Titan™ User Manual

P/N MAUSER-TITAN • REV 07 • ISS 20AUG15

Copyright © 2015 UTC Fire & Security Australia Pty Ltd. All rights reserved.

Trademarks and patents

The Titan name and logo are trademarks of UTC Fire & Security.

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

Manufacturer

UTC Fire & Security Australia Pty Ltd t/a Interlogix
A UTC Building & Industrial Systems company

Ground Floor, 10 Ferntree Place
Notting Hill, Victoria, 3168, Australia

Contact information

For contact information, see www.interlogix.com.au.

Content

Important information ii
Preface iii

Chapter 1 Introduction 5
Product overview 6
Getting started 7

Chapter 2 Control system setup 13
Access control 14
Alarm control 21
Automation zone control 29

Chapter 3 Users 33
Creating departments 34
Managing user records 34
Advanced user procedures 46

Chapter 4 Security cards 51
Designing a card layout 52
Creating and issuing cards 56
Writing smart cards or fobs 60

Chapter 5 Reports 61
Reports menu 62
History menu 65

Chapter 6 Operation 69
Operating Titan 70
Record-keeping 74

Chapter 7 Administration 77
Administering your Titan system 78
Maintaining the Titan database 85
Administering Challenger systems 103

Chapter 8 Support 113
Troubleshooting 114
Contacting technical support 117

Index 119

Important information

Limitation of liability

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

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

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, Interlogix assumes no responsibility for errors or omissions.

Preface

Titan™ is security system software that can be used for both Challenger® V8 and Challenger® Series control panels.

Note: “Challenger Series” includes Challenger10, ChallengerSE, and ChallengerLE models, except as noted.

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

- Manage user records
- Create and issue ID cards
- Generate reports
- Acknowledge and respond to alarms

Notes

- Programming windows can vary depending on the version of Challenger panel selected (for example, see Figure 7 and Figure 8 on page 15). Unless otherwise noted, this manual will use screen images based on Challenger Series examples.
- Challenger Series capacities and features vary depending on the model.
- Challenger V8 capacities and features described in this manual are based on firmware version 8.128 or later.

For details of capacities and programming options, refer to the *Challenger Series Programming Manual* or the *Challenger V8 & V9 Programming Manual*, as appropriate. Also refer to Titan help.

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 system management software
- 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 “Support” for instructions on obtaining technical support.

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

Notes

- Uninstall any previous version of Titan before you install a new version.
- A qualified service person, complying with all applicable codes, should perform whatever hardware installation is required.

- If you plan to use Titan as system management software, see “Using Titan as system management software” on page 114.

Chapter 1
Introduction

Summary

This chapter provides an overview of Titan and instructions for getting started using the software.

Content

Product overview 6
Getting started 7
System selection 8
Main menu.....9
Right-click shortcuts 10
Standard toolbar.....10

Product overview

The Challenger system 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.

Getting started

Titan may be launched from the Titan program group or from the Titan desktop shortcut (if using a shortcut, see also “Troubleshooting” on page 114).

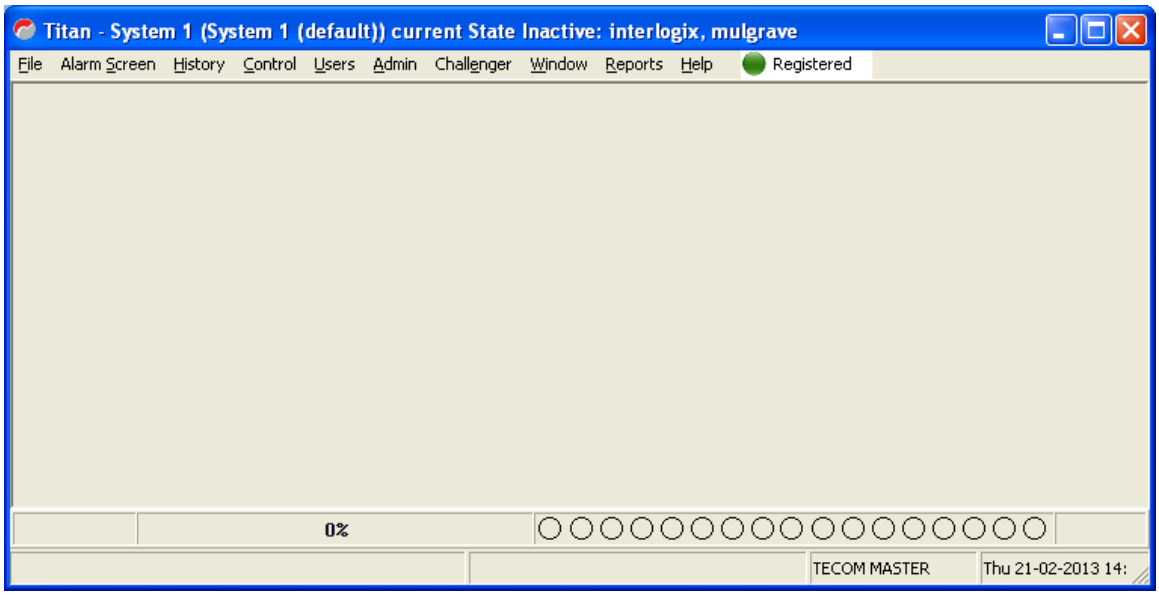
The Titan login window appears (Figure 1 below).

Figure 1: Login window (Titan Security System version shown)



The default operator ID is “TECOM MASTER”, and is not intended for normal use (the default password should be changed to protect the system and prevent unauthorised access). 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 2 below).

Figure 2: Work area

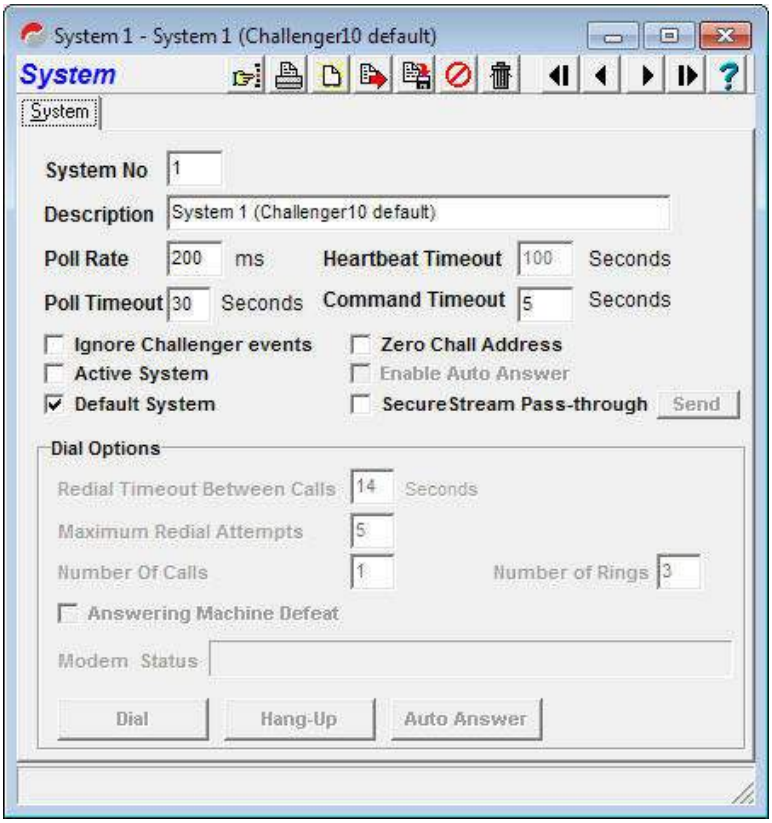


After login the menus and commands available to you as a Titan operator depend on the menu permissions allocated to your operator record (see “Managing operator records” on page 79). Menus that are not included in an operator’s permissions are greyed and unavailable when the operator logs in.

System selection

After you log on to Titan, select the system you want to manage (Figure 3 below). Skip this step if you have only one system.

Figure 3: System window

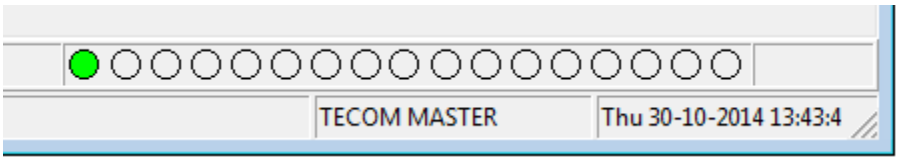


To activate a system and connect to a Challenger:

1. Go to File > Open System to open the System window, and use the toolbar buttons (see Figure 5 on page 11) 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.

The state of the system’s port connections display at the bottom of the Titan work area (Figure 4 on page 9).

Figure 4: Connection indicators



Connection indicators display the state of the system's port connections (direct, modem, card programmer, and 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.

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, isolating/deisolating an input, and updating the firmware on a Challenger Series panel.

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 105 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.

Right-click shortcuts

The Titan work area (Figure 2 on page 7) has a right-click menu for quick access to (opening and closing) the following windows:

- “View Cmd Queue” opens or closes the Command Queue window from the Admin menu.
- “View Timed Cmd Queue” opens or closes the Timed Command Queue window from the Admin menu.
- “View Live Event Log” opens or closes the Live Event Log window from the History menu.
- “View Challenger State” opens or closes the Challenger State window from the File menu.
- “View Alarms” opens or closes the Alarm Screen.

Standard toolbar

Most windows in the Titan software contain a standard toolbar used to perform basic functions (Figure 5 on page 11).

Figure 5: Standard Titan toolbar



Key to Figure 5:

(1) Search. The Search button brings up a window (based on the cursor location) 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.

(2) Upload. The Upload button loads information from the Challenger panels in your system into your computer.

(3) Download. The Download button sends information from your computer to the Challenger panels in your system

(4) Print. The Print button prints the current record.

(5) New. The New button creates a new record.

(6) Save. The Save button saves the current record information.

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

(8) Delete. The Delete button deletes the current record.

(9) First. Scroll to the first record.

(10) Previous. Scroll to the previous record.

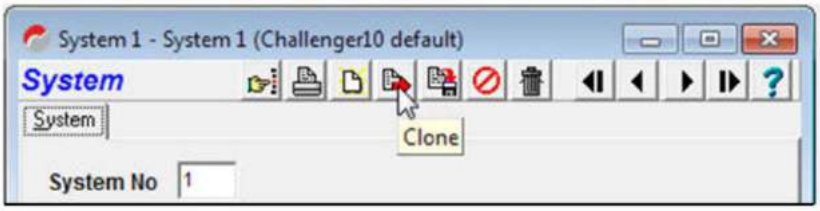
(11) Next. Scroll to the next record.

(12) Last. Scroll to the last record.

(13) Help. The Help button launches the help information for the current window.

The System window also has a Clone button (Figure 6 below).

Figure 6: System window Clone button



Refer to “Cloning a system” on page 84 for further details.

Chapter 2
Control system setup

Summary

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, area groups, regions, and holidays.

Content

Access control....14
- Creating time zones....14
- Creating door groups....16
- Creating floor groups....17
- Creating regions....18
- Creating holidays....18
- Naming holiday types....19

Alarm control....21
- What is an alarm group?....21
- Programming alarm groups....23
- Managing alarm groups....23
- Programming area groups....24

Automation zone control....29
- What is an automation zone?....29
- Programming automation zones....29
- Controlling automation zones....30

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: hard time zones based on specific time periods, and soft time zones based on events. This section describes how to program hard 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.

Challenger Series time zones are made up of one to eight sub-time zones (Figure 7 on page 15), and Challenger V8 time zones are made up of one to four sub-time zones (Figure 8 on page 15).

Each time zone is made up of sub-time zones containing: a start time, an end time, the weekdays that the sub-time zone is valid, and an option to make the sub-time zone valid on programmed holidays.

To set up a time zone:

1. Go to Challenger > Time Zones.
2. Double-click the Challenger no. field to select the Challenger panel you want to work with.

Figure 7: Time zones window for Challenger Series

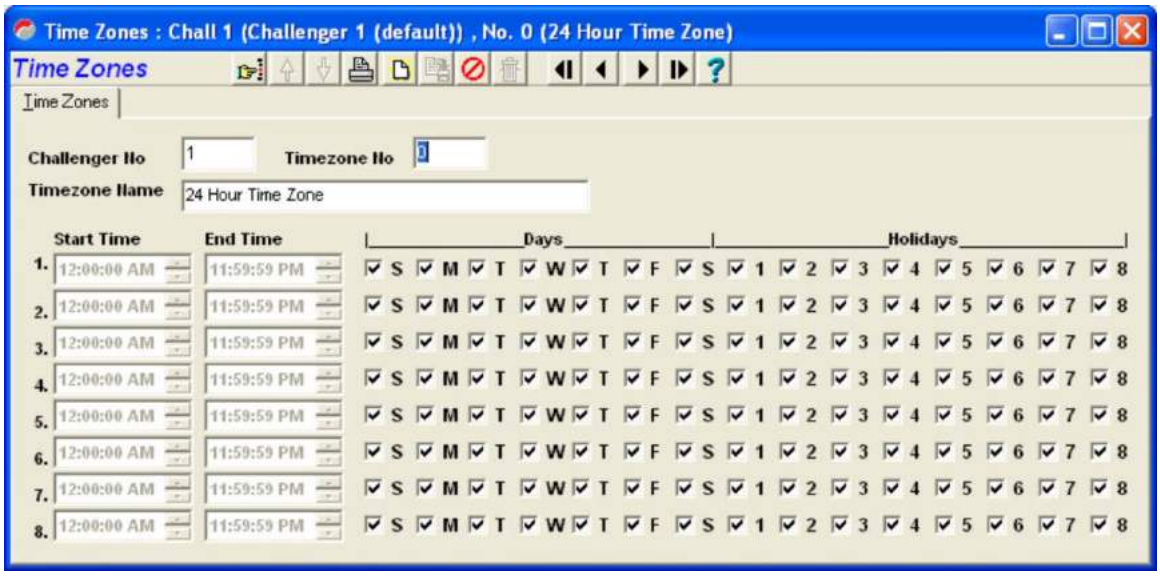
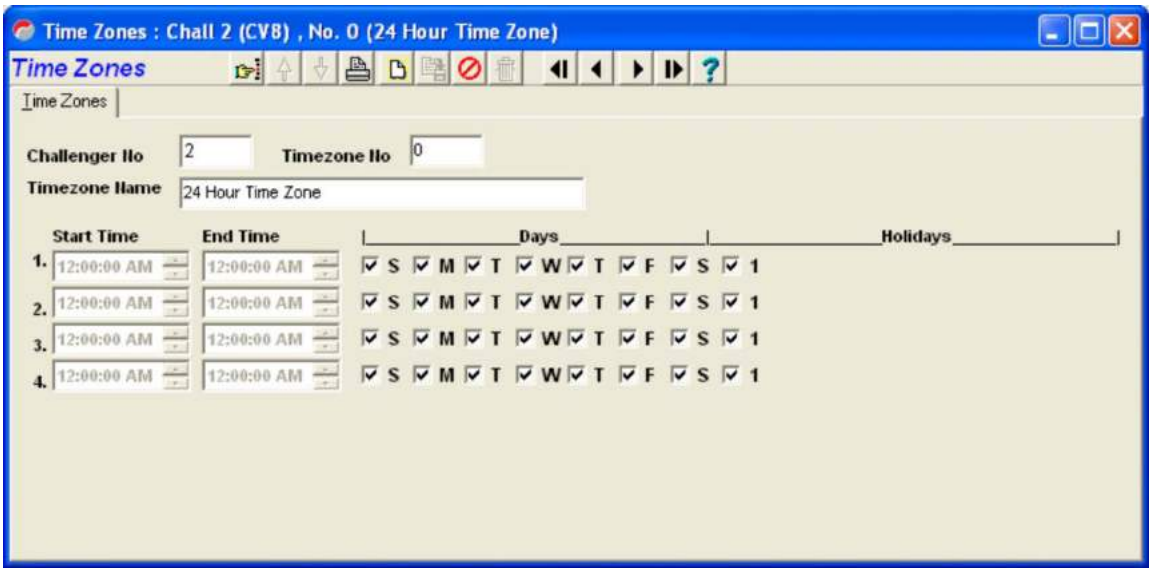


Figure 8: Time zones window for Challenger V8



3. In the Time Zones window (Figure 7 above or Figure 8 above), click New.
4. Enter a name for the time zone in the Timezone 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.
6. Populate the check boxes for the days of the week on which you want the sub-time zone to be valid.
7. Populate at least one of the Holidays check boxes (one through eight) if you want the sub-time zone to be valid on the corresponding holiday types (see “Creating holidays” on page 18). Leave all Holidays check boxes blank if you do not want the sub-time zone to be valid on a holiday type.
8. Click Save.

Creating door groups

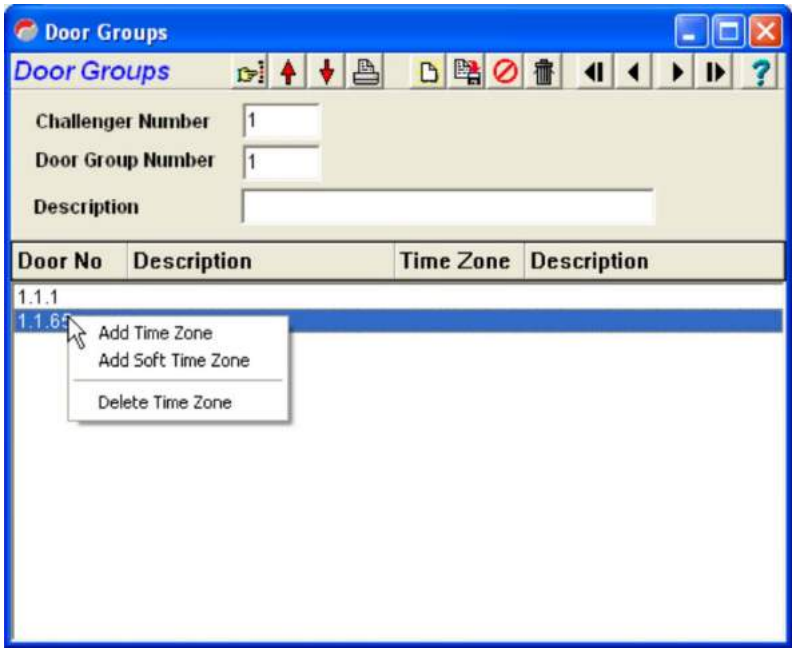
Door groups are used to specify when access to specific doors or lifts will be granted. After creating door groups, you can assign them to users. (For more information on assigning door groups to users, see Chapter 3 “Users” on page 33).

A Challenger panel can have up to 255 door groups.

To create a door group:

1. Go to Users > Door groups.
2. Double-click the Challenger Number field to select the Challenger panel you want to work with.

Figure 9: Door groups window (showing right-click menu)



3. In the Door groups window (Figure 9 above), click New.
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 or Add Soft Time Zone as needed. Alternatively, select Delete Time Zone to remove the selected time zone.
7. From the Time zone list, select the time zone or soft time zone that corresponds to when the door group needs to access the door, and then click OK.
8. Repeat steps 5 to 7 for each additional door you want to add to the door group.
9. Click Save.

Creating floor groups

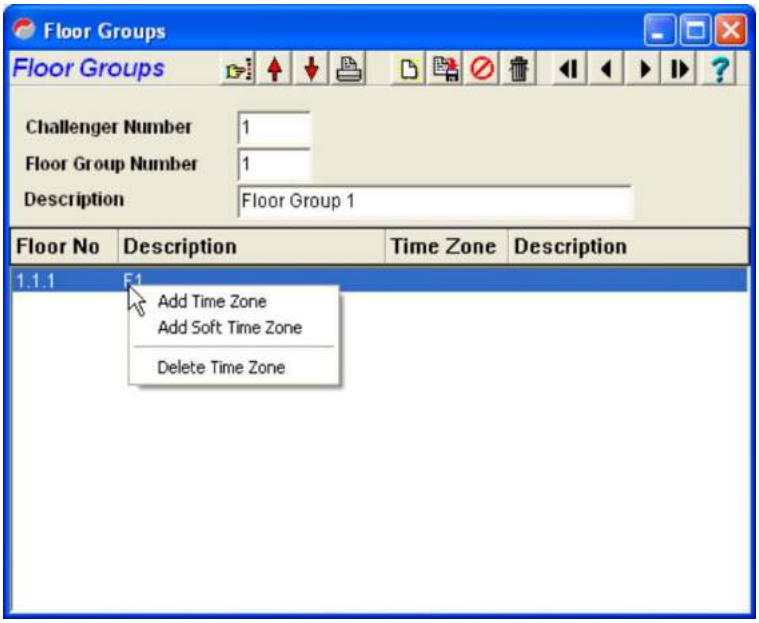
Floor groups are used to specify when access to specific floors will be granted. After creating floor groups, you can assign them to users. (For more information on assigning floor groups to users, see Chapter 3 “Users” on page 33).

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.

To create a floor group:

1. Go to Users > Floor groups.
2. In the Floor groups window (Figure 10 below), click New.

Figure 10: Floor groups window (showing right-click menu)



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 or Add Soft Time Zone as needed. Alternatively, select Delete Time Zone to remove the selected time zone.
7. From the Time zone list, select the time zone that corresponds to when the floor group needs to access the floor, and then click OK.
8. Repeat steps 5 to 7 for each additional floor you want to add to the floor group.
9. Click Save.

Creating regions

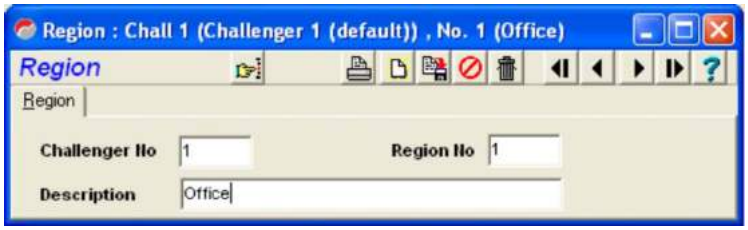
Regions are used by 4-Door/Lift Controller DGPs in combination with anti-passback, and they also allow Challengers to report where users can be found (see “Users by region” on page 64).

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

To create regions:

1. Go to Challenger > Intelligent Access Controller > Regions.
2. In the Regions window (Figure 11 below), click New.

Figure 11: 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

Challenger can have 24 holiday records. A holiday is a specified date (or range of dates) during which users are denied access during times that they would normally be permitted access. For example, a user may be able to disarm the system and unlock a door during working hours except on defined holidays.

Challenger Series holidays can be designated as recurring, so you don’t need to reprogram holidays that fall on the same dates every year.

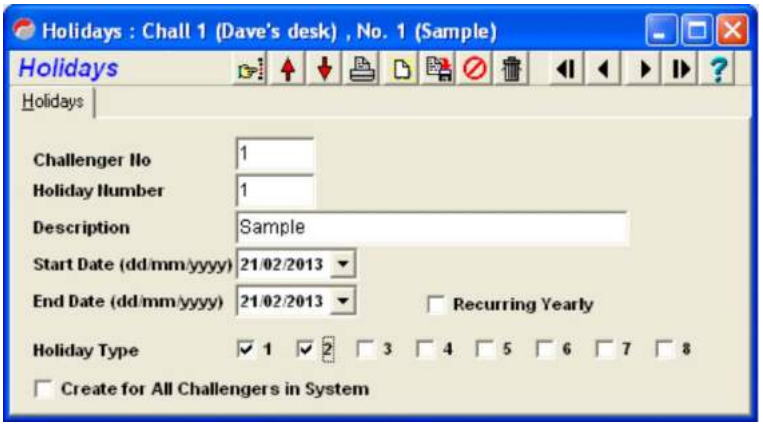
Some users may require access during holidays. This functionality is provided via the time zone in the user’s alarm group that allows access during holidays (via the holiday type).

Holidays can have one or more holiday types numbered 1 to 8, and should be named to record their purpose (see “Naming holiday types” on page 19). For example, there can be four holiday records in a year for school holidays. Each of these holiday records can be designated as holiday type 1 (optionally named “School holidays”) and is linked to the time zone in the alarm group for users who need access during school holidays, but not for other types of holidays (such as public holidays).

To create holidays:

1. Go to Users > Holidays.
2. In the Holidays window (Figure 12 below), click New.

Figure 12: 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 start date of the holiday from the calendar.
6. For multi-date holidays (Challenger Series only), from the drop-down list, select the end date of the holiday from the calendar.
7. For holidays that occur on the same date each year (Challenger Series only), check Recurring Yearly.
8. Select at least one Holiday Type checkbox (Challenger Series only) to enable the holiday record.
9. To create the holiday for all panels (of the same version) check Create for all Challengers in system.
10. Click Save.

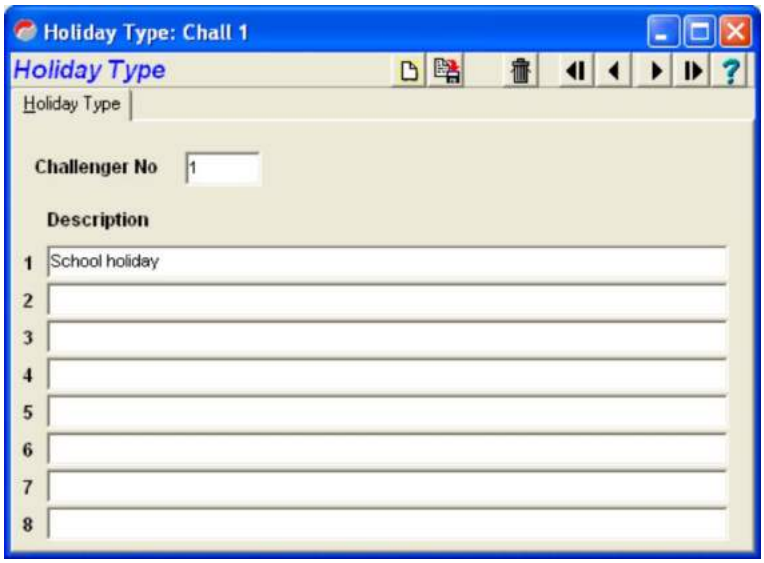
Naming holiday types

A Challenger Series panel can have one or more holiday types numbered 1 to 8. Optionally use the holiday types window to record a description for each holiday type. It is not needed for programming holidays: it is provided only as a reminder of what the eight holiday types are used for (for example, “School holidays”).

To name holiday types:

1. Go to Users > Holiday Types.
2. In the Holiday Type window (Figure 13 on page 20), click New.

Figure 13: Holiday type window



3. Double-click the Challenger No field to select the Challenger Series panel you want to work with.
4. Enter a description for each holiday type that you want to name.
5. 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.

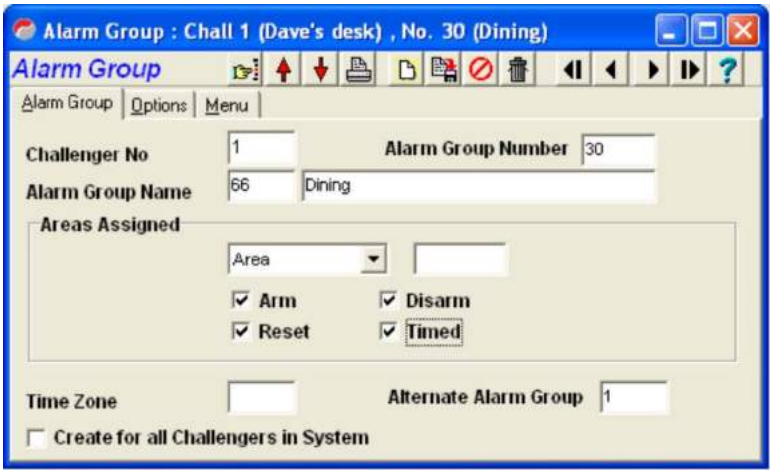
What is an alarm group?

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 33 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 14 below).

Figure 14: Alarm Group window



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

The three tabs in the Alarm group window are described in the following sections.

Alarm Group tab

The Alarm Group tab (Figure 14 above) 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.

An alarm group can only control functions in areas that are assigned to it.

Challenger Series application:

- The alarm group can be assigned a single area or an area group (see “Programming area groups” on page 24).
- When linked to a single area, the alarm group controls the area’s permissions for arming, disarming, alarm reset, and for timing.
- When linked to an area group, the area group controls each area’s permissions for arming, disarming, alarm reset, and for timing.

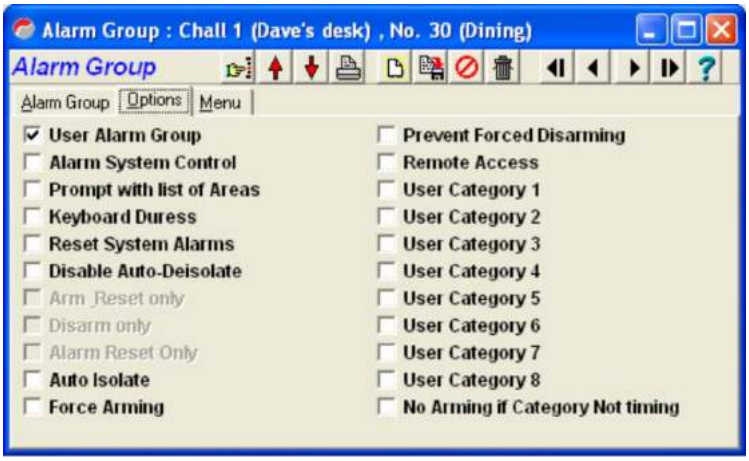
Challenger V8 application:

- The alarm group can be assigned one or more areas.
- The permissions for arming, disarming, and alarm reset are controlled via the alarm group’s alarm system control (and other) options.
- The alarm group’s timing functions are controlled via user categories.

Options tab

The Options tab (Figure 15 below) displays the panel options assigned to the alarm group.

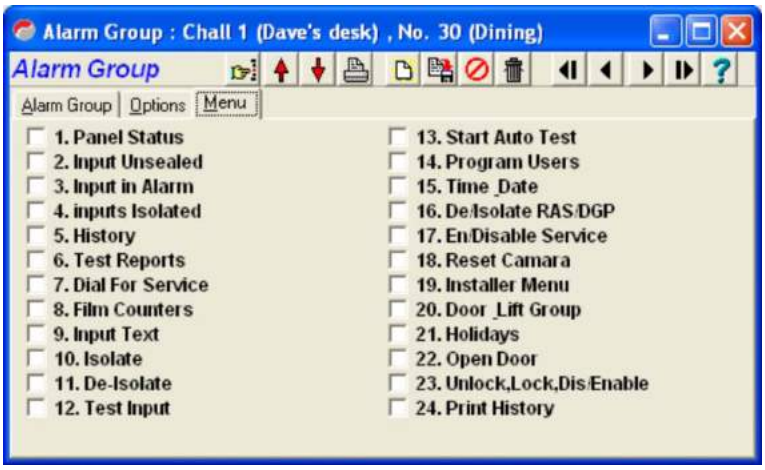
Figure 15: Alarm group options



Menu tab

The Menu tab (Figure 16 on page 23) displays the keypad menu options assigned to the alarm group. Menu options are assigned in accordance with the authorisation level of the alarm group: only installers should be assigned option 19 Installer Menu.

Figure 16: Alarm group menu options (subject to Challenger version)



Programming alarm groups

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.

Challenger Series alarm groups 4 to 10, and Challenger V8 alarm groups 7 to 10 are marked “spare”. Do not use.

Alarm groups 11 to 29 are pre-programmed with standard settings but can be changed if required. Alarm groups 14 to 29 are pre-set for areas 1 to 16. Alarm groups 30 and above are programmable to suit individual system requirements.

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 affect 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, and then click Save.

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 17 on page 24).

Figure 17: Alarm group list



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 then click the Save when finished.

Note: Do not use Challenger Series alarm groups 4 through 10 (marked “Spare”).

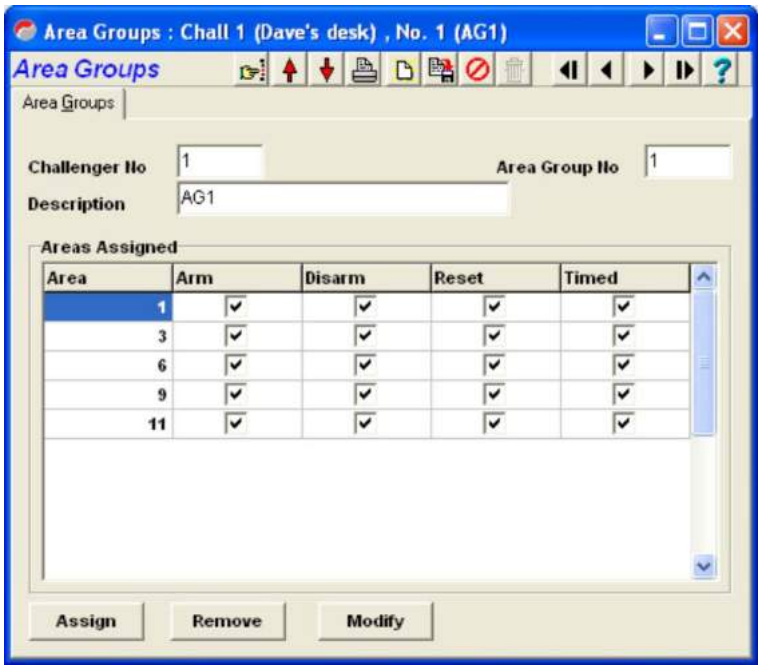
Programming area groups

Depending on panel model, a Challenger Series system can have up 99 areas, so the concept of area groups is used to manage multiple areas.

As described in “Alarm Group tab” on page 21, the area group controls each area’s permissions for arming, disarming, alarm reset, and for timing.

Go to Challenger > Area Groups to open the Area Group window (Figure 18 on page 25).

Figure 18: Area Groups window



Any area group can be modified.

Working with multi-area systems

New or defaulted Challenger panels can arm and disarm all areas. This functionality is accomplished via Area Group 1. Area Group 1 is used in the following Alarm Groups:

- Alarm Group 2-Master RAS or Door
- Alarm Group 3-Master Code (Installer)
- Alarm Group 11-High Level User Master
- Alarm Group 12-Low Level User Master
- Alarm Group 13-All Area User Code

Notice that Area Group 1 is used by both RAS 1 (via Alarm Group 2) and the installer user 50 (via Alarm Group 3).

Note: If the Challenger panel does not need all areas, we recommend removing unneeded areas from Area Group 1.

Selecting areas

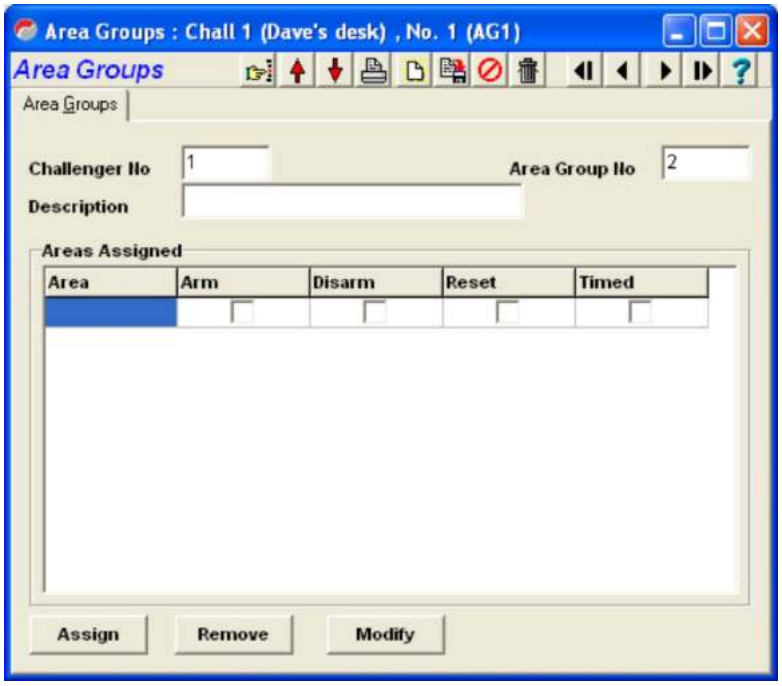
Use the Areas Assigned list to select one area or multiple areas. Click an area number in the left-hand column to select an area. When an area is selected, the entire row is blue (Figure 18 above).

To select multiple areas, hold the Ctrl key as you click area numbers (Figure 22 on page 28).

Creating a new area group

1. Click the New button to display an empty area group window (Figure 19 below).
2. Type a name in the Description field.
3. Click Assign, and then add at least one area to the group.
4. Click Save.

Figure 19: Area Groups window (new record)



Assigning areas

Click the Assign button to select areas from the list of 16 default areas plus previously-defined custom areas (Figure 20 on page 27).

Figure 20: Area list window



Select the required areas, and then click OK to add it to the area group. Hold the Shift key to select a range of areas; hold the Ctrl key to select single areas.

Removing areas

From the Area Group window (Figure 18 on page 25), select an area or areas, and then click the Remove button. The areas will be removed from the group instantly.

Note: Take care when removing areas: Areas are removed from the area group instantly without any need to save the area group record.

Modifying areas

Area permissions for arming, disarming, alarm reset, and for timing can be modified in two ways:

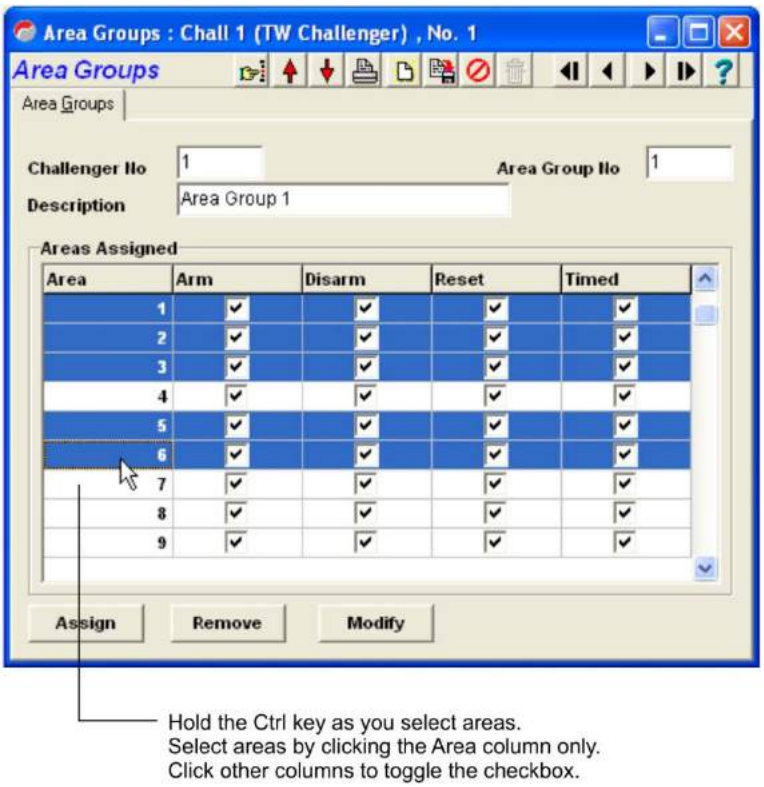
- On a per-area basis from the Areas Assigned list. Click the checkbox that you want to toggle, and then click on a different row. The area's permissions will be modified instantly.
- In bulk by selecting multiple areas (see Figure 22 on page 28), and then clicking the Modify button. The Area Options window displays (Figure 21 on page 28).

Figure 21: Area modify window



Set the permissions for arming, disarming, alarm reset, and for timing that you want to apply to all selected areas, and then click OK.

Figure 22: Multiple area selection



Automation zone control

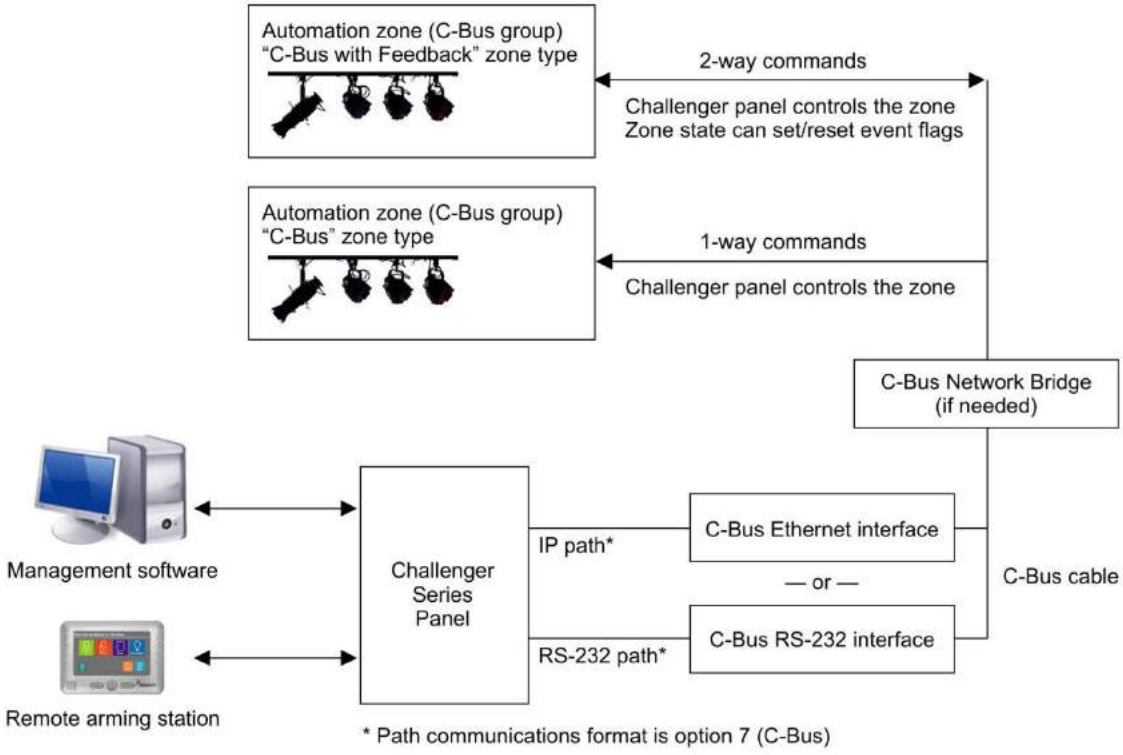
What is an automation zone?

An automation zone is one or more building devices (including C-Bus® devices) that can be controlled by a Challenger Series panels using firmware version V10-06 (or later).

Figure 23 below is a general overview of the relationship between a Challenger panel and two automation zones (C-Bus groups).

Note: A C-Bus Network bridge would probably not be required in the system depicted.

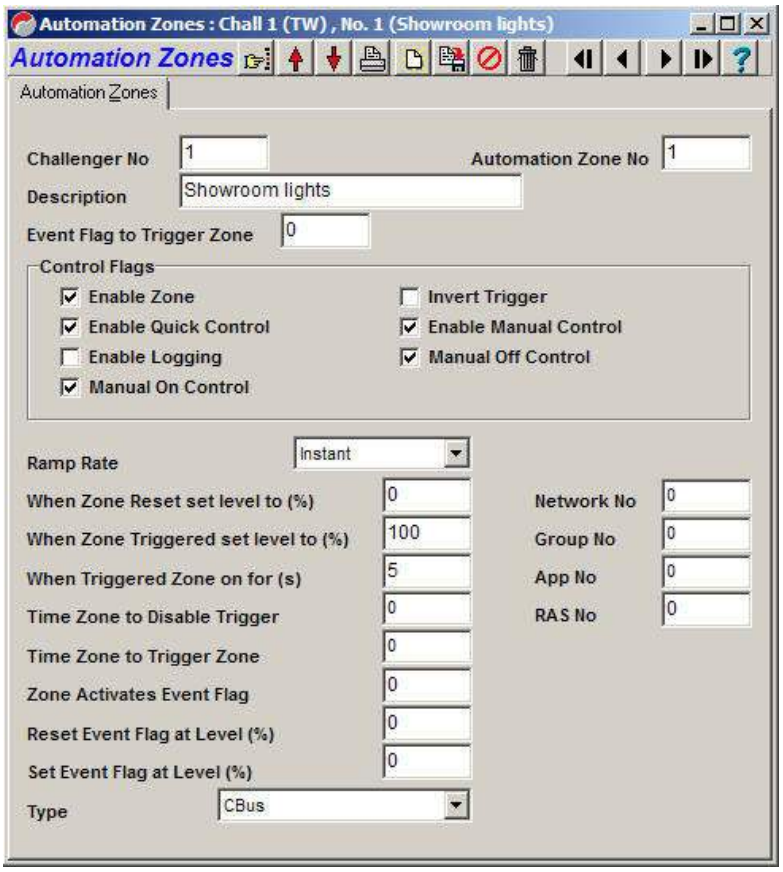
Figure 23: Automation overview diagram



Programming automation zones

Go to Challenger > Automation Zones to open the Automation Zones window (Figure 24 on page 30).

Figure 24: Automation Zones programming window



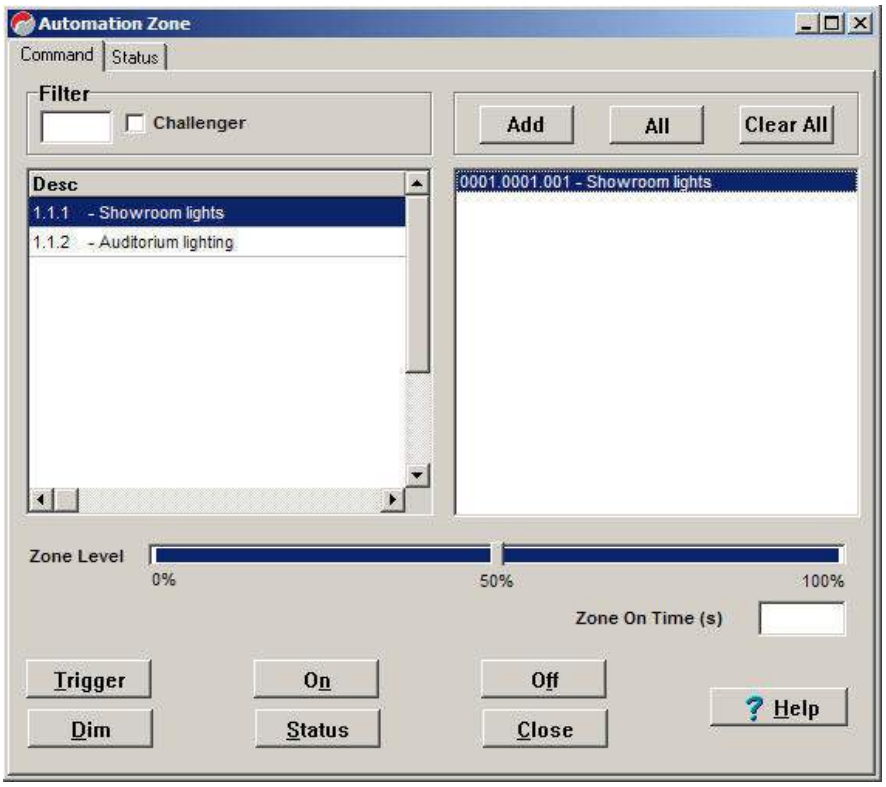
Use the Automation Zones programming window to configure the way in which the Challenger panel will interact with one or more building devices in a C-Bus group.

Refer to *Titan help* or *Challenger Series Programming Manual* REV 06 (or later) for details about using this window.

Controlling automation zones

Go to Control > Automation Zone to open the Automation Zones control window. Click the Command tab (Figure 25 on page 31).

Figure 25: Automation Zones control window, Command tab



The list on the left-hand side displays all the Challenger panel's automation zones. The list on the right-hand side displays the automation zones to be controlled.

Use the buttons at the top of the window to move automation zones into the right-hand side, as follows:

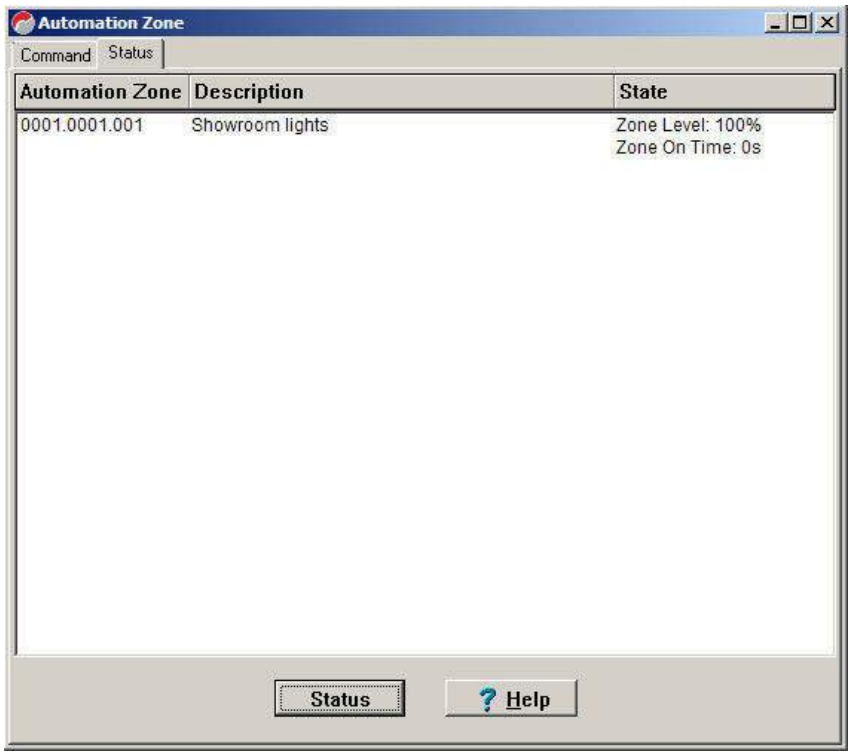
- Add — Specify a Challenger panel and one or more automation zones, and then add them to the right-hand side.
- All — Adds all available items to the right-hand side.
- Clear All — Clears the list of items.

Alternatively, double-click an item in the left-hand side to copy it to the right-hand side. Double-click an item on the right-hand side to remove it.

Refer to *Titan help* or the *Challenger Series Programming Manual* REV 06 (or later) for details about controlling automation zones.

Click the Status tab to request the current state of a selected automation zone (highlighted in the right-hand side of the Command tab).

Figure 26: Automation Zones control window, Status tab



Click Status to request the current state.

Chapter 3
Users

Summary

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

Content

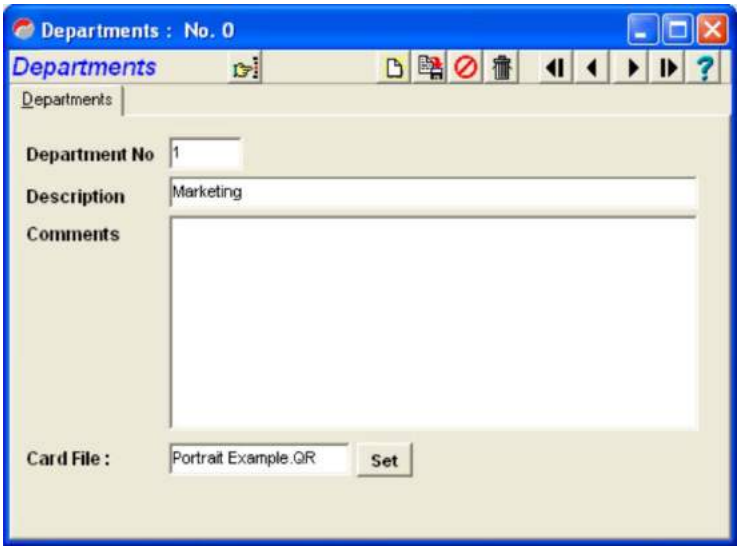
Creating departments 34
Managing user records 34
Advanced user procedures 46

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 window (Figure 27 below).

Figure 27: Departments window



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.

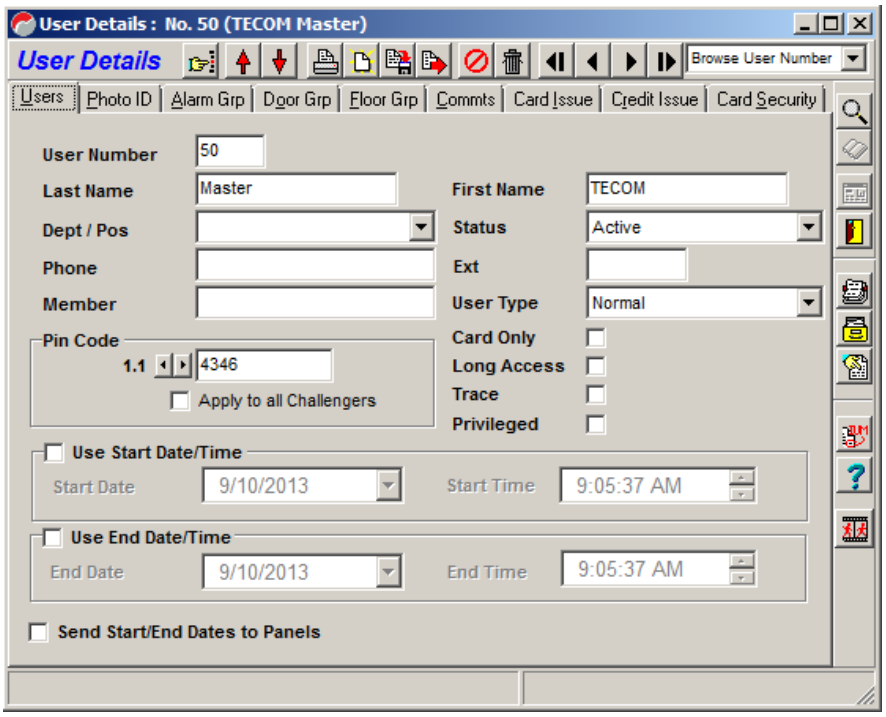
See “Designing a card layout” on page 52 for details about creating card formats.

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 28 on page 35) 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 28: User details window

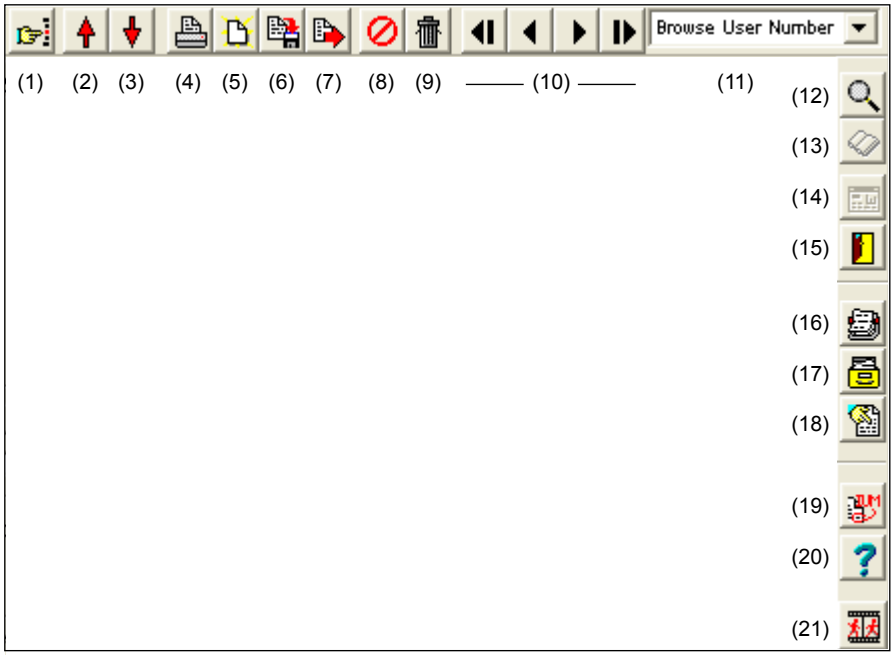


Let's look at the buttons and tabs in the user details window.

Quick access buttons

The User details window has quick access buttons on the top and right-hand sides (Figure 29 below) for common tasks. These quick access buttons are functional regardless of which window tab is displayed.

Figure 29: User details quick access toolbars



Key to Figure 29:

(1) Search
(2) Upload
(3) Download
(4) Print
(5) New record
(6) Save
(7) Bulk Save
(8) Cancel
(9) Delete
(10) First, previous, next, and last
(11) Browse selection
(12) Advanced user search
(13) Photo album
(14) Read card
(15) Last door details
(16) User journal
(17) User history
(18) User-defined fields
(19) IUM teach mode
(20) Help
(21) Reset anti-passback

The quick access buttons are described below.

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 allow you to select a range of user numbers from one or all Challenger panels.

Print: Prints the current user record information.

New: Creates a new user record.

Save: After making changes to a user's record, you must save the record.

Bulk save: Saves the current user and displays a Bulk User Save dialogue box.

The Bulk User Save dialogue box enables 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.

Advanced user search: Click to open the User search window (Figure 30 below). This is different from the Search button in that it allows you to search for users based on any number of criteria (first name, last name, department, etc.). Refer to Titan help for details.

Figure 30: User search window

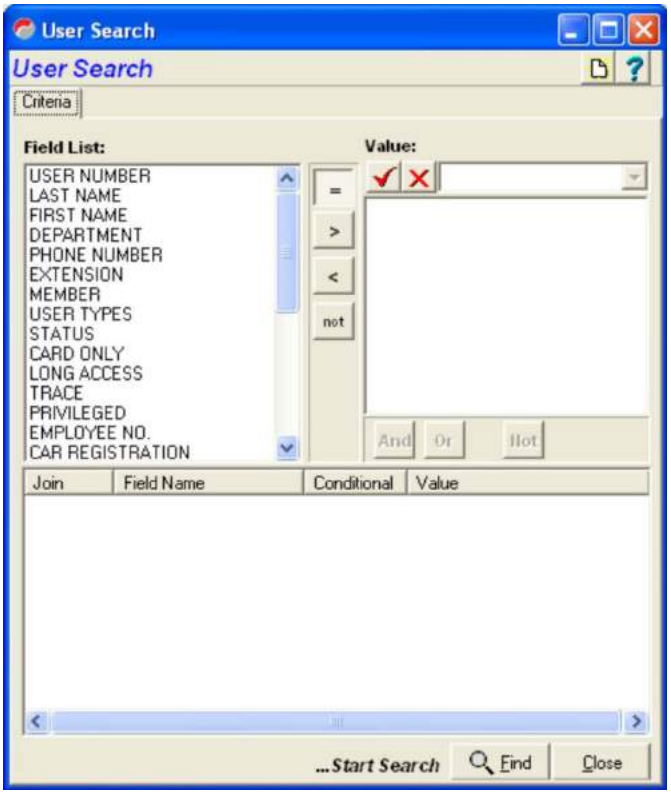


Photo album: The photo album is a collection of photos, user numbers and names for a group of users. The photo album allows you to preview or print a user photo album. This button is active after you find users via the User search window (Figure 30 above).

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

Last door details: This button shows the last door that the user opened.

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 43).

IUM teach mode: Quick method of collecting a card's raw card data, see "Collecting raw card data in IUM teach mode" on page 46.

Help: Launches the Titan help for the Users window.

Reset anti-passback: Click to reset the user's region record when you need to clear an anti-passback violation, see "Clearing an anti-passback violation" on page 48. After resetting, the user record must be downloaded to the 4-Door/Lift Controller DGP.

User detail window 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 31 on page 43). 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 34. For information on selecting an image for a photo ID card, see "Using a photo or captured image" on page 56).

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.

Note: The settings in this field are ignored for all users in the system if Save Start/End Dates to Panels is used.

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 V8 panels with expanded memory can have user-defined PIN codes for the first 1,000 users. Challenger Series panels (and Challenger V8 panels with IUM) can have user-defined PIN codes for all users (see Table 1 on page 109). 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 anti-passback" restrictions. **Note:** Privileged is only available on 4-Door/Lift Controller DGP readers.

Use Start Date/Time: Check the Use Start Date/Time check box if you want this user to be active only past a particular date and time. If used:

- Click the Start Date arrow, and then select the date of activation from the calendar.
- In the Start Time field, click the hours segment, and then use the up and down arrows to select the required value. Repeat for minutes and then for seconds.

For more details, see "Managing user start and end dates" on page 40.

Use End Date/Time: Check the Use End Date/Time check box if you want this user to be deactivated past a particular date and time. If used:

- Click the End Date arrow, and then select the date of deactivation from the calendar.
- In the End Time field, click the hours segment and then use the up and down arrows to select the required value. Repeat for minutes and then for seconds.

For more details, see "Managing user start and end dates" on page 40.

Save Start/End Dates to Panels: Check the Save Start/End Dates to Panels check box if you want all users in the system to be:

- Activated at the affected panels on the specified start date and time (any required alarm, door, and floor groups will be downloaded).

- Deactivated at the affected panels on the specified end date and time.

Notes:

- Do not use Save Start/End Dates to Panels in systems that have Intelligent 4-Door Controllers, Intelligent 4-Lift Controllers or Challenger V8 panels.
- If used, this setting ignores users' Status settings (active, void, lost, or expired).

For more details, see "Managing user start and end dates" below.

Managing user start and end dates

The Users tab in Titan 3.2 and later has the following checkboxes (and related fields) to manage the activation and deactivation of user records in Challenger panels:

- Use Start Date/Time
- Use End Date/Time
- Send Start/End Dates to Panels. This command affects all user records system-wide (for all Challenger Series panels in the Titan system). It controls how the other two commands operate, as described below.

When the Send Start/End Dates to Panels check box is **cleared** (default):

- Use Start Date/Time. When the user record (with a start date and time in the future) is saved the user is downloaded to the panel immediately (without access groups). An "Activate User" command is placed in Titan's timed command queue to be downloaded (with access groups) to the panel at the start date and time.
- Use End Date/Time. When the user record (with an end date and time in the future) is saved a "Cancel Expired User" command is placed in Titan's timed command queue to be downloaded to the panel at the end date and time. A user with access will lose access at the end date and time.

Note: The cleared setting is recommended for Titan systems that contain Intelligent 4-Door Controllers, Intelligent 4-Lift Controllers or Challenger V8 panels. It requires that Titan be connected at the applicable dates and times because of the commands stored in the timed command queue.

When the Send Start/End Dates to Panels check box is **checked**:

- Use Start Date/Time. When the user record is saved the start date and time is downloaded to the panel (any required alarm, door, and floor groups are also downloaded). Titan's timed command queue is not used, and Titan does not need to be connected to the Challenger Series panel at the start date and time. The user's Status settings in Titan are ignored.
- Use End Date/Time. When the user record is saved the end date and time is downloaded to the panel. Titan's timed command queue is not used, and Titan does not need to be connected to the Challenger Series panel at the end time. The user's Status settings in Titan are ignored.

Note: The checked setting must not be used for Titan systems that contain Intelligent 4-Door Controllers, Intelligent 4-Lift Controllers or Challenger V8 panels.

Uploading users

The following rules apply when uploading users from a Challenger Series panel to Titan:

- If a user's start and end dates are set to 0 in the panel, then the dates programmed for the user in Titan will not be affected.
- If a user's start and end dates are programmed in the panel (not 0), then these dates will be uploaded to Titan.
- If any of the panel's users have a start or end date not set to 0, then the Send Start/End Dates to Panels check box will be set to checked automatically (it will apply system-wide).

Photo ID tab

Use this tab to create and issue a security card for your employee (see "Creating and issuing cards" on page 56 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 (you can filter by system, or filter by Challenger panel). Select the required alarm groups and click OK.

Use the "Duplicate" button to select an alarm group and assign it to the user for every Challenger panel in the system.

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 (you can filter by system, or filter by Challenger panel). Select the required door groups and click OK. Access to each door in a group may be restricted by a time zone.

Use the "Duplicate" button to select a door group and assign it to the user for every Challenger panel in the system.

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 (you can filter by system, or filter by Challenger panel). Select the required floor groups 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.

Use the "Duplicate" button to select a floor group and assign it to the user for every Challenger panel in the system.

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 column indicates the Challenger number
- Status column indicates the current status of the card (Active, Disabled, Void, Reassigned or Lost)
- Raw card data column indicates a special number when an IUM is installed. There are 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 column indicates the card number.
- Site code column indicates the site or facility code.
- PIN code column indicates the PIN code.
- Status changed column indicates the date and time when the last status change has been made to this card user.
- Programmed column indicates whether 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 60 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 57 for details).

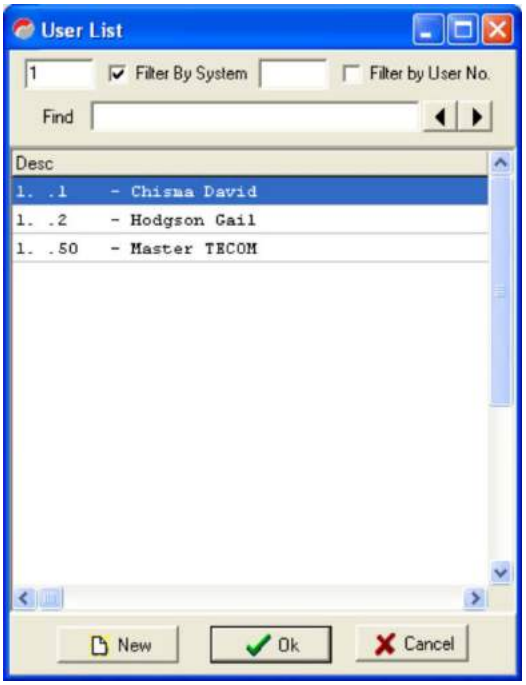
Card security: Set the access level and the locations where the credits can be used. (See "Card security (location/access rights)" on page 59 for details).

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 31 below), or the User search button to search for the user's name or a part of the name.

Figure 31: User list



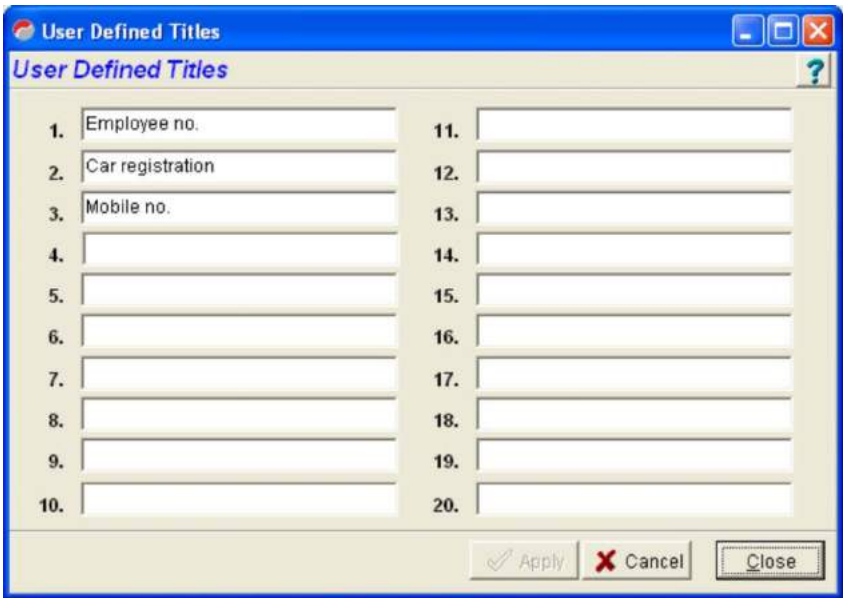
When you locate the record you want to edit with either search method, double-click the user record or highlight the user record and click OK to display the record in the User details window. Make the desired changes and click the save icon to save the information.

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 32 on page 44).

Figure 32: 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 Figure 29 on page 35). Enter the information for each user-defined title, then click the Save button. The User defined fields button is also used to view user information that has previously been saved in the user-defined fields.

Figure 33: 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 28 on page 35) 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 29 on page 35) to open the Bulk User Save dialogue box.

Figure 34: 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). 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.

Click Apply to perform the selected bulk function.

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 Raw Card Data field in the User Details window (Card Issue tab).

To collect raw card data in IUM teach mode:

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 29 on page 35).
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.

Note: Challenger Series panels have a setting in System Options to record the Card Learn RAS number. The Card Learn RAS is used to enter a user's card data into the Challenger system by badging the card at the reader during the user creation process via RAS, not via Titan.

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.

Tip: Challenger Series panels are IUM format only, so site codes are not needed for the panel itself. However, site code and offset are used in Titan for generating raw card data. When a new user is created in Titan, user card data is populated based on the IUM format (card format) selected in the Challenger window (Options tab), and the site code and offset values configured in the System Options window (System Options Part 3 tab).

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 35 on page 48).
- 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

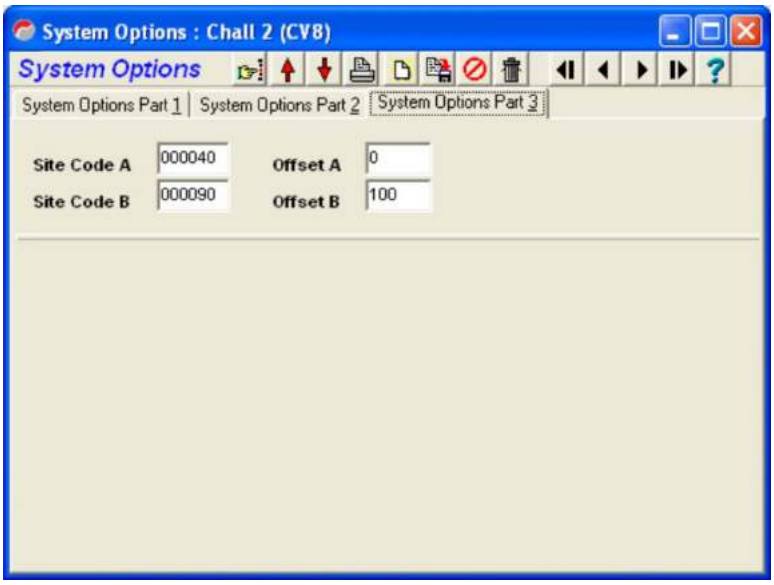
If the required offset is outside of the range -32,767 to +32,767, Titan automatically adjusts the offset value when the record is saved. For example:

- 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 a batch of cards with a different site code:

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 35 on page 48.
5. Save the record.

Figure 35: Site codes and offsets



Clearing an anti-passback violation

Anti-passback 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 anti-passback 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 anti-passback).

Alternatively, the operator can click Reset anti-passback in the User Details window (Figure 29 on page 35), 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.

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. If applicable, select either Site Code A or Site Code B, which will be used to generate the raw card data. The site code values are programmed in each Challenger panel's system options.
6. Alternatively, select the "Update using" radio button, and then:
   - Click the Card Type arrow, and then select the required card format.
   - Type the Site Code value (the acceptable range of values depends on the selected card type).
   - Type the Offset value, if a card offset is required.
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

Summary

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.

Content

Designing a card layout 52
Creating and issuing cards 56
- Using a photo or captured image 56
- Using smart cards for credit 57
- Card security (location/access rights) 59

Writing smart cards or fobs 60

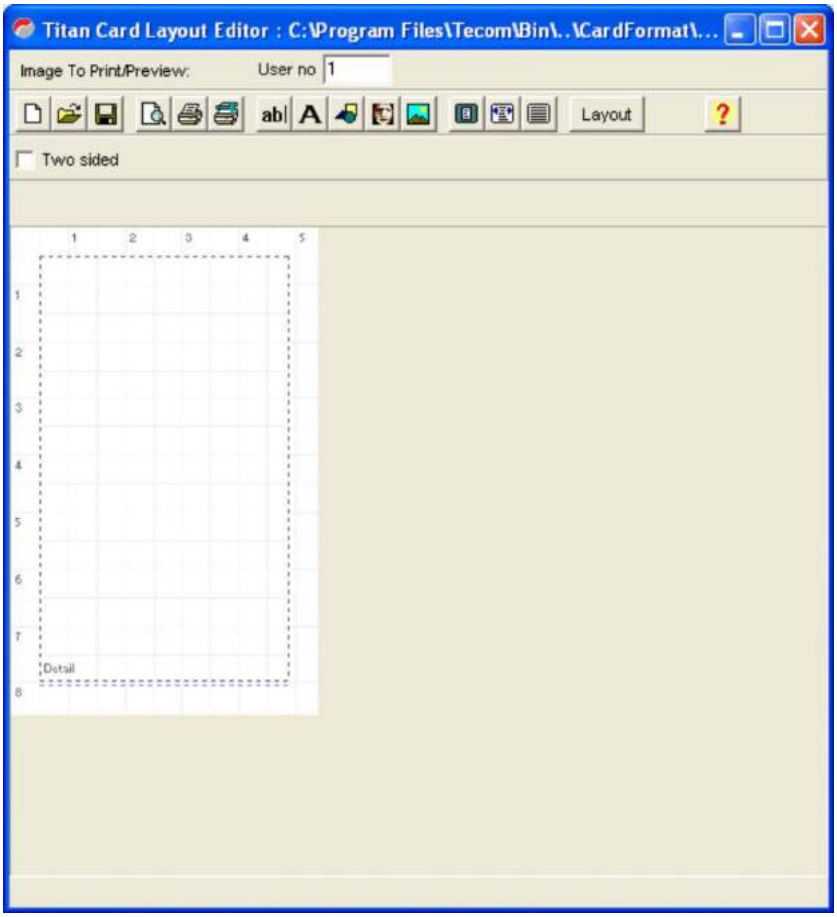
Designing a card layout

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 36 below).

Figure 36: Card layout editor



The Card layout editor has buttons that are used to create or edit card designs (Figure 37 on page 53).

Additional buttons display below top line, depending on the selected task.

Figure 37: Card layout editor buttons



Key to Figure 37:

(1) New: Creates a new card layout

(2) Open: Opens a previously saved card layout

(3) Save: Saves the current card layout

(4) Print preview: Previews the current card layout before printing

(5) Print: Prints the current card layout

(6) Print setup: Configures printer settings

(7) Add db field: Adds a database field or function to the card layout

(8) Add label: Adds normal text to create labels in the card layout

(9) Add shape: Adds a shape to the card layout (circle, rectangle, lines)

(10) Add db image: Defines an area on the layout to place the user's image

(11) Add image/background: Adds an image or background to the card layout

(12) Fit height: Fits card layout view to window height

(13) Fit width: Fits card layout to window width

(14) No scaling: Displays card layout at full size

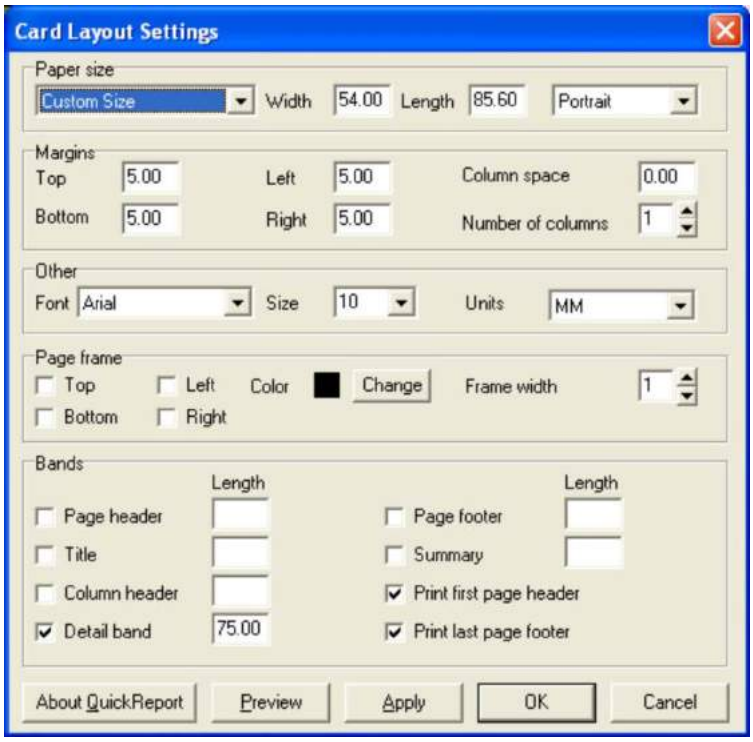
(15) Layout: Opens the card layout settings dialogue box (Figure 38 on page 54)

(16) Help: Opens the Card layout help topic

(17) Two sided check box

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 38 on page 54).

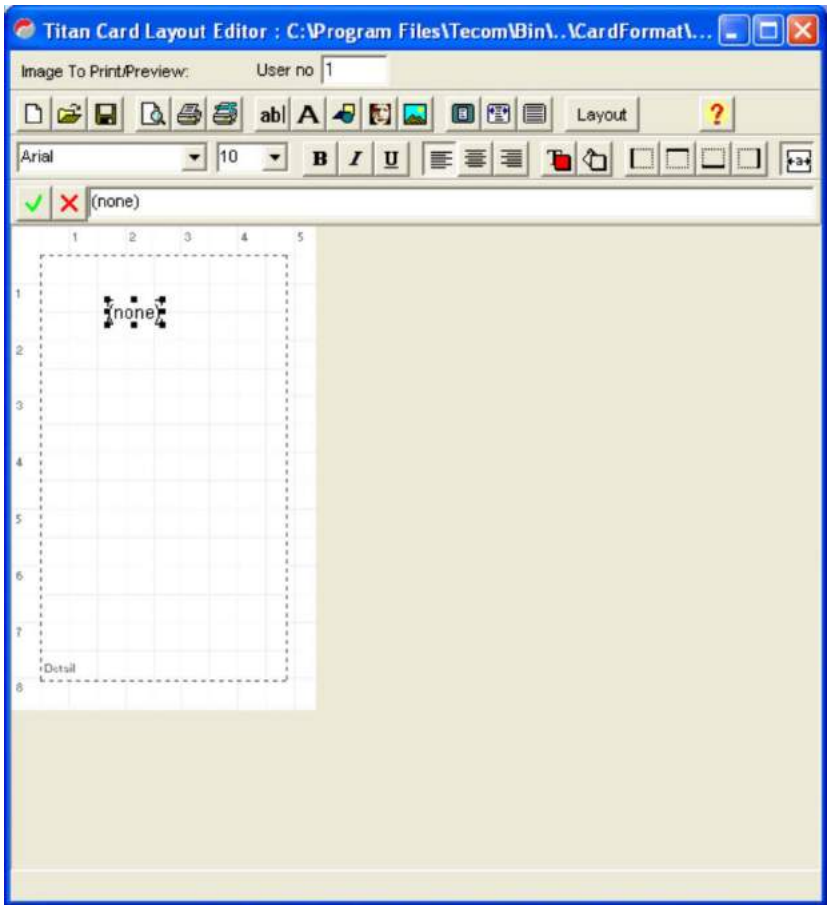
Figure 38: Card layout settings window



To design a card layout:

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, and then click Apply. Click OK to close this window.
3. Optionally, if you have duplex card printer (one that prints on both sides of the Photo ID card) and want to create a two-sided layout, select Two sided on the Card Layout Editor window (Figure 37, item 17).
4. Click the Add image/background button (Figure 37, item 11) to add a background or an image to the card layout, such as the company logo. New options appear under the main toolbar.
5. 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.
6. Click the Add label button (Figure 37, item 8) to add a text label, such as “Name” or “Department”, to the layout. Click in the card layout where you want to place the label.
7. After you add the label, new options appear to allow you to format the text (Figure 39 on page 55). Note the text field “(none”) in the toolbar. Replace the text with your own label, and then click the green check button to apply the change. Use the text formatting toolbar to format your new label.

Figure 39: Add label window



8. Click the Add db field button (Figure 37, item 7) to add a database field to the layout. This loads the user data directly from the user database.
9. After you add the database field, new options appear in the Card layout editor, similar to the Add label options. Click the **fx** button to open the Expression Wizard window (Figure 40 below).

Figure 40: Expression wizard (with one field added)



10. 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, and then click OK.
11. Use the Expression Wizard buttons to refine the database fields. For example, Figure 40 on page 55 contains the simple expression LayoutData._FIRST_NAME, which would print 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
    ```
12. After you've built your expression, click Validate to check it.
13. Click OK again to close the Expression Wizard. The field now appears in the card layout. Use the formatting toolbar to format the field, and then click the green check button to activate the changes.
14. 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, and then use the grid to align it.
15. Click the Print preview button to preview the current card layout for the selected user number.
16. Click Close and change the user number field to preview another user.
17. When you are satisfied with the layout, click Save.

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

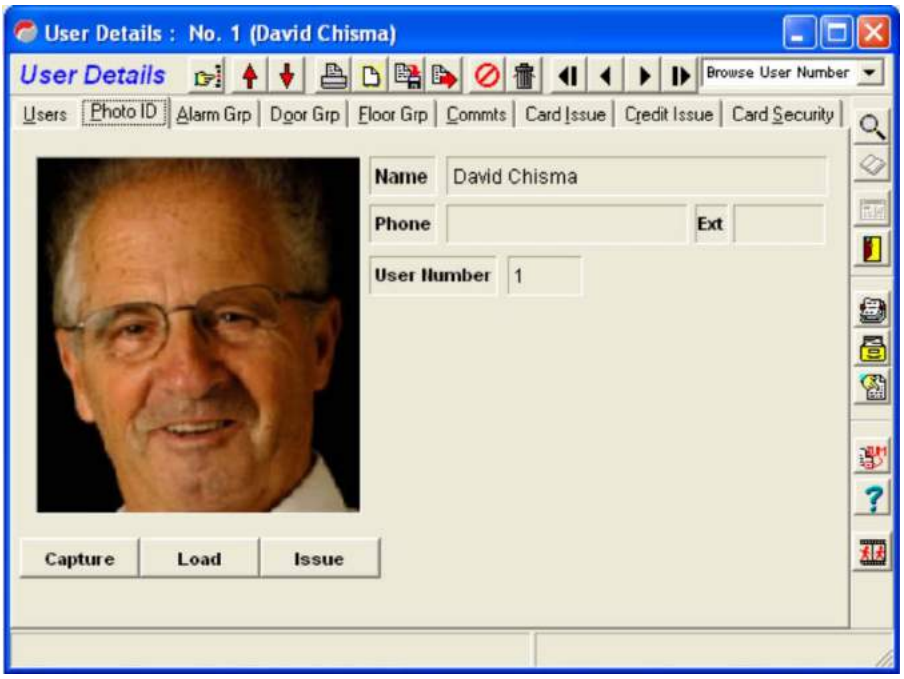
Creating and issuing cards

This section describes how to set up and print a layout on a user card. See "Writing smart cards or fobs" on page 60 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 41 on page 57).

Figure 41: 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 centre 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

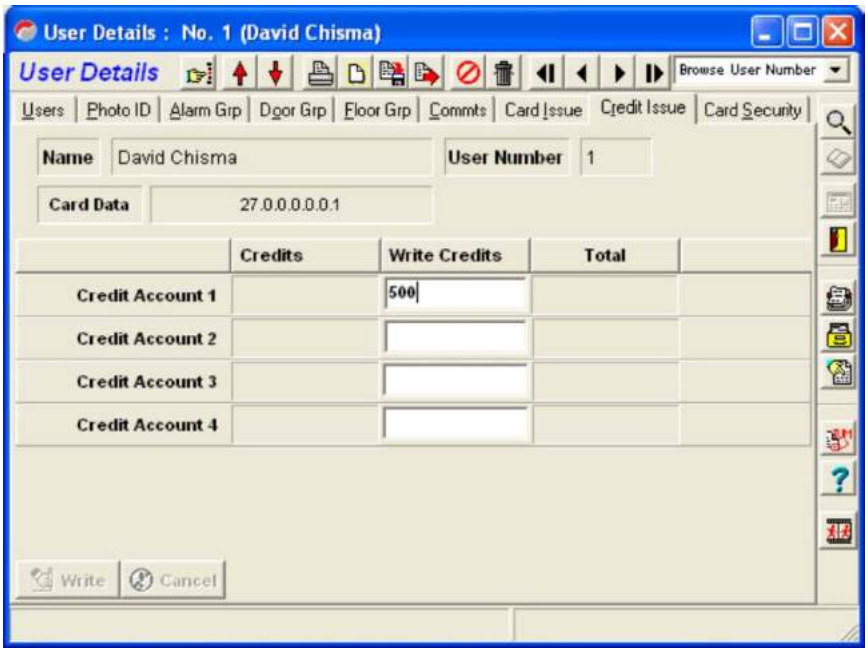
Smart cards or fobs may be used for resource control (credit use). For example, a tennis court may issue smart cards to members in order to operate lighting at night. The credit functionality could, for example, provide 10 hours of lighting before the card would have to be 'recharged'.

Note: Smart cards do not offer the same functionality as genuine credit cards (such as Visa, American Express, and so on). In the context of smart cards, ‘credit’ refers to token values allocated to a card and ‘credit accounts’ refers to groups of credits. We recommend 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 42 below).

Figure 42: 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-hand corner 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 60 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.

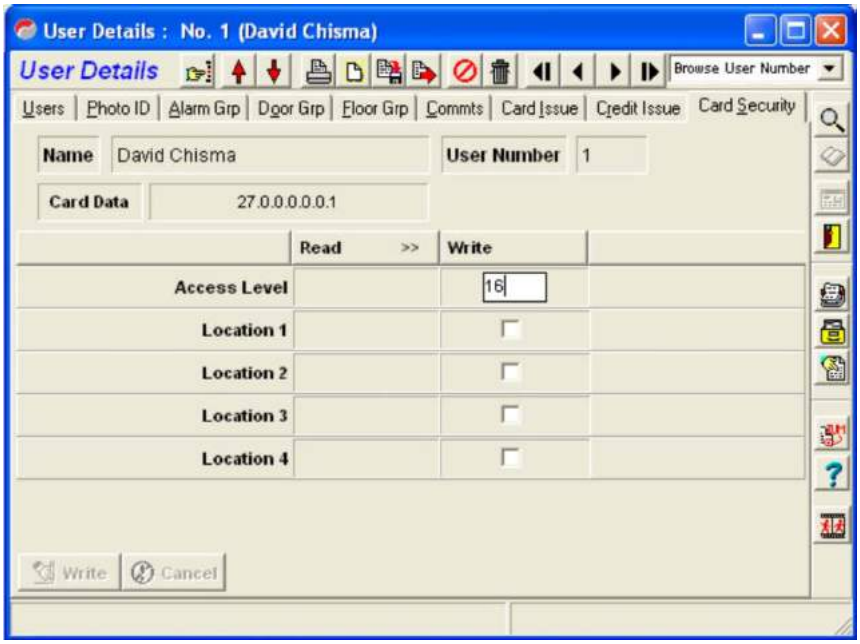
Card security (location/access rights)

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 43 below).

Figure 43: 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, and 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. Writing cards is typically used to program a smart card, or to add account credits, and so on.

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

To write a card:

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

Summary

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.

Content

Reports menu 62
- User reports 62
- Admin reports 63
- Challenger reports 64
- Print all reports 64
- Users by region 64
- Muster 65
- Event tree 65

History menu 65
- Custom history reports 65
- User history by department 67

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 (.WMF) format by clicking Print and then clicking the Save Report button in the print preview window.

Note: Do not save reports in .RTF or .TXT formats because you may not produce acceptable results.

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 44 on page 63).

User summary: Displays summary data for a range of users or all users of a specified Challenger (see Figure 45 on page 63). 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 67.

Figure 44: User report window



Figure 45: 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

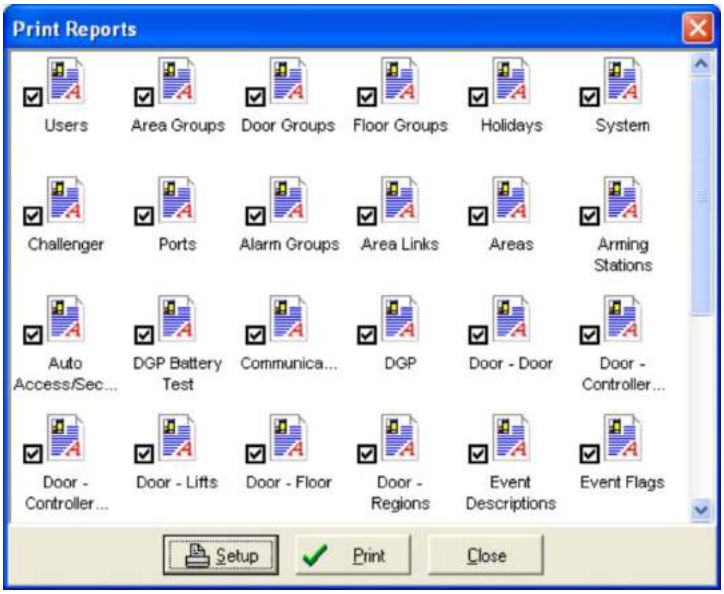
Challenger reports print programming details of a single Challenger panel and are accessed by selecting Reports > Challenger.

Some examples of Challenger panel reports are: Area groups, 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 46 below).

Figure 46: Print all reports window



Click to 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

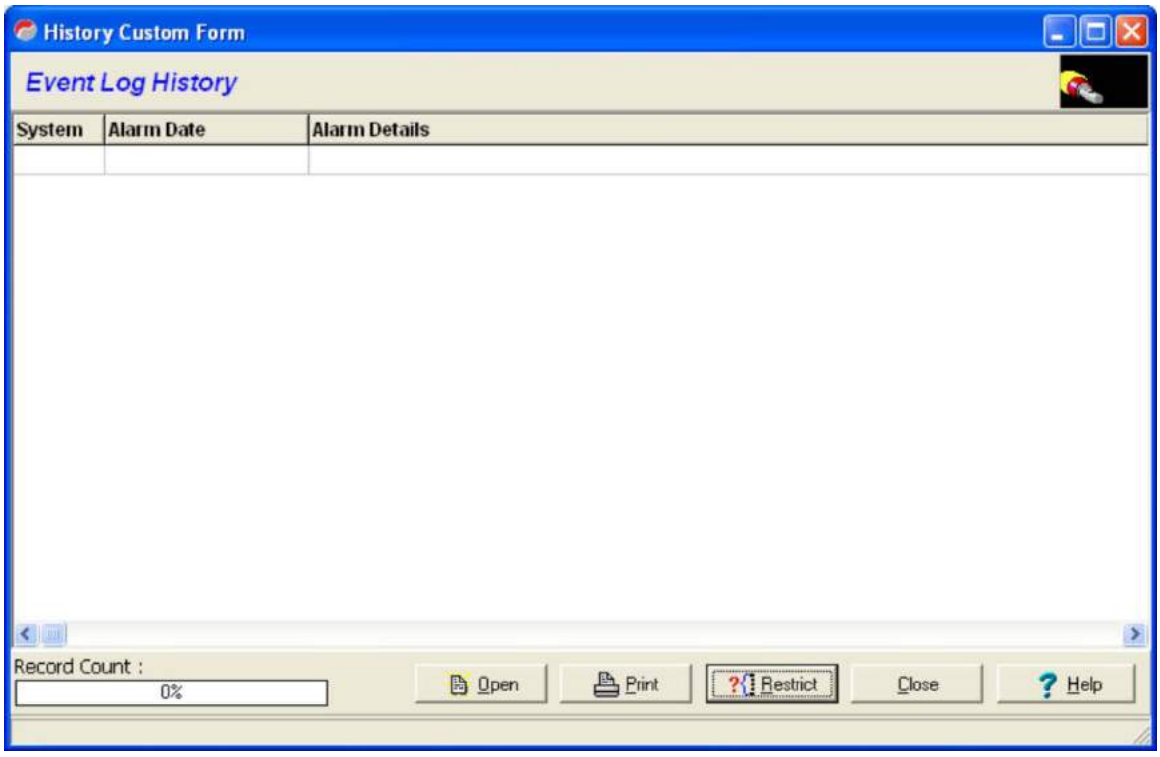
You can view or print a custom history report from either:

- Data contained in the live event log
- Saved data

To create a custom history report:

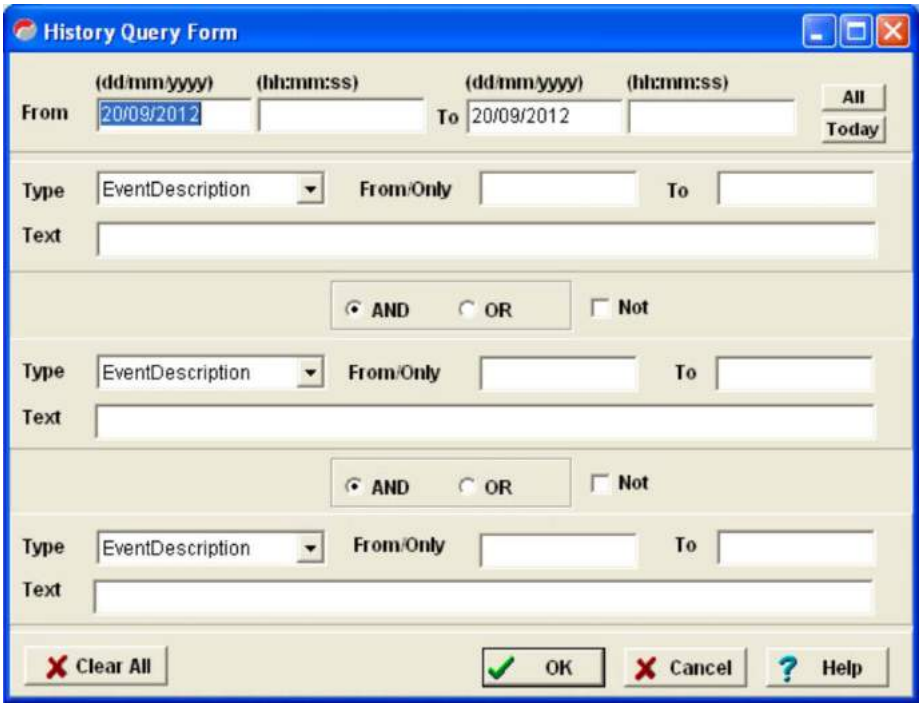
1. Go to History > Reports > Custom. The Custom History Restrict window displays (Figure 47 below).

Figure 47: Custom History Restrict window (initial state)



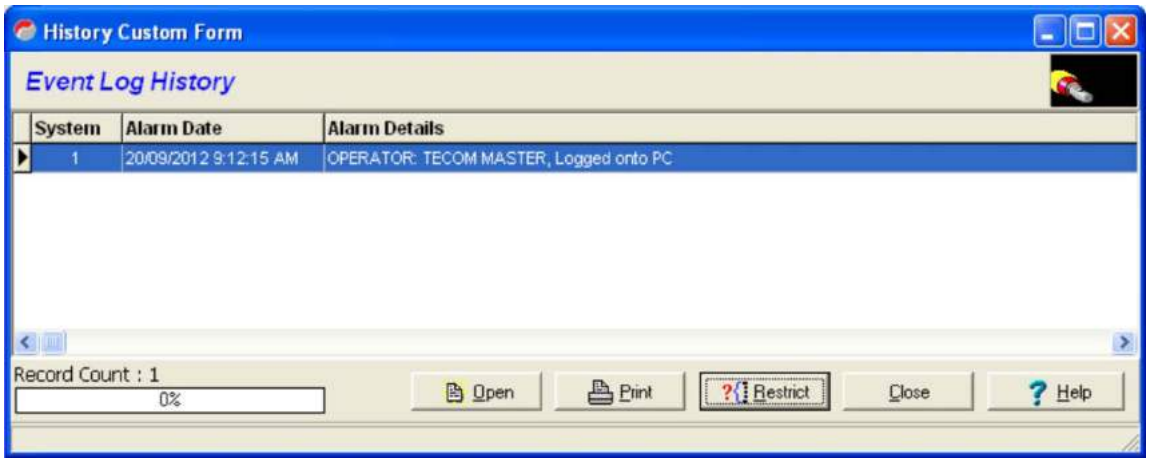
2. If you want a report based on data contained in the live event log, click Restrict to open the history query window (Figure 48 below).
3. Alternatively, if you want a report based on previously saved data, click Open to select the history file. The path and filename of the open file displays below the record count display. Click Restrict to open the history query window.

Figure 48: 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 49 on page 67). Double-clicking any of these entries will bring up a window explaining the details of the event.

Figure 49: 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.

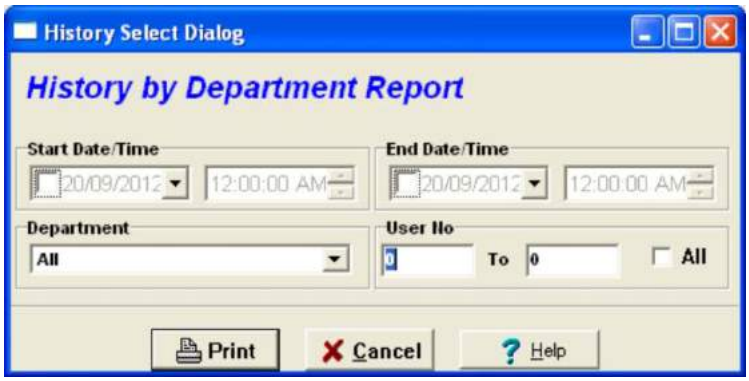
User history by department

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 50 below).

Figure 50: User history by department report window



Chapter 6
Operation

Summary

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.

Content

Operating Titan 70
- Using the Control menu 70
- Responding to alarms 72
- Remote dial-up connection 73
- Managing times and dates 73
- Recording manual events 73
- Managing alarm ‘help action’ messages 73

Record-keeping 74
- Live Event Log 74
- User Journal Viewer 74
- Reports 74
- Full Log upload 74

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 common security commands
- Check the status of items to ensure 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 82).

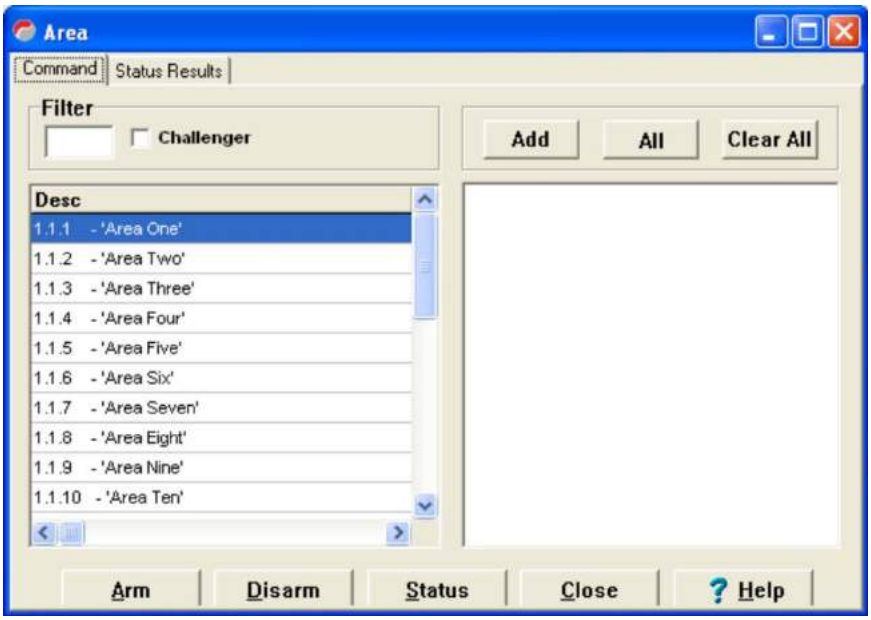
Arming an area

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

To control an area:

1. Go to Control > Area to open the Area window (Figure 51 on page 71).
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.

Figure 51: Control area window



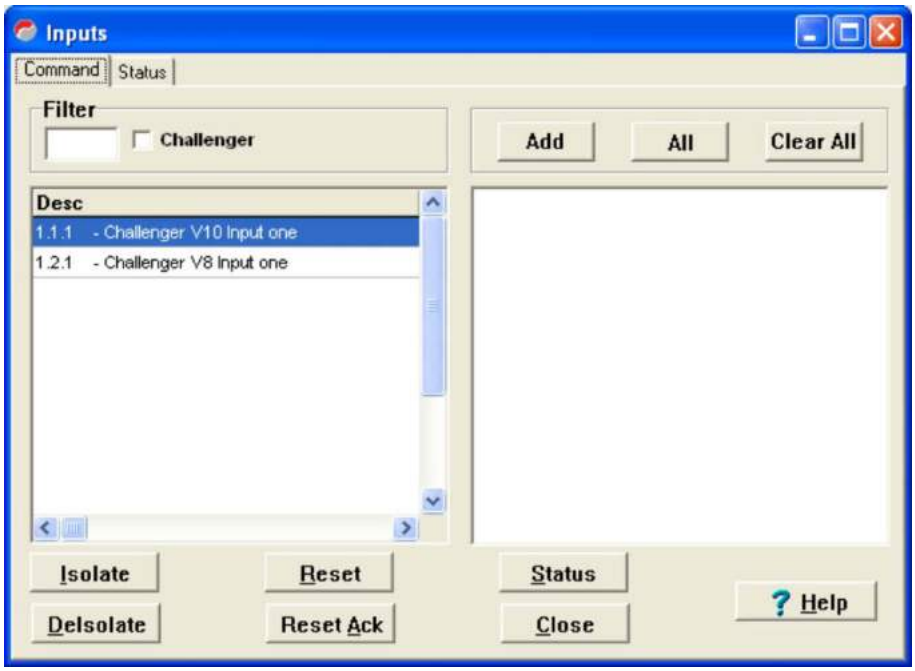
Isolating an input

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:

1. Go to Control > Input to open the Inputs window (Figure 52 on page 72).
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.

Figure 52: Control inputs window



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 pre-programmed 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 73 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 pre-programmed 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 pre-programmed 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 re-alarm after a pre-set 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 a speed appropriate to 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 65 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 V8 panel firmware 8.112 (or later) or Challenger Series.

Chapter 7
Administration

Summary

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.

Content

Administering your Titan system 78
- Connecting to Challenger panels 78
- Viewing and managing command queues 78
- Managing operator records 79
- Defining alarms 81
- Managing system maps 82
- Cloning a system 84

Maintaining the Titan database 85
- System Manager 85

Administering Challenger systems 103
- Managing Challenger panel settings 103
- Adding a panel 105
- Challenger panel programming 105
- Upgrading Challenger device firmware 106
- Upgrading Challenger system capacity 108
- Migrating a Challenger V8 system to Challenger10 110
- Upgrading a Challenger10 (pre V10-06) panel 111

Administering your Titan system

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

- “Connecting to Challenger panels” below
- “Viewing and managing command queues” below
- “Managing operator records” on page 79
- “Defining alarms” on page 81
- “Managing system maps” on page 82
- “Cloning a system” on page 84

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 Series panels directly via USB connection. Additional connection types may be used, such as RS-232, modem or Ethernet (no additional hardware required).

Note: ChallengerSE panels’ onboard Ethernet, USB, and RS-232 communications ports are time-limited and will automatically disconnect after 60 minutes (however, the connection timer can be restarted via RAS to extend the time). In order to have unlimited connection, the panel must be fitted with a communications module (such as a TS1091 Enhanced Communications Licence).

Titan is typically connected to Challenger V8 panels directly via serial connection. Additional connection types may be used, such as modem or Ethernet (may require additional hardware).

You can connect up to 16 Challenger panels simultaneously. We recommend that you do not exceed 16 simultaneous connections. When connecting via modem, only one Challenger may be connected at a time.

Refer to Titan 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.

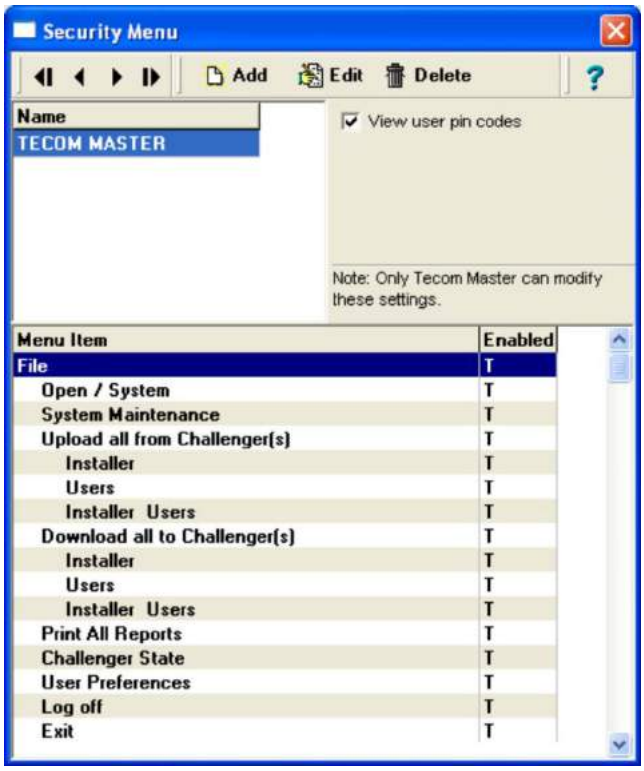
Managing operator records

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 53 on page 80). Menus that are not included in an operator's permissions are greyed and unavailable when the operator logs in.

Figure 53: Security menu window



Adding an operator

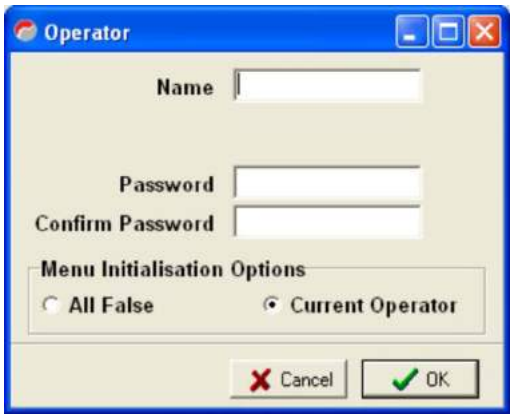
The Security menu window displays a list box of operator records. The default TECOM MASTER operator record is provided with Titan.

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 53 above) 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 54: New operator window



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

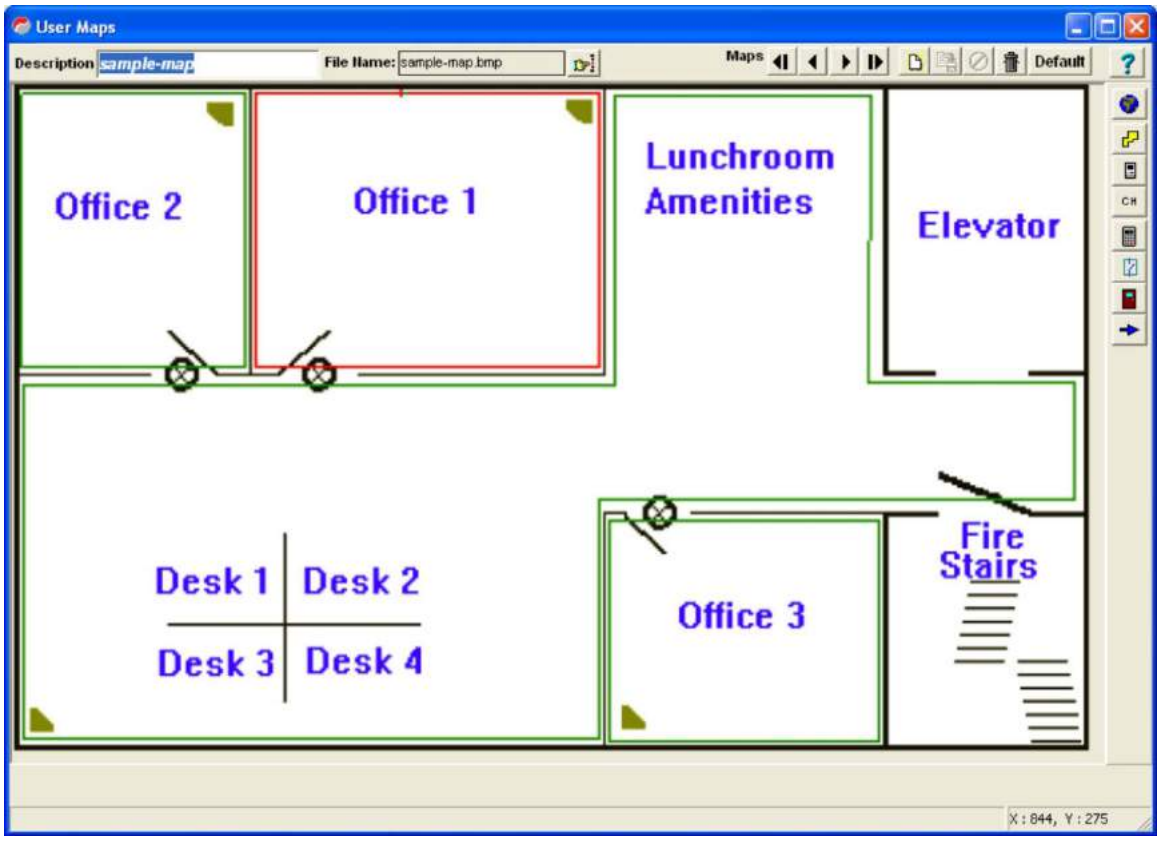
Prior to adding a map, you need a suitable .bmp file to serve as the background image, over which you'll place icons. Store the .bmp file in a location you can later navigate to (for example, in C:\Program Files\Tecom\Bin\Images).

To add a map:

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 (Figure 55 on page 83). 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.
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.

Figure 55: User maps (editing) window



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.

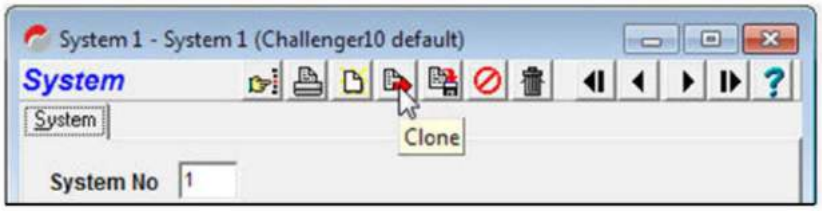
When a device has been linked to a map icon, the icon flashes when the device is in alarm. If the map contains several devices in alarm simultaneously, the icons for all the devices in alarm will be flashing. You can identify a particular device in alarm by selecting the alarm in the Alarm acknowledgment 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, de-isolate, to open the control window, or to view the history log.

Cloning a system

Cloning a system copies the Challenger panel and system data from an existing system into a new system.

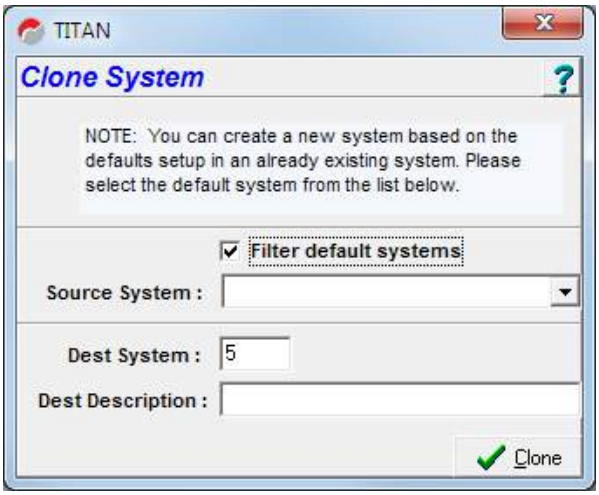
Figure 56: System window Clone button



To clone an existing system:

1. From the System window, click the Clone button to open the Clone System window (Figure 57 below).
2. In the Clone System window, click the “Source System” arrow, and then select a system to clone.

Figure 57: Clone System window



The “Filter default systems” check box is populated in order to list only the systems that are designated as default systems (the “Default System” check box is populated on the respective System window). Clear the “Filter default systems” check box in order to choose any system for cloning.

3. Type a new name in the “Dest Description” field. If left blank, the new system will have the same name as the source system (but it can be edited later).
4. Click the “Clone” button.

Maintaining the Titan database

All data used and generated by Titan are stored in a database on the Titan computer.

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.

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.

A routine maintenance strategy typically involves the following tasks:

- Regularly run System Manager, or otherwise configure your computer so that System Manager starts automatically.
- Backup events. See “Backing up a system” on page 87.
- Export system, users, and user journals. See “Exporting a system” on page 89.
- Purge a selected range of records. See “Purging a system” on page 93.
- Backup the database. See “Backing up the Titan database” on page 98.
- Verify that the operations have been completed successfully. See “Checking the job log” on page 102.

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).

We recommend that you use one of the following maintenance regimes:

- **Robust maintenance regime:** We recommend 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:** We do 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

The Titan system maintenance utility starts automatically and runs minimised each time the computer is started. If it’s not running, use one of the following actions to start it:

- Click (typically) Start > All Programs > Tecom > Titan > System Manager.
- In Titan go to File > System Maintenance.

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.

WARNING: 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 “Purging a system” on page 93 for details.

The following sections describe System Manager functions.

Backing up a system

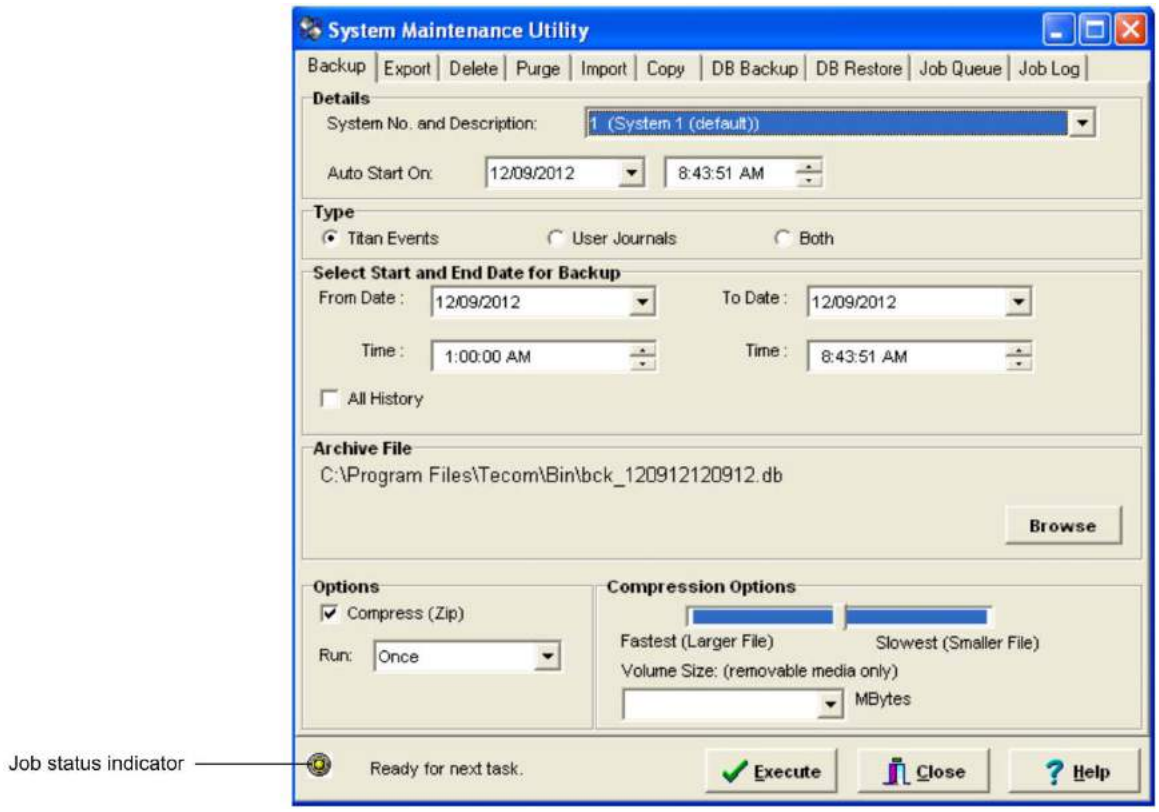
Backup saves a Titan system’s entire event history or a selected portion to a backup file with optional file compression. Backup is typically used for:

- 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 58 on page 88.

Figure 58: 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:

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 58 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.

Exporting a system

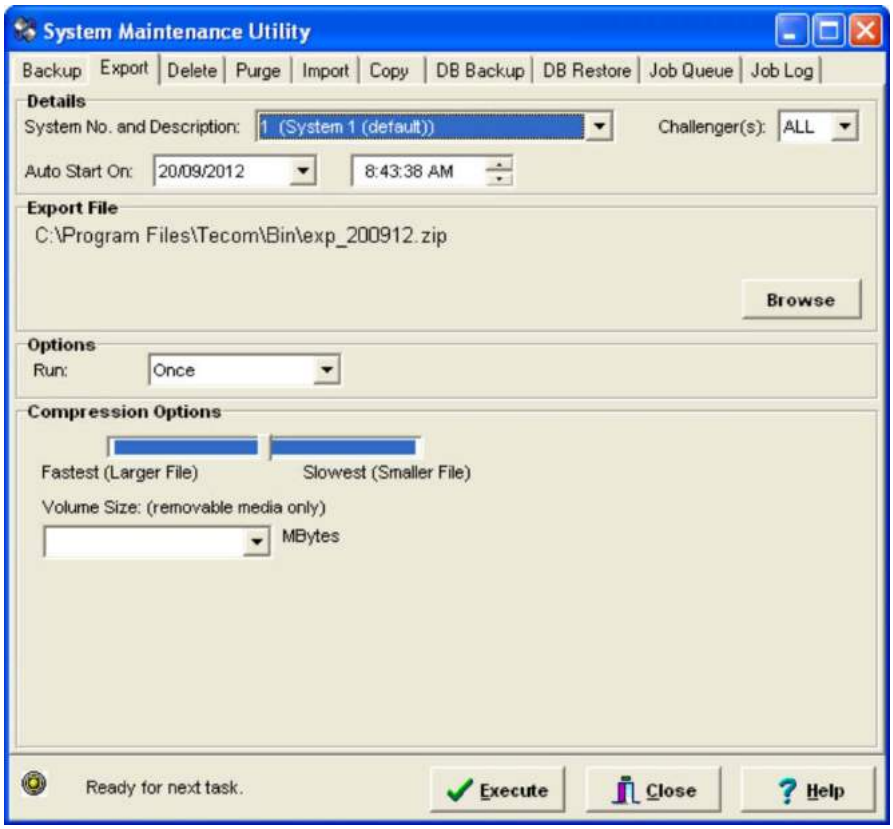
Export backs up a Titan system, the system's user journals, and one or more selected Challengers. Export is typically used:

- 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 "Importing a system" on page 95).

The Export tab is shown in Figure 59 on page 90.

Figure 59: Export tab



To export a system:

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 58 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.

Deleting a system

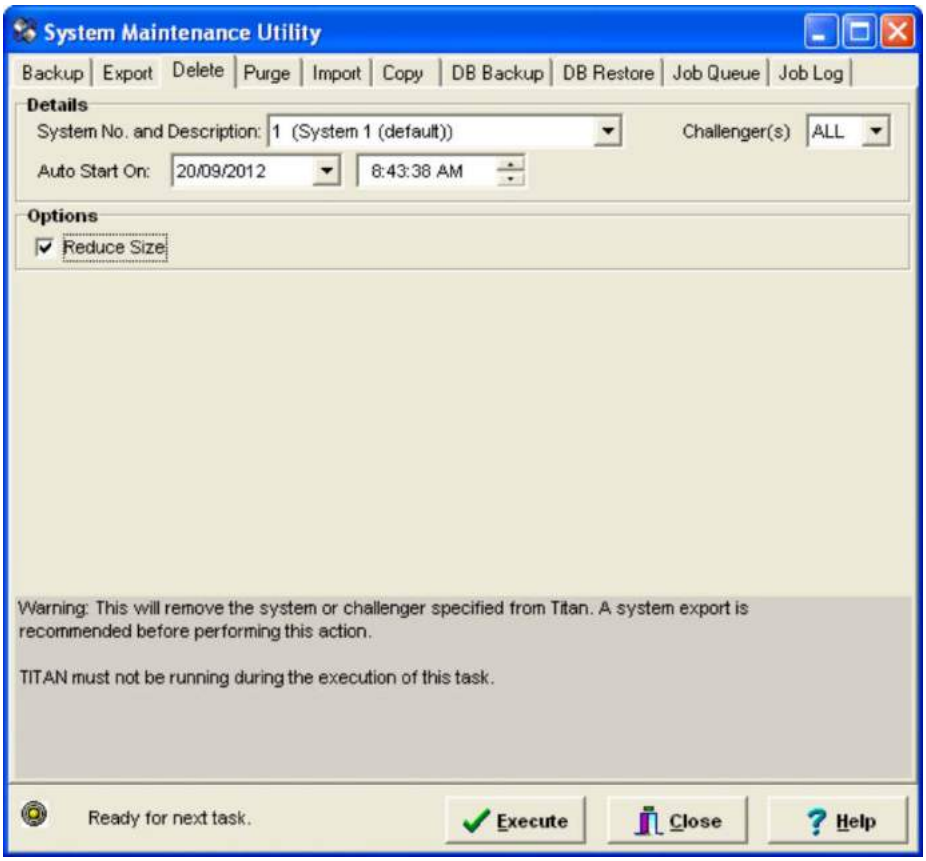
Delete permanently removes an entire Titan system or selected Challenger(s) from Titan. Delete is used when a system or a Challenger on a system is no longer required.

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 “Backing up a system” on page 87 and “Exporting a system” on page 89 for details.

The Delete tab is shown in Figure 60 on page 92.

Figure 60: Delete tab



To delete a system:

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. Click Execute. You'll be prompted for your Titan user ID and password.
8. Type your Titan user ID and password, and then click Execute. The Job Queue tab displays.
9. Check the job status indicator (shown in Figure 58 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.

Purging a system

Use Purge for normal housekeeping and maintenance. The Purge tab is shown in Figure 61 below.

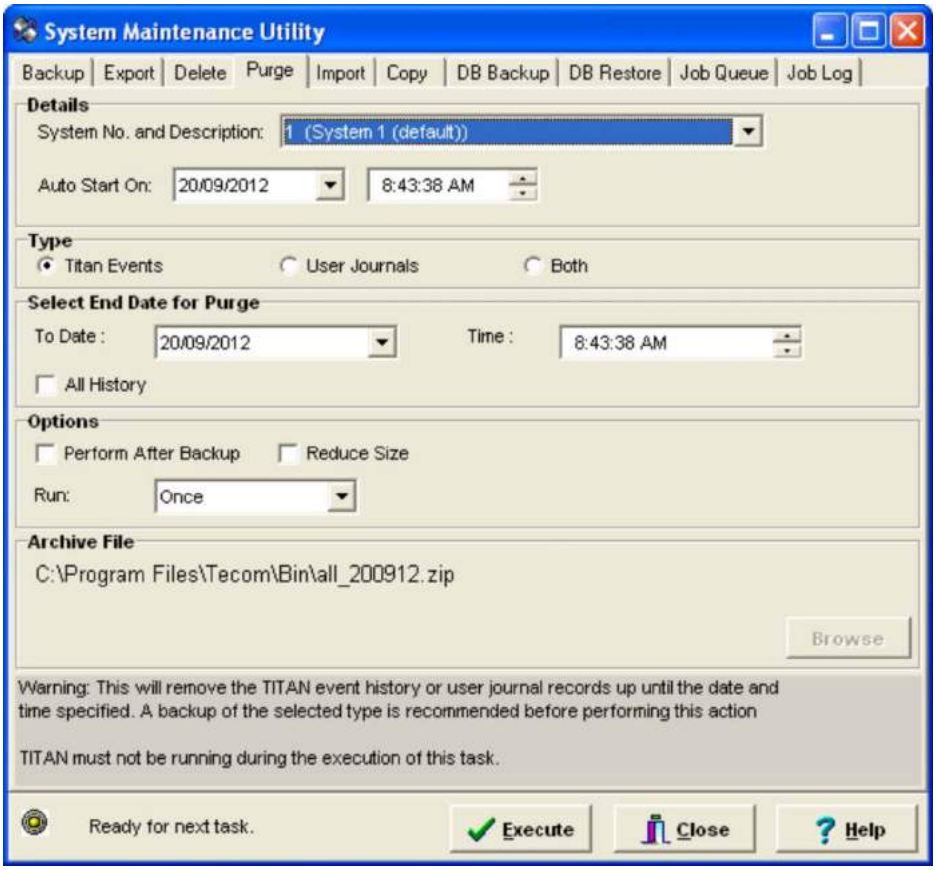
We recommend that you purge unneeded records from your system frequently in order to control the size of the database, and use the Reduce Size option to reduce the database file size. The frequency that you purge your system determines the range of records that you need to purge (and therefore the length 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 “Backing up a system” on page 87 and “Exporting a system” on page 89 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 61: Purge tab



To purge a system:

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. 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.
10. 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.
11. Click Execute. You'll be prompted for your Titan user ID and password.
12. Type your Titan user ID and password, and then click Execute. The Job Queue tab displays.
13. Check the job status indicator (shown in Figure 58 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.

14. After the purge, the job status indicator displays yellow to indicate that processes are idle. Check the job log (see “Checking the job log” on page 102) to verify that the purge was successful.

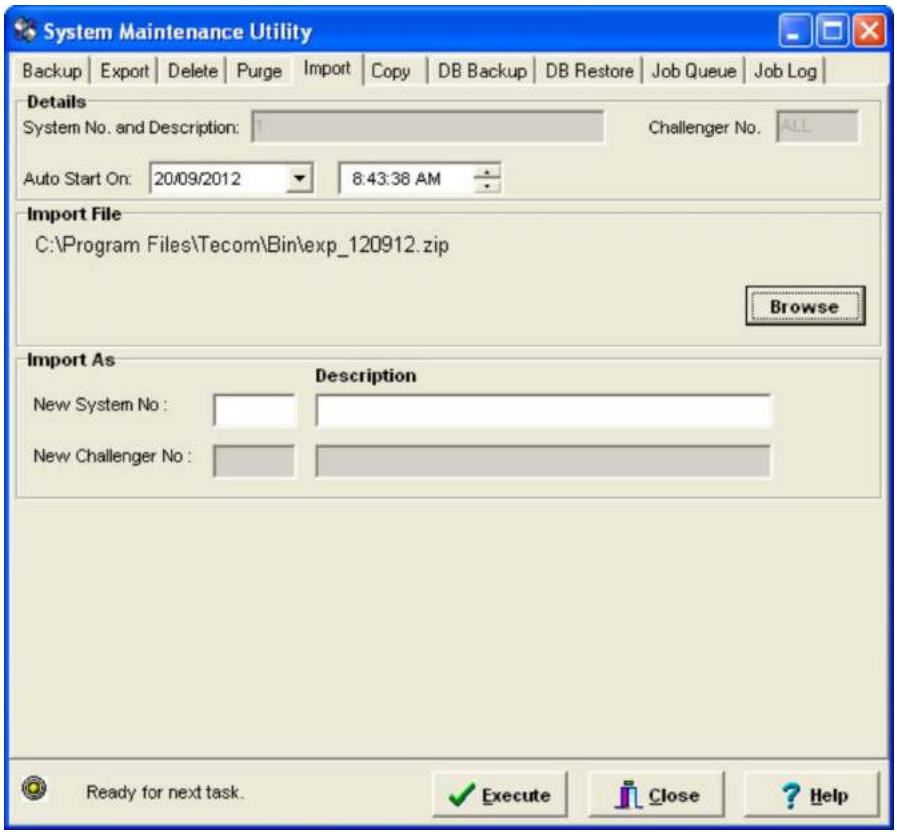
Importing a system

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 62 below.

Figure 62: Import tab



To import a system or a Challenger:

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 58 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.

Copying 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.

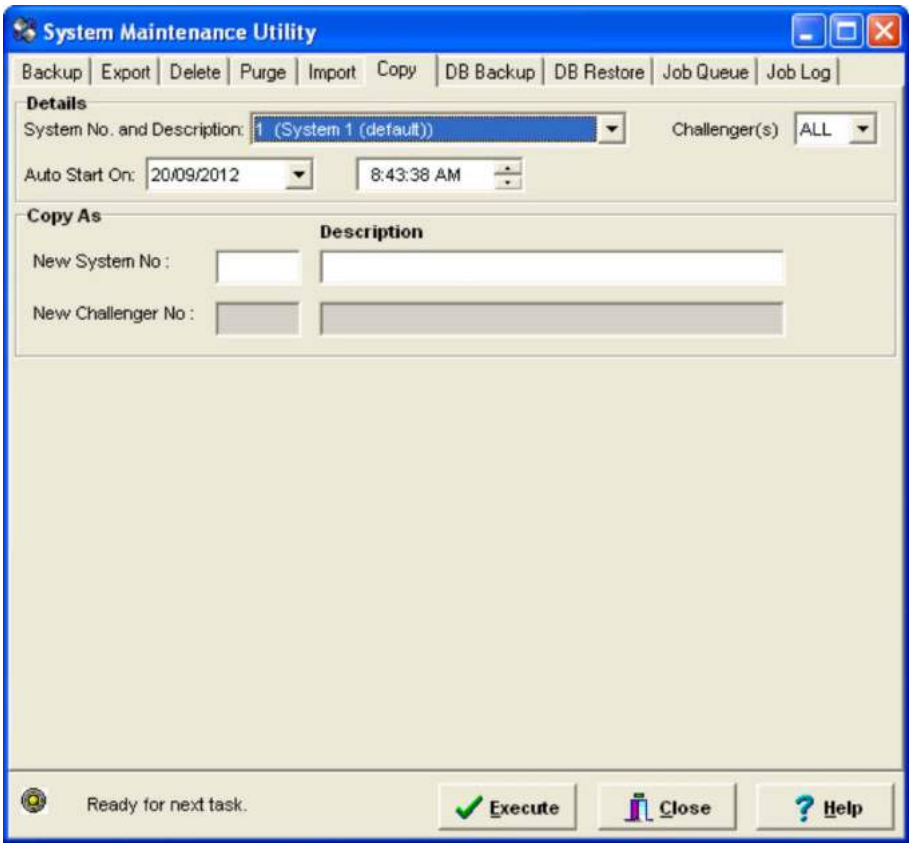
Note: If you copy a single Challenger, the Challenger's user records are not copied.

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 63 on page 97.

Figure 63: Copy tab



To copy a system or a Challenger:

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.

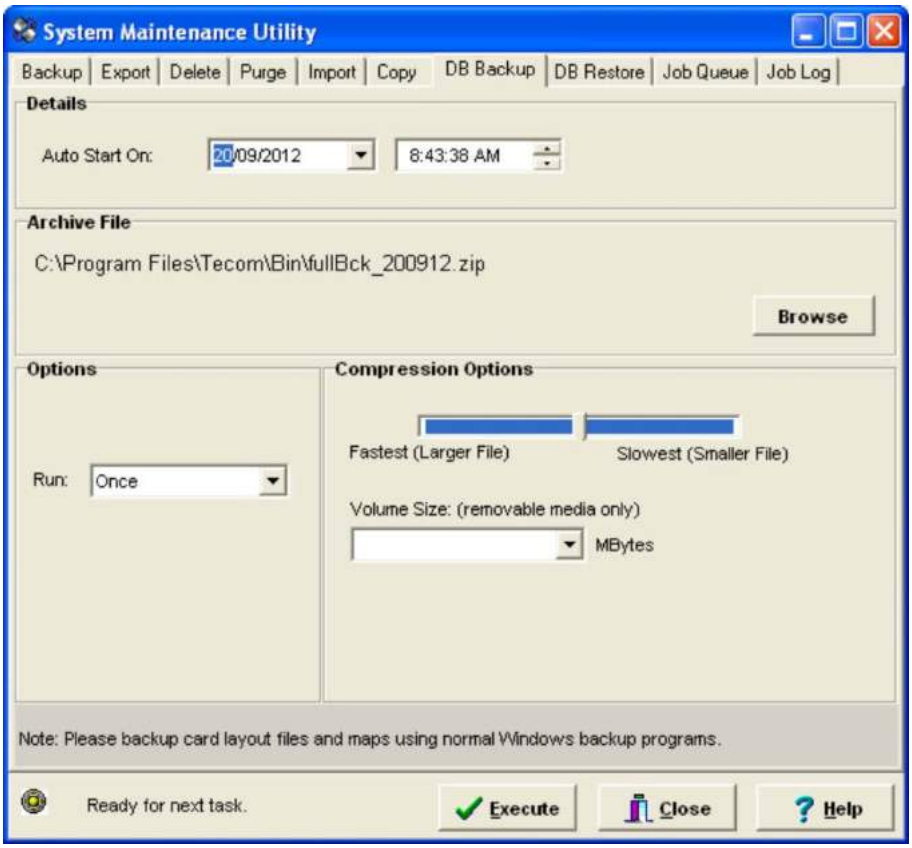
12. Check the job status indicator (shown in Figure 58 on page 88) at the scheduled time. The job status indicator will flash green to indicate that the copy is in progress. Alternatively, check the job queue.

Backing up the Titan database

Use the DB Backup tab to perform or schedule a hot backup of the Titan 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, timed command queue, card layout files, or maps.

The DB Backup tab is shown in Figure 64 below.

Figure 64: 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. Drag the Compression Options slider to adjust the amount of data compression (or use the default value).

7. 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.
8. Click Execute. The Job Queue tab displays.

Note: If you're backing up the Titan database frequently, check the archive file location periodically and delete unneeded backups.

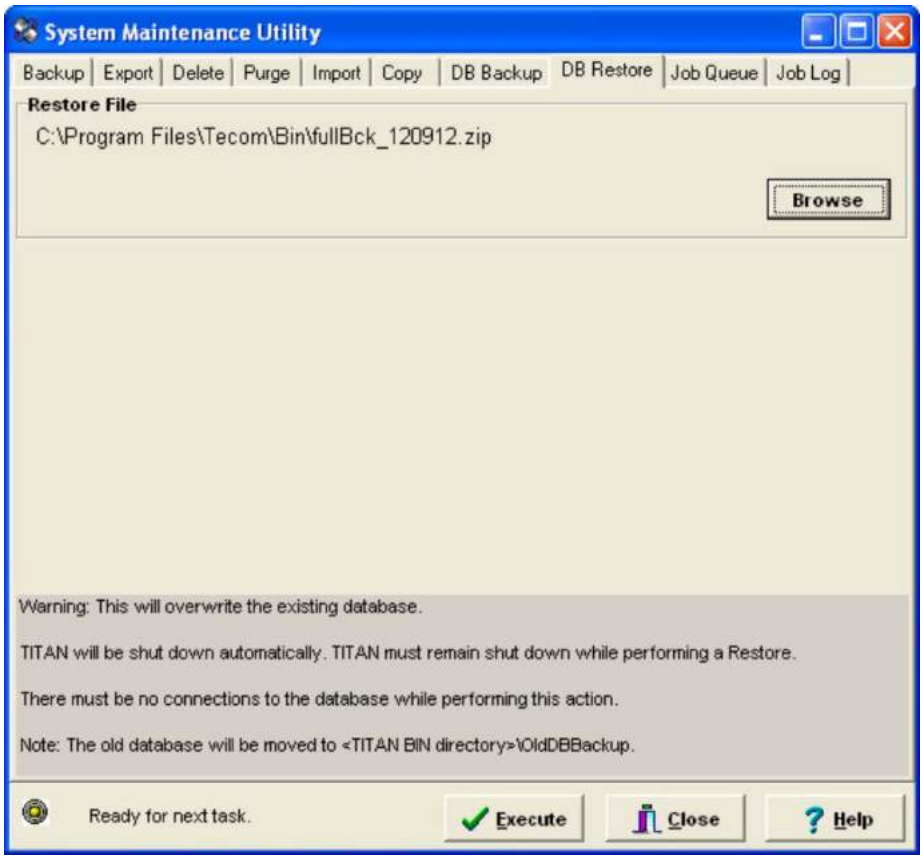
Restoring the Titan database

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 65 below.

Figure 65: DB Restore tab



To restore the Titan database:

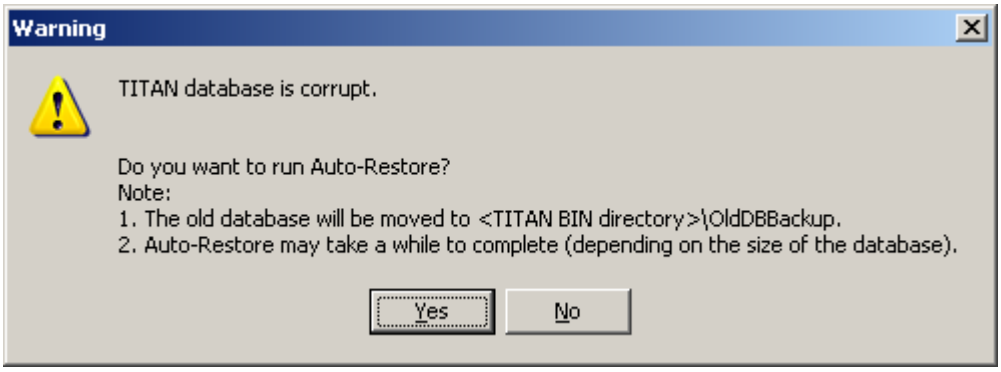
1. Start System Manager (if not automatically started).
2. Click the DB Restore tab.

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 start up, if Titan detects that the database has been corrupted, the message shown in Figure 66 below displays.

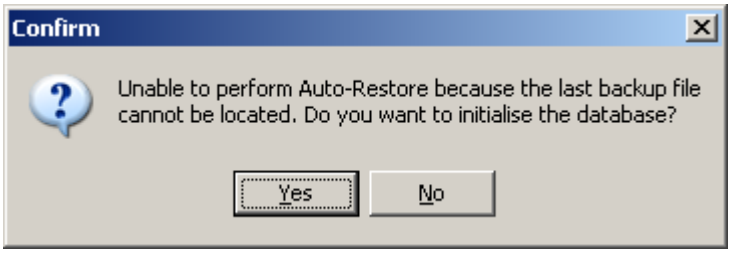
Figure 66: Auto restore message



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 67 below.

Figure 67: Backup file not found message

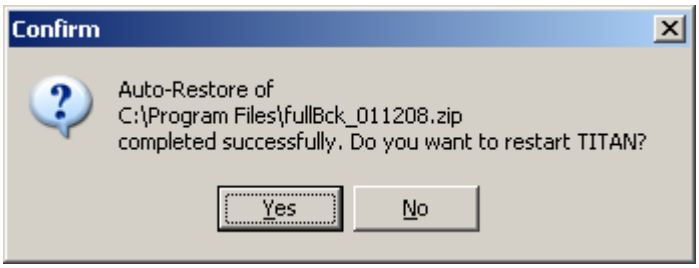


Select Yes to run auto-restore without a backup file and to initialize the database.

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 68 on page 101.

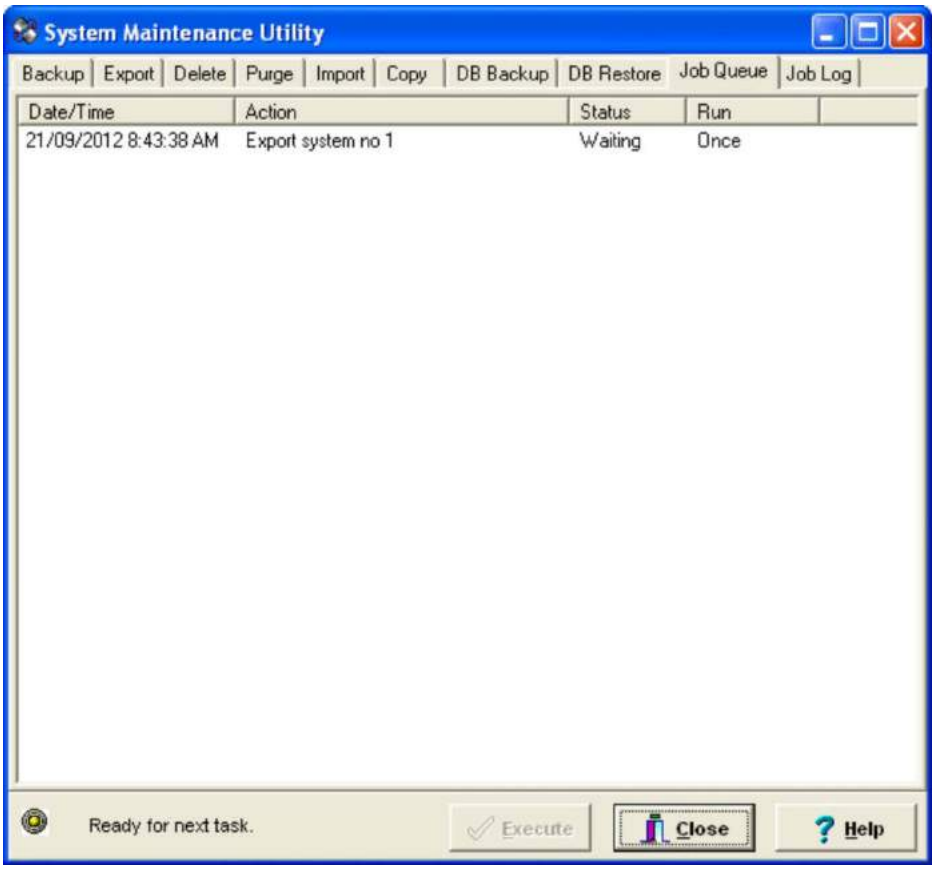
Figure 68: Auto restore complete message



Check the job queue

The job queue lists any jobs waiting or in progress. The job queue tab is shown in Figure 69 below.

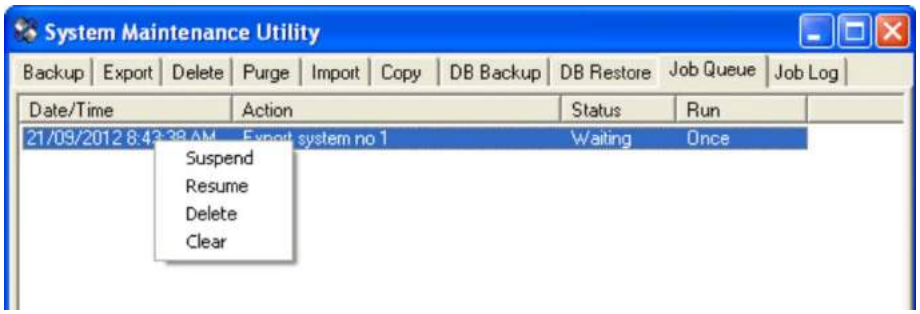
Figure 69: Job Queue tab



To view the job queue:

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 70 on page 102). Jobs cannot be suspended or paused after they start, only before they are set to begin.

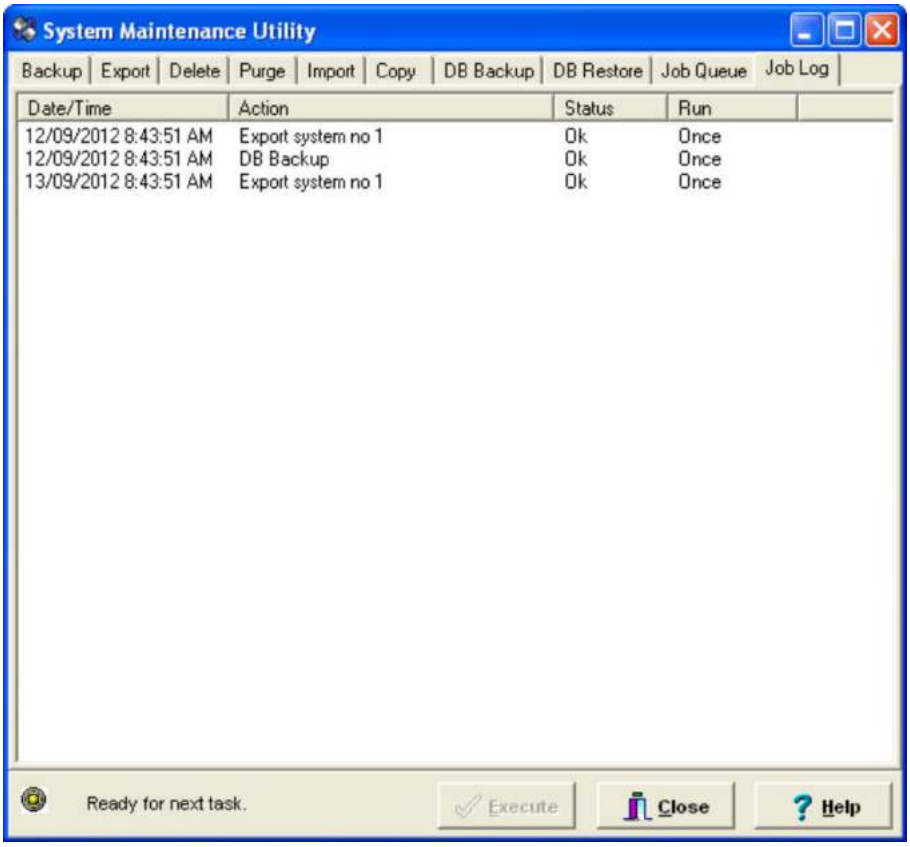
Figure 70: Job queue right-click menu



Checking the job log

Use the job log to check whether a job has been completed successfully. The job log tab is shown in Figure 71 below.

Figure 71: Job log tab



To view the job log:

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 systems

This section describes the following administrative tasks:

- "Managing Challenger panel settings" below
- "Adding a panel" on page 105
- "Challenger panel programming" on page 105
- "Upgrading Challenger device firmware" on page 106
- "Upgrading Challenger system capacity" on page 108
- "Migrating a Challenger V8 system to Challenger10" on page 110

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 72 below) displays for a Challenger panel in your system. See the following sections for descriptions of each field.

Figure 72: Challenger window



Challenger tab

Type: Indicates whether the panel is a Challenger10, Challenger10 (pre V10-06), or a Challenger V8 panel. The Type setting can be changed from Challenger V8 to Challenger V10 to upgrade the panel. Once a record has been saved as a Challenger V10 type, it cannot be changed to a Challenger V8 type. See “Migrating a Challenger V8 system to Challenger10” on page 110.

IUM installed: Select to indicate that the panel has IUM (intelligent user memory) used to increase the number of users, alarm groups, door groups, and floor groups in your system. See Table 1 on page 109 for details. This field is greyed for Challenger Series panels because all Challenger Series panels are IUM.

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 for a Challenger Series panel’s specific communications path via Install menu option 9. Communications. For a Challenger V8 panel use Install menu option 29. Computer Connection.

Description: Type a description of the Challenger panel. The description will be downloaded to Challenger Series panels that have firmware version V10-06 (or later). For other Challenger versions the description will be used in Titan only.

Upload Description From Challenger button: Retrieve the description programmed in Install menu option 42-Challenger Name.

Download Description to Challenger button: Send the description programmed in Titan to the Challenger panel.

Location: Describe the panel’s 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 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 is programmed for a Challenger Series panel’s specific communications path via Install menu option 9. Communications (labelled “account code”). For a Challenger V8 panel use Install menu option 9-Communications.

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 call-back number when it detects a call-back trigger.
- UDP/IP: Use for event-driven IP communication.
- USB: The Challenger Series panel is connected directly to the computer via a USB cable.

SecureStream Pass-through: Select to designate the Challenger as an IP panel able to receive data from Titan via a SecureStream IP Receiver computer or a Tecom IP Receiver computer. The Titan system must also have SecureStream Pass-through enabled (see Figure 3 on page 8).

Options tab

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 "Collecting raw card data in IUM teach mode" on page 46).

Adding a panel

To set up a new Challenger panel, click New. The Challenger window displays (Figure 72 on page 103) 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.

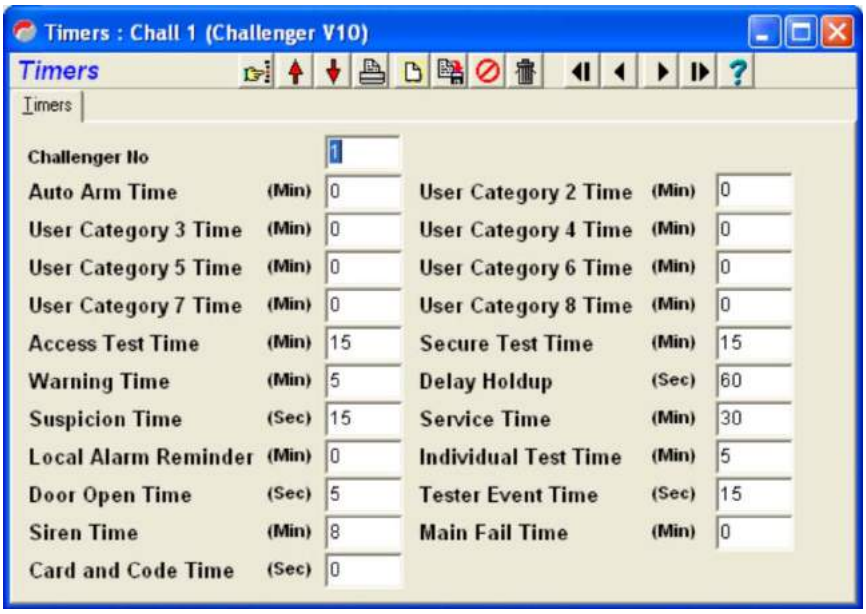
Refer to "Managing Challenger panel settings" on page 103 or Titan help for details about using the Challenger window.

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 73 on page 106).

Figure 73: Timers programming



Upgrading Challenger device firmware

The firmware or touchscreen button images for certain Challenger Series devices may be upgraded via Titan's Firmware Upgrade facility, as described in this section.

Notes

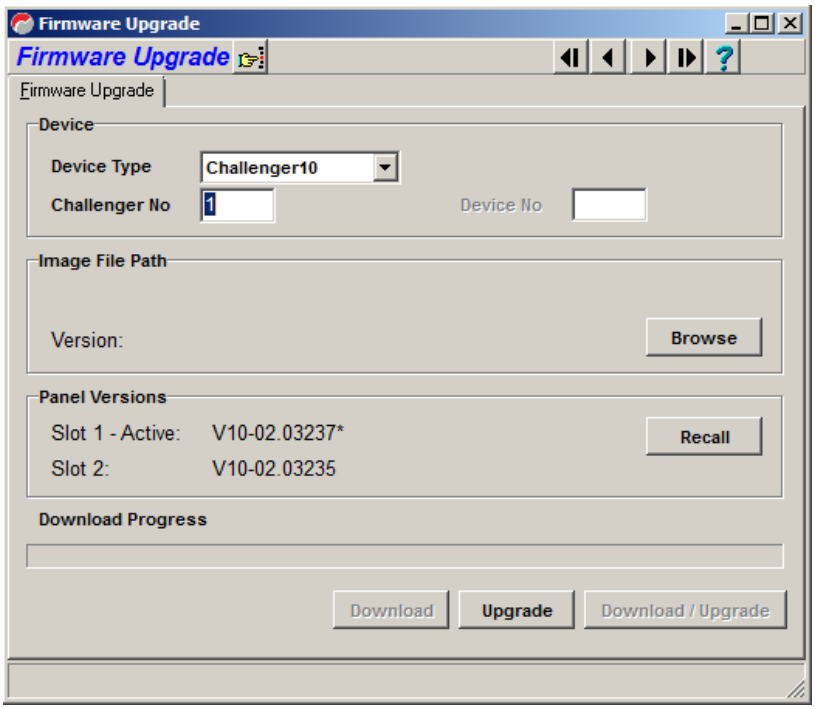
- Upgrading a device's firmware or images via Titan requires Titan version 3.3 (or later), and a firmware upgrade file stored on the Titan computer.
- If upgrading an early version of Challenger Series panel firmware to version V10-06 or later, refer to "Upgrading a Challenger10 (pre V10-06) panel" on page 111 for additional details.
- If Titan is connected to the Challenger panel via USB connection, Titan requires extra time (about 20 s) to complete the upgrade or rollback because it needs to re-create a new connection with panel. Titan displays a message "Titan needs to reinitialise the USB panel connection. Please wait until it is complete".
- If upgrading both firmware and images for a Touchscreen RAS via Titan, we recommend that you upgrade the images first and the firmware second. Either way will work, however, at the end of the process Titan will display the new firmware version in the Firmware Upgrade window if the firmware was upgraded last.
- Upgrading individual LAN devices (including RAS firmware or touchscreen button images) can take considerable time (tens of minutes), depending on the number of polled devices on the Challenger LAN.

To upgrade a device's firmware or images:

1. Connect the Challenger panel to Titan and activate the system.
2. From the Control menu, select Firmware Upgrade to open the Firmware Upgrade window (Figure 74 on page 108).
3. Click the Device Type arrow and select Challenger10, DGP, Touchscreen RAS, Memory Expander, or 3G Communication Module.
4. If the system contains multiple Challenger panels, type the number of the Challenger10 panel to be upgraded in the Challenger No field, or click the Search button and select the panel from the Challenger list.
5. The field label displays "Device No" or "Location"", as appropriate. If you are upgrading DGP or RAS firmware, type the DGP or RAS number in the Device No field, or click the Search button and select the DGP or RAS from the list. If you are upgrading firmware on an onboard module (such as a 3G Communication Module), double-click the Location field, and then select the required module from the list.
6. Click Browse to find and select the firmware or images upgrade file. The upgrade file is a zip file and will be opened automatically by Titan. Do not attempt to unzip the upgrade file.
7. Click Download to send the upgrade file to the device to be upgraded. A status bar displays to indicate the progress.
8. Click Upgrade to begin the upgrade process. A status bar displays to indicate the progress. The upgrade process may take several minutes (depending on connection speed). A completion message displays when finished.

Tip: You can click the Download/Upgrade button to send the upgrade file to the device and then begin the upgrade process automatically.

Figure 74: Firmware Upgrade window



After a successful upgrade, the Firmware Upgrade window displays Slot 1 and Slot 2 labels. “Active” beside a slot number indicates that it’s currently in use by the panel.

If you’ve upgraded the Touchscreen RAS images, then repeat the process and select the firmware upgrade zip file in step 6 to upgrade the firmware (if applicable).

Upgrading Challenger system capacity

Upgrading a Challenger10 panel’s memory

A standard Challenger10 panel has sufficient memory for 2,000 IUM users. User capacity can be expanded to 65,535 via a TS1084 Memory Expansion Module.

Upgrading a ChallengerSE panel’s memory

A ChallengerSE panel has sufficient memory for 100 IUM users. User capacity can be expanded to 2,000 via a TS1082 User Expansion Licence Module, or 65,535 via a TS1084 Memory Expansion Module.

Upgrading a Challenger V8 panel’s memory

Challenger V8 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.

WARNING: 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. We recommend 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 1: Challenger V8 memory application (version 8.128 or later)

Memory	Users	PINs	Name files	Alarm Groups	Door Groups	Floor Groups	Time Zones
Standard (Small)	50	50	50	138	10	10	24
Standard (IUM tiny)	50	50	50	138	10	10	24
1 MB exp. (Large)	11,466	1,000	200	255	255	128	46
1 MB exp. (IUM mini)	2,000	2,000	200	255	255	128	46
4 MB IUM (IUM small)	17,873	17,873	200	255	255	128	46
8 MB IUM (IUM large)	65,535	65,535	200	255	255	128	46

Upgrading Challenger V8 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.

Converting Challenger V8 to software IUM:

1. Ensure the Challenger V8 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 48).

Alternatively, add hardware IUM to a Challenger V8 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 48).

Migrating a Challenger V8 system to Challenger10

The overall process to upgrade a Challenger V8 panel to Challenger10 is in two parts.

Part 1: Convert the Challenger record in Titan

1. Connect Titan to the Challenger V8 panel, and make it the active system.
2. Upload the Challenger V8 database to Titan to backup the data, if needed. We recommend that you back up the Challenger V8 panel’s data by using the Export function in System Manager.
3. If the Challenger V8 panel has IP connections to management software, IP Receiver, and so on, record the IP addresses and configuration details for reuse later.

4. Deactivate the system.
5. Select Admin > Challenger, and then display the record for the Challenger V8 panel to be migrated. The Type field will have Challenger V8 selected.
6. Click the Type arrow, select Challenger10, and then click Save. Click Yes when asked if you want to continue. When finished, the Type field will have Challenger10 selected (you cannot convert back to Challenger V8).

If the migration was successful, a message displays: “Successfully migrated. When panel is first set online, Titan will ask you to synchronise the panel with Titan installer database. Note that you will need to download users separately. Note that the V8 default alarm groups from 4 to 6 (if used) will need to be migrated to V10 manually”. Alarm group number 4, 5, and 6 are not applicable to Challenger10.

If the migration was not successful, a message displays: “Error encountered in the migration. Please restore your backup using System Manager”.

Part 2: Install hardware and connect to Titan

1. Power down the Challenger V8 panel, remove all cabling, and replace the PCB with a Challenger10 PCB. Reconnect cabling (most cabling reconnects in the same location as on the V8 PCB).
2. Repower the Challenger panel. A new (or defaulted) Challenger10 panel is armed, and the RAS LED for area 1 illuminates.
3. Connect the Challenger10 panel to Titan, and make it the active system (see Connecting to a Challenger10 panel for details).

Note: When the first converted panel is online, Titan displays the message “Titan has detected that one or more Challenger10 panels has not been synchronised after migration. It is strongly recommended that the panels are synchronised to ensure that the programming in Titan matches the programming in the panel. Do you wish to proceed with panel synchronisation?” Select Yes to synchronise. Titan first uploads the comms of the converted panel and then downloads the configuration (except users) from Titan to the panel.

Depending on how the Challenger10 panel is connected to Titan, at least one of the ten communications paths is already programmed. Paths 1, 2, and 3 are preconfigured for CID Dialler, USB Installer, and Management Software (path 3 is enabled). Configure these and other communications paths as needed.

Upgrading a Challenger10 (pre V10-06) panel

Challenger Series panels with firmware version V10-06 (or later) no longer use numbered text words for naming things like areas, inputs, and so on. Challenger10 now uses descriptions that are based on text instead of numbers.

When you upgrade an earlier version (pre-V10-06) of panel firmware to version V10-06 (or later), then all names based on text words will be deleted from the panel. However, after upgrading the panel firmware, Titan can migrate its copy of

the panel's text words to descriptions, and then you can download the descriptions to the panel.

We recommend that you use System Manager to back up the Challenger panel's database before converting Challenger10 (pre-V10-06) to Challenger10.

The following is a typical upgrade process via Titan:

1. From the File menu, select Open/System, populate the "Active System" check box, and then save to connect to the Challenger10 panel.
2. From the File menu, select "Upload all from Challenger(s)" to upload (at least) the Installer programming into Titan.
3. From the Control menu, select "Firmware Upgrade" to upgrade the panel's firmware.
4. After the firmware upgrade has completed, clear the "Active System" check box, and then save to disconnect from the panel.
5. From the Admin menu, select Challenger, and then go to the record for the upgraded panel.
6. Click the Type arrow, select "Challenger10", and then save the record. Titan displays a warning message to ensure that you've backed up the database. Click Yes to continue.
7. Titan displays a warning message that there in no rollback option after migrating text words to descriptions. Click Yes to continue.
8. When finished migrating text words to descriptions Titan displays "Text words have been successfully migrated to descriptions". Click OK to continue.
9. From the File menu, select Open/System, populate the "Active System" check box, and then save to connect to the Challenger10 panel. Titan displays a message "Do you wish to download descriptions (entity names) to Challenger10 panels?". Click Yes to continue.

Chapter 8
Support

Summary

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

Content

Troubleshooting 114
Contacting technical support.....117

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 117).

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”.

Using Titan as system management software

Titan is a software tool for programming, controlling, and monitoring Challenger integrated intrusion and access control systems. Titan is both an installer tool, plus it can be used as system management software to maintain and control the Challenger system.

When used as system management software we recommend the following settings for the Titan computer.

- **Disable Internet Time:** To check if the Titan computer’s clock is automatically synchronized by an Internet time server, double-click the time in the Windows system tray to display the Date and Time Properties window. If the Date and Time Properties window has an Internet Time tab, clear the Automatically synchronize with an Internet time server check box.
- **Disable Auto Updates:** Open the Control Panel, and then double-click Automatic Updates. Clear the Automatic (recommended) check box.

Tools supplied with Titan

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

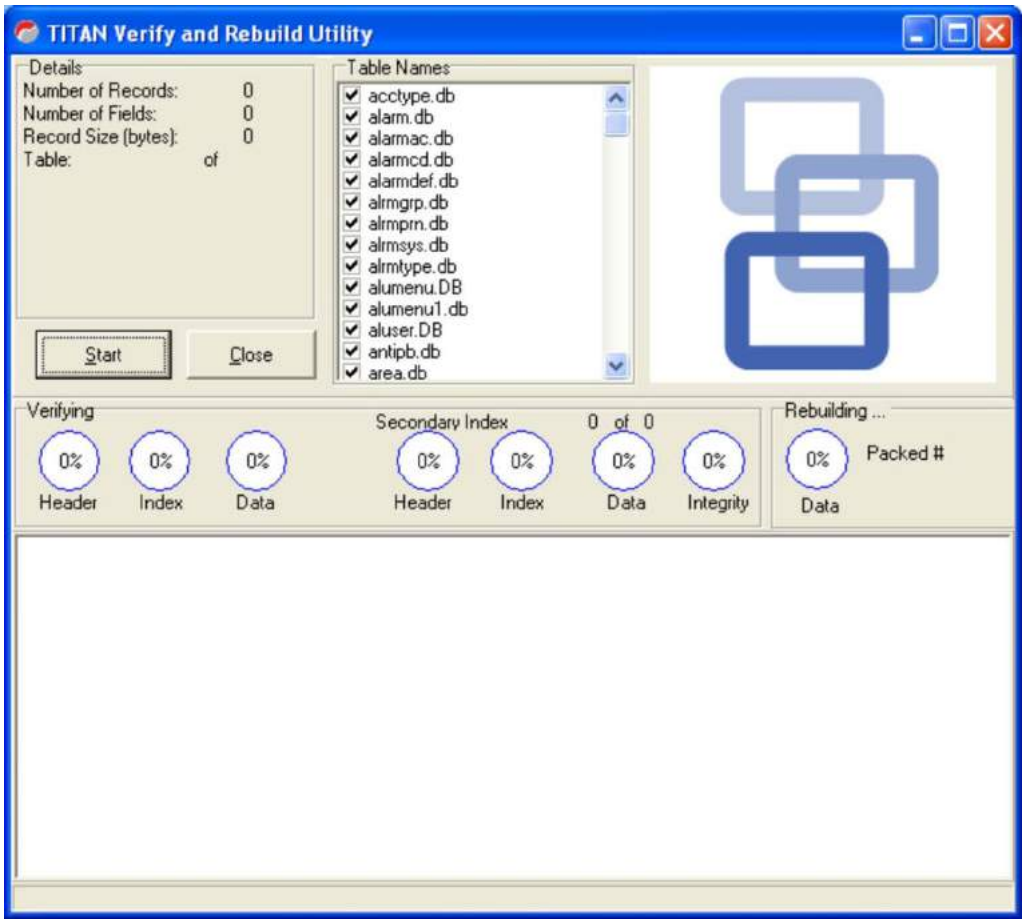
- See “System Manager” on page 85.
- See “Titan Verify and Rebuild Utility” below.
- See “Titan Database Pack Utility” on page 116.

Titan automatically attempts to restore the database if it detects a problem. See Restore the Titan database on page 103.

Titan Verify and Rebuild Utility

If your system crashes and your Titan database is corrupted, you can use the Titan Verify and Rebuild Utility (Figure 75 on page 115) to rebuild your database.

Figure 75: Titan Verify & Rebuild window



To rebuild your database:

1. Backup your database.
2. Click (typically) Start > All Programs > Tecom > Titan > 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

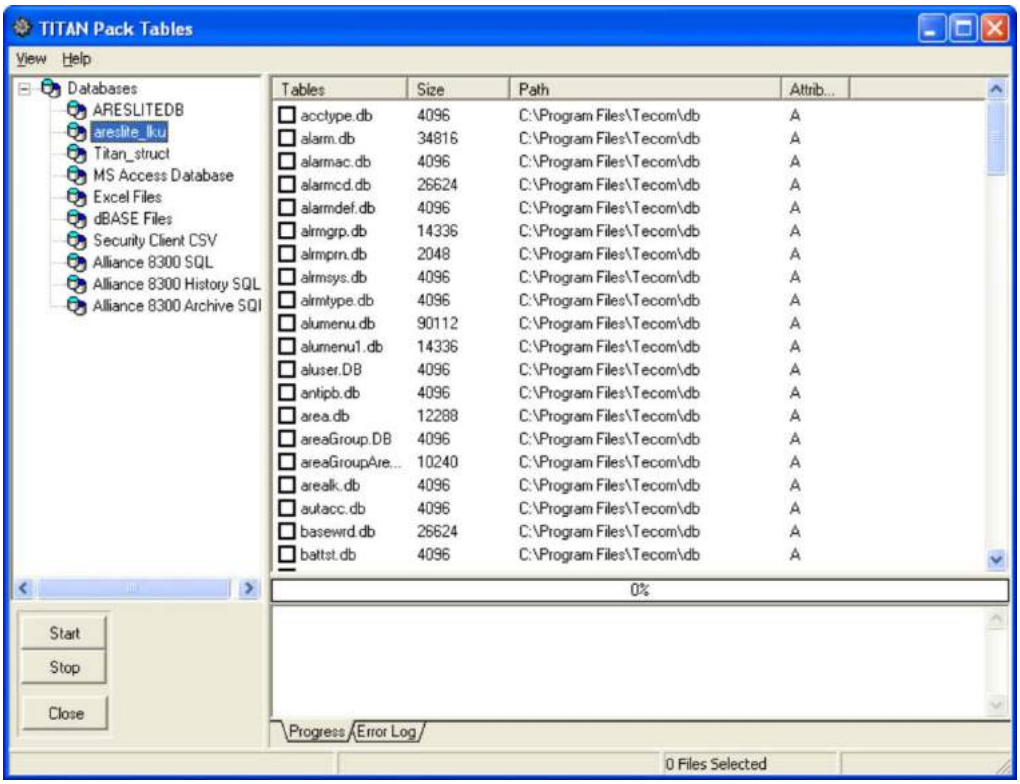
When events are deleted from the Titan history, they are removed from your hard drive. However, due to the nature of hard drives, some remaining space will always be left behind in your database.

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.

We recommend that you routinely use Titan system maintenance utility for normal housekeeping and maintenance (see “Purging a system” on page 93).

Alternatively, you can use the Titan Database Pack Utility (Figure 76 below) to compact the Titan database.

Figure 76: Titan database pack utility



To compact the Titan database:

1. Click (typically) Start > All Programs > Tecom > Titan > 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.

Contacting technical support

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

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

Index

A

access control, 14
acknowledge
  alarm, 83
admin report
  Challenger, 63
  ports, 63
  system, 63
admin reports, 63
alarm group
  alarm group tab, 21
  menu tab, 22
  options tab, 22
alarm group, 21
alarm group
  programming, 23
alarm group
  managing, 23
alarm group
  adding users, 41
alarm screen, 73
antipassback, 18, 38, 39, 48
area groups, 24
automation control, 29
automation zones, 29
auto-restore, 100

C

card layout, 34
  card layout editor, 52
cards
  photo ID, 56
  security, 59
Challenger
  memory, 108
  programming, 105
  set up, 103
Challenger set up
  communication mode, 104
  computer address, 104
  description and location, 104
  IUM format, 105
  IUM installed, 105
  IUM teach, 105
  number, 104
  phone number, 104
  port, 104
  SecureStream enabled, 105
  TS2000 route, 104
  type, 104
clearing an antipassback violation, 48
cloning a system, 11, 84
command queue, 78
commands
  control, 83
connection
  indicators, 9
  LEDs, 9
contact details, 2
control
  access, 14
  areas, 70
  automation, 29
  commands, 70
  inputs, 71
creating
  Challenger panel, 105
  door groups, 16
custom history restrict, 66

D

database
  backup, 98
  restore, 99
DB Backup, 98
DB Restore, 99
department, 38
  programming, 34
dialup connection, 73
door group
  adding users, 41

E

end date, 39

F

firmware
  upgrade, 106
firmware version 8.128, 109

floor group
adding users, 42
floor groups, 17
full log upload, 9

H

history report
custom, 65
history by department, 67
holidays, 18

I

inputs
isolating, 71
isolating an input
isolate, 71
IUM
hardware, 110
installing, 109
software, 109
IUM teach, 46

L

login, 7

M

manual incident, 73
map
editing, 83
menu
admin, 10
alarm screen, 9
Challenger, 10
control, 9
file, 9
help, 10
history, 9
reports, 10
users, 10
window, 10
menu permissions, 8
migrating V8 to V10, 110

P

photo album, 37
photo ID, 34, 41

R

raw card data, 46, 105
regions, 18
reports
user reports, 62
right-click shortcuts, 10

S

Save Start and End Dates to Panels, 39
SecureStream enabled, 8
smart card, 42, 51
credit use, 42
smart cards
credit, 57
standard toolbar, 10
start date, 39
starting
database pack utility, 116
Titan, 7
verify & rebuild, 114
system
open, 8
system maintenance utility
backup, 87
copy, 86, 96
database backup, 98
database restore, 99
delete, 85, 91
export, 85, 89
import, 86, 95
job log, 102
job queue, 101
purge, 86, 93
System Manager, 85

T

technical support, 117
time zones, 14
toolbar
standard, 10

U

Updating raw card data, 48
user
advanced search, 37
end date, 39
history, 37
name, 38
number, 38
PIN, 39
privileged, 39
start date, 39
status, 38
trace, 39
type, 38
journal, 37
user accounts
quick access buttons, 35
user details tabs, 38
user details, 35
user history, 67
user records
creating, 34
user report

door groups, 62
floor groups, 62
holidays, 62
user summary, 62
users, 62
users in group, 62

V

version, software, iii