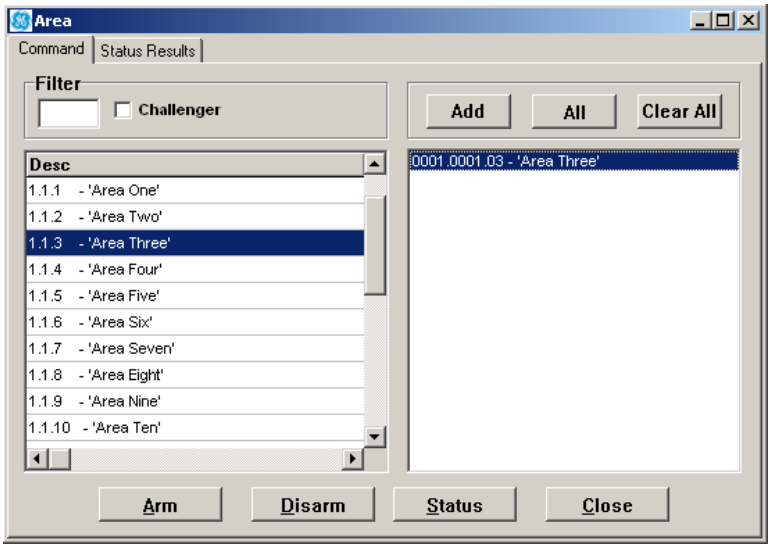
Arming an area

You can control which areas in your system are armed and disarmed.

To control an area, do the following:

1. Go to **Control > Area** to open the *Area* window (*Figure 41* on page 69).

Figure 41. Area window



2. Double-click an area listed in the left-hand side of the window to copy it to the right-hand side.
3. Click **Arm** to send the command to the Challenger for the items in the right-hand side of the window.
4. Click **Status** to display the events or current status of each area.

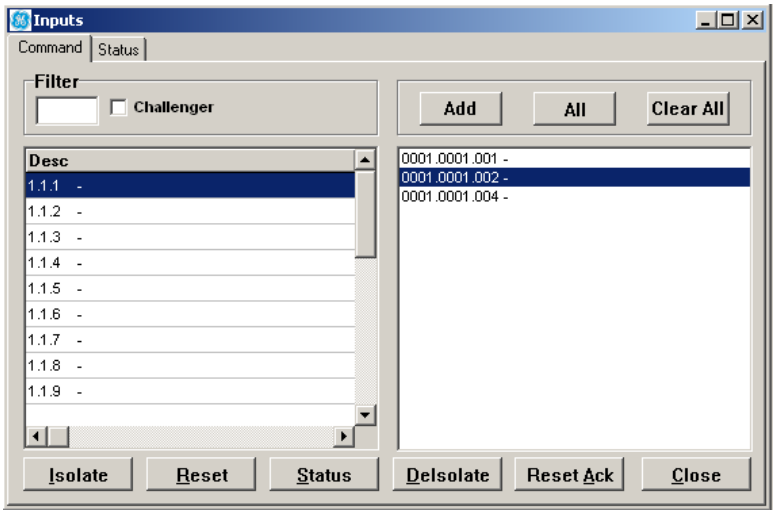
Isolating an input

You can work with your installation company on occasions when you need to isolate your security system. For example, to stop a faulty sensor from reporting while the system is armed, your installer can arrange to isolate the input associated with the sensor. The input can be reactivated when the fault is corrected.

To isolate an input, do the following:

1. Go to **Control > Input** to open the *Inputs* window (*Figure 42* on page 70).

Figure 42. Inputs window



2. Double-click an input listed in the left-hand side of the window to copy it to the right-hand side.
3. Click **Isolate** to send the command to the Challenger for the items in the right-hand side of the window.
4. Click **Status** to display the events or current status of each input.

Responding to alarms

Your security dealer will work closely with you to define the types of warnings and alarms needed for your business. This might be as simple as generating an exception report (such as keeping track of all the "Access Denied" card readings on certain doors) to sounding a local alarm and calling the police.

Your installer can set up a map (a floor plan or picture of your facilities) and mark it with icons so that you can see which devices are in alarm status. You and your installer may also load the system with preprogrammed instructions to follow when certain alarms occur. For example, if a storeroom door is forced open, your system could advise you to call the department manager and give you the manager's name and phone number. See *Managing alarm 'help action' messages* on page 72 for details.

Your system will prompt you with an alarm screen when an alarm is activated and needs a response. If your system has site maps, the appropriate map may appear when an alarm is triggered. You can click the map navigation buttons to page through additional maps.

You must acknowledge any alarms that are triggered on your security system. To acknowledge an alarm, double-click the alarm to bring up the *Alarm Acknowledgement* window with details of that alarm and any preprogrammed instructions (such as manager names and phone numbers). You can annotate details about the alarm and your response in the *Alarm Acknowledgement* window. These notes will be saved in the history log.

After you acknowledge the alarm, the *Alarm Acknowledgement* window and all associated instructions, floor plans, etc. will disappear. When you have finished adding notes and performing any preprogrammed instructions called out in the *Alarm Acknowledgement* window, click **OK** to send your alarm acknowledgement to the history log and reset any inputs that are in alarm.

Note: If your system has been programmed to remind you about alarms, it will automatically realarm after a preset time unless the cause has been fixed, no matter how many times you acknowledge the alarm.

To view a list of all alarms received by TITAN, select the **Alarm screen** menu to bring up the *Alarms* window. Double-click an alarm in the list to bring up the *Alarm Acknowledgement* window and display the details of the alarm.

Remote dial-up connection

It is possible to set up your Challenger system so that you can call in from a remote location and check the system. Ask your security dealer how to configure your system to accept remote calls. Your computer modem must be able to communicate at 300 bps or 2400 bps (depending on the panel version) in order to connect with a Challenger panel.

Managing times and dates

Operators can synchronise the time and date used by Challenger panels to the time and date used by TITAN.

Select **Control > Time & Date** to open the *Date & times* window. On the left-hand panel, scroll to the required Challenger panel and double-click to add it to the right-hand panel (repeat for additional Challenger panels if required). Select either the computer system time

or enter a user defined time, and click **Set** to send the time/date set command to the Challenger panels.

You can check a Challenger panel's time and date by using the **Recall** command.

Recording manual events

Operators can enter messages (recorded with their name) into the history log.

Select **Control > Add manual incident** to open the *Manual incident* text entry window. Type a message (typically a description of the event) and click **Add**.

Managing alarm 'help action' messages

Alarms for inputs can display help action messages in the *Alarm acknowledgement* window.

Alarm help action messages are typically set up by your installer or security dealer. The information in this section is provided in case you need to, for example, change the help action message displayed in the *Alarm acknowledgement* window.

Help action messages are contained in text (.txt) files stored in the folder *C:\Program Files\Tecom\Bin\InputHelp* and associated with an input in the *Input details* window.

To create or edit a help action message for an input, select **Challenger panel > Input database** and navigate to the required input record. The *Help filename* field displays the path and name of a text file, if already programmed. Use the buttons next to the *Help filename* field to either locate a new text file or to open the existing text file for editing. Text can then be entered and saved for this input.

Record-keeping

The History menu provides access to records of all acknowledged alarms and system events via the following menu options:

Live Event Log. The Live Event Log is a fast and simple way to determine the location of the input that caused an alarm. It is a real-time record of various TITAN events, including:

- Events reported by the Challenger(s) in your security system.
- Alarms that have been activated and acknowledged.
- Challenger programming changes performed by your TITAN software.

Double-click an event in the log to display the event along with any alarm response details entered when the alarm was acknowledged.

User Journal Viewer. The User Journal window displays a history of all programming changes for user records. It is updated every time a user's details are changed. Select the relevant entry and click View to display the user's details as of a particular date.

Reports. See *History menu* on page 63 for details of history reports.

Full Log upload. The Full Log Upload option enables a technician to upload (without removing) alarm events and/or access events from one or more Challenger panels.

Uploaded event logs are displayed in the Full Log Upload window. Displayed logs can be saved for later filtering and viewing in Event Log History window.

Note: Full Log Upload requires Challenger panel firmware 8.112 or later.

Chapter 7 Administration

This chapter explains how to perform administrative functions in your TITAN system, such as connecting to Challenger panels, maintaining operator records, modifying system maps, maintaining the database, importing or exporting system data, and maintaining Challenger panels.

In this chapter:

Administering your TITAN system

The *Admin* menu contains advanced functions that allow you to administer your system. This sections in this chapter describe the following administrative tasks:

- *Connecting to Challenger panels*
- *Viewing and managing command queues*
- *Managing operator records*
- *Defining alarms*
- *Managing system maps*

Connecting to Challenger panels

Connections and initial setup of your system should only be attempted by your supplier or trained personnel.

TITAN is typically connected to Challenger panels directly via serial connection (default setting). However, in the case of TITAN single-user the following additional connection types may be used:

- By modem to a Challenger's on-board modem, or to a separate modem attached to the Challenger via a computer interface. Your modem must be able to communicate at 300 bps or 2400 bps (depending on the panel version) in order to connect with a Challenger panel.
- By TCP/IP to a Challenger's TS0898 Ethernet Interface.

By using serial and/or TCP/IP connections, you can connect to multiple (up to 16) Challenger panels simultaneously. GE recommends that you do not exceed 16 simultaneous connections. When connecting via modem, only one Challenger may be connected at a time.

Refer to *TITAN online help* for details about connecting to Challenger panels.

Viewing and managing command queues

Command queue

Select **Admin** > **Command queue** to display the *Command queue* window.

The command queue lists all commands waiting to be sent to all Challenger panels in a system. A blue (progress) bar at the bottom of the screen indicates that commands are waiting in the queue. Commands will be sent to the Challenger panels the next time the system is active and connected.

The command queue is saved as part of the system: if you switch to a different system or if you log off, the original system's command queue will be displayed next time the system is opened.

Use the command queue toolbar buttons to:

- Delete a selected command.
- Clear all commands from the queue.

Timed command queue

Select **Admin** > **Timed command queue** to display the command queue times window.

The timed command queue works in the same way as the command queue, but this one lists commands that are awaiting scheduled activation.

For example, if two employees are to start next Tuesday, 26th of October, and their user settings and cards have already been created, the commands to activate these cards will remain in the timed command queue until Tuesday, 26th of October when they are moved into the command queue for downloading to the Challenger panel.

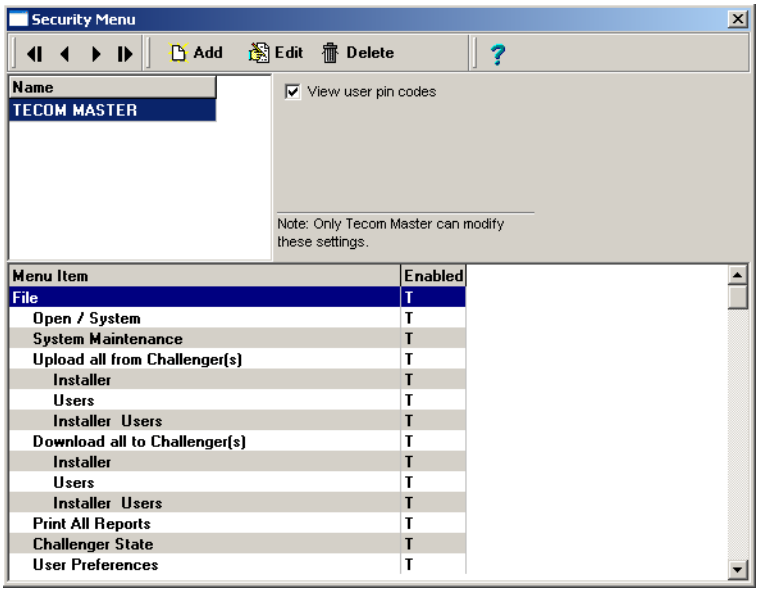
Managing operator records

Operators are typically set up by your installer or security dealer. The information in this section is provided in case you need to, for example, add a new operator or change a password.

An operator is a person (such as an installer, security personnel, or administrator) who can log into TITAN.

Select **Admin > Security menu** to manage operator records, including passwords and the Challenger menu options that operators can access. The *Security menu window* opens (*Figure 43*). Menus that are not included in an operator's permissions are grayed and unavailable when the operator logs in.

Figure 43. Security menu window



Adding an operator

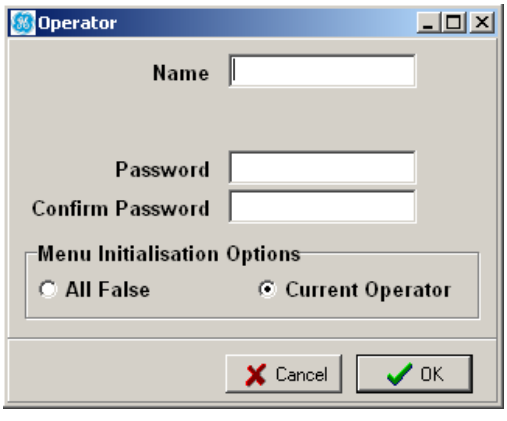
The Security menu window displays a list box of operator records. The default TECOM MASTER operator record is provided with TITAN.

Note: The default operator is configured with the default Challenger panel password. Please take care that the password is changed before leaving your system unattended!

To add a new operator on the system, click **Add** from the *Security menu window* (*Figure 43* on page 78) and an empty details window will appear allowing you to enter the new operator's details.

You have the option of setting all menu options to False, or to the same as yourself (current operator), with the exception of *view user PIN codes*, which can be enabled only by the TECOM MASTER operator.

Figure 44. New operator dialog



Type the new operator's name (TITAN uses only capital letters in operator names), and password.

Below the user name is a list of every Challenger menu option. By double-clicking on an option, that option is toggled between T (user has access) and F (user does not have access). An operator's menu permissions both simplify the choices that an operator has to make in their work, and protects the integrity of the TITAN system.

An operator is not allowed to change the T/F value of a menu option that they do not have access to. For example, if I do not have access to the 'Challenger' menu, then I cannot change it on other peoples' permissions.

Editing an operator

To change an operator's password, click the operator's name and then click **Edit**. To modify an operator's access, click the operator's name and then check or clear menu options displayed for that operator. You cannot grant another operator more menu permissions than you have.

Defining alarms

The system and panel events that are received by TITAN and are reported to the operator as alarms are typically set up by your installer or security dealer. The information in this section is provided in case you need to change which events are reported as alarms.

Go to **Admin > Set alarms** to configure which events reported by the panel are treated as alarms in TITAN. Use the scroll bar or the Find window to find an event, and then double-click it to toggle between Yes (alarm event) and No (not an alarm event) states.

Select **Close** to save changes and to close the window.

Managing system maps

Maps are typically set up by your installer or security dealer. The information in this section is provided in case you need to, for example, replace a map's background image (bitmap file) for changes in your premises.

Maps are graphical images consisting of a bitmap image file typically representing a building floor plan or site, with icons representing Challenger devices such as areas, inputs, or doors that are added to the map in TITAN. The icon images can be easily changed if required.

The map (bitmap plus icons) can be used to identify the location of alarms, respond to alarms, and to issue control commands to the system. If the system contains multiple maps, icons can also enable the operator to quickly move between maps by clicking the icon (instead of using the navigation buttons at the top of the *Display maps* window).

A map can be set as a default map to display when an operator logs in (*Show default map* must be selected in **File > User preferences**).

Adding a map

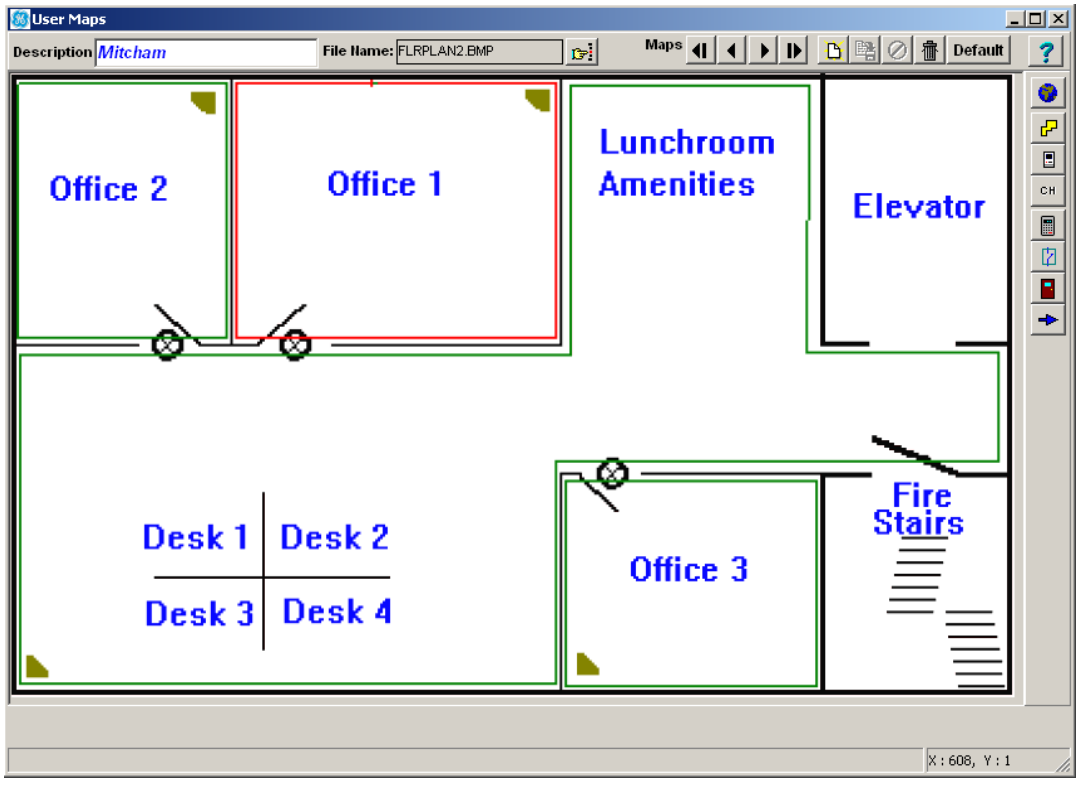
Prior to adding a map, you need a suitable .bmp file to serve as the background image, over which you'll place icons. Store the .bmp file in a location you can later navigate to (for example, in *C:\Program Files\Tecom\Bin\Images*).

To add a map, do the following:

1. Select **Admin > Add/edit map** to open the *User maps (editing)* window.
2. Click **New** to create a new map file. The *Open* dialog displays, with which you select the required .bmp file.
3. Click **Open** to add the file to the *User maps (editing)* window. The Description field is automatically populated from the file name. However, you can overtype the default description if required.
4. Click **Save** to save the record.

Note: If you edit the .bmp file in an external editor, the changes will be displayed in TITAN the next time you view the map file.

Figure 45. User maps (editing) window



5. Use the buttons on the right of the *User maps (editing)* window to add icons to the map. If the icon is associated with the device, Challenger displays a dialogue for you to select the device. New icons are initially placed at the top left corner of the background image: drag the icon to the required location.

Displaying maps

The *User maps* window can be launched in several ways:

- A map can be set as a default map to display when an operator logs in (a map must be set as default, and Show default map must be selected in **File > User preferences**).
- Select **Admin > Display maps**.
- Click **Map** on the *Alarm acknowledgment* window, if the device in alarm is linked to a map icon.

When a device has been linked to a map icon, the icon flashes when the device is in alarm. If the map contains several devices in alarm simultaneously, the icons for all the devices in alarm will be flashing. You can identify a particular device in alarm by selecting the alarm in the *Alarm acknowledgment* window, and TITAN displays a box around the associated icon.

You can acknowledge a device in alarm from the associated *User maps* window by right-clicking the icon and selecting **Acknowledge**. Depending on the device type, the right-click menu also enables you to select commands for isolate, deisolate, to open the control window, or to view the history log.

Maintaining the TITAN database

All data used and generated by TITAN are stored in a database on the TITAN computer. In the case of a TITAN multi-user system, the database is on the TITAN server. TITAN's database stores all the records for event history, TITAN systems, users, user journals, and Challengers.

TITAN stores its records in a database (DB) file. The DB file holds information about users, user journals, systems and all events. As time passes, the DB file increases in size and the system slows down as the excess records increase. The limitations of your hardware will decide how many records are excessive.

Warning and deletion thresholds can be set for disk space free and number of history event records to warn operators to remove excess records. (In TITAN multi-user, go to **File > User Preferences** and select the **Automatic Event Deletion** tab).

It is essential to safeguard valuable system data by planning a backup strategy for the TITAN database. The system maintenance utility (*System Manager*) simplifies the task of managing and implementing a backup strategy. *System Manager* also keeps TITAN multi-user running at optimal speed by enabling security managers to safely purge excess records from TITAN databases before TITAN's database grows too large.

A routine maintenance strategy typically involves the following tasks:

1. Regularly run *System Manager*, or otherwise configure your computer so that *System Manager* starts automatically.
2. Backup events. See *Backup a system* on page 87.
3. Export system, users, and user journals. See *Export a system* on page 90.
4. Purge a selected range of records. See *Purge a system* on page 93.
5. Backup the database. See *Backup the TITAN database* on page 101.
6. Verify that the operations have been completed successfully. See *Check the job log* on page 107.

System Manager

System Manager (system maintenance utility) has eight user-programmable functions and two job reports as follows:

Backup Events. Used by the security manager to backup some or all of TITAN events and/or user journals, for a selected system. This is typically used for housekeeping, or before purging or deleting. It can be used later to view events.

Export. Used by the security manager to take a snapshot of a TITAN security system or a particular Challenger. A system export does not include events, and a Challenger export does not include events or users. This is typically used for housekeeping, or before purging or deleting. It can be used later to restore a system and its user journals.

Delete. Used by the security manager with TITAN system maintenance rights to permanently delete an entire TITAN system or a particular Challenger from a system. This is typically used when a TITAN system or Challenger is no longer required. The *Reduce Size* option is used to actually delete the events marked for deletion.

Purge. Used by the security manager with TITAN system maintenance rights to mark TITAN events or user journals for deletion or for overwriting by new events. This is typically used to keep the database from growing excessively large over time. The *Reduce Size* option is used to compact the database after deleting records.

Import. Used by the security manager or installation technician to restore an exported system or a Challenger on a system.

Copy. Used by the security manager to copy an entire TITAN system or a particular Challenger into an existing system. This is typically used to quickly create a new system in TITAN.

DB Backup. Used by the security manager to perform or schedule a hot backup of the TITAN (single-user) database.

DB Restore. Used by the security manager to perform a cold restore of a backed up TITAN (single-user) database.

Job Queue (report). Used by the security manager or installation technician to check pending jobs.

Job Log. Used by the security manager or installation technician to check whether jobs have been successful.

Choosing a maintenance strategy

As a basic safety precaution and as good housekeeping, regularly back up TITAN system data and events (for example, to CD or to your network).

GE recommends that you use one of the following maintenance regimes:

Robust maintenance regime. GE recommends the robust maintenance regime, especially for sites with large numbers of users and daily events. Perform maintenance daily or weekly, using minimal purge settings.

Conservative maintenance regime. Perform maintenance weekly, monthly, or when warnings for event history record or disk space free thresholds appear, using medium purge settings.

Minimal maintenance regime. *GE does not recommend the minimal maintenance regime.* Perform maintenance weekly or monthly, or when system is automatically deleting events or the disk is full, using extensive purge settings.

Starting the system maintenance utility

Use one of the following actions to start the *TITAN system maintenance utility*:

- Click (typically) **Start > Programs > TITAN Security System > System Manager**.
- In TITAN go to **File > System Maintenance**.
- Create a desktop shortcut to *System Manager* (SystemMgr.exe) so that you can quickly start it when required.
- Add a shortcut to *System Manager* (SystemMgr.exe) to your Windows startup folder so that it starts each time the computer is started.

Scheduling jobs

You can schedule any of the *System Manager* jobs by setting an *Auto Start On* time and date for the job to run. For example, you can automate backups by setting an *Auto Start On* time and date, and programming a periodic run cycle. Scheduled jobs may be viewed in the Job Queue window.

Note: *System Manager* must be running at the *Auto Start On* time in order for the job to execute, and it must be kept running as long as the job status indicator flashes green. If you intend to schedule jobs, it is recommended that you add *System Manager* to your Windows startup folder so that it starts each time the computer is started.

CAUTION: Take care when scheduling a job to run at a future date if the job involves prerequisites. For example, the purge job should not be done without first backing up data, and attending to other important prerequisites. See *Purge a system* on page 93 for details.

The following sections describe *System Manager* functions.

Backup a system

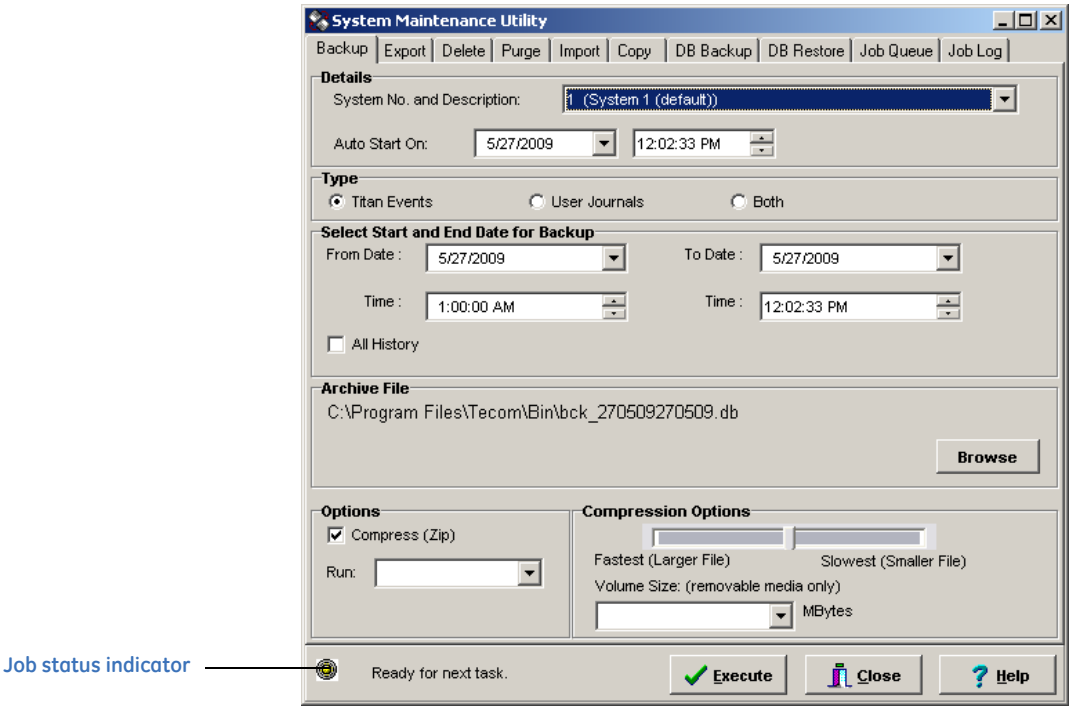
Backup (*Figure 46* on page 88) saves a TITAN system's entire event history or a selected portion to a backup file with optional file compression. *Backup* is typically used for:

- Normal housekeeping and maintenance.
- Prior to deleting or purging a system.
- Automatic, multiple backups.

Note: TITAN events or user journal records cannot be restored to the database after backing up. TITAN events may be viewed in TITAN using the **History > Reports > Custom**. User journal records may be viewed using the **History > User Journal Viewer** command.

The *Backup* tab is shown in *Figure 46* on page 88.

Figure 46. Backup tab



The job status indicator displays the following:

- Green—the job is running.
- Yellow—the job queue is idle.
- Red—an error occurred during a job.

To backup a system, do the following:

1. Start *System Manager* (if not automatically started).
2. Click the *Backup* tab.
3. Click the **System No. and Description** arrow and select the TITAN system to backup.
4. Select an **Auto Start On** date and time. You can use this setting, along with a selected **Run** frequency, to schedule the job to start automatically.

5. Select the type of backup: TITAN Events, User Journals, or both.
6. Select **From** and **To** dates and times for the records you wish to backup. Alternatively, check the **All History** checkbox to backup records for all dates.
7. Accept or change the archive location of the backup. File names must not contain only numbers and must not contain special characters.
8. OPTIONAL—Check the **Compress** (ZIP) tick box to activate the compression options for the archive.
9. OPTIONAL—Select a compression level with the **Compression Options** slider. (The faster the compression, the bigger the file and vice versa).
10. OPTIONAL—Select or enter a volume size to break the zip file into blocks. This allows you to copy large files across more than one removable medium. Leave the field blank to create a single file.
11. Click the **Run** arrow and select the required frequency to program periodic backups:
    - Once—The backup runs one time.
    - Daily—The backup runs every day at the specified auto-start time.
    - Weekly—The backup runs at the specified auto-start date and time, and repeats every week from the auto-start date.
    - Monthly—The backup runs at the specified auto-start date and time, and repeats on the first day of every month from the auto-start date.
    - Quarterly—The backup runs at the specified auto-start date and time, and repeats on the first day of every third month from the auto-start date.
    - Half Yearly—The backup runs at the specified auto-start date and time and repeats on the first day of every sixth month from the auto-start date.
    - Yearly—The backup runs at the specified auto-start date and time and repeats on the first day of every twelfth month from the auto-start date.
12. Ensure the removable medium (if used) is blank and ready. Click **Execute**. The Job Queue tab displays.
13. Check the job status indicator (shown in *Figure 46* on page 88) at the scheduled time. The job status indicator will flash green to indicate that the backup is in progress. Alternatively, check the job queue.

Export a system

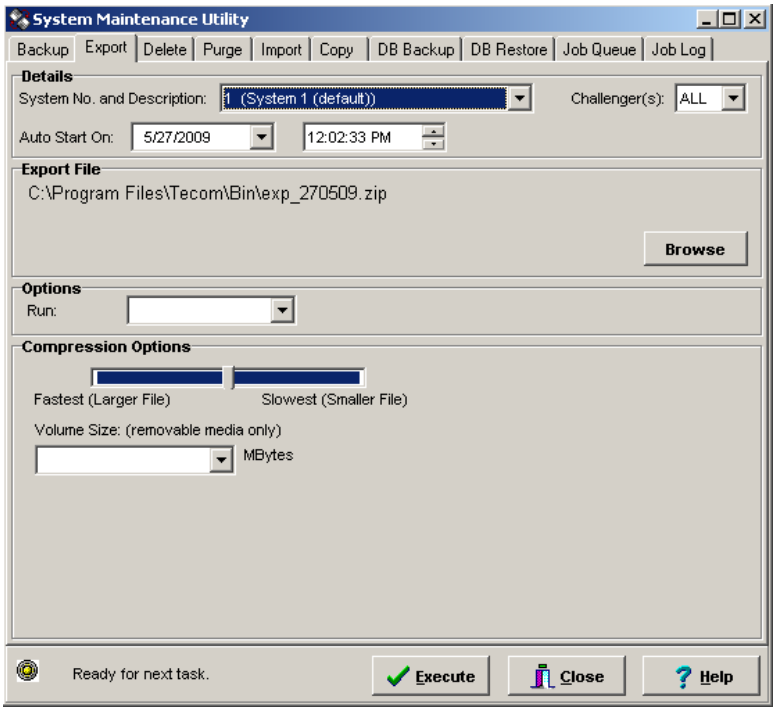
Export (*Figure 47*) backs up a TITAN system, the system's user journals, and one or more selected Challengers. *Export* is typically used:

- For normal housekeeping and maintenance.
- Before deleting or purging a system.

Note: To restore an exported system and its user journals later, or add a Challenger to a system, use the import function (see *Import a system* on page 96).

The *Export* tab is shown in *Figure 47*.

Figure 47. Export tab



To export a system, do the following:

1. Start *System Manager* (if not automatically started).
2. Click the *Export* tab.

3. Click the **System No. and Description** arrow and select the TITAN system to export.
4. OPTIONAL—Click the **Challenger(s)** arrow and select a Challenger number to export, or select **All** to export the entire system (in each case without users).
5. Select an **Auto Start On** date and time. You can use this setting, along with a selected **Run** frequency, to schedule the job to start automatically.
6. Accept or change the location and name of the zip file. The default file name is based on the current date (e.g., “exp_140906.zip” if created on 14 September 2006). If you want to use a non-default file name, it must contain at least one letter and may not contain special characters (except underscore). For example, “exp_14-09-06.zip” cannot be used because it contains hyphens.
7. OPTIONAL—Select a compression level with the **Compression Options** slider. (The faster the compression, the bigger the file and vice versa).
8. OPTIONAL—Select or enter a volume size to break the zip file into blocks. This allows you to copy large files across more than one removable medium. Leave the field blank to create a single file.
9. Click the **Run** arrow and select the required frequency to program periodic exports:
    - Once—The export runs one time.
    - Daily—The export runs every day at the specified auto-start time.
    - Weekly—The export runs at the specified auto-start date and time, and repeats every week from the auto-start date.
    - Monthly—The export runs at the specified auto-start date and time, and repeats on the first day of every month from the auto-start date.
    - Quarterly—The export runs at the specified auto-start date and time, and repeats on the first day of every third month from the auto-start date.
    - Half Yearly—The export runs at the specified auto-start date and time and repeats on the first day of every sixth month from the auto-start date.
    - Yearly—The export runs at the specified auto-start date and time and repeats on the first day of every twelfth month from the auto-start date.
10. Ensure the removable medium (if used) is blank and ready. Click **Execute**. The Job Queue tab displays.

11. Check the job status indicator (shown in *Figure 46* on page 88) at the scheduled time. The job status indicator will flash green to indicate that the export is in progress. Alternatively, check the job queue.

Delete a system

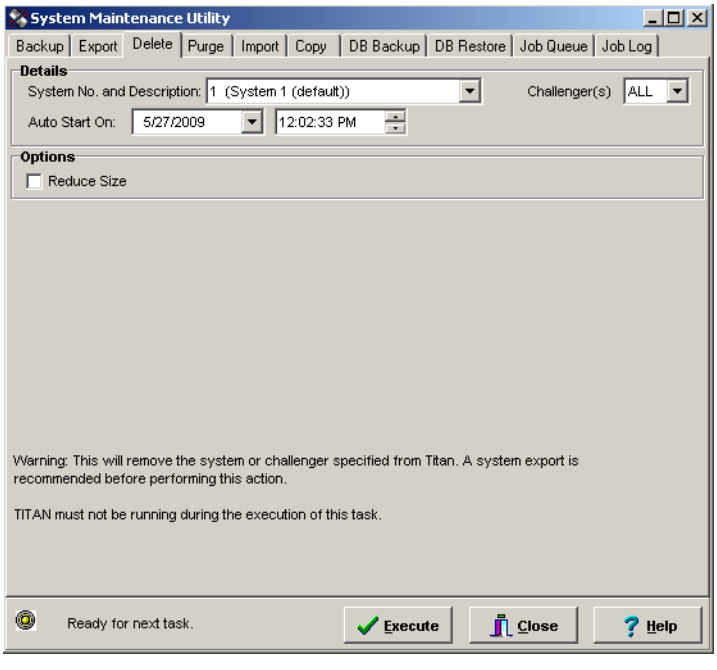
Delete permanently removes an entire TITAN system or selected Challenger(s) from TITAN. In the case of TITAN multi-user, the TITAN server must be offline. *Delete* is used when a system or a Challenger on a system is no longer required.

The only way to restore a deleted system is to use the import function using previously exported files for the same system.

Note: Backup and export all records before deleting or purging them to avoid losing data that might be needed later. See *Backup a system* on page 87 and *Export a system* on page 90 for details.

The *Delete* tab is shown in *Figure 48*.

Figure 48. Delete tab



To delete a system, do the following:

1. Start *System Manager* (if not automatically started).
2. Click the *Delete* tab.
3. Click the **System No. and Description** arrow and select the TITAN system to delete.
4. Click the **Challenger(s)** arrow and select a Challenger to delete, or select **All** to delete the entire system.
5. Select an **Auto Start On** date and time to schedule the job to start automatically.
6. Select the **Reduce Size** checkbox to permanently remove the deleted records from the database. Using this option will increase the time required to perform this task, but should shrink the database size.
7. In the case of TITAN multi-user, select **Force Shut Down of Clients** to ensure that TITAN clients are shut down. The **Force Shut Down of Clients** option is not shown in *Figure 48* on page 92.
8. Click **Execute**. You'll be prompted for your TITAN user ID and password.
9. Type your TITAN user ID and password, and then click **Execute**. The Job Queue tab displays.
10. Check the job status indicator (shown in *Figure 46* on page 88) at the scheduled time. The job status indicator will flash green to indicate that the deletion is in progress. Alternatively, check the job queue.

Purge a system

Use *Purge* for normal housekeeping and maintenance. The *Purge* tab is shown in *Figure 49* on page 94.

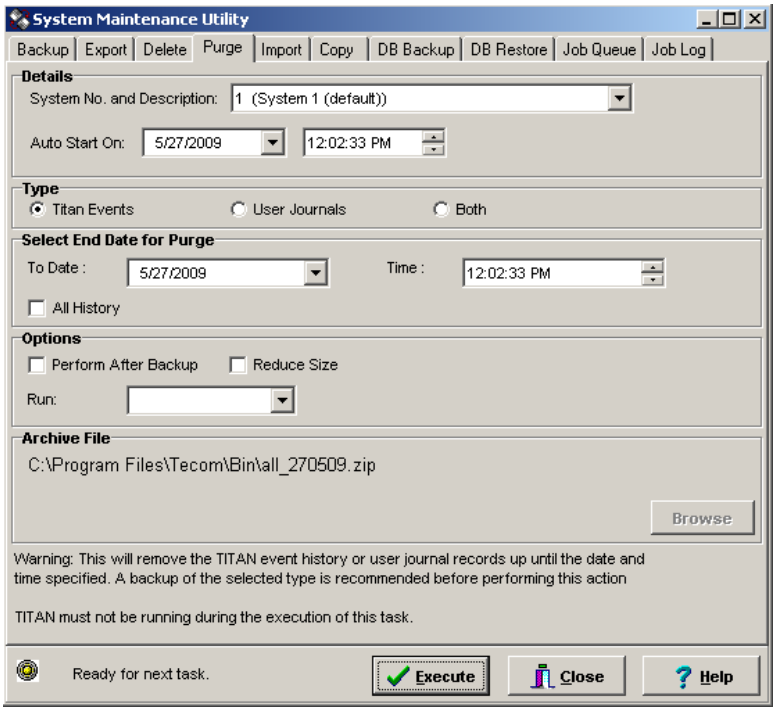
GE recommends that you purge unneeded records from your system frequently in order to control the size of the database, and use the *Reduce Size* option to reduce the database file size. The frequency that you purge your system determines the range of records that you need to purge (and therefore the length of time required). The greater the frequency, the smaller the range of records needs to be.

Note: Backup and export all records before deleting or purging them to avoid losing data that might be needed later. See *Backup a system* on page 87 and *Export a system* on page 90 for details.

Purge permanently deletes TITAN events and/or user journal records (depending on version).

TITAN events may be viewed or opened in TITAN by using the **History > Reports > Custom** command. User journal events may be viewed or opened in TITAN by using the **History > User Journal Viewer** command.

Figure 49. Purge tab



To purge a system, do the following:

1. Start *System Manager* (if not automatically started).
2. Click the *Purge* tab.
3. Click the **System No. and Description** arrow and select the TITAN system to purge.
4. Select an **Auto Start On** date and time to schedule the job to start automatically.
5. Select TITAN events, user journals, or both (TITAN events and user journals).

6. In the **Select End Date for Purge** fields, select a date and time before which the selected record types will be purged (records after the selected date and time are left untouched). Alternatively, select **All History** to delete selected record types for all dates.
7. Select the **Perform After Backup** checkbox to ensure that history is purged only after a successful backup has been done.
8. Select the **Reduce Size** checkbox to permanently remove the deleted records from the database. Using this option will increase the time required to perform this task, but should shrink the database size.
9. In the case of TITAN multi-user, select **Force Shut Down of Clients** to ensure that TITAN clients are shut down. The **Force Shut Down of Clients** option is not shown in *Figure 49* on page 94.
10. Click the **Run** arrow and select the required frequency to program periodic purges:
    - Once—The purge runs one time.
    - Daily—The purge runs every day at the specified auto-start time.
    - Weekly—The purge runs at the specified auto-start date and time, and repeats every week from the auto-start date.
    - Monthly—The purge runs at the specified auto-start date and time, and repeats on the first day of every month from the auto-start date.
    - Quarterly—The purge runs at the specified auto-start date and time, and repeats on the first day of every third month from the auto-start date.
    - Half Yearly—The purge runs at the specified auto-start date and time and repeats on the first day of every sixth month from the auto-start date.
    - Yearly—The purge runs at the specified auto-start date and time and repeats on the first day of every twelfth month from the auto-start date.
11. Accept or change the location of the zip file. The file will be named with today's date (e.g., exp_140906 = export of 14 September 2006). File names must not contain only numbers and must not contain special characters.
12. Click **Execute**. You'll be prompted for your TITAN user ID and password.
13. Type your TITAN user ID and password, and then click **Execute**. The Job Queue tab displays.

14. Check the job status indicator (shown in *Figure 46* on page 88) at the scheduled time. The job status indicator will flash green to indicate that the purge is in progress. Alternatively, check the job queue.
15. After the purge, the job status indicator displays yellow to indicate that processes are idle. Check the job log (see *Check the job log* on page 107) to verify that the purge was successful.

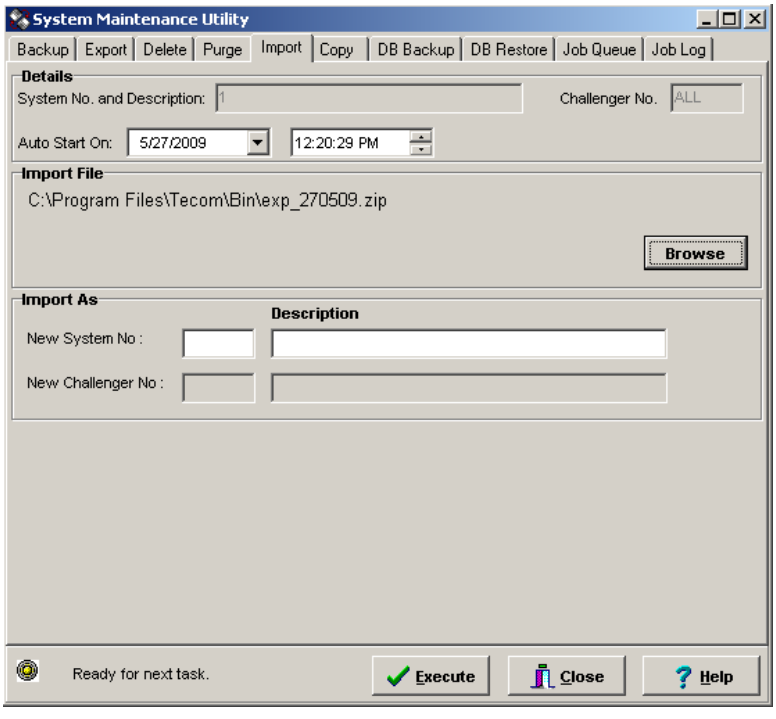
Import a system

Import restores a system or Challenger from previously exported files. It can be used for:

- Recovering an accidentally deleted system and its user journals.
- Quickly creating a new system.
- Adding a duplicate Challenger to an existing system.

The *Import* tab is shown in *Figure 50*.

Figure 50. Import tab



To import a system or a Challenger, do the following:

1. Start *System Manager* (if not automatically started).
2. Click the *Import* tab.
3. Select an **Auto Start On** date and time to schedule the job to start automatically.
4. Click **Browse** to select the file you need (there may be more than one exported file in the list). When the export file is chosen, the original details for the exported system and Challengers display in the System No. and Challenger No. fields.
5. Type a system number in the **New System No.** field. If you are importing a complete system, the system number cannot already exist in TITAN (you cannot overwrite an existing system). If you are importing a Challenger, it can only be imported into an existing system.

6. Type a description for the new system. This field will be unavailable if only a single Challenger was selected in the original export file.
7. If applicable, type a Challenger number in the **New Challenger No.** field. This field will be unavailable if the All Challengers option was selected in the original export file. If you are trying to duplicate a Challenger by importing it into an existing system, give the Challenger a number that is not already in that system.
8. If applicable, type a description for the new Challenger. This field will be unavailable if the All Challengers option was selected in the original export file.
9. Click **Execute**. The Job Queue tab displays.
10. Check the job status indicator (shown in *Figure 46* on page 88) at the scheduled time. The job status indicator will flash green to indicate that the import is in progress. Alternatively, check the job queue.

Copy a system

The *Copy* command copies an entire TITAN system with one or all of its Challengers. This may be used to:

- Quickly create a new system or Challengers.
- Serve as an online backup of Challenger programming settings.

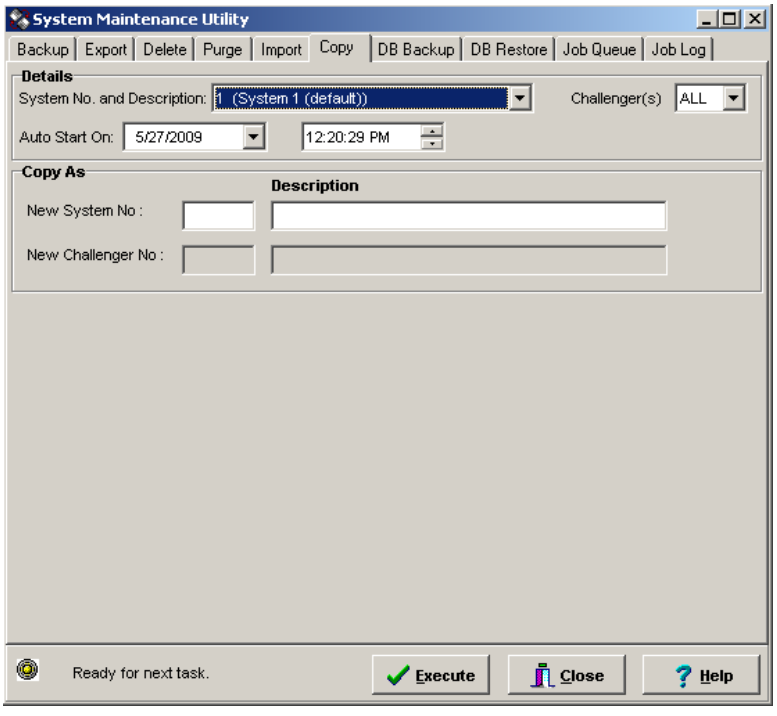
Note: If you copy a single Challenger, the Challenger's user records are not copied.

Copying an entire TITAN system copies all Challenger programming settings (history is not copied because it has no relevance to a new Challenger). The following items are copied:

- Challengers (programmed in **Admin > Challenger**)
- All Challenger details (programmed in **Challenger** menu)
- All users (programmed in **Users** menu)
- System poll rate (programmed in **File > Open/System**)
- Timeout settings (programmed in **File > Open/System**)
- Ports (programmed in **Admin > Ports**)
- Maps (programmed in **Admin > Add/Edit Maps**)

The *Copy* tab is shown in *Figure 51* on page 100.

Figure 51. Copy tab



To copy a system or a Challenger, do the following:

1. Start *System Manager* (if not automatically started).
2. Click the *Copy* tab.
3. Click the **System No. and Description** arrow and select the TITAN system to copy.
4. Click the **Challenger(s)** arrow and select a Challenger to copy, or select **All**.
5. Select an **Auto Start On** date and time to schedule the job to start automatically.
6. If copying a complete system, type a system number in the **New System No.** field. The system number cannot currently exist in TITAN (you cannot overwrite an existing system).
7. Type a description for the new system.
8. If copying a Challenger only, type a system number that already exists.

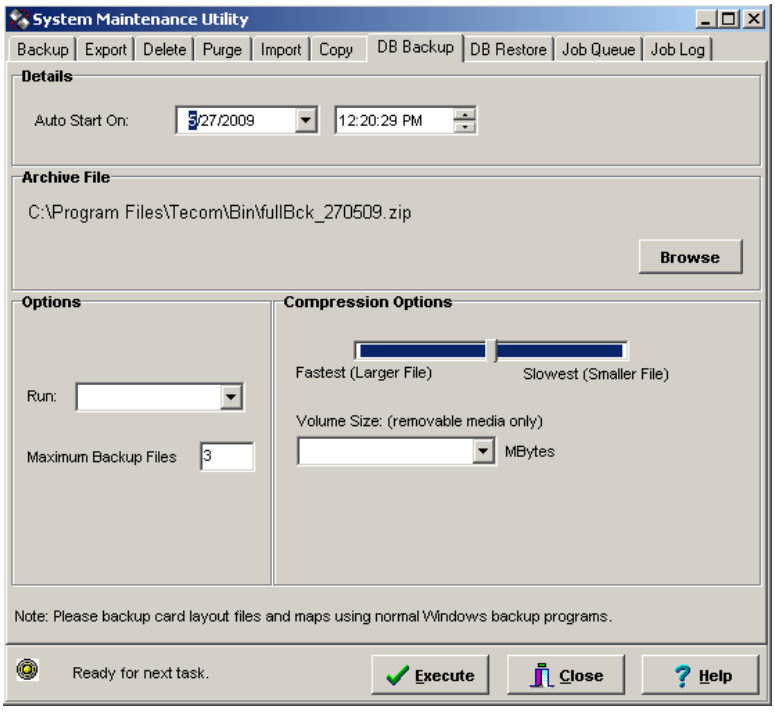
9. If applicable, type a Challenger number in the **New Challenger No.** field. This field will be unavailable if the All Challengers option is selected.
10. If applicable, type a description for the new Challenger.
11. Click **Execute**. The Job Queue tab displays.
12. Check the job status indicator (shown in *Figure 46* on page 88) at the scheduled time. The job status indicator will flash green to indicate that the copy is in progress. Alternatively, check the job queue.

Backup the TITAN database

Use the *DB Backup* tab to perform or schedule a hot backup of the TITAN (single-user) database. Hot backup means that the backup is performed without closing TITAN. DB Backup backs up all systems and history data, but does not backup the command queue or the timed command queue. The command queues cannot be backed up.

The *DB Backup* tab is shown in *Figure 52* on page 102.

Figure 52. DB Backup tab



To backup the TITAN database:

1. Start *System Manager* (if not automatically started).
2. Click the *DB Backup* tab.
3. Click the **Auto Start On** arrows to select a date and time to begin the backup.
4. The archive file location and name are set by default. If required, click **Browse** to specify a new location or file name.
5. Click **Run** and select the frequency that you want to run the backup, or select **Once** for a single instance.
6. Type a number in the **Maximum Backup Files** field (or use the default value).
7. Drag the **Compression Options** slider to adjust the amount of data compression (or use the default value).

8. If backing up to removable media (specified in step 4), click the **MBytes** arrow and select the size of the media. The removable media must be in the drive at the time of the scheduled backups.
9. Click **Execute**. The Job Queue tab displays.

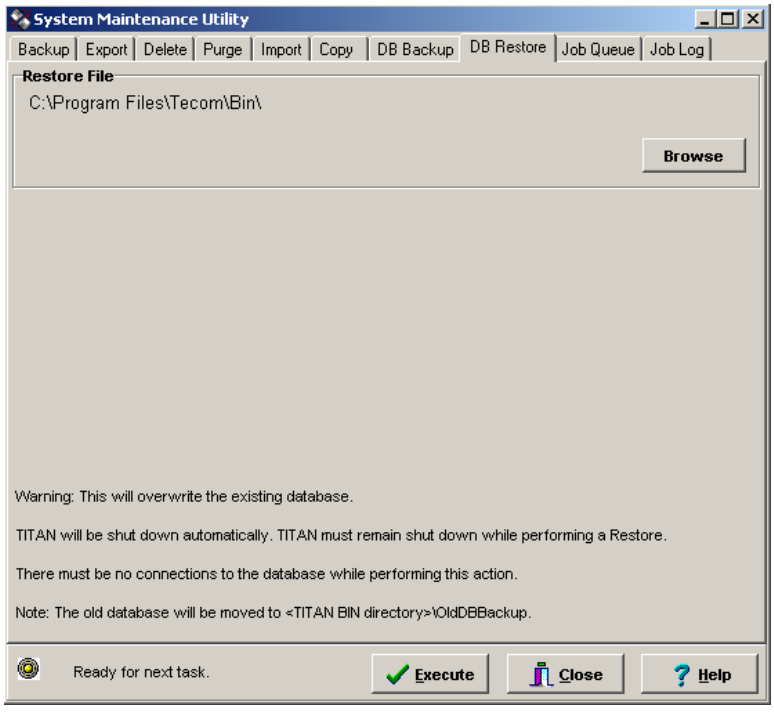
Restore the TITAN database

Use the *DB Restore* tab to perform a cold restore of the TITAN (single-user) database, for example, in case of corrupted data. Cold restore means that the restore must be performed with TITAN shut down.

If TITAN is running when you attempt to restore a database, TITAN will be shut down automatically. TITAN must remain shut down while performing a restore. There must be no connections to the database while performing this action.

The *DB Restore* tab is shown in *Figure 53* on page 104.

Figure 53. DB Restore tab



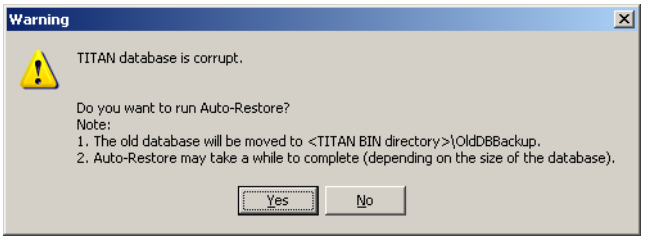
To restore the TITAN database:

1. Start *System Manager* (if not automatically started).
2. Click the *DB Restore* tab.
3. Click **Browse** to browse to a location and file name of a previously-saved backup (Zip) file.
4. Click **Execute**. The Job Queue tab displays.

The old TITAN database will be moved to *C:\Program Files\Tecom\Bin\OldDBBackup* and the previously-saved backup will replace the old database.

On startup, if TITAN detects that the database has been corrupted, the message shown in *Figure 54* on page 105 displays.

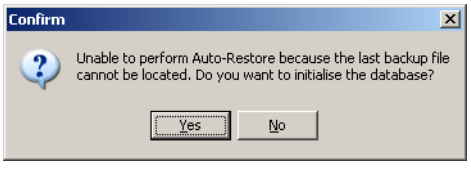
Figure 54. Auto restore message



Select **Yes** to run auto-restore. The corrupted TITAN database will be moved to *C:\Program Files\Tecom\Bin\OldDBBackup*. Alternatively, select **No** if you want to run *System Manager* manually and use the *DB restore* command.

System Manager attempts to restore the database from a previously-saved backup file. If a backup file isn't available, you have the option of initializing the database (all previous changes will be lost). Refer to *Figure 55*.

Figure 55. Backup file not found message

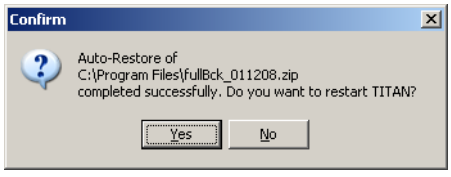


Select **Yes** to run auto-restore without a backup file and to initialize the database.

Note: If you initialize the database, the TITAN database will be restored to its default state and all changes to Challenger programming will be lost. After initializing the TITAN database, you may need to connect to each Challenger panel and use the **Upload all from Challenger(s)** command to retrieve each panel's data.

When finished restoring or initializing the database, *System Manager* displays a completion message and asks if you want to restart TITAN. Refer to *Figure 56* on page 106.

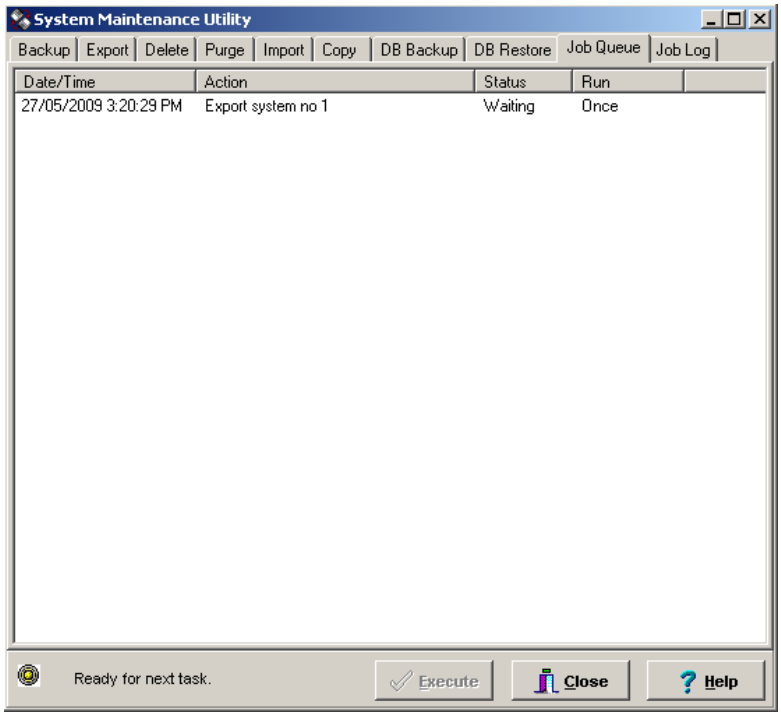
Figure 56. Auto restore complete message



Check the job queue

The job queue lists any jobs waiting or in progress. The job queue tab is shown in *Figure 57* on page 106.

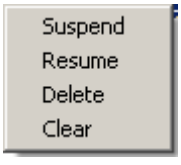
Figure 57. Job Queue tab



To view the job queue, do the following:

1. Start *System Manager* (if not automatically started).
2. Click the **Job Queue** tab.
3. To suspend, delete, resume a job, or clear all jobs from the queue, right-click the job and select an option from the menu (*Figure 58*). Jobs cannot be suspended or paused after they start, only before they are set to begin.

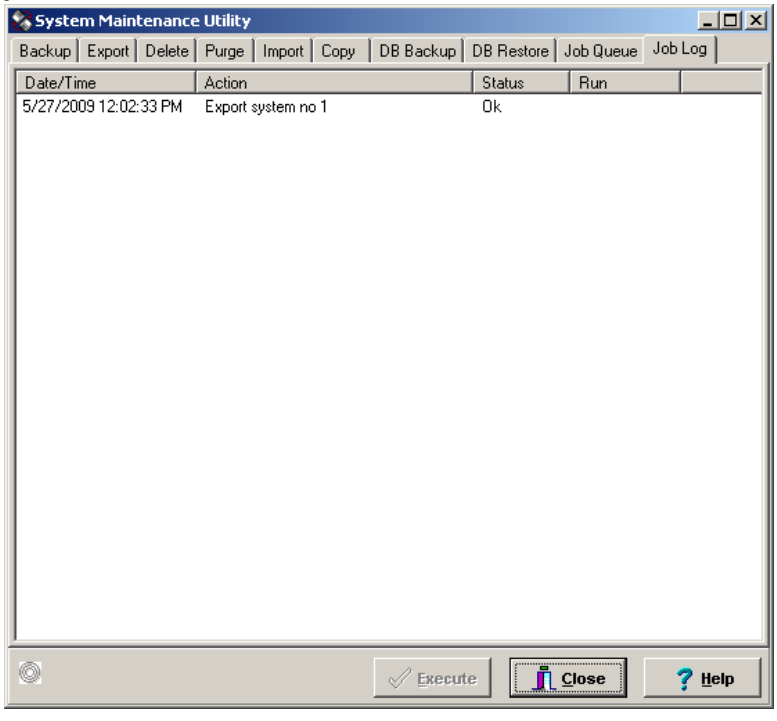
Figure 58. Job queue right-click menu



Check the job log

Use the job log to check whether a job has been completed successfully. The job log tab is shown in *Figure 59*.

Figure 59. Job log tab



To view the job log, do the following:

1. Start *System Manager* (if not automatically started).
2. Click the **Job Log** tab.
3. Check the log entry for items such as a Purge. The job log displays three states:
   - OK—indicates that the job was successfully executed.
   - Failed—indicates that the job was not successfully executed.
   - Cancelled—indicates that the job was deleted. Pending jobs that have been cancelled via the job queue's *Clear* option are not shown.
4. To remove all entries from the job log, right-click a job and select Clear from the menu.

Administering Challenger panels

This section describes the following administrative tasks:

- *Managing Challenger panel settings*
- *Adding a panel*
- *Challenger panel programming*
- *Upgrading a panel's memory*

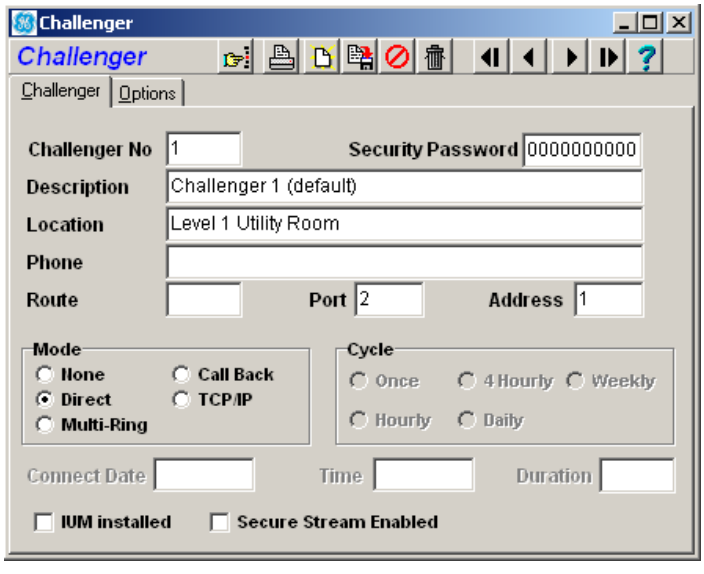
Managing Challenger panel settings

Select **Admin > Challenger** to create or modify the options required for TITAN to communicate with Challenger panels.

Note: The system must be inactive before you can change the panel options.

The *Challenger* window (*Figure 60*) displays for a Challenger panel in your system. See below for a detailed description of each field.

Figure 60. Challenger window in TITAN single-user



Challenger no. This field displays the number of the Challenger panel in the current TITAN system.

Security Password. The 10-digit password that is programmed in the Challenger's Installer Programming menu option 29.

Description and location. These fields describe the panel and its location.

Phone. The phone number (including PABX number) of the Challenger. Used when dialling in to a remote Challenger.

Route. Used when communicating with the Challenger via a TS2000 Network Master Receiver.

Port. The port used to communicate with the Challenger. See *Ports* in TITAN online help for details.

Address. The computer address enables TITAN to communicate with the Challenger. This field is filled in automatically by TITAN and is always the same as the Challenger number. The computer address must be programmed into the Challenger under Installer Option 9-Communication Options.

Mode. Select one of the following:

- None: The Challenger is ignored by TITAN and is not polled.
- Direct: The Challenger is connected directly to the computer via a Computer Interface or serial connection.
- Multi-ring: TITAN will dial a remote Challenger according to the options set in the Challenger's communications options.
- Call Back: The Challenger will dial TITAN using its programmed callback number when it detects a call-back trigger.
- TCP/IP: Use for event-driven TCP/IP communication.

IUM installed. Select to indicate that the panel has IUM (intelligent user module) used to increase the number of users, alarm groups, door groups, and floor groups in your system. See *Table 2, V8 Challenger memory application (version 8.128 or later)* on page 113 for details.

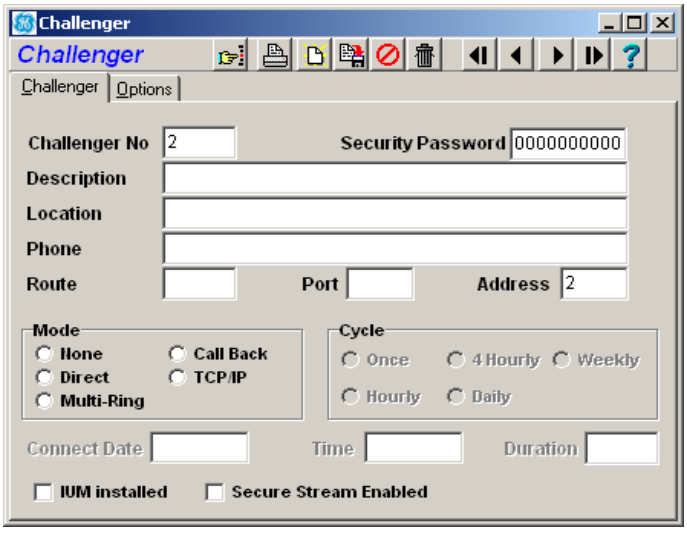
SecureStream enabled. Select to designate the Challenger as an IP panel able to receive data from TITAN via the SecureStream IP computer. The TITAN system must also have SecureStream IP enabled (see *Figure 4* on page 6).

The *Options* tab displays the IUM format (card format) and the IUM teach device reader number for the panel. The IUM format defines what type of card can be recognised by the panel. The learn reader number identifies the remote arming station used to read raw card data into user records (see *IUM teach mode* on page 30).

Adding a panel

To set up a new Challenger panel, click **New**. The *Challenger* window displays (*Figure 61*) and automatically assigns the panel number. Enter a description and the location of the panel, and verify that the information in the other fields is correct. Click the *Options* tab to enter the settings for the IUM format and the IUM teach device reader number. Click **Save** when you are finished.

Figure 61. New Challenger window



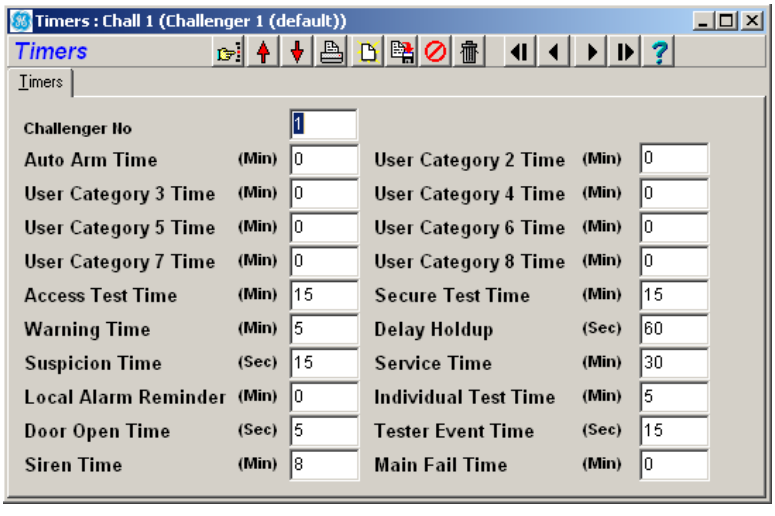
Refer to *TITAN online help* for details about using the *Challenger* window.

Challenger panel programming

This manual is not a programming manual. However, at times it may be necessary for an operator to view or edit details of Challenger panel programming.

To view a Challenger panel's programming details, select **Challenger** from the main menu, and then select the required menu option (for example, Timers). In this manner authorised operators can navigate to detailed programming screens for every item (see *Figure 62*).

Figure 62. Full programming view of timers



Upgrading a panel's memory

Challenger panels and their memory configurations are typically set up by your installer or security dealer. The information in this section is provided as a reference to help you understand the differences between panels and how they handle user information.

CAUTION: *Incorrect use of the settings described in this section could cause loss of user data resulting in users being unable to access, or to exit, a facility by means of their cards or PIN codes. GE recommends that changes to system memory be performed only by trained installers or security dealers.*

A Challenger V8 panel with standard memory can be upgraded to expanded memory or intelligent user memory (IUM). IUM enables the panel's users to have PIN codes and up to 48 bits of raw card data (standard is 26 bits). These users are referred to as IUM users.

IUM allows more information to be downloaded to the Challengers in your system. The default card information available on systems without IUM is 26 bits or Tecom ASC 27 bits. With IUM installed, you expand the amount of card information to 48 bits. And depending on the amount of hardware memory added, you can have up to 65,535 users programmed into your system.

From the **Admin > Challenger** menu, each Challenger can be checked to see if the IUM is installed. The *IUM Installed* box is ticked when a Challenger has IUM.

Table 2. V8 Challenger memory application (version 8.128 or later)

Memory	Users	PIN codes	Name files	Alarm Groups	Door Groups	Floor Groups	Time Zones
standard	50	50	50	138	10	10	24
standard with software IUM	50	50	50	138	10	10	24
1 MB exp. (TS0882)	11,466	1,000	200	255	255	128	46
1 MB exp. (TS0882) with software IUM	2,000	2,000	200	255	255	128	46
4 MB IUM (TS0883)	17,873	17,873	200	255	255	128	46
8 MB IUM (TS0884)	65,535	65,535	200	255	255	128	46

Challenger V8 panels using firmware version 8.128 or later, and fitted with TS0882, TS0883, or TS0884 memory modules have extended alarm group, door group, floor group, and hard time zone capacities.

Alarm groups. The quantity of alarm groups is increased from a total of 138 to a total of 255.

Door groups. The quantity of door groups is increased from a total of 128 to a total of 255.

Floor groups. The quantity of floor groups is increased from a total of 64 to a total of 128.

Hard time zones. The quantity of time zones is increased from a total of 24 to a total of 46 (time zone numbers 1 to 24 and 42 to 63).

Upgrading to IUM

When configuring a Challenger panel to use IUM, the existing records for users, door groups, and floor groups are erased from the panel's memory. You must back up these records (if required) and re-program them into the control panel after installing memory.

As of panel firmware version 8.128, Challenger panels that are not fitted with TS0883 or TS0884 hardware IUM modules can be programmed to use software IUM.

Software IUM. Use the following steps to upgrade a non-IUM Challenger system to use software IUM:

1. Ensure the control panel uses firmware version 8.128 or later. Obtain firmware if needed.
2. Go to **File > Upload all from Challenger panels > Users** to obtain the current user records from the panel.
3. Power down the Challenger system.
4. Install firmware version 8.128 or later (unless already installed).
5. Reset the Challenger panel (refer to *Clearing the memory* in the *Challenger V8 & V9 Programming Manual* for details).
6. Power up the panel.
7. Use RAS Install menu option *14 Defaults* to program software IUM mode (default option 95).
8. Connect with TITAN.
9. Download the system back into the control panel.
10. Use the *Update Raw Card Data* command to create or update raw card data for the panel's user records (see *Updating raw card data* on page 41).

Hardware IUM. Use the following steps to add hardware IUM to a Challenger panel:

1. Purchase the memory module for the panel and corresponding modules for any Intelligent Access Controllers, if applicable.
2. Go to **File > Upload all from Challenger panels > Users** to obtain the current user records from the panel.
3. Power down the panel.
4. Reset the Challenger panel (refer to *Clearing the memory* in the *Challenger V8 & V9 Programming Manual* for details).
5. Install the IUM modules and associated firmware (if required).
6. Power up the panel.
7. Connect with TITAN.
8. Download the system back into the control panel.
9. Use the *Update Raw Card Data* command to create or update raw card data for the panel's user records (see *Updating raw card data* on page 41).

Chapter 8 Troubleshooting, Support

This chapter provides information to help you troubleshoot problems and contact technical support in case you need assistance with your GE equipment.

In this chapter:

Troubleshooting

This section provides details about known problems, and repair utilities supplied with TITAN and offers technical support contacts in case you need assistance. (See *Contacting technical support* on page 124).

Problem. Windows creates temporary files on desktop when running TITAN from a desktop shortcut.

Solution. Right-click TITAN's desktop shortcut and select Properties. Define a *Start in* location as, for example, "*C:\Program Files\Tecom\Temp*".

Tools supplied with TITAN single-user

The following tools and utilities are provided via the TITAN program group:

- See *System Manager* on page 85.
- See *TITAN Verify and Rebuild Utility* on page 118.
- See *TITAN Database Pack Utility* on page 120.

TITAN single-user automatically attempts to restore the database if it detects a problem. See *Restore the TITAN database* on page 103.

Tools supplied with TITAN multi-user

The following tools and utilities are provided via the TITAN program group:

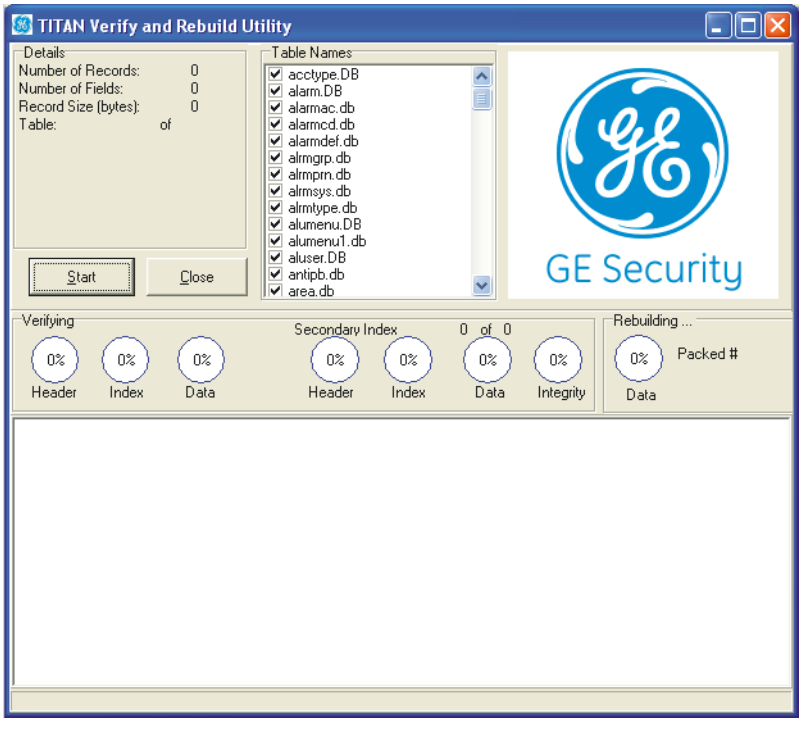
- See *System Manager* on page 85.
- See *TITAN Repair Wizard* on page 122.

TITAN Verify and Rebuild Utility

This utility applies to TITAN single-user only.

If your system crashes and your TITAN single-user database is corrupted, you can use the *TITAN Verify and Rebuild Utility* (*Figure 63*) to rebuild your database.

Figure 63. TITAN Verify & Rebuild window



To rebuild your database, do the following:

1. Backup your database.
2. Click (typically) **Start > Programs > TITAN Security System > TITAN Verify & Rebuild**.
3. All the tables are selected by default. If you don't want to rebuild all the tables, right-click a table name and select **De-Select All** to clear all the check boxes. Then click the check boxes for the tables you want to rebuild.
4. Click **Start**. TITAN will then scan each database and verify that it is not corrupted. If it finds the database is corrupted, it will rebuild it and will attempt to fix any problems with the database.
5. When the *TITAN Verify and Rebuild Utility* is finished it will display the message "No unrepairable error(s) were Detected".

6. Look under *C:\Program Files\Tecom\db* for corrupted files. Corrupted files with be marked with an underscore character (for example, *alarm.mb* will become *alarm_.mb*). Delete all files that are marked with an underscore, except for the following three files: *config_01*, *config_01.px*, and *config_01.val*.
7. Restart TITAN after this process has been completed. If the problem still occurs, contact your installer or distributor.

TITAN Database Pack Utility

This utility applies to TITAN single-user only.

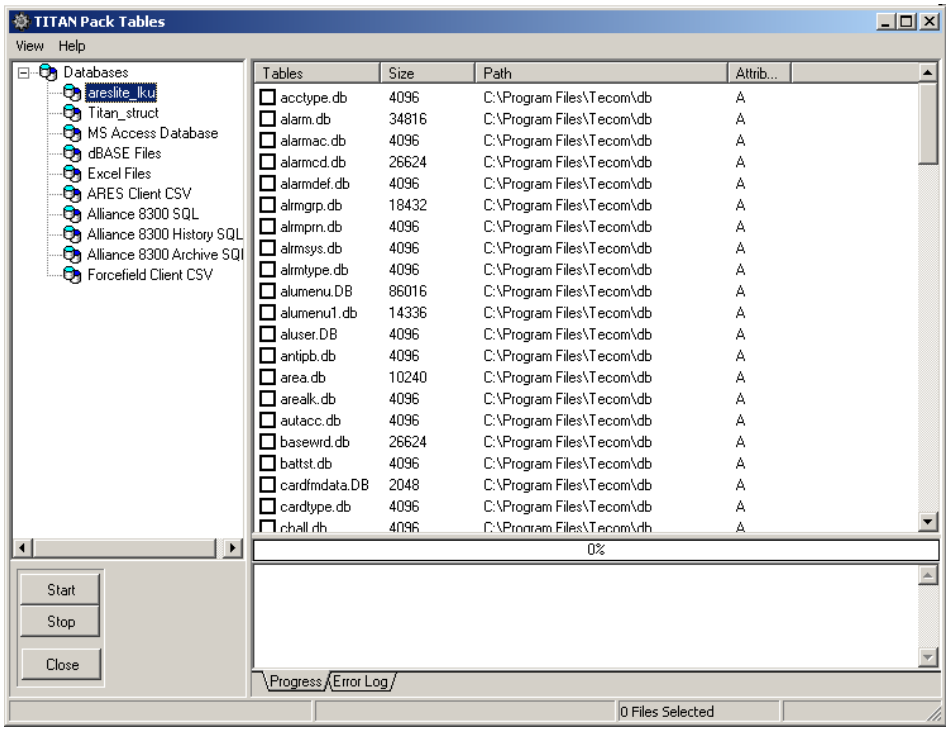
When events are deleted from the TITAN history, they are removed from your hard drive. However, due to the nature of hard drives, some remaining space will always be left behind in your database.

After a period of time (depending on how busy your TITAN and Challenger system is) this space can grow to fill your hard drive. Because of this, you will need to compact your database from time to time, to remove the space and make sure your database size is at its optimum.

GE recommends that you routinely use *TITAN system maintenance utility* for normal housekeeping and maintenance (see *Purge a system* on page 93).

Alternatively, you can use the *TITAN Database Pack Utility* (*Figure 64* on page 121) to compact the TITAN database.

Figure 64. Database pack utility



To compact the TITAN database, do the following:

1. Click (typically) **Start > Programs > TITAN Security System > TITAN Database Pack Utility**.
2. On the left-hand side of the window, double-click Databases to expand it.
3. Select **areslite_lku** to populate the right-hand side of the window.
4. All the tables are deselected by default. Right-click a table name and choose **Select All** to check all the check boxes.
5. Click **Start**. TITAN will cycle through these .db files and compact them if necessary. This will pack the database and reduce the size of your databases and save disk space.
6. When finished, click **Close** to close the utility.

TITAN Repair Wizard

This utility applies to TITAN multi-user server only.

If your system crashes and your TITAN multi-user database is corrupted, you can use the *TITAN Repair Wizard* (*Figure 65*) to rebuild your database.

Figure 65. TITAN Repair Wizard

CAUTION: *Improper use of this utility, or terminating the process before it finishes (either intentionally or accidentally via a power interruption) may result in loss of data. GE advises that you backup your database before using this procedure.*

To rebuild your database, do the following:

1. Disconnect all clients from the TITAN multi-user server.
2. Close the TITAN client application running on the TITAN multi-user server computer.
3. Click (typically) **Start > Programs > TITAN Security System > Server Control Manager** and select Shut Down Server.
4. Click (typically) **Start > Programs > TITAN Security System > TITAN Repair Wizard**.

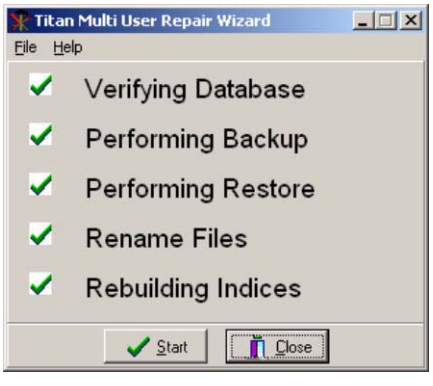
Note: If problems are found in the TITAN database, the backup and restore process launches automatically and could take several hours to complete. During the backup and restore process, it may appear that nothing is happening. Do not terminate the process before it finishes.

5. Click **Start**. The Wizard checks the database and automatically launches if problems are found. If no problems are found, the Wizard provides the opportunity to proceed anyway (*Figure 66* on page 123).

Figure 66. Repair Wizard confirmation dialogue box

6. If needed, click **Yes** to begin the process of rebuilding your database.
7. When the backup and restore process finishes (*Figure 67*) click **Close**.

Figure 67. Repair Wizard completion screen



Contacting technical support

For assistance installing, operating, maintaining, and troubleshooting this product, refer to this document and any other documentation provided. If you still have questions, contact your installation company for assistance.

Alternatively, you may contact GE Security's technical support during normal business hours (Monday through Friday, excluding holidays, between 9:00 a.m. and 5:30 p.m. AEST).

Table 3. Sales and support contact information

	Sales	Technical support
Phone	+61 3 9239 1200	
Fax	+61 3 9239 1299	
E-mail	sales@gesecurity.com.au	techsupport@gesecurity.com.au

Note: Be ready at the equipment before calling for technical support.

Index

A

B

C

D

E

F

G

H

I

L

M

O

P

R

S

T

U

V

W