tecom
Security Commander

Security Commander Administration Manual and Operation Guide

P/N 1069971 • REV 07 • ISS 20AUG15

Trademarks and patents The Security Commander 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, VIC, 3168, Australia

Contact information For contact information see our Web site: www.interlogix.com.au.

Content

Important information

Security Commander Administration Manual and Operation Guide is a comprehensive guide to Security Commander or Security Commander Lite for both the system administrator and the installation technician to program, configure, and use the Security Commander or Security Commander Lite systems. It supplements and expands the operator information contained in the *Security Commander Help* and provides a level of detail required by advanced operators such as system administrators and installation technicians.

This manual does not describe how to plan and structure an entire security and access control system — it describes only how to manage the operation of Security Commander in an existing security and access control system.

It is assumed that the security and access control system is in place and Security Commander client and server computers have been installed and licensed in accordance with the *Security Commander Installation Manual*.

It is further assumed that users of this manual have read and understood the *Security Commander Installation Manual*.

Note: Client computers are not supported in Security Commander Lite.

Related documentation

Refer to the following:

- *Security Commander Help*: Provides reference information, such as screen and field descriptions, along with instructions for system administrator duties, such as configuring Challenger control panels.
- *Security Commander Installation Manual*: Provides information for Integration Technicians to set up, install, and configure a Security Commander or a Security Commander Lite system.
- *Security Commander Photo ID User Guide*: Provides instructions for users of the optional Photo ID package (not available in Security Commander Lite).
- *Security Commander CCTV Interface Guide*: Provides interface instructions for CCTV equipment (not available in Security Commander Lite).
- *Security Commander API Manual*: Security Commander API (Application-Program Interface) provides the ability to import data from external applications such as a Human Resource Management System (not available in Security Commander Lite).

Typographical conventions

This manual uses certain notational and typographical conventions to make it easier for you to identify important information.

Table 1: Notational and typographical conventions

Item	Description
Command sequences	Where appropriate, command sequences are abbreviated with the “>” symbol. For example, the command “Click Start, and then click Run” is written as “Click Start > Run”. **Note:** The command Start > Run, means open a Windows command prompt. Some Windows versions do not have Run in the Start menu by default, but it may be added.
Command alternatives	Many commands can be executed in a variety of ways including menu bar, tool bar, shortcut keys, right-click, or double-click. In general, commands are described from their menu bar location only, even when alternatives exist.
Keys	Capitalized, for example “press Enter”.
Keystrokes	Text that you type is indicated in Courier New font. For example, “Type `dcomcnfg`”.
Expanding a “tree” view	The word “expand” is used to indicate that selections may be hidden. For example, the command “Click the ‘+’ box next to Computers” is written as “Expand Computers”.
Notes	Notes alert you to information that can save you time and effort.
Caution	Cautions are displayed to advise the user that failure to take or avoid a specified action could result in loss of data.

System introduction

Software editions

Security Commander Lite is a cut-down edition of system management software intended for small Challenger systems. Security Commander Lite runs on a single server computer, with no additional clients. The number of simultaneous connections to active Challenger control panels is limited to five.

Certain features of the full Security Commander edition are not available in Security Commander Lite:

- Photo ID and badge design
- Video integration
- Client computers
- User import API
- Email notification
- Client monitor
- Graphic maps

Refer to the *Software Comparison Matrix* for a detailed comparison of Tecom's management software products.

Challenger panel versions

Security Commander may be used with the following types of Challenger panels:

- Challenger V8 control panels using firmware version 8.128 (or later) and fitted with a memory expansion module model TS0882, TS0883, or TS0884. This configuration is called "V8 Extended".
- Challenger10, ChallengerSE, or ChallengerLE control panels using firmware version V10-06 (or later). These panels are called "Challenger Series".

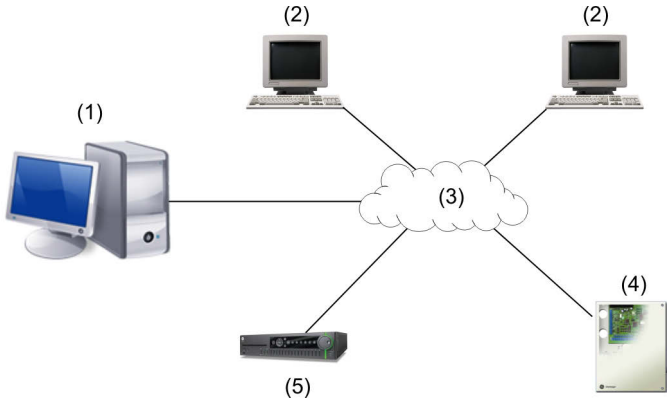
The term "Challenger Series" does not apply to legacy products such as Challenger V8.

Note: Challenger10, ChallengerSE, and ChallengerLE control panels have differing capacities. Refer to the topic "Challenger Series features" in Security Commander help for details.

System overview

Subject to the limitations described in "Software editions" above, Security Commander is a client-server security system management application with the ability to communicate over a LAN or WAN. Figure 1 on page 2 depicts the relationship between a Security Commander server and remote Security Commander clients (Security Commander Lite does not support remote clients or CCTV).

Figure 1: Security Commander with two remote clients and a digital video recorder



(1) Security Commander Server

Server components:

- Security Commander user interface
- Security Commander Databases
- Photo ID (optional application)
- Alliance 8300 Diagnostics (service)
- Alliance 8300 System Manager (service)
- Alliance 8300 Manager (service)
- MS SQL (service)

(2) Security Commander Client PC

Client computer components:

- Security Commander user interface
- Photo ID (optional application)
- Alliance 8300 Diagnostics (service)
- Alliance 8300 System Manager (service)
- Alliance 8300 Manager (service)

(3) IP LAN or WAN*

(4) Challenger control panel

(5) DVR

* WAN data transfer latency can significantly reduce the Security Commander application's usability.

Key concepts

This section discusses the key concepts that you need to consider when using Security Commander, in particular the differences from other security management systems that you may be familiar with.

Controller setup

All new control panels defined in Security Commander are issued with a default installer (assigned badge no. 50) to enable the control panel to be programmed initially.

See "Master badge group" on page 58 for details.

Person profiles

A Person Profile is an optional means of quickly applying a standard set of access groups to new person records (see "Person" on page 56).

Persons

On the Personnel menu, click Person to define a potential* user of the security system. A Person Profile can be imported into a Person record to quickly assign a standard set of access rights (see "Person" on page 56).

*A potential user becomes a user when a badge (or PIN) is assigned via the Badge form.

Badges

In Security Commander, the term “badge” can refer to a:

- Smart card or key fob
- Magnetic stripe card
- PIN
- Combination of card and PIN

In other words, a badge may be a physical device, a number entered at a keypad, or both.

It is the badge data that is downloaded to a control panel. See “Badges” on page 56 for more information.

Facilities

On the Administration menu, click Facility to define facility records.

Facilities are used to partition the Security Commander database. Only operators who have access to a particular facility can see devices which have that facility assigned to them.

It is recommended that you create facilities and associate new control panels to facilities from the very start (assign a facility to a control panel record before saving the record). This will help ensure that all the data related to the control panel is kept within the same database partition and will help speed access to data.

Note: After a control panel has an assigned facility, uploaded devices for the control panel will automatically be assigned to the same facility.

Operators can be assigned to one or more facilities and can choose which facilities to be active at any given time. Usually, operators assigned with a permission of System Administrator are assigned to all facilities. All records have the default "Ignore Facilities", which means that the records are not under facility protection; therefore, those records are visible to all operators.

Creating and using facilities are separate things:

- To create a facility, use the Facility tab on the Facility form.
- To assign a facility to the required operator, use the Facilities tab on the Operator form.
- To manage a facility’s state, use the Operations > Select Facilities command. Facilities assigned to an operator are active by default. A facility may be set to “Available” (inactive) when it’s not needed. For example, a facility may be created for future use and then made inactive to prevent the facility from being accidentally selected by the operator when using various forms.

Note: If you, as an operator, do not have a particular facility assigned to you, that facility will not be available to you from the Facilities list on various forms.

Event-triggered video

Note: This option is not available in Security Commander Lite.

ON the Administration menu, click Event Trigger to define event-triggered video records. Event triggers allow you to move up to four PTZ (pan tilt zoom) cameras into pre-set positions in response to specific door/reader transactions and/or alarm transactions.

This function can be used, for example, to obtain a video image at a door if someone attempts entry using a badge that has been identifies as ‘lost’, or if an intrusion alarm is generated. In addition, a tag can be automatically sent to the DVR for marking the recorded video and for changing the camera’s recording rate appropriately.

Refer to the *Security Commander CCTV Interface Guide* for more information.

Badge groups

The purpose of badge groups is to provide flexibility in setting up multi-panel security systems where some panels must cater for a large number of users (such as a main entrance) and other panels that cater for smaller numbers of users (such as individual departments on different floors).

Badge Groups are based on Badge Formats, as listed in “Badge groups” on page 57, or custom formats. After creating a new badge group, assign the badge group to a Challenger control panel via the Badge Groups tab on the Controller Setup form.

Using Challenger V8 control panels as an example, the following illustrates how a combination of large and small control panels in the same system can be handled by managing badge groups:

- Challenger control panel A controls the building’s main entrance and it has a memory size of IUM large (Intelligent User Memory), which enables the control panel to handle up to 65,535 users.
- Challenger control panel B controls the building’s administration offices and it has a memory size of IUM mini (Intelligent User Memory), which enables the control panel to handle up to 2,000 users. A special Badge Group has been created and assigned to Challenger control panel B named Administration Staff. Whenever a change occurs in Security Commander to a person’s record or access rights assigned to the Administration Staff, Security Commander automatically downloads (sends) the required user data to Challenger control panel B.
- Challenger control panel C controls the building’s engineering offices and also has a memory size of IUM mini (Intelligent User Memory), which enables the control panel to handle up to 2,000 users. A special Badge Group has been created and assigned to Challenger control panel B named Engineering Staff. Whenever a change occurs in Security Commander to a person’s record or access rights assigned to the Engineering Staff, Security Commander automatically downloads (sends) the required user data to Challenger control panel C.

- Challenger control panel A has been assigned the Badge Groups Administration Staff and Engineering Staff (among others). Whenever a change occurs in Security Commander to a person's record or access rights belonging to either the Administration Staff or the Engineering Staff, Security Commander automatically downloads (sends) the required user data to Challenger control panel A (as well as to Challenger control panel B or Challenger control panel C, as needed).

For more information see "Badge groups" on page 57 and "Challenger control panel memory" on page 59.

Setting up Security Commander

This chapter describes how to set up Security Commander or Security Commander Lite to a minimum degree in order to connect to a control panel and to upload data.

Once you have installed the Security Commander software on the server and clients (if applicable) you will need to log in to the server computer and set a few parameters.

Getting ready

Items to consider

Note: Some options are not available in Security Commander Lite.

As part of the task of integrating Security Commander into an existing security and access control system there are a number of points that you'll need to consider. It will save time if you prepare or obtain this information before sitting down in front of Security Commander and having to think about it as you come to it. The main points are as follows:

- Permissions: In addition to the default System Administrator what operator permission categories will you need?
- Operators: In addition to the default Security Commander operator login "secure" what operators will you need? (The default Security Commander operator has System Administrator operator permission.)
- Access Rights: Access rights are defined by three access groups (alarm group, door group, and floor group), and can be quickly applied to person records via defined person profiles. In addition to the default Master Installer Profile, what access rights definitions will you need?
- Facilities: A facility is a way to organize records in the Security Commander database by, for example, a location. See also "Defining facilities" on page 8.
- Personnel Types: In addition to the default Permanent, Contractor, and Temporary, what personnel types will you need? A personnel type can be associated with a specific badge design.
- Badge Designs: Default badge designs are provided as a starting point but must be edited to suit your needs. A badge design can be associated with personnel types so that, for example, you can tell from the badge which staff members are permanent and which are contractors. Security Commander workstations require Photo ID to be installed and licensed in order to edit badge designs.
- Department: Department names are used in person records and reports for sorting purposes.

Tasks to be performed

Table 2 below describes the Security Commander tasks required to verify that the Security Commander installation is complete and functioning correctly.

Table 2: Initial Setup of Security Commander

Task		Menu > Form	Reference
1.	Start Security Commander and log in	File > Login	page 7
2.	Add yourself as an operator in Security Commander	Administration > Operator	page 8
3.	Program system parameters	Administration > Parameters	page 9
4.	OPTIONAL: Create facilities	Administration > Facility	page 8 See also the *Security Commander Help*.
5.	Add the client computers to the Security Commander server computer database (Not available in Security Commander Lite)	Administration > Client	See *Adding Security Commander Clients* in the *Security Commander Installation Manual*.
6.	Set up client computers	Not applicable	This table
7.	Connect to a control panel	Operations > Controller Utility	page 10
8.	Retrieve data from the control panel	Right-click > Upload	page 15

For information on advanced setup topics see the *Security Commander Help*.

Starting Security Commander

To start Security Commander:

1. Select Start > All Programs > Tecom > Security Commander > Security Commander to run the application. Alternatively, double-click the Security Commander desktop icon.

2. The login screen displays automatically when Security Commander starts. Use the default Login ID ‘secure’ and previously defined password to log in.

Note: In order to log into Security Commander from a client computer:

- You must have a valid Security Commander operator login ID and password.
- Security Commander on the server computer must be licensed.

- The database services on the server computer must be running (the easiest way to ensure this is to have Security Commander running on the server computer).

Accessing Security Commander Help

To access the *Security Commander Help*, press the F1 key. Alternatively, from the Help menu, click Help Topics.

Note: You do not have to be logged in to access help.

Adding an operator

Add yourself as an operator in Security Commander. This will allow Security Commander to record the steps you take in setting up the system.

To add yourself as an operator in Security Commander:

1. From the Administration menu, click Operator.
2. On the File menu, click New Record. The Operator form displays in edit mode (the Save Record command is enabled).
3. Add your details to the Operator form. Various permissions are available initially referring to certain tasks (like security, reception or System Administrator). Select an appropriate permission.

   For detailed information about setting up an operator, refer to the *Security Commander Help*.
4. Save the Operator form, log off, and then log in as the new operator.

Defining facilities

The Security Commander database can be partitioned and related records can be grouped. In Security Commander, these groups are called facilities. A Facility option can be designated on most forms throughout the system and any number of facilities can be defined.

It is good practise to create facilities and associate new control panels to facilities from the very start (assign a facility to a control panel record before saving the record). This will help ensure that all the data related to the control panel is kept within the same database partition and will help speed access to data.

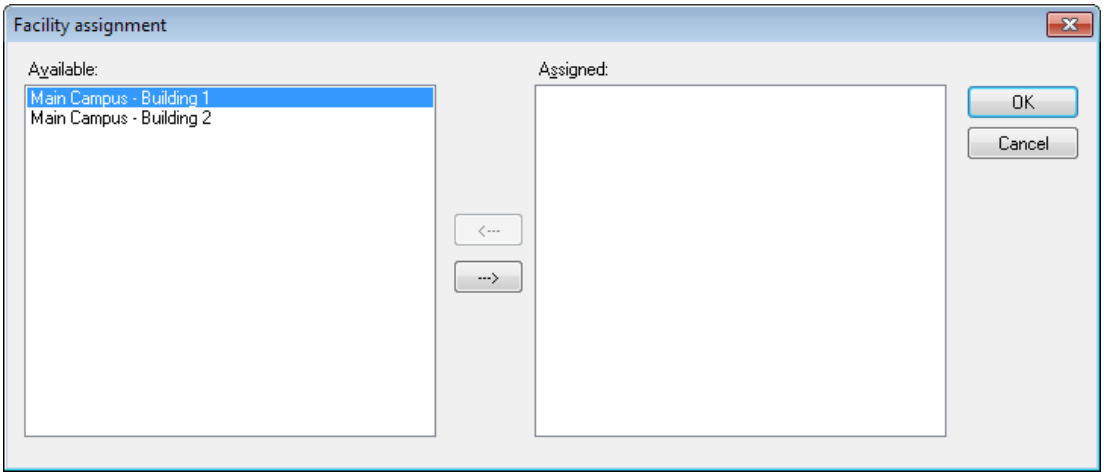
Operators can be assigned to one or more facilities and can choose which facilities to be active at any given time. Usually, the system administrator is assigned to all facilities. All records have the default Ignore Facilities, which means the records are not under facility protection; therefore, those records are visible to all operators. You can assign more than one facility to an operator.

For more information about setting up a facility, refer to the *Security Commander Help.*

To assign the operator to a facility:

1. From the Administration menu, click Operator.
2. On the Search menu, click Search to display the operator records.
3. Select the operator to which you want to assign to a facility. (If only one operator record was created, it will be displayed.)
4. Click the Facilities tab.
5. Click Assign Facilities.

   Result: The Facility Assignment dialog displays.



   In this example there are two facilities available: Main Campus - Building 1 and Main Campus - Building 2. We want to assign an operator to the Main Campus - Building 1 to allow the operator to assign badge holders to that facility only.

6. In the Available column, select the facility that you want to assign to the operator.
7. Click the right arrow button to move the selection to the Assigned column.
8. Click OK. In the given example the facility Main Campus Building 1 now displays in the Assigned column.
9. On the File menu, click Save Record to save the changes.

Setting system parameters

System settings for Security Commander are determined by the Parameters form. On the Parameters form, you can specify, among others:

- To archive history on a specific time interval, such as daily, weekly, or monthly; or to archive history immediately
- To print badge and alarm activity and to which printers
- To change the names of the labels that will be used globally for the user fields and address fields, etc.

Note: For the changes on the Parameters form to take effect, you must save the change and then stop and restart the Security Commander services. The easiest way to do this is to restart the computer.

For more information on these items, refer to *Security Commander Help*.

Challenger control panel connections

When a Security Commander computer is connected to a controller (Challenger control panel), the computer is said to be the host of the controller. The details of the controller and its connection to the host are defined by a Security Commander controller record.

Note: When creating controller records, it is good practise to avoid using a host computer that is likely to have its computer name changed. Any Security Commander computer (server or client) that has had its computer name changed will lose communication with all controllers hosted by that computer. In such a case, the controller records for affected panels would have to be deleted and then recreated using the new computer name.

The Security Commander computer may be connected to a Challenger control panel in the following ways:

- See “Setting up a network connection” below.
- See “Setting up a direct serial connection” on page 11.
- See “Setting up a dial-up connection” on page 13.

Setting up a network connection

The Challenger control panel fitted with a suitable IP Interface can be connected via Internet Protocol (IP) to the Security Commander computer via a LAN or WAN to provide control and upload and download capabilities.

Note: Challenger Series control panels have native IP support so do not need an IP interface.

Refer to Figure 1 on page 2 for an example of a control panel connected to a Security Commander computer via IP. A Challenger control panel may be hosted by (connected to) either a Security Commander server or client computer. A Challenger V8 control panel must be fitted with a TS0898 or TS0099 IP interface.

Refer to the IP interface's installation instructions for details of connecting a Challenger V8 control panel to a management software computer.

Setting up Security Commander for an IP connection

To log in to Security Commander and define the Challenger control panel:

1. In the Challenger menu, click Setup. The Controller Setup form displays in search mode (the Save Record command is disabled).
2. On the File menu, click New Record. The Controller Setup form displays in edit mode (the Save Record command is enabled).

3. Type a description (a name) to identify the control panel.
4. Click the Facility arrow and select the facility that the control panel will belong to. See “Facilities” on page 3 for details about facilities.
5. On the Definition tab, define the control panel (for more information, press F1 for Security Commander Help).
6. On the Communications tab, click the Communication Type arrow and select IP.
7. Under IP Settings, specify the IP address and the port number of the Challenger control panel.
8. For Challenger V8 panels, type the Encryption Key (if used) in the 16 encryption key fields. See “Using encryption keys” below for details.
9. If the control panel and the Security Commander computer are located in different time zones, click the Time zone tab to select the control panel’s time zone.
10. On the File menu, click Save Record.

Note: Prior to connecting to a control panel for the first time you may wish to suppress the receiving of events. See “Connecting and uploading data” on page 15 for details.

Using encryption keys

When setting up a connection to a control panel, you have two options regarding encryption:

- Establish communications without using encryption. In this case, troubleshooting a failed connection may be easier because you don’t have an incorrect encryption key as a potential fault. However, some steps will need to be repeated to set up encryption in both Security Commander and the IP Interface after communications have been established.
- Use encryption from the outset. In this case, troubleshooting a failed connection may be more difficult because you have the 16 encryption key fields to check in both Security Commander and the IP Interface. This is the more secure option because unencrypted control panel data is not transmitted over the network.

Setting up a direct serial connection

A Security Commander computer may connect directly to a Challenger V8 control panel fitted with a Computer-Printer Interface. The Security Commander computer’s serial COM port connects to the RS-232 port A on the Computer-Printer Interface.

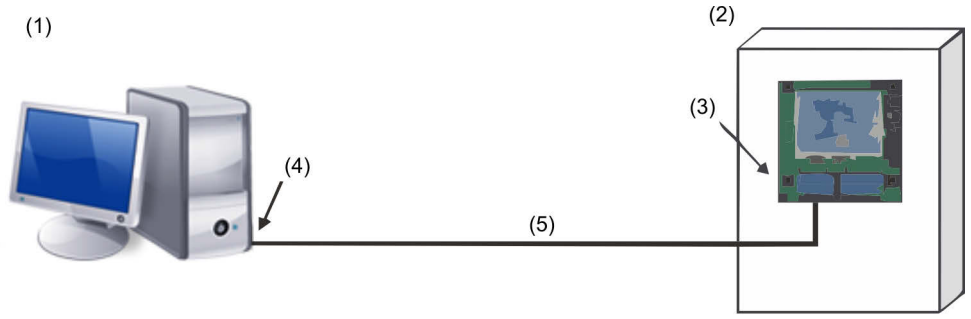
Note: Challenger Series control panels have native RS-232 support (J15) and do not need a Computer-Printer Interface.

A Challenger V8 control panel's RS-232 service port (J15) may be used for a temporary connection to the Security Commander computer. Refer to the *Security Commander Help* for details.

Multiple control panels may be connected to the same serial port (multidrop) by using a combination of RS-485 LAN to Isolated RS-232 Interfaces. Reduced communication speed may prohibit the use of multidrop with large capacity systems.

Note: For best performance, every control panel should be connected to a corresponding serial port on the Security Commander computer.

Figure 2: Direct connection to Challenger V8 control panel via Computer-Printer Interface



(1) Security Commander Computer
(2) Challenger control panel
(3) Computer-Printer Interface (Port A)
(4) Serial port (for example, COM1)
(5) RS-232

Prerequisite data — Security Commander computer

You need to know the COM port number for the Security Commander computer.

Prerequisite data — Challenger control panel

You need the following details about the Challenger control panel:

- Memory size (for example, IUM Large)
- Computer address (for example, 27)
- Password (for example, 0123456789)

Use a remote arming station (RAS) to interrogate the Challenger control panel for computer address and password, and ensure that the setting for Security Attempts will allow communications.

Use the following process to set up a direct connection between the Security Commander computer and a Challenger control panel.

Setting up Security Commander for a serial connection

To define the Challenger control panel:

1. In the Challenger menu, click Setup. The Controller Setup form displays in search mode (the Save Record command is disabled).

2. On the File menu, click New Record. The Controller Setup form displays in edit mode (the Save Record command is enabled).
3. Type a description (a name) to identify the Challenger control panel.
4. Click the Facility arrow and select the facility that the Challenger control panel will belong to. See “Facilities” on page 3 for details about facilities.
5. On the Definition tab, define the Challenger control panel (for more information, press F1 for Security Commander Help).
6. On the Communications Settings tab, click the Communication Type arrow and select Serial.

   Note: Challenger Series control panels can connect at 57600 baud. Challenger V8 control panels can connect at 4800 baud.
7. Under Serial / Dial-Up, click the Com Port arrow and select the port that will be used to connect to the Challenger control panel.
8. If the Challenger control panel and the Security Commander computer are located in different time zones, click the Time zone tab to select the control panel’s time zone.
9. On the File menu, click Save Record.

Note: Prior to connecting to a Challenger control panel for the first time you may wish to suppress the receiving of events. See “Connecting and uploading data” on page 15 for details.

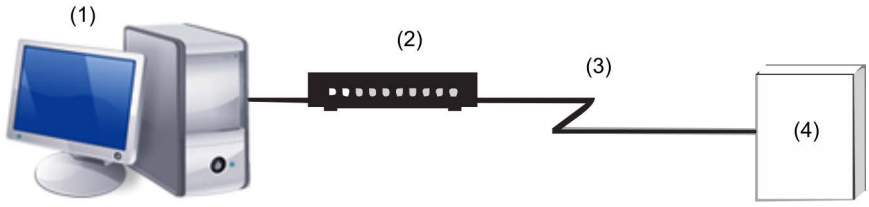
Setting up a dial-up connection

A Security Commander client computer fitted with an approved modem may connect to a Challenger control panel’s onboard modem via dial-up. Challenger Series control panels will auto-negotiate the best modem speed.

Challenger V8 control panels using firmware version 8.105 or later (and using corresponding hardware) can communicate at 2400 baud. Other versions are limited to 300 baud. On the Challenger menu, click Communications, and then select Communications to open the Challenger Comms Setup Form. Click the More tab to select the modem answer speed.

Note: The Challenger V8 control panel may alternatively use an external modem connected via the RS-232 port A on an optional Computer-Printer Interface module. This option is not fully supported at present.

Figure 3: Dial-up connection via modem



(1) Security Commander Computer
(2) Modem
(3) PSTN line
(4) Challenger control panel

Prerequisite data — Security Commander computer

You need to know the telephone number of the modem that the Security Commander computer will use for connecting with dial-up Challenger control panels.

Prerequisite data — Challenger control panel

You need the following details about the Challenger control panel:

- Memory size (for example, IUM Large)
- Computer address (for example, 27)
- Password (for example, 0123456789)
- Phone number

Use a RAS to interrogate the Challenger control panel for computer address and password, also ensure that the setting for Security Attempts will allow communications.

Use the following process to set up a dial-up connection between the Security Commander computer and a Challenger control panel.

Setting up Security Commander for a dial-up connection

Note: You must program the modems to be used by the Security Commander system in the Parameters form > Communications Setting tab, and then restart the Security Commander server for the settings to be in effect. Refer to the *Security Commander Help* for details.

To define the Challenger control panel:

1. In the Challenger menu, click Setup. The Controller Setup form displays in search mode (the Save Record command is disabled).
2. On the File menu, click New Record. The Controller Setup form displays in edit mode (the Save Record command is enabled).
3. Type a description (a name) to identify the Challenger control panel.
4. Click the Facility arrow and select the facility that the Challenger control panel will belong to. See “Facilities” on page 3 for details about facilities.

5. On the Definition tab, define the Challenger control panel (for more information, press F1 for on-line help).
6. On the Communications tab, click the Communication Type arrow and select Dial-Up.
7. On the Dial Settings tab, type the phone number of the dial-up Challenger control panel.
8. Select the other Dial Settings options, as needed (for more information, press F1 for Security Commander Help).
9. If the Challenger control panel and the Security Commander computer are located in different time zones, click the Time zone tab to select the Challenger control panel's time zone.
10. On the File menu, click Save Record.

Note: Prior to connecting to a Challenger control panel for the first time you may wish to suppress the receiving of events. See "Connecting and uploading data" below for details.

Connecting and uploading data

You must upload (retrieve) a database from a Challenger control panel for the first time.

To upload a database from a Challenger control panel:

1. On the Operations menu, click Controller Utility. The Controller Utility form displays with the new Challenger control panel listed.

   Note: Suppress receiving events from the Challenger control panel until after uploading the full database. This enables Security Commander to learn details of the alarms to be reported, and so avoids the alarms being lost and reported as warnings in the diagnostic log.
2. Right-click the Challenger control panel in the Controller Utility form and clear the Accept Events option to suppress receiving events from the Challenger control panel.
3. Right-click the Challenger control panel in the Controller Utility form and select Set Online. Security Commander initiates communication with the device. After communication has been established, the status field displays Connected.
4. Right-click the Challenger control panel in the Controller Utility form and select Upload > Full Database to copy the entire database from the controller into Security Commander.
5. If you suppressed events in step 2, you may now select the Accept Events option if you want to receive events.

Completion

After connecting to a Challenger control panel and uploading data, you have verified the operation of Security Commander. This concludes the installation process.

Operator interface

Introduction

This chapter describes the Security Commander workspaces and the methods of selecting operator commands.

The Security Commander login ID identifies an operator, and every operator has assigned permissions to use various Security Commander menu items. There may be menu items described in this chapter that a particular operator does not have permission to use, or the use might be restricted to read-only.

Security Commander 2.2 (and later) remembers certain monitoring forms such as the Alarm Monitor or Alarm Graphics Viewer used by the operator. The forms are recorded at logout, so when the operator next logs in (at the same workstation) the forms are automatically reopened.

In addition to possible restriction over menu options, an operator's use of Security Commander may be further restricted by the application of facilities. For example, an operator responsible for facilities A and B will not see Challenger control panels, devices, or various transactions associated with facility C.

Where permission defines access rights to the menu items, facilities provide a filter on data shown in the forms related to menu items.

The use of permissions and facilities enables a Security Commander operator to work with only the items that may require the operator's attention.

Starting Security Commander

1. Select Start > All Programs > Tecom > Security Commander > Security Commander to run the application. Alternatively, double-click the Security Commander desktop icon.

2. The login screen displays automatically when Security Commander starts. Use the default Login ID "secure" and the assigned password to log in, or use your assigned login ID and password (if applicable).

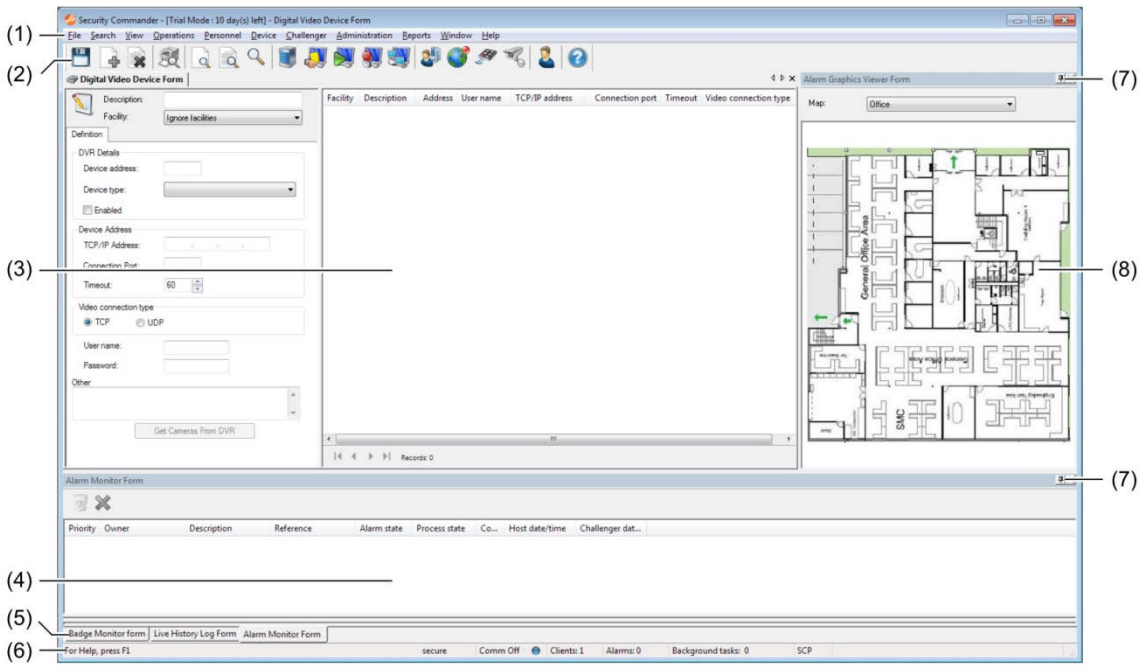
Main window

After starting Security Commander and logging in, the main window displays the following items:

- Menu bar (described in "File menu" on page 22)
- Toolbar (described in "Toolbar" on page 18)
- Status bar (described in "Status bar" on page 19)

The main window is shown in Figure 4 below.

Figure 4: Security Commander Main Window



(1) Menu bar
(2) Toolbar
(3) Undocked work space
(4) Bottom-docked work space
(5) Tab names in bottom-docked work space
(6) Status bar
(7) Auto Hide button
(8) Side-docked work space

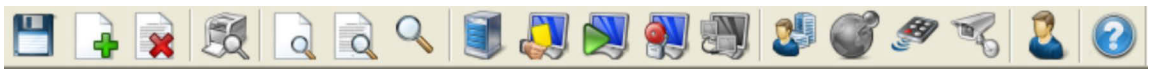
The Security Commander 2.2 main window has the following features:

- Programming forms automatically fill the available workspace (Figure 4 above, item 3).
- Monitoring forms may be docked at the bottom (item 4) or side (item 8) of the main window, or may be dragged via the form's title bar to float anywhere on the computer's screen(s), inside or outside of the main window.
- Monitoring forms have an Auto Hide button by which docked windows can be minimised to a tab at the bottom or side.
- Monitoring forms that are open when the operator logs out are automatically reopened in the same position (inside or outside of the main window) when the operator next logs in (at the same workstation).

Toolbar

Toolbar buttons are a quick way to access commonly-used menu items.

Figure 5: Security Commander Main Window Toolbar



From left to right the Toolbar buttons apply the following commands:

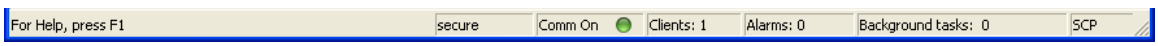
- Save button (see “Save Record” on page 22)
- New Record button (see “New Record” on page 22)
- Delete Record button (see “Delete Record” on page 22)
- Print Preview button (see “Print Preview Report” on page 23)
- Clear Search button (see “Clear Search” on page 24)
- Recall Search button (see “Recall Search” on page 24)
- Search button (see “Search” on page 25)
- Controller Utility button (see “Controller Utility” on page 26)
- Badge Monitor button (see “Badge Monitor” on page 26)
- Live History Log button (see “Live History Log” on page 26)
- Alarm Monitor button (see “Alarm Monitor” on page 26)
- Client Monitor button (see “Client Monitor” on page 26)
- Person in Region button (see “Persons In Regions” on page 26)
- Alarm Graphics Viewer button (see “Alarm Graphics Viewer” on page 27)
- Device Control and Status button (see “Device Control and Status” on page 27)
- Digital Video Viewer button (see “Video ” on page 27)
- Person form button (see “Person” on page 28)
- Help button (click the Help button and then click the Security Commander screen to get help). Alternatively, press F1 to access the help.

If you prefer to work without the Security Commander toolbar, in order to provide additional workspace, use the View > Toolbar command to hide the toolbar.

Status bar

The Status Bar option displays the status of the Security Commander system, restricted to the operator’s assigned facilities.

Figure 6: Security Commander Main Window Status Bar



The Security Commander status bar indicates the following:

- For Help, press F1.
- Current operator login ID (the operator in Figure 6 above is ‘secure’).
- Communication port status.
- Number of clients connected (including the server) for the facilities assigned to the current operator (see “Defining facilities” on page 8 for details).

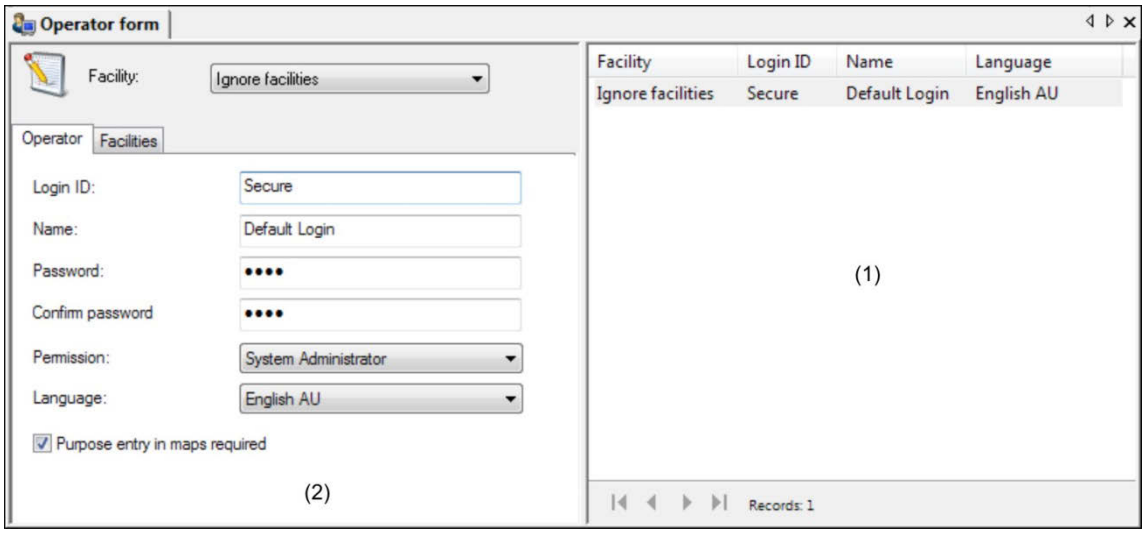
- Number of alarms for the facilities assigned to the current operator (see “Defining facilities” on page 8 for details).
- Number of background tasks taking place at the Security Commander server computer. If the Status Bar indicates a background task is running, do not shut down the Security Commander services until the task is complete.
- Status of Smart Card Programmer (SCP) shown in Figure 6 on page 19 as blank (not available).

If you prefer to work without the Security Commander status bar, in order to provide additional workspace, use the View > Status Bar command to hide the status bar.

Forms

Many Security Commander functions involve the use of forms that have a left-hand side and a right-hand side.

Figure 7: Operator form



(1) List of records (result of a search)

(2) Details of the selected record

The right-hand side of the form displays:

- A list of search results.
- The details of a saved record.

Tip: When multiple records are displayed, click a column heading to sort the list by the column. Click a second time to sort in the other direction.

The left-hand side of the form displays:

- Details of the record currently selected in the list of search results.
- Data entry fields for new records.

Using search criteria

The form's data entry fields serve as criteria fields when performing searches. For example, if a facility is selected prior to searching, only the records associated with the facility are searched.

Tab pages

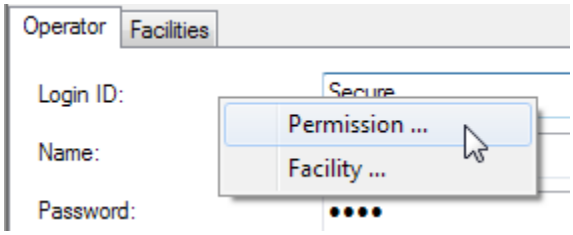
Some forms are used for several types of data entry, which may be grouped into tab pages for ease of use. For example, the Operator form in Figure 7 on page 20 has two tabs:

- Operator tab where the operator's details are recorded.
- Facilities tab where particular facilities are assigned to the operator.

Shortcuts

Right-click: Security Commander provides right-click menus on the left-hand side of most forms (below the tab) for quickly accessing related forms. For example, the Operator form (either tab) has right-click shortcuts to the Permission form and Facility form.

Figure 8: Example of right-click shortcut to Permission form, from the Operator form



Double-click: The Controller Setup form, Configuration tab provides double-click access to the Challenger control panel's devices and configuration settings.

Expand the "+" signs to view the Challenger control panel options and devices, and then double-click the required item to open the form.

Security Commander Help

Information about forms is provided in a number of ways.

- For general help about the form, press F1 when the form is active to view the help topic associated with the form.
- For help about a certain part of the form, click the Help toolbar button and then click the item you want help on.
- Some forms have their own toolbars. Hold the cursor over a toolbar button to display the name of the button's command.

Main menu command reference

The Security Commander menu bar provides access to most commands.

This section is a reference to the main menu commands, as described in the *Security Commander Help*. This section contains only summary information: please refer to the help for detailed information.

Some menu items have corresponding toolbar buttons — these are indicated below the heading (as applicable). Some menu items have corresponding keyboard shortcuts — these are indicated in brackets in the heading.

Note: For *Security Commander Help*, press the F1 button on your keyboard.

File menu

Save Record

The Save Record command (press Ctrl+S) saves changes made to the current record. If you do not save the changes, they will be discarded.

The Save Record command is available:

- When a form that manages records (such as the Badge form) is open in edit mode.
- For operators assigned with permissions of ‘update’ or ‘all’ for the selected type of record.
- After a New record is created.

The Save Record button is disabled (greyed) following the Clear Search command, or when there is nothing to save.

New Record

The New Record command (press Ctrl+N) creates a new record and enables the Save Record button.

For some record types, the new record is preloaded with default data (except where default data is potentially damaging or confusing).

The New Record command is available:

- When a form that manages records (such as the Badge form) is open
- For operators assigned with permissions of ‘update’ or ‘all’ for the selected type of record

Delete Record

The Delete Record command (press Ctrl+Del) deletes the current record. The Delete Record command is available only when a form is open and contains records, such as the Badge form, and you have been given all permissions.

Note: Take care using the Delete Record command, because deleted records cannot be recovered.

Some forms do not have a delete command.

Notes

The Notes command opens a text file (notes.txt) in which you can record site-specific information. The program used to edit this file is the program that has been associated with TXT files in Windows, usually Notepad. Notes.txt is saved to your Security Commander directory.

Logoff

The Logoff command (press Ctrl+L) allows you to log off the system without exiting Security Commander. While logged off, no one can enter data into Security Commander but it continues to communicate with the Challenger control panels, store alarm and badge transactions in the history database, and notify you about alarms. See the Client form for information on turning alarm notifications on and off.

Print Setup

On the File menu, click Print Setup to select your printer, printer properties, paper source, and orientation.

Print Preview Report

The Print Preview Report command (press Ctrl+R) allows you to preview a report before printing it. A printer must be added to your computer system in order for this feature to work.

Note: On the Preview Report screen, the Total: field represents the number of records in the database and not the number of records that matched your search criteria.

Print Report

The Print Report command (press Ctrl+P) allows you to send the current report to the currently-selected printer.

Export

The Export command allows you to select an export format for your report. There are a variety of formats available including text, Word for Windows, Lotus, HTML and Excel.

Select an export destination for the report to the application, a file, database, Exchange Folder, or Microsoft Mail (MAPI).

Save Template As

Run this command to save the report template under a new file name.

Set As Default Template

Use this command to select a report template to use as the default template. This template will automatically be loaded whenever you open this report form.

Create Default Template

Use this command to clear the template selection from a report so that a new template can be created from scratch (not based on any other template).

After clearing the Template field on the report form, use the Save Template As... command to name the new template, and then use the Set As Default Template command to make the template the default setting for the report type.

Delete Template

Use this command to clear the current report template

Exit

On the File menu, click Exit to log out the operator and shut down the Security Commander client application.

Search menu

Clear Search

The Clear Search command (press F7) clears all data in the current form. Use this command when the form has data and you wish to start a new search.

Note that the command does not conduct a search nor does it affect any data in the database. It only clears data from the form in preparation for a search. The Clear Search command is available only when a form that contains records is open, such as the Badge form.

This button can also be used to abort a change to a record.

Recall Search

The Recall Search command (press F8) refills the current form with the last search criteria data. Use this command when you wish to recall the last search criteria. The command does not conduct a search or affect any data in the database. The Recall Search command is available only when a form that contains records is open, such as the Badge form.

Search

The Search command (press F9) conducts a search in the database for all records that match the search criteria data you enter in the form. The records found by the search are displayed in the search results window. Data can be in any number of fields in the form or any number of tabs. If no data is entered, then all records will be displayed.

Only records that match all fields in which data are entered are displayed. Asterisks (*) can be placed in text boxes to indicate any characters. For instance, in the Badge form, entering an A* in the Description field will display all badge records that have a description starting with A. Entering *a in the description field will display all badges that have a description ending with a.

If A* is in the Description field and Active is in the Status field, only those badge records with a description starting with A and a status of Active will be displayed. The Search command is available only when a form that contains records is open, such as the Badge form.

View menu

Toolbar

The Toolbar option determines whether or not the toolbar is visible across the top of your Security Commander screen. This is a toggle selection. See also “Toolbar” on page 18.

Status Bar

The Status Bar option displays the status of the Security Commander system, restricted to the operator’s assigned facilities. This is a toggle selection.

See also “Status bar” on page 19.

Flat Toolbar

The Flat Toolbar item is not a selectable option and has no relational capability. It is the look of the Security Commander display after login.

Split

The Split command allows you to change the horizontal size of the search results window on a form using either the mouse or the keyboard.

Alternatively, click the vertical separator and drag it to the required position.

Next Pane

The Next Pane command (press F6) moves the cursor between the main form and the search results window.

Refresh

The Refresh command (press F5) to update the values displayed on the current form.

Operations menu

Controller Utility

The Controller Utility command (press Ctrl+F7) allows you to monitor communications, control and program the Challenger control panel.

Badge Monitor

The Badge Monitor command (press Ctrl+F8) allows you to monitor badge activity (for example, people badging their cards to get through doors).

Live History Log

The Live History Log command (press Ctrl+F6) allows you to monitor both alarm and badge activities (events generated by Challenger panels).

Alarm Monitor

The Alarm Monitor command (press Ctrl+F9) allows you to monitor alarm activity.

Client Monitor

Note: This option is not available in Security Commander Lite.

The Client Monitor command (press Ctrl+F10) allows you to obtain client information such as client type, Photo ID status, and connection status.

Persons In Regions

The Persons In Regions form enables you to monitor the presence of users in the specified regions.

Alarm Graphics Editor

Note: This option is not available in Security Commander Lite.

The Alarm Graphics Editor command (press Ctrl+M) allows you to add icons on graphical map views to point out the location and type of incoming alarms. You cannot create a map using Security Commander; create it using the program of your choice and save it in a .WMF, .EMF, .BMP, .JPG or .PNG format.

Alarm Graphics Viewer

Note: This option is not available in Security Commander Lite.

The Alarm Graphics Viewer command (press Alt+F7) allows you to view the maps of your facility that were created. These maps point out the location and type of incoming alarms.

Device Control and Status

The Device Control and Status command (press Alt+F8) allows you to control Challenger devices and retrieve their states. Devices include areas, RASs, lifts, doors, inputs, DGPs, and relays. See “Managing Challenger devices” on page 70 for details.

Video Console

Note: This option is not available in Security Commander Lite.

The Video Console command (press Alt+F9) opens a video command and control application that allows you to monitor digital video recorders (DVRs) and their associated cameras, control live video, as well as search and play back recorded video events.

Search DVR Footage

The Search DVR Footage command allows you to search history or archive databases for tagged video footage, and display the footage via the Video Console.

Change Password

The Change Password command menu opens the Change Password form which allows you to change your password.

Select Facilities

The Select Facilities command opens the Set Active Facilities form which allows you to change the facilities currently in use.

Camera Footage on alarm

Note: This option is not available in Security Commander Lite.

Select the Camera Footage on Alarm option to automatically display camera footage on alarm, if a corresponding trigger is defined. The video window will be displayed until an operator will close it manually. In case the camera window is displayed and new alarm occurs, the video will be switched only if the priority of the new alarm is higher.

Show map on alarm

Note: This option is not available in Security Commander Lite.

If enabled, the map containing the device in alarm (if any) will open automatically.

See also “Alarm Graphics Editor” on page 26.

Personnel menu

Person

On the Personnel menu, click Person (or press Alt+F10) to enter a person record into the system and assign access rights (optionally by importing a defined Person Profile).

See also “Person” on page 56.

Person Profile

On the Personnel menu, click Person Profile to define a set of access groups. A Person Profile is an optional means of creating and quickly applying a standard set of access groups to new person records.

See also “Person profile” on page 55.

Personnel Type

On the Personnel menu, click Personnel Type to create groupings of employees. There are three provided with the system: Permanent, Contractor and Temporary. You can also assign a badge design to the personnel type.

Department

On the Personnel menu, click Department to create departments which can then be assigned to person records.

Import Users

On the Personnel menu, click Import Users to import users, badges, and images, via a CSV file.

See “Importing user data via CSV file” on page 122 for details.

Badge

On the Personnel menu, click Badge to identify persons in the Challenger system. Badges may have a site code and a badge number. Alternatively badges may be learned by the system without using site code or card numbers.

The Challenger term “Badge” applies to badges and/or a PIN (personal identification number) — a number that is entered on a RAS keypad.

See also “Badges” on page 56.

Badge Groups

On the Personnel menu, click Badge Groups to tell the Security Commander system which badges need to be downloaded to which Challenger control panels. Badge groups are linked to Challenger control panels via the Controller Setup form, Badge Groups tab.

See also “Badge groups” on page 57.

Badge Design

Note: This option is not available in Security Commander Lite.

On the Personnel menu, click Badge Design to create a format or design that will print on the badge. See also *Security Commander Photo ID User Guide*.

Card Programmer

Security Commander may have multiple sites with TS0870P Smart Card Programmers for programming user cards (badges) and reader configuration cards.

The Card Programmer menu contains the following options:

- Programmer Setup. Click Programmer Setup set up a connection to the Smart Card Programmer.
- Site Setup. Click Site Setup to set up the properties for each site’s Smart Card Programmer.
- Labels. Click Labels to set up account labels for use with Smart Card credit application.
- Configuration Card. Click Configuration Card to set up reader configuration cards.

Device menu

The Device menu contains:

- Alarms form
- CCTV Digital Video Devices and Cameras (not available in Security Commander Lite)

Alarms

The Alarm command allows you to modify the records that are automatically generated when you define a device.

See also “Configuring alarms” on page 52.

CCTV > Digital Video Device

Note: This option is not available in Security Commander Lite.

The Digital Video Device menu item opens the Digital Video Device form that allows you to define, configure, and request status of your digital video devices.

CCTV > Camera

Note: This option is not available in Security Commander Lite.

The Camera form menu item of the Device menu opens the Camera form, allowing you to edit your camera database records.

Challenger menu

Setup

Open the Challenger Setup form to define or edit the details of a Challenger control panel.

Note: A Challenger Series control panel's IP address must be entered on the Comm Devices Setup form (Ethernet tab), and on the Challenger Setup form (Communications tab).

Alarm Groups

Refer to "Alarm groups" on page 55.

Door Groups

Refer to "Door groups" on page 55.

Floor Groups

Refer to "Floor groups" on page 55.

Holidays

The Holidays menu allows you to enter 24 different holidays for the Challenger control panel.

A holiday is a specified date (or range of dates for Challenger Series control panels) 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.

Some users may require access during holidays. This functionality is provided via a time zone in the users' alarm group that allows access during any holidays (Challenger V8) or during holidays that have matching holiday types (Challenger Series).

Time zones

Time zones are used to create time slots in which certain events can take place. For example: to automatically arm areas, disable users, or to activate relays to unlock a door.

'Hard' time zones are assigned to alarm groups, door groups, floor groups, relays/outputs, arm/disarm timers, and out of hours access reporting, or to restrict/enable some Challenger operations during specific time periods.

There are two main types of time zone:

- ‘Hard’ time zones are programmed to be valid according to times and days. They are typically used to enable or disable facilities at specific times (and to allow access for designated users during holidays). Time zone 0 is not programmable, but is a 24-hour time zone (always valid).
- Soft time zones are programmed to be valid when a relay is active. Soft time zone 25 is not programmable, but is valid during the service time.

Soft time zones

Select a time zone to follow a relay. When the relay is active, the time zone is valid, and when restored, invalid. This is reversed if relay is inverted.

Soft time zones are used, for example:

- To prohibit the use of a keypad, unless a key switch on an input is active
- To allow an area to be disarmed only if another area is first disarmed

Areas

The Areas form is used to record information relating to an individual area and can be programmed with a number of options, like the area name, entry and exit times, event flags, and so on.

Area Groups

Depending on model, a Challenger Series control panel can have up to 99 areas. To help manage areas, one or more areas can be incorporated into area groups. There can be 255 area groups.

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

Inputs

Use Inputs to program all input parameters. Each input is a physical input on the Challenger control panel, a DGP or a plug-in input expander.

RASs

RASs (Remote Arming Stations) are devices used to provide system control, such as arming or disarming of areas to users. Depending on the type of arming station, additional functions may be available.

DGPs

This DGP menu contains a mixture of data entry fields and check boxes and enables or disables DGPs (Data Gathering Panels). Also the type of DGP can be programmed.

Relays

This option links a relay (output) to an event flag and/or a time zone, and records the text to be displayed in the Active column of the Challenger Control and Status form when the relay is set or reset from the form.

Macro Logic

This function is used to activate an event flag or an input under specific logic conditions.

Up to four relays or event flags can be included in the logic equation. Each relay or event flag in the logic equation can be programmed as an AND or OR function and can also be programmed to invert the logic. Programming options are provided so that the result of the equation (event flag or input) will pulse, time, on delay, off delay or latch when true.

Note: It is very important to plan the macro logic carefully on paper, noting all details, and the origin of every input and/or event flags, before attempting to program.

Doors

Use Doors Setup to program individual doors associated with Intelligent Access Controller.

Lifts

The Lifts Setup form is used to set up all lift options for four-lift controllers.

Floors

Displays the details for a floor on a four-lift controller. This has to be programmed before floor groups can be assigned.

Regions

Regions are used by Intelligent Access Controllers in combination with anti-passback. Security Commander also uses regions to be able to report on which region users can be found.

Door/Lift Controller

Use the Challenger 4 Door Lift DGP Setup to program Intelligent Access Controller options.

Note: You must use the Challenger > DGP Setup form to define an Intelligent Access Controller DGP before using this form.

DGP Macro Logic

Macro logic provides a powerful tool for activating event flags when specific events occur. These events are macro inputs being triggered, logic equations combining the macro inputs, and timed/latched relay conditions.

Up to four macro inputs may be included in the logic equation. A macro input is an event flag. Each macro input in the logic equation can be programmed as an AND or an OR function and may be inverted.

Options are provided so that the macros result will trigger a macro relay, which may be: a pulse, timed, on delay, off delay or latched when activated.

Panel Options > System Options

The System options menu is slightly different from most other windows; it is a one-off record for each Challenger control panel. Every Challenger control panel has only one System options record. This function is used to record options common to the whole system.

Panel Options > Custom LCD message

The Custom LCD message allows you to modify the text displayed on the RASs connected to the panel. You may enter up to 32 characters for this text. You will only see this text displayed on the RASs if there are no alarms, system or fault messages.

Panel Options > Next Service

Program a starting date to display a routine service reminder message “Maintenance” on the Challenger control panel’s LCD RAS's, and optionally add text to the message. For example, program a date and the text “- call 9239 1200” to display “Maintenance - call 9239 1200” starting on the programmed date.

The reminder message is cleared when the technician programs a new reminder date.

Panel Options > Auto Reset

This function is used to program the Challenger control panel to automatically reset alarms. The reset of alarms are for selected areas (determined by an alarm group) and are reset after a predetermined time that is programmed in this window. Use this facility when it may not always be possible to reset an alarm manually.

Panel Options > Timers

The Timer Setup form is slightly different from most other windows, it is a one-off record for each Challenger control panel. Every Challenger control panel has only one Timer database record. All the fields are data entry fields and have a range of blank (representing zero) or 1 to 255.

Program all system-wide timers in this section.

Panel Options > Auto Access/Secure

Time zones are used to automatically arm and/or disarm areas. Areas being armed or disarmed automatically do not require any operator action.

Panel Options > Battery Test

This menu contains details regarding the battery test to be run for any batteries on the Challenger control panel system data bus. All batteries are tested sequentially to prevent power problems. If a battery is disconnected for more then 10 minutes, a warning will be given.

During the battery test, the Challenger control panel and/or DGPs, and all auxiliary driven devices, are powered from the battery. Devices are tested one at a time, making sure that not all devices switch to battery test at the same time.

Panel Options > Clock Correction

This command allows a correction factor to be programmed into the Challenger control panel to compensate for a Challenger control panel clock that may be running slightly fast or slow.

Panel Options > Text Words

This function is one of the ways to add user-defined words to the pre-defined Challenger word library. All words in the library are identified by a reference number. The pre-defined word library uses reference numbers 001 to 544, additional user-defined words use reference numbers from 900 to 999 (Challenger V8 only).

Challenger Series control panels using firmware version V10-06 (or later) do not use text words.

Panel Options > User Categories

In Challenger Series application, user categories 1 to 8 provide timing for areas that are configured for timed disarming or for delayed arming (via vault programming).

For Challenger V8 control panels, user categories restrict alarm groups arming and disarming behaviour. It is an excellent tool to provide additional security options to Users.

For example: During the daytime, shops in a shopping mall are not allowed to arm or disarm adjacent shops, but during night time they are able to arm and reset.

Panel Options > Vault

Vault areas, when armed, are areas that will automatically arm other areas after a preset delay time.

By using a special programming procedure, a user category timer starts when all of the vault areas are armed. When the timer expires, a non-vault area linked to the vault areas will automatically arm.

Note: This option is not supported in ChallengerLE.

Panel Options > Area Links

In an intruder alarm with multiple areas, the entrance to the premises may be shared by all areas. This shared area should only be armed when the last area is armed. The shared area is known as a common area.

The simplest way to have a common entrance is by assigned multiple areas to an input. This input will only generate an alarm if all assigned areas are armed. The longest exit and entry times for the areas will be used.

The other way to create a common area is by using a dedicated area. By linking another area to this common area, the common area will arm automatically when the last (linked) area is armed. As soon as any of the linked areas disarm, the common area will also disarm.

Panel Options > Input Shunts

This option is used to program up to 32 shunt timers for Challenger10 or ChallengerSE; or 16 shunt timers for Challenger V8 or ChallengerLE. Each shunt timer controls a shunt procedure.

A shunt procedure inhibits an active input from generating an alarm during a certain time period.

- An input shunt is initiated when a relay is activated, for example, by a door unlocking or by a keypad entry.
- During the shunt time the input is inhibited.
- If the input is still active after the shunt time has expired, the input may generate an alarm, depending on the input type and the status of the area.
- The shunt timers may be programmed individually to control each input shunt.
- Before the shunt timer expires, a warning may be given.
- An input shunt stops a door generating an alarm when it’s opened.

Panel Options > Event Descriptions

This lists all event flags programmed in the Challenger control panel, along with a description for each.

Panel Options > Summary Event Flags

Program the values of summary event flags. Valid entries are blank (representing zero) or numbers in the range of 1 to 255.

These event flags are activated when any of the conditions specified exist in the system. Default setting (blank) is no event. The system alarm/fault event flags will be latching if Latching System Alarms is set to YES in System Options.

Note: You can use any event flag number that isn't already being used for something else.

Panel Options > Holiday Types

The Challenger Series concept of holiday types provides greater flexibility in controlling access for users who need to use the Challenger system during holidays.

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

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

Panel Options > Printer

Program the details for printers attached to Challenger V8 control panels.

Note: This option does not apply to printers attached to Challenger Series control panels. In Challenger Series control panels, printers are configured in communications path programming.

Panel Options > Password Attempts

Use Password Attempts to define the number of password attempts permitted by the Challenger V8 control panel when a device (such as a Security Commander computer) is attempting to connect.

Note: This option does not apply to Challenger Series control panels. Challenger Series password attempts are configured in communications path programming.

Communications > Comm Devices

Set up the hardware devices that Challenger Series control panels will use for communications.

Note: A Challenger Series control panel's IP address must be entered on the Comm Devices Setup form (Ethernet tab), and on the Challenger Setup form (Communications tab).

Communications > Comm Paths

Set up the communications paths that the Challenger Series control panel can use.

Communications > Communications

The Communications form defines the Challenger V8 control panel's setting for communications and reporting.

Communication setting must also be defined for the Challenger control panel record in Security Commander via the Challenger Setup form (Communications tab).

Communications > Ethernet

The Ethernet window is used to program the Challenger V8 control panel's IP interface (for example, to enable encryption) from the Security Commander computer and then download the settings to the IP interface.

Administration menu

Operator

The Operator command opens the Operator form that allows you to set up individuals as users for the Security Commander system and assign the facilities to which they have access.

Permission

The Permission command opens the Permission form that allows you to define Operator access to various forms within Security Commander.

Client

Note: This option is not available in Security Commander Lite.

The Client command opens the Client form allowing you to define a client computer.

API Connections

Note: This option is not available in Security Commander Lite.

The API Connections command opens the API Connections form that allows you to define records to enable external applications to interface with Security Commander. See also the *Security Commander API Manual*.

Instruction

The Instruction command opens the Alarm Instructions form that allows you to create instructions to link with alarms. The instructions will then appear on the Alarm Monitor when the alarm occurs.

Response/Purpose

The Response/Purpose command opens the Response/Purpose form that allows you to create a predefined response to an alarm or a purpose for a control option. These responses/purposes are used in the Alarm Monitor or any control command in the Operations menu.

Parameters

The Parameters command opens the Parameters form that allows you to establish settings for the entire application, such as archive intervals and appropriate modems.

Override

Note: This option is not available in Security Commander Lite.

The Override command opens the Override form that allows an operator to generate a T/A (time in attendance) transaction. This information is written to history.

LogFile

The LogFile command opens the Logfile form. The LogFile form allows you to select your computer and name the LogFile, and enter the path and directory in which to place your LogFile.

Diagnostic Setting

The Diagnostic Setting command opens the Diagnostic Setting form that allows you to define what debug information will go to the diagnostics log. This is a good place to start for troubleshooting.

Note: Apply these settings only on request of appropriate Support personnel to avoid logging unnecessary data in the diagnostic logs.

Diagnostic Viewer

The Diagnostic Viewer command allows you to view what's happening on the system. The debug messages displayed by the DiagView program are determined by the items you select in the Diagnostic Setting form.

CCTV Alarm

Note: This option is not available in Security Commander Lite.

The CCTV Alarm command opens the CCTV Alarm form that allows you to link a CCTV Interface and alarm to Security Commander so that the CCTV alarms will display on the Security Commander Alarm Monitor.

Note: This feature is currently not supported.

Camera Preset

Note: This option is not available in Security Commander Lite.

When you select Camera Preset from the Administration menu, the Camera Preset form displays, allowing you to define PTZ camera presets to select from.

Event Trigger

Note: This option is not available in Security Commander Lite.

Event Trigger allows you to move up to four PTZ (pan tilt zoom) cameras into preset positions in response to specific door/reader transactions and/or alarm transactions.

Alarm Category

Alarm categories are used in the Alarm form and the Alarm History Report to provide a means of filtering large numbers of alarms. Use the Alarm Category Setup form to create new alarm categories.

Alarm Notifier

Alarm notifier allows you to define alarm notification for particular events. The email settings are configured in the Parameter form. See *Security Commander Help* for more details on the email notification parameters.

Facility

The Facility command opens the Facility form that allows you to define the desired facility, such as Building One and Building Two.

Map Background Editor

Note: This option is not available in Security Commander Lite.

This form is necessary to setup the application used for editing images that are used as map background.

Point Type Icons

Note: This option is not available in Security Commander Lite.

Use the Point Type Icons command to setup description and state icons for supported Challenger point types. You can change the default icon for each state a point type may have.

Panel Migration

Use Panel Migration to upgrade a Challenger V8 control panel to a Challenger Series control panel. The process to upgrade Challenger V8 to Challenger Series is in two parts:

- Convert the Challenger record in Security Commander from Challenger V8 to Challenger Series.
- Install Challenger Series hardware and connect to Security Commander.

Refer to “Panel Migration” in *Security Commander Help* for details.

Reports menu

Refer to “Reports and templates” on page 74 for details about the following reports:

- Person report
- Badge
- Persons in Regions

- Persons in Door Groups
- Persons in Floor Groups
- Persons in Alarm Groups
- Administration
- Challenger
- Floor Access
- Door Access
- Area Access
- Challenger Groups
- Roll Call
- History
- Badge History
- Time and Attendance History
- Operator History
- External Reports

Window menu

Cascade

This command allows you to control multiple windows or forms. If you have several forms open but not visible, use this command for a cascading view of your forms with the active form taking precedence on the display screen.

Tile

This command allows you to control multiple windows or forms. If you have several forms open but not visible, use this command to view all forms tiled side-by-side on your display screen.

Arrange Icons

This command allows you to control multiple windows or forms. If you have several forms in progress, you can temporarily minimize a form from view. Use this command to arrange the minimized form icons across the bottom of your Security Commander window.

Help menu

Help Topics

Select Help Topics (press F1) to launch the Security Commander Help.

About Security Commander

This screen displays the software version, service pack number, copyright information, and contact information.

Setting system parameters

The Parameters form (located in the Administration menu) will be one of the first parts of Security Commander you need to use. For example,

- Before you define a Challenger control panel and connect to it, you might want to be set up to print alarm activity.
- Before you add any photos to Person records, you need to ensure that the photo aspect ratio is set correctly.

System-wide (global) settings for Security Commander are specified on the Parameters form, including:

- The database archive history (daily, weekly, or monthly)
- Whether to print badge and alarm activity and to which printer(s)
- Alarm notifier email settings
- Alarm sound settings
- Photo aspect ratio for capturing images
- The names of the labels that will be used globally for the user fields and address fields
- Identification of modems that are used to communicate with Challenger control panels

The Parameters form is divided into six tab pages:

- Settings tab (see “Settings tab” below).
- User Fields tab (see “User Fields tab” on page 44).
- Address Fields tab (see “Address Fields tab” on page 44).
- Communication Settings tab (see “Communication Settings tab” on page 44).
- Clear Archive tab (see “Clear Archive tab” on page 45).
- Badge Learn tab (see “Badge Learn tab” on page 46).

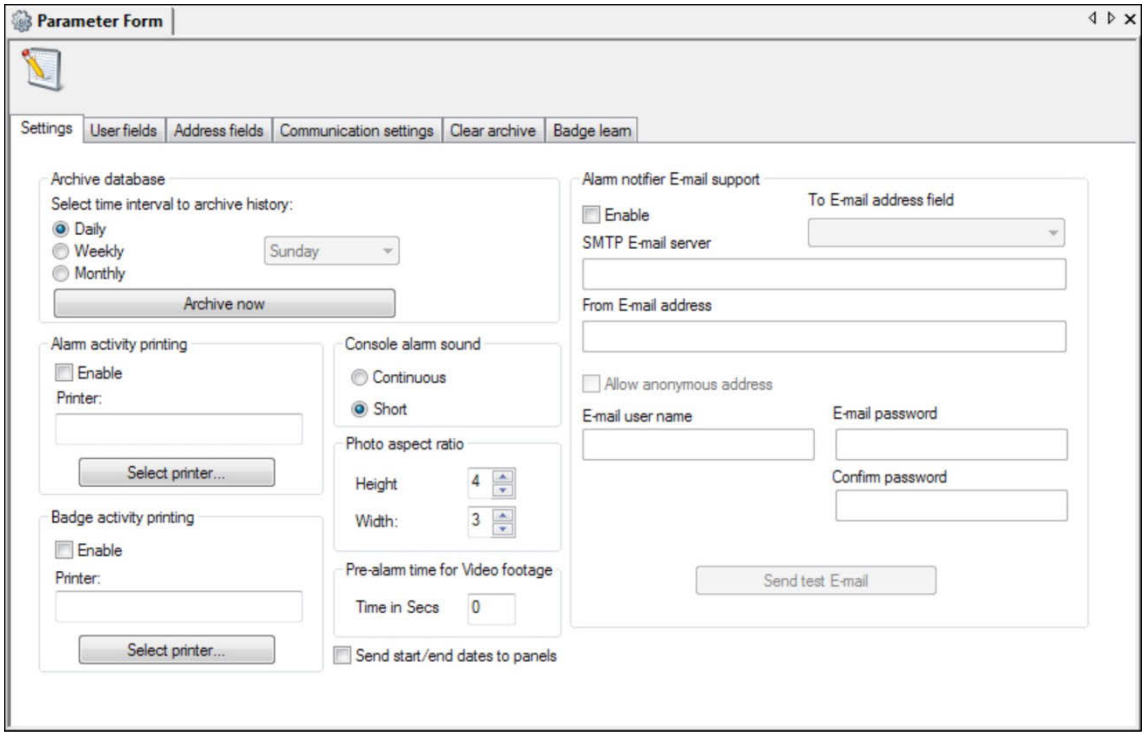
Settings tab

Archive Database

Archiving moves history events from the main history database to the archive database.

In the Archive Database section (see Figure 9 on page 42), select to archive history on a daily, weekly, or monthly basis. You can also archive it immediately by pressing Archive Now button.

Figure 9: Parameter form, Settings tab



Note: The default setting is to archive history on a daily basis. It is recommended that you use the default setting. Whatever setting you choose, you must monitor the size of the Security Commander history and archive databases to ensure that each database remains under 10 GB and that the databases do not completely fill the hard disk.

If you select:

- Daily (default setting): The archive is created every day some time between midnight and 1A.M.
- Weekly: The archive is created every week on the day you select sometime between midnight and 1A.M.
- Monthly: The archive is created on the first day of the month some time between midnight and 1A.M.

Archive now

Press this button to archive the history immediately.

Note: If you selected Weekly, there must be at least seven days following the installation date to first archive. For example, if a system was installed on Tuesday and the archive is scheduled for Sunday, the archive will not take place on the first Sunday after installation. Archiving will begin on the second Sunday following the installation.

The Archive Database setting assumes that the Security Commander server is running. If it isn't, then the next time Security Commander is started and a transaction is received, the archive is created.

Alarm Activity Printing

Note: This option is not available in Security Commander Lite.

You must enable and select a printer and route alarms to print in order for alarm activity to print.

Console alarm sound

Select Continuous to sound a continuous tone on alarm until the alarm is acknowledged. Alternatively, select Short to sound a short tone when alarms are detected. Sounds for alarms have to be set up separately if needed.

Badge activity printing

Note: This option is not available in Security Commander Lite.

You must enable and select a printer and route badges to print in order for badge activity to print.

Photo Aspect Ratio

Note: This option is not available in Security Commander Lite.

Enter a number for the height and the width. The aspect ratio controls the relationship between the height and width of the photos. This setting controls the photos displayed in the Capture program, on the Person form, and in the Badge Designer program.

Pre-alarm time for Video footage

When an alarm occurs, operators typically need to see video of events that preceded the alarm. You can avoid having to rewind by entering a value in the "Time in Secs" field. For example, if you enter 10, then alarm-triggered video will begin to display from 10 seconds prior to the alarm.

Send start/end dates to panels

Check the "Send start/end dates to panels" check box if you want all badges in the system to be:

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

Notes:

- Do not use "Send start/end dates to panels" in systems that contain 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).

Alarm Notifier E-mail Support

Note: This option is not available in Security Commander Lite.

Sets up the email settings for the alarm notifier (defined in the Administration > Alarm Notifier menu). The following options are available:

- To E-mail Address Field: Select the user field, which will be used as an email address of the notification recipients.
- SMTP E-mail Server: The SMTP email sending address.
- From E-mail Address: The email address shown in the “From” field of the email message.
- Allow Anonymous Address: Select this option if the above SMTP server does not require an authorization. Otherwise the settings below are necessary to configure.
- E-mail User Name: The login of the SMTP server account.
- E-mail password, Confirm Password: The password for the SMTP server account.

Click Send Test E-mail to send test email to the address defined in “From E-mail Address”.

User Fields tab

User Fields Labels

Displays the current labels for the 90 user fields on the Person form. Select a label to change it.

New label

To change the label of a user field, highlight the desired user field and type the new label. The user field label can be up to 32 characters long.

Address Fields tab

Displays the current labels for the five address fields on the Person form. To change a label, type over the existing text. The address field label can be up to 32 characters in length.

Communication Settings tab

Use this tab of the Parameter form to allocate the client modem pool: modems to be used by the server and client computers for communicating with dial-up Challenger control panels.

Note: Any change in this section requires Security Commander services to be restarted.

Clients list

Select a computer in the Clients list.

Note: Client computers are not available in Security Commander Lite. If the server computer has a modem, then it will be listed in the Clients list.

Available modems

Available modems lists all the registered modems for the selected computer. Click to select one or more modems to enable them to be used by Security Commander (running on the selected computer) to connect to a Challenger control panel.

Modems reserved for incoming calls

Click the Modems reserved for incoming calls arrows to specify the number of modems you want to reserve on the selected computer.

Note: The number of modems selected in the Available modems list must be greater than the number of reserved modems in order to make outgoing calls.

Disconnect after idle

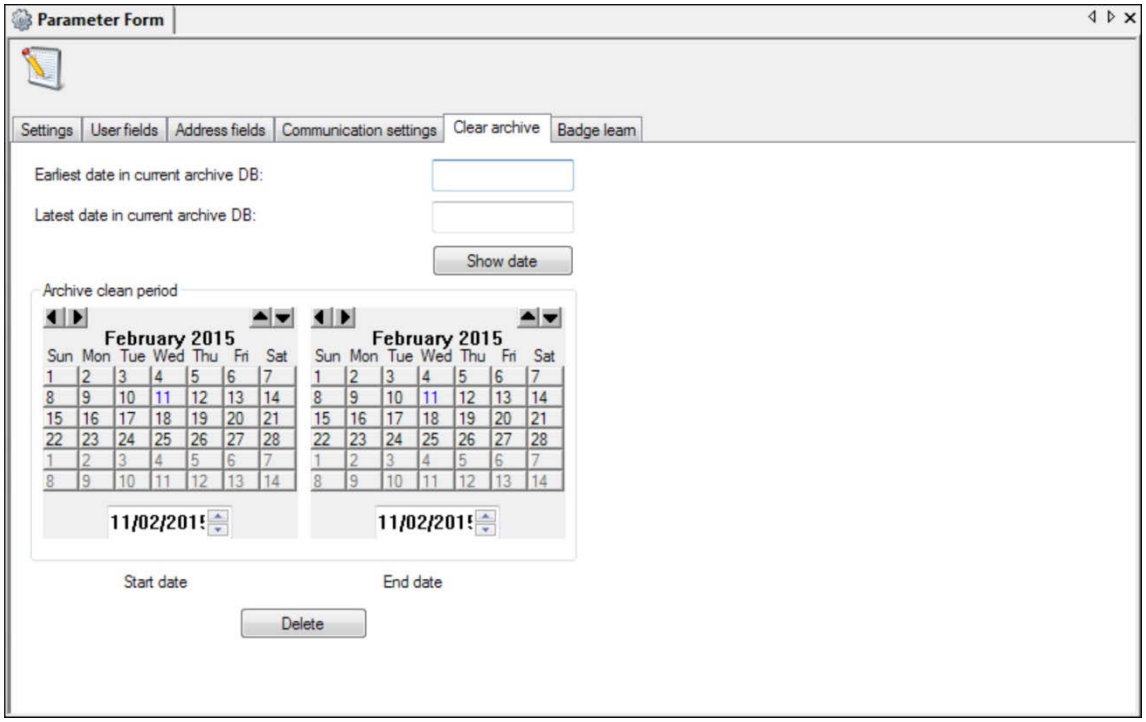
Click the Disconnect after idle arrows to select the number of minutes you wish the system to wait before disconnecting from the Challenger control panel when the connection is idle (there is no history or database information being exchanged or control/status commands issued).

If you select 0, the connection will not be automatically disconnected by Security Commander when idle.

Clear Archive tab

The Clear Archive tab is depicted in Figure 10 below.

Figure 10: Parameter form, Clear Archive tab



Earliest Date in Current Archive DB

This shows the oldest date for an event stored in the Archive database.

Latest Date in Current Archive DB

This shows the most recent date for an event stored in the Archive database.

Show date

If you have an archive database, click Show Date and the Earliest Date in Current Archive DB and Latest Date in Current Archive DB will display. If you do not have an archive database, the two date fields will state No Record.

Archive Clean Period

Select the Start Date of the data that you want to remove from your database by selecting the month, then the day to begin your archive.

Select the End Date of the data that you want to remove from your database by selecting the month, then the day to end your archive.

Delete

Press Delete after selecting Start Date and End Date to remove from your database.

Note: The deletion of an archive database is taking place in the background. Progress is indicated on the status bar. This may take hours to complete and is dependent on the size of the Archive database and the hardware components of your computer.

Badge Learn tab

The Badge Learn tab is used to specify badge learn devices (one, several, or all RASs or doors where badge readers are used). A badge learn device is used to quickly enter raw badge data into Security Commander.

Restrict

Select Restrict to prevent all RASs and doors (available to the operator) from being used as badge learn devices on the LAN. When Restrict is selected (default setting), the Edit button is enabled.

Edit

Use the Edit button to add badge learn devices (RASs or doors) to the Badge Learn Devices window. Only the listed badge learn devices may be used to enter raw badge data into Security Commander (as long as Restrict is selected).

Permissions, facilities, and operators

Before individuals can access, use, or administer the Security Commander program, they must be set up as operators. The setup sequence is as follows:

- Security Commander permissions and facilities must be created before operators.
- When operators are set up, they must have permissions and one or more facilities assigned. If no facility is assigned, then the operator can see only records set as 'Ignore Facilities'.
- At any given time, an operator can choose which facilities to be active from the list of facilities available to that operator.

Notes:

- Client computers are not available in Security Commander Lite.
- Operators using a Security Commander client computer and working over a network connection (via either a domain or a workgroup) must be logged into the client computer's operating system using a login ID and password combination that provides appropriate access permissions to the shared folders on the Security Commander server computer. Security Commander installation DOES NOT create any users or permissions under the domain environment.

Creating Security Commander permissions

Permissions are assigned to operators and define what operators can do within Security Commander. Use the Permission form to create permission records.

For example, if a Personnel Officer needs to use the Personnel menu, certain reports, and the Change Password command, you can define a permission that provides access to these functions and no others (other menu options would be greyed the next time the operator logs in).

To locate and view existing records, press the Search button. A list of records will display. You may either press the Add button to add a new record OR search and view or change an existing record.

Security Commander comes with a System Administrator permission that allows full action on all forms and is assigned to the default operator. Additional permissions are:

- Super User (no installer options)
- Installer (restricted personnel options)
- Security (possible permissions for security guards)
- Reception (possible permissions for reception desks)

Any of the available permissions may be changed. You may wish to create more restrictive permissions. Apply the System Administrator permission ONLY to those operators fully trained in Security Commander.

Permission form

The Forms list on the Permission form displays the form permissions for the selected Permission record. The list can be viewed in two modes:

- Show by Group: Lists the menu groups (File, Operations, Device, Administration, Reports) followed by the menu items in each group. The permission assigned to each group and item is indicated by an action icon.
- Show by Action: Lists the actions (none, read, update, and all) followed by the forms assigned to each action.

Right-click the Forms list to select the required view, or to open the Operator form, which shows permissions assigned to existing operators.

The Forms list displays the forms within the Security Commander program organised by their menu structure. A “+” sign on the left side indicates hidden submenus. You may apply an action to the entire menu, or you can click the “+” to display submenus to apply a mix of actions within the sub-menus.

Four types of actions can be assigned to forms:

- None: Means that no access is given to that form.
- Read: Means that read only access is given. The form and the associated records can be viewed but not modified.
- Update: Means that the records on that form can be viewed and modified.
- All: Means that the records on that form can be viewed, modified and deleted.

Mixed is not an action to be assigned. It is used only on this form to signal that any forms beneath a group have different actions assigned.

Adding a permission

Add a new permission record to Security Commander.

To add a permission in Security Commander:

1. On the Administration menu, click Permission.
2. On the File menu, click New Record. The Permission form displays in edit mode (the Save Record command is enabled).
3. Type a name to describe the new permission in the Description field.
4. Click the “+” beside each form category to display the list of forms. Initially, all forms have the action “None” assigned (no permissions).
5. Select a form and then select the required action (if you need to change the action from None). Repeat for each form name.
6. Save the Permission form.

Creating facilities

The Security Commander database can be partitioned and related records can be grouped. In Security Commander, these groups are called facilities. A Facility option can be designated on most forms throughout the system and any number of facilities can be defined. Using facilities will result in showing only those records in a form that have no facility assigned, or are part of the active facilities for an operator.

Note: It is good practise to create facilities and associate new Challenger control panels to facilities from the very start (assign a facility to a Challenger control panel record before saving the record). This will help ensure that all the data related to the Challenger control panel is kept within the same database partition and will help speed access to data.

Operators can be assigned to one or more facilities and can choose which facilities to be active at any given time. Usually, the system administrator is assigned to all facilities.

All records have the default Ignore Facilities, which means the records are not under facility protection; therefore, those records are visible to all operators.

Creating and using facilities are separate things:

- To create a facility, use the Facility form.
- To assign a facility to the required operator, use the Facilities tab on the Operator form.
- To manage a facility's state, use the Select Facilities command from the Operations menu.

Note: If you, as an operator, do not have a particular facility assigned to you, that facility will not be available to you from the Facilities list on various forms.

Adding a facility

To add a facility in Security Commander:

1. On the Administration menu, click Facility.
2. On the File menu, click New Record. The Facility form displays in edit mode (the Save Record command is enabled).
3. Type a name to describe the new facility in the Description field.
4. Save the Facility form.

Creating operators

An operator is an individual who can access and control the Security Commander software.

A Security Commander operator has a login ID and password for Security Commander. This login ID and password is independent of the operator's Windows user account login ID and password.

Adding an operator

When using the Operator form to search for existing records, use the Ignore Facilities selection to display all operator records. Alternatively, search using a specific facility to locate operators assigned to a particular facility (but not the facilities assigned to an operator).

The Operator form is used to:

- Assign the operator to a facility.
- Define an operator's login ID, name, and password.
- Assign Permission to an operator. Permissions define the actions that operators may perform within Security Commander. Click the Operator tab and then click the Permission arrow to select permission from the list. Permissions are created on the Permission form.

  Note: To reduce operator's permissions, be sure to block access to Permission and Operator menus.
- Assign facilities to operator. Once assigned, the facility is added to the Facility list on various forms when that operator is logged in. Click the Facilities tab to assign a facility to a selected operator. Facilities are created on the Facility form.

To add an operator in Security Commander:

1. On the Administration menu, click Operator.
2. On the File menu, click New Record. The Operator form displays in edit mode (the Save Record command is enabled).
3. Type the operator's login ID (the name that the operator will use to log in to Security Commander).
4. Type the operator's name.
5. Type the operator's initial password (the operator can change this later using the Operations > Change Password command). The password field displays each character as *.
6. Click the Permission arrow and select the operator's permission from the list of the available permissions.
7. Click the Language arrow and select the operator's language.
8. Define if the operator has the option to enter a purpose for issuing a control command in maps, or from the control options in the Operations menu.
9. Click the Facilities tab, and then click the Assign Facilities button to display the Facility Assignment dialog. This dialog lists the facilities available for assignment to this particular operator.
10. Assign the required facilities to the operator.
11. Save the Operator form.

Managing facilities

Facilities assigned to an operator are active by default.

A facility may be set to ‘Available’ (inactive) when it’s not needed. For example, a facility may be created for future use and then made inactive to prevent the facility from being accidentally selected by the operator when using various forms.

Configuring devices

Refer to the following sections to set up Security Commander and Challenger devices:

- Alarms (see “Configuring alarms” below).
- Digital Video Devices* (see “CCTV > Digital Video Device” on page 29.
- Cameras* (see “CCTV > Camera” on page 30).
- Challenger control panels (see “Setup” on page 30). See also “Configuring Challenger control panel” on page 53.
- Door groups (see “Door Groups” on page 30)
- Floor groups (see “Floor Groups” on page 30).
- Holidays (see “Holidays” on page 30).
- Point Types (see “Point Type Icons” on page 39).

* Not available in Security Commander Lite.

Refer to the *Security Commander Help* for more details about these options.

Configuring alarms

Alarm records are automatically created by Security Commander when various device records are created. For example, when a Digital Video Recorder record is created using the Device > CCTV > Digital Video Device form and is given a description “Second DVR”, Security Commander automatically creates alarm records for the DVR with the following attributes:

- The Description field displays the alarm description, for example, “DV Disk Full Alarm”.
- The Facility field displays the facility that Digital Video Recorder record was assigned to.
- The Owner Description field displays “Second DVR”, which is the content of the description field for the Digital Video Device record.
- The Owner Type field displays “DVRs”, which identifies the alarm owner (such as a Challenger control panel or DVR) by the generic type of device.
- The Category field displays the alarm category, such as “CCTV Alarm”.
- The Monitor field displays if the alarm should be shown in the Alarm Monitor.

When first opened, the Alarm form displays in Search mode. The New Record command is not an option for this form because Alarm records are generated by the system. The Save command becomes active only when alarms are displayed in the list on the right-hand side of the window (see page “Forms” on page 20).

The total number of alarms can become quite large; therefore it’s useful to filter the search.

For example, to display only the alarms from a particular facility:

1. On the Search menu, click Clear Search to clear the form of data.
2. Click the Facility arrow and select the required facility from the list. (The facility must be both active and assigned to you as an operator.)
3. On the Search menu, click Search to display all alarm records that have been created for the facility.

In the same manner, other fields can be used to filter the search. Refer to the *Security Commander Help* for further details.

For a shortcut menu to related forms, move the mouse pointer below any of the tabs and click the right mouse button.

Configuring individual alarms

After selecting the required alarm on the right-hand side of the window, edit the details as required on the Alarm or Instruction tabs, and then save the alarm record.

Configuring alarms in bulk

Right-click below either the Alarm tab or the Instruction tab, and then select the Bulk Modification… command to use Bulk Modification mode.

Bulk Modification mode enables you to select multiple alarms on the right-hand side of the window and then change attributes across all of the selected alarms (for example, to assign a particular facility to all of the alarms from a particular DVR).

To exit from Bulk Modification mode, either save the alarm from to save any changes, or use the right-click shortcut a second time to toggle the form to its normal state.

Configuring Challenger control panels

Note: Before saving a new record for a Challenger control panel with existing users, remove the MASTER badge group to avoid overwriting user 50 in the Challenger control panel.

The process of setting up a Challenger control panel in Security Commander is simplified when the Challenger control panel has previously been set up. In this case, all that’s required is to define the Challenger control panel record in Security Commander, connect to the panel, set it online, and upload (retrieve) the panel’s database for editing in Security Commander.

The uploaded database populates or updates the default values in the Security Commander database, except for:

- User records
- Facility assignment
- Device descriptions

This process is described in the *Security Commander Installation Manual*.

In cases where a new Challenger control panel is being set up, it is useful to know the most efficient sequence for programming and where in Security Commander various steps are performed. Refer to “Chapter 4 Common tasks” in the appropriate *Challenger Programming Manual* for details of standard and advanced alarm system programming.

Configuring DVRs and cameras

Refer to the *Security Commander CCTV Interface Guide* (REV 3 or later) and the *Security Commander Help* for details.

Note: This option is not available in Security Commander Lite.

Access rights, persons, and badges

A user (person with a badge) may gain access to areas, doors, or floors protected by the security system.

Security Commander uses a number of concepts to control access rights, persons, and badges. This chapter describes these concepts.

Access rights

The process of controlling access begins with the three *access groups* — alarm groups, door groups, and floor groups — which define the relationship of alarms, devices (such as readers), and time zones to a Challenger control panel.

For example, a department manager would require a particular set of access rights for managers, and these could be assigned to him in his person record.

A Person Profile is an optional means of quickly applying a standard set of access groups to new person records (see “Person” on page 56).

Alarm groups

Alarm groups provide the means to control the system intrusion alarm functions (also called alarm control). Alarm groups have areas and time zones, menu options, and panel options.

Alarm groups are assigned to persons (optionally via person profiles), and to each door or RAS to perform functions. This provides flexibility when determining a person’s access to, and control of, the system.

Door groups

Door groups specify when access to a specific door or arming station will be granted. Door groups are assigned to persons (optionally via person profiles).

Each door group may have a different time period (time zone) when access to the door or arming station will be granted.

Floor groups

Floor groups specify when access to a specific floor will be granted. Floor groups are assigned to persons (optionally via person profiles).

Each floor group may have a different time period (time zone) when access to the door will be granted.

Person profile

The Person Profile defines a set of access rights for a category of person (such as “Office Staff”), which share a set of access rights. Access rights are determined by:

- Alarm Groups determine the areas, Challenger control panel commands, and menu options that can be used by the person.

- Door Groups determine the doors (readers) that can be accessed by the person, and within which times.
- Floor Groups determine the floors that can be accessed from a lift by the person, and within which times.

A Person Profile is an optional means of quickly applying a standard set of access groups to new person records (see “Person” below).

Person

The Person form is used to enter a person record into Security Commander, assign access rights (optionally by importing a defined Person Profile), and to manage PINs and badges that will be used with the person record.

You will enter information such as the name and address, assign access rights, assign a department or user fields and even capture a photo.

Access rights are assigned via the Person form’s Personnel tab, Alarm groups tab, Door groups tab, or Floor groups tab. Optionally use the right-click command “Import Profile” on any of these tabs to apply a Person Profile’s settings to the Person record.

Badges

On the Personnel menu, click Badge to define badge records.

A badge has a unique identity number. This is either a badge number and site code for known formats, or a 48-bit number (called Raw Card Data). In Security Commander, the term ‘badge’ also applies to a PIN (personal identification number) that is entered on a RAS keypad.

When a badge is assigned to a person, and it belongs to a badge group that is indicated for download to a Challenger control panel, the badge will be downloaded (sent) as a user to the Challenger control panel (and any associated Intelligent Access Controllers), as long as the badge is ‘active’. As a result of this association between badges and Challenger control panels, certain conditions control how users can be added to any system. These are:

- Each person-badge combination is represented by a ‘user number’ at the Challenger control panel.
- Challenger10 and ChallengerSE control panels support 2,000 IUM users (with name and PIN). The optional memory expansion module increases the capacity to 65,535 IUM users.
- ChallengerLE control panels support 100 IUM users (with name and PIN) and cannot be expanded.
- Challenger V8 user numbers greater than 50 require a memory expansion module.
- Challenger V8 user numbers above 11,466 require an IUM (Intelligent User Memory) memory expansion module.

- In a Challenger V8 system with 1 MB expanded memory, only user numbers in the range 1 to 1000 (out of a total 11,466 users) can have PIN codes. In a system with 1 MB expanded memory and software IUM, then user numbers in the range 1 to 2000 (out of a total 2000 users) can have PIN codes.
- In a Challenger V8 system with 1 MB, 4 MB, or 8 MB expanded memory, only the first 200 user numbers can have their names programmed to their user number in the Challenger control panel (although in Security Commander all users can have names).

For more information see “Challenger control panel memory” on page 59.

Every new Challenger control panel that you create will have default badge groups listed according to the default types* selection that was made when the Security Commander database was created.

* Each default type corresponds to a set of default hardware settings to provide for regional differences between Challenger control panels.

Badge groups

On the Personnel menu, click Badge Group to define badge groups. See “Badge groups” on page 4 for introductory information.

Badge groups tell the Security Commander system which badges need to be downloaded to which Challenger control panels.

The Challenger Badge Groups Setup Form has three fields that use the term “default”, but mean different things. These fields are:

- **Default panel type**. If creating a new badge group, select either “All panel types”, or “Australian” to have the badge group available when you create a new Challenger control panel (Challenger Setup Form, Badge groups tab).
- **Use as default badge group**. Select the “Use as a default badge group” check box if you want new badge records to be automatically populated with this badge group (and a site code if specified).
- **Default site code**. Enter a default site code for the badge group. If this badge group is used as a default for new badge records, then new badges will automatically be populated with this site code.

Security Commander has badge groups to accommodate the following badge formats:

- Tecom ASP
- Hughs 34 bit
- Wiegand 26 bit
- Raw data
- PIN code
- ATS Wiegand 30 bit
- ATS Wiegand 32 bit
- Aritech Mag Stripe
- Wiegand 37 bit

- Hughs 35 bit
- HID C1000 35 bit
- Master Installer Type (depending on the languages selected when the database was created)

Note: See “Master badge group” below for information on MASTER Installers.

Master badge group

All new Security Commander Challenger control panel records are created with at least one ‘Master’ badge group. Master Installer type (assigned Badge No. 50) enables a new Challenger control panel to be programmed initially.

We recommend that the MASTER badge group is removed from the panel’s assigned badge groups as soon as it is not needed, for the following reasons:

- The master PINs may be used on the Challenger control panel, possibly resulting in unauthorised use.
- The existence of the master installer badge using badge number 50 can cause conflicts where an operator uses one of these badge numbers for a badge or PIN. If attempts were made to add the badge group to the panel, such a conflict could prevent all badges of the group from being downloaded to a Challenger control panel until it is resolved.

If you wish to have your own special Installer PINs, then you must create PIN-only records using the Badge Setup form. Assign badge number 50 to use the same locations in the Challenger control panel memory as previously used by the default badge groups.

Assigning badge groups

On the Challenger menu, click Setup to define a Challenger control panel. When a Challenger control panel is first defined, use the Badge Groups tab to define which badge groups are eligible* for downloading (sending) to the Challenger control panel.

* For a badge to be downloaded to a Challenger control panel, the following rules apply:
  - The Badge Group must be assigned to the Challenger control panel.
  - The Badge Group must be assigned to the badge.
  - The badge is assigned to a person.

Note: Remove all unneeded badge groups before saving the new Challenger control panel record in Security Commander. See “Master badge group” above for details.

Use the Badge Groups tab on the Controller Setup form to add or remove Badge groups that the Challenger control panel will use.

To edit the list, click Assign Badge Groups to display the Assignment dialog.

Select the required badge group in the Available list and move it to the Assigned list to add the badge group to the Challenger control panel.

Alternatively, select a badge group in the Assigned list and move it to the Available list to remove the badge group from the Challenger control panel.

When adding a Challenger control panel with the default badge groups, the default Master Installer will be downloaded to the Challenger control panel as users, along with any additional badges that have been assigned to the panel's default badge groups. To prevent this, remove the badge groups prior to saving the record.

Challenger control panel memory

The use of memory expansion modules governs the number of users available to Challenger control panels and Intelligent Access Controllers.

Challenger Series memory expansion

Memory expansion depends on the panel type:

- Challenger10 panels support 2,000 users. This capacity can be expanded to 65,535 users via a TS1084 Memory Expansion Module.
- ChallengerSE panels support 100 users. This capacity can be expanded to 2,000 users via a TS1082 User Expansion Licence or 65,535 users via a TS1084 Memory Expansion Module.
- ChallengerLE panels support 100 users and cannot be expanded.

Challenger V8 memory expansion

Standard Challenger V8 control panels without memory expansion support 50 users, but are not currently supported in Security Commander.

The following Challenger V8 memory configurations are supported in Security Commander:

- Large (1 MB expansion) supports 11,466 users.
- IUM mini (1 MB expansion, software IUM) supports 2,000 IUM users.
- IUM small (4 MB expansion, hardware IUM) supports 17,873 IUM users.
- IUM large (8 MB expansion, hardware IUM) supports 65,535 IUM users.

Badge records in Security Commander

In Security Commander the closest counterpart to Challenger control panel users are badges. In fact, a badge represents a collection of users across multiple Challenger control panels.

A badge will create a user record for a Challenger control panel under the following conditions:

- The badge is assigned to a person
- The badge belongs to a badge group that has associated Challenger control panels (users will only be created in those Challenger control panels)
- The badge is active

In Challenger V8 control panels without hardware IUM or software IUM, the badge number directly corresponds to the user number in the Challenger control panel (therefore, the user number refers to the physical badge number).

In Challenger control panels with hardware IUM or software IUM, the badge number may or may not correspond with the user number in the Challenger control panel (raw card data is used, not the badge number).

For these Challenger control panels, Security Commander applies the following rules:

- If a matching user number is available, the user number and badge number are the same.
- If a matching user number is not available, Security Commander selects the first available user number in the Challenger control panel starting from 1 and working up to the maximum permitted by the Challenger control panel's user memory.

Note: On the Reports menu, click Badge, and then select the "Badge to users" report type to identify the assignment between badges and user numbers on all applicable control panels.

Learning badge data

A badge's raw card data can be learnt into Security Command in two ways via the Badge Setup form, Badge definition tab:

- Click the "Auto" button, and then present the badge to a badge learn device to populate the "Raw badge data" field. The "Auto" button is enabled only when the badge format is "raw data". See "Using the Auto button" below.
- Present the badge to a badge learn device, and then click the "Learn" button to launch the Learn Badge Data form. The "Learn" button is enabled only when the badge format is "raw data". See "Using the Learn " on page 61 for details.

Using the Auto button

The Auto button automatically populates the badge's "Raw badge data" field from data received from a badge learn device.

To learn badge data via the Auto button:

1. Use the Badge learn tab on the Parameters form to specify the device(s) to be used for learning badges.
2. On the Badge Setup form, click the Auto button.
3. Present the badge to a badge learn device. When the badge learn process is complete, the badge data is displayed in the 'Raw badge data' field on the Badge Setup form.

Using the Learn button

The Learn Badge Data form is used to search the Security Commander history database for unknown badge data from one or all badge learn devices (card readers on either a Challenger system LAN or an Intelligent Access Controller local LAN). Badges that are known to the system do not need to be learned.

To learn badge data via the Learn button:

1. Use the Badge learn tab on the Parameters form to specify the device(s) to be used for learning badges.
2. On the Badge Setup form, click the Learn button to open the Learn Badge Data form.
3. On the Learn Badge Data form, click the Learn device arrow and select the required device, or use the default <ALL LEARN DEVICES> to search all learn devices available to the operator.
4. Click the Facility arrow and select a facility to limit the search. This field is active only when <ALL LEARN DEVICES> is selected.
5. Click the Time window arrow and select the required time and date settings (hardware date and time) for the search. Depending on the dates selected and the archive database settings on the Parameter form, you may need to select Include Archive database in search.
6. After specifying the search criteria, or accepting the default settings, click Find to perform the search. The label on the button changes to Refresh. If any search criteria is changed, click Refresh to update the badge data list
7. Select the required unknown badge data, and then click OK to learn the raw badge data into Security Commander. When the badge learn process is complete, the badge data is displayed in the ‘Raw badge data’ field on the Badge Setup form.

Detailed instructions are contained in the *Security Commander Help*.

Using time and attendance readers

There are two types of readers that may be used for time and attendance functionality (clocking on and off):

- There can be 16 RASs (readers or keypads) on the Intelligent Access Controller’s local LAN designated as “time attendance readers” (programmed in the Challenger Doors Setup Form > Reader options tab).
- TS0867 and TS0869 Intelligent Access Controllers can have four additional readers connected to the onboard Wiegand interfaces (marked “DOOR 1”, “DOOR 2” and so on).

Note: See also “Time and Attendance History” on page 77 for additional requirements.

Using RASs for time and attendance

If using card readers on the controller's local LAN, the functionality is determined by the RAS address. By default, there are eight Clock On readers and eight Clock Off readers on the local LAN, as listed in Table 3 below.

Table 3: Local LAN default RAS functionality

Door	Default Clock On Readers		Default Clock Off Readers	
1	1	5	9	13
2	2	6	10	14
3	3	7	11	15
4	4	8	12	16

Badging a card on a Clock On card reader automatically clocks you on. Badging a card on a Clock Off card reader automatically clocks you off.

Using an LCD RAS

When used as a time and attendance reader, the LCD RAS will display the time and date similar to the following:

```
8:59   03/02/14
Clock On _
```

Users can clock on and off using two methods, described as follows.

Method 1: Clock On

To clock on, key in the user PIN and press On. The current time and date will appear for about a second before this screen appears:

```
Access granted
Clocked on
```

Method 1: Clock Off

To clock off, key in the user PIN and press Off. The current time and date will appear for about a second before this screen appears:

```
Access granted
Clocked off
```

Method 2 (LCD keypad only): Clock On

To clock on, first press * to toggle the state so that Clock On is displayed, then key in the user PIN and press Enter.

```
8:59   03/02/14
Clock On _
```

Method 2 (LCD keypad only): Clock Off

To clock off, first press * to toggle the state so that Clock Off is displayed, then key in the user PIN and press Enter.

```
8:59   03/02/14
Clock Off _
```

Using Wiegand readers for time and attendance

The four onboard Wiegand interfaces are considered as IN readers for the four doors or lifts, unless they are assigned the same lock relay.

If two Wiegand interfaces (for example, “DOOR 1” and “DOOR 2”) use the same lock relay, then the one with the lower door number is the Clock On reader and the one with the higher door number is the Clock Off reader.

Controlling operations

This chapter deals with the tasks associated with the Security Commander Operations menu.

Refer to the *Security Commander Help* for more details about these options.

Some options have corresponding toolbar buttons — these are indicated below the heading (as applicable).

Managing Challenger control panels

Controller utility

The Controller Utility allows you to monitor Challenger control panel state and issue commands to one or more selected Challenger control panels using either Controller Utility toolbar or right-click shortcut. In the following list, commands are available from both the toolbar and right-click shortcut except where noted.

The Controller Utility form provides commands for devices. Not all commands may be available for particular devices. Possible commands are:

- Edit: Edit the properties of the selected Challenger control panel using the Controller Setup form.
- New: Define a new Challenger control panel using the Controller Setup form.
- Change state: Set the selected offline Challenger control panel online, or set the selected online Challenger control panel offline.
- Dial / Hang-up: Enabled only when the selected intrusion Challenger control panels are dial-up type, and have the same connection status (for example, currently connected). A dial or hang-up command applies to all selected Challenger control panels.
- Download >Badges Database: Send the badges database to the selected Challenger control panels.
- Download > Installer Database: Send the installer database to the selected Challenger control panels.
- Download >Full Database: Send both the badges and installer databases to the selected Challenger control panels.
- Upload > Installer Database: Receive the installer database from the selected Challenger control panels.
- Upload > Door / Floor Groups, Holiday Database (right-click shortcut): Receive the door groups, floor groups, and holiday database from the selected Challenger control panels.

- Upload > Full Database: Receive the installer database and the door/floor groups, and holiday database from the selected Challenger control panels.

  Note: Uploading of the badges database is not supported in the current release of Security Commander. However, if a PIN has been changed on a keypad for an existing badge in the database, the new PIN is uploaded, the related badge details updated and propagated to all panels in the network.
- Accept Events (right-click shortcut): The default setting is enabled, where the Accept Events menu item is marked with a tick and events sent by the Challenger control panel are received by Security Commander. The Challenger control panel may still be connected but events are not processed by Security Commander. See “Accepting events” below for details.
- Queue Outgoing (right-click shortcut): The default setting is disabled, and commands are transmitted from Security Commander to the Challenger control panel. When selected, a tick appears next to the Queue Outgoing menu item. The Challenger control panel may still be connected but outgoing commands from Security Commander to the Challenger control panel are suspended and queued until the Queue Outgoing is set to disabled or cleared. See “Queuing outgoing events” below for details.
- Clear Message Queue (right-click shortcut): Clears the download buffer, which also includes configuration downloads and user downloads.
- Date and Time (right-click shortcut): Opens the Date and Time Control form for the selected Challenger control panels. Select multiple Challenger control panels to set the local date & time for all selected Challenger control panels simultaneously. This setting will be displayed on local RAS LCD displays and reported to management software.
- Remove Controller Panels (right-click shortcut): Hides the selected Challenger control panel(s) from the list. To restore, close and re-open the Controller Utility form.

Accepting events: Right-click the Controller Utility form to clear the Accept Events setting. Clearing this setting causes Security Commander to suppress receiving events from the Challenger control panel. Some reasons for suppressing events are:

- You might want to upload (receive) the full database from the Challenger control panel before accepting events. Doing so enables Security Commander to learn details of the alarms to be reported.
- An installer may need to connect to a Challenger control panel for maintenance without accepting events.

Queuing outgoing events: Right-click the Controller Utility form to select the Queue Outgoing setting. This setting causes Security Commander to suppress sending data to the Challenger control panel. Some reasons for queuing outgoing data are:

- Allow operators to make configuration changes without the changes being sent prematurely by Security Commander.

- Allow installers to make all necessary configuration changes, and apply those changes during times of low risk.

Monitoring badges

Badge Monitor

The Badge Monitor command opens the Badge Monitor form that allows the operator to monitor badge activity (according to the operator's facility assignment, see "Operator interface" on page 17).

In the following list, commands are available from both the toolbar and right-click shortcut except where noted.

Note: Some options are not available in Security Commander Lite.

The Badge Monitor commands are as follows:

- Resume: Starts the scrolling of badge activity. This command is active only if you pressed the Pause button. All badge activity that occurred while the Pause command was on will be displayed once you select resume.
- Pause: Suspends the scrolling of badge activity on the Badge Monitor.
- Clear: Clears all badge activity from the Badge Monitor.
- Badge... (right-click shortcut): Opens the Badge form.
- View Live Video (right-click shortcut): For a selected badge transaction with a camera icon displayed, use this shortcut to automatically access live video from camera(s) associated with the door/RAS's badge transaction, as defined by its event trigger. This option is not available in Security Commander Lite.

  Note: The DVR must be online and in record mode.
- View Recorded Video (right-click shortcut): For a selected badge transaction with a camera icon displayed, use this shortcut to automatically playback recorded video from camera(s) associated with the reader's badge transaction, as defined by its event trigger. This option is not available in Security Commander Lite.

  Note: The DVR must be online and not in error condition or serving another request for playback of recorded video.
- Quick Launch (right-click shortcut): For a selected badge transaction with a camera icon displayed, use this shortcut to automatically access live video and playback recorded video from camera(s) associated with the door/RAS's badge transaction, as defined by its event trigger. This option is not available in Security Commander Lite.
- Swipe & Show: Shows additional details on badge transactions for assigned Swipe & Show readers. Details include person last & first name, profile, region, picture (when available) and badge history. If a valid event trigger is set, live camera images will show next to the Swipe and Show form.

- Assign Swipe & Show Readers: Identifies for which readers Swipe & Show data should automatically be shown.

Notes

- The DVR must be online and not in error condition or serving another request for playback of recorded video.
- A badge activity must have a DVR association in order to enable video options on the right-click menu. Camera and door/arming station association (linking) is accomplished using the menu Administration > Event Trigger.

Monitoring alarms

Alarm Monitor

The Alarm Monitor displays alarm (input) activity. An alarm is displayed on the Alarm Monitor if the Monitor field was selected in the Alarm form.

All acknowledgments are recorded in both Operator and the Alarm History. In addition, all responses are recorded when the alarm is acknowledged.

There are three sections to this form:

- The top section or pane lists the alarms.
- The second pane lists any alarm instructions assigned to the current (highlighted) alarm.
- The third pane allows you to respond to an alarm by either selecting a predefined response or entering your own.

In the following list, commands are available from both the toolbar and right-click shortcut except where noted.

Note: Some options are not available in Security Commander Lite.

The Alarm Monitor commands are as follows:

- Remove All (toolbar): Remove all alarms on the Alarm Monitor regardless of whether the alarms are acknowledged or unacknowledged as long as it was not defined on the Alarm form as requiring an acknowledgment. An operator must have an ALL permission for the Alarm Monitor in order to have access to this icon.
- Remove Individual (toolbar): Remove one or more alarms without waiting for them to reset. The alarms can be unacknowledged and cleared as long as it was not defined on the Alarm form as requiring an acknowledgment.
- Show Inactive Alarms (right-click shortcut): For tracking purposes, you may select Show Inactive Alarms to display previously acknowledged alarm states that have not yet been removed from the display.
- Alarm: Right-click shortcut to the Alarm form.

- Alarm Graphics Viewer: Right-click shortcut to the Alarm Graphics Viewer form. This option is not available in Security Commander Lite.
- Alarm Graphics Editor: Right-click shortcut to the Alarm Graphics Editor form. This option is not available in Security Commander Lite.
- View Live Video (right-click shortcut): For a selected alarm transaction with a camera icon displayed, use this shortcut to automatically access live video from camera(s) associated with the alarm's transaction, as defined by its event trigger. This option is not available in Security Commander Lite.

  Note: The DVR must be online and in record mode.
- View Recorded Video (right-click shortcut): For a selected alarm transaction with a camera icon displayed, use this shortcut to automatically playback recorded video from cameras associated with the alarm's transaction, as defined by its event trigger. This option is not available in Security Commander Lite.

  Note: The DVR must be online and not in error condition. For DVR range it may not be serving another request for playback of the recorded video.
- Quick Launch (right-click shortcut): For a selected alarm transaction with a camera icon displayed, use this shortcut to automatically access live video and playback recorded video from cameras associated with the alarm's transaction, as defined by its event trigger. This option is not available in Security Commander Lite.

  Notes

  - The DVR must be online and not in error condition. For DVR range it may not be serving another request for playback of the recorded video.
  - An alarm activity must have a DVR association in order to enable video options on the right-click menu.

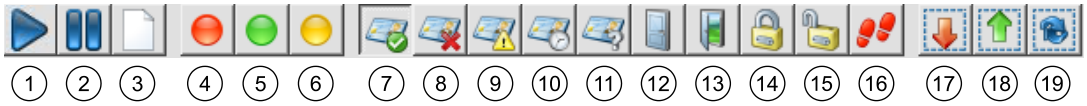
Combined monitoring

Live History Log

The Live History Log allows the operator to monitor various types of events, subject to the operator's facility assignment, and based on the selected filters.

Use the toolbar to select filters (the types of events to monitor) and to control the display of events in the window. In the image below, only the Valid badge button (item 7) is shown as selected.

Figure 11: Live History Log toolbar



1. Resume: Starts the scrolling of events. This command is active only if you have selected Pause. All events that occurred during pause will be displayed once you select resume.
2. Pause: Suspends the scrolling of events on the Live History Log.
3. Clear: Clears all events from the Live History Log.
4. Active: Show alarms.
5. Inactive: Show alarm resets.
6. Trouble: Show fault events.
7. Valid: Show valid badge transactions.
8. Invalid: Show invalid badge transactions.
9. Lost: Show lost badge transactions.
10. Overdue: Show overdue (expired) badge transactions.
11. Unknown: Show unknown badge transactions.
12. Close: Show door close commands.
13. Open: Show door open commands.
14. Lock: Show door lock commands.
15. Unlock: Show door unlock commands.
16. Trace: Show traced user events.
17. Select all: Show all events.
18. Deselect all: Show no events.
19. Refresh: Update window.

Right-click functions depend on the type of the selected event. For alarms, please refer to the “Alarm Monitor” on page 67. For badges, see “Badge Monitor” on page 66.

Creating and using alarm maps

Alarm Graphics Editor

Note: This option is not available in Security Commander Lite.

The Alarm Graphics Editor allows an authorised technician to create a map (graphical view) of alarm states for the alarms you select, and to create links to other maps.

For example, the operator might start off with a facilities map with an alarm point on a building. If the alarm point has been defined as a jump to the building's map, clicking the icon will display the building map, and so on. Jump points to other maps do not need to be linked to an alarm.

A map has a background image, which can be a bitmap, a vector drawing, or a combination of both bitmaps and vector drawings, saved in Windows Metafile (.WMF), Enhanced Metafile (.EMF), Joint Photographic Experts Group (.JPG), or Bitmap (.BMP) format.

Applications such as Microsoft Visio, Microsoft PowerPoint, CorelDraw, Adobe Illustrator, and many other drawing applications can save images in any of these formats. The same background image file may be used to create a number of different map files by using different views and different magnifications of the background, with different alarm, camera, and jump points superimposed.

Alarm Graphics Viewer

Note: This option is not available in Security Commander Lite.

The Alarm Graphics Viewer command opens the Alarm Graphics Viewer that allows the operator to view maps created in Alarm Graphics Editor. These maps indicate the location and type of incoming alarms.

Use the Alarm Graphics Viewer to select and display an alarm graphics map. Maps can contain icons that represent the physical locations of one or more devices such as doors or cameras. The icons can change appearance to indicate conditions of trouble, alarm, or reset.

An icon may be linked with another map (for example, to display a room within a building). Click a linked icon to view the other map.

Managing clients

Note: This option is not available in Security Commander Lite.

See "Managing network client computers" on page 72 for details about this topic.

Managing Challenger devices

On the Operations menu, click Device Control & Status (or press Alt+F8) to control a connected Challenger control panel's areas, RASs, lifts, doors, inputs, DGPs, and relays, and to retrieve their states.

Refer to *Security Commander Help* for detailed instructions about each device.

Note: Your ability to see and control devices may be restricted by your assigned operator facilities.

Use the Area, RAS, Lift, Door, Input, DGP, and Relay tab pages to select and control devices in the following manner:

- Select an item in the list, and then click the "Get Status" button to retrieve the current state from a connected Challenger control panel.

- If you want to send control commands to the panel, you can click the Purpose "..." button to select a predefined purpose/response, or you can type in the Purpose text box to describe the reason for the command. These comments are written to the operator history file and appear in the purpose field of the Operator History report.
- Use the “Set state to” buttons to send commands to the control panel for the selected items.
- After you send a command, click the “Get Status/Refresh” button to see the new state.

Managing digital video

Note: This option is not available in Security Commander Lite.

Video Console

On the Operations menu, click Video Console (or press Alt+F9) to open a video command and control application that allows you to monitor digital video recorders and their associated cameras, control live video, as well as search and play back recorded video events.

Changing your password

The Change Password menu opens the Change Password form which allows you to change your password.

Selecting facilities

The Select Facilities command opens the Set Active Facilities form which allows you to change the facilities currently in use.

Camera footage on alarm

Note: This option is not available in Security Commander Lite.

On the Operations menu, click “Camera footage on alarm” to automatically display camera footage on alarm, if a corresponding trigger is defined. The video window will be displayed until an operator will close it manually. In case the camera window is displayed and new alarm occurs, the video will be switched only if the priority of the new alarm is higher.

Show map on alarm

Note: This option is not available in Security Commander Lite.

On the Operations menu, click “Show map on alarm” to automatically display the map that has objects with the alarm assigned.

Managing network client computers

Note: Client computers are not available in Security Commander Lite.

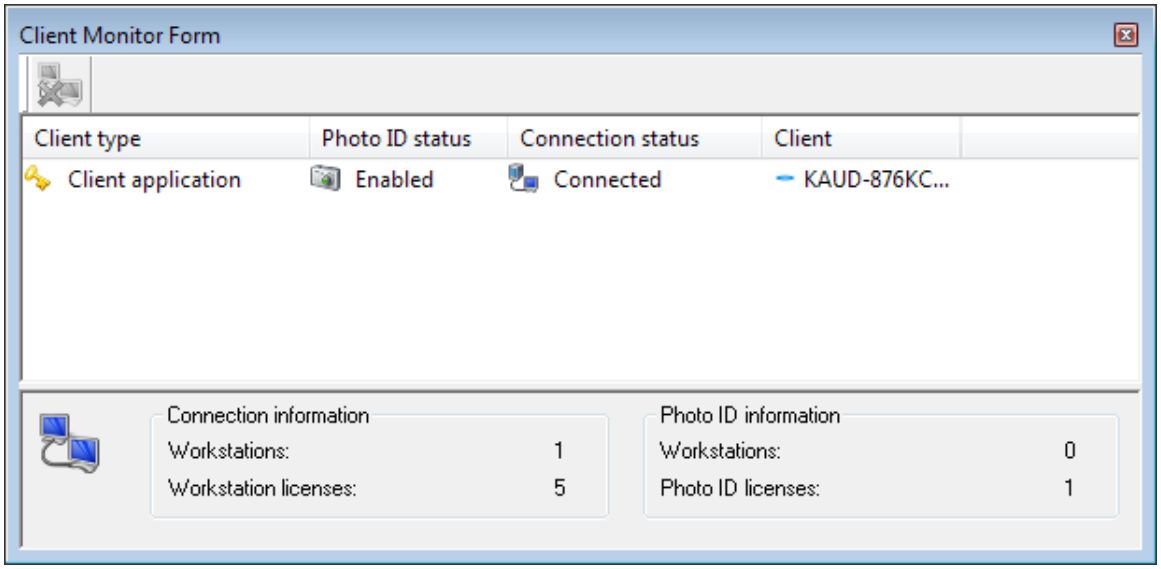
In order for your networked clients to connect to the server computer, the server computer must know who they are. You may refer to the Client Monitor form to obtain client type, Photo ID status, and connection status. You may use the Client form to add, modify, and remove computers from the network.

Client Monitor form

Note: This option is not available in Security Commander Lite.

On the Operations menu, click Client Monitor to open the Client Monitor form (or click the toolbar button displayed above).

Figure 12: Client Monitor form



The top of the Client Monitor form displays all currently defined network clients, their Photo ID status, and their connection status.

The Photo ID status is either Enabled or Disabled. If enabled, this client counts as taking a Photo ID license. You cannot enable Photo ID on more network clients than you have Photo ID licenses. The Photo ID license allows you to capture images and signatures, create badge designs, and print badges. Without a license, you cannot create badge designs and print badges.

The connection status is either Connected or Disconnected. If the network client is disconnected, it is not added to the number of active licenses; the number of active licenses is only increased if the client is connected. To connect the client, log in on that computer. An application running on the Server computer counts the licenses used.

The bottom of the Client Monitor form displays the number of licenses currently in use along with the total number of licenses allowed.

In the following list, commands are available from both the toolbar and right-click shortcut except where noted.

The Client Monitor commands are as follows:

- Disconnect Client: Disconnects the selected client.
- Client form: Right-click shortcut to the Client form to, for example, enable or disable Photo ID for the particular Security Commander client.

Client form

Note: This option is not available in Security Commander Lite.

On the Administration menu, click Client to define a client computer.

Adding clients

You can add clients that are already set up on the network. When you click the Browse button, you receive a view of all computers that Security Commander can find on your network. Select the ones you wish to use.

You can add as many clients as you want. However, only the licensed maximum can connect to the server at the same time. For specific features of the Client form, refer to the *Security Commander Help*.

Modifying/removing clients

To remove a client from the network, it must be disconnected. This can be done by having that client exit, or by selecting the client on the Client Monitor form and clicking Disconnect on the toolbar, or selecting Disconnect from the shortcut menu of the Client Monitor form. You MUST have a permission action of All, which is set on the Permission form, in order to disconnect clients.

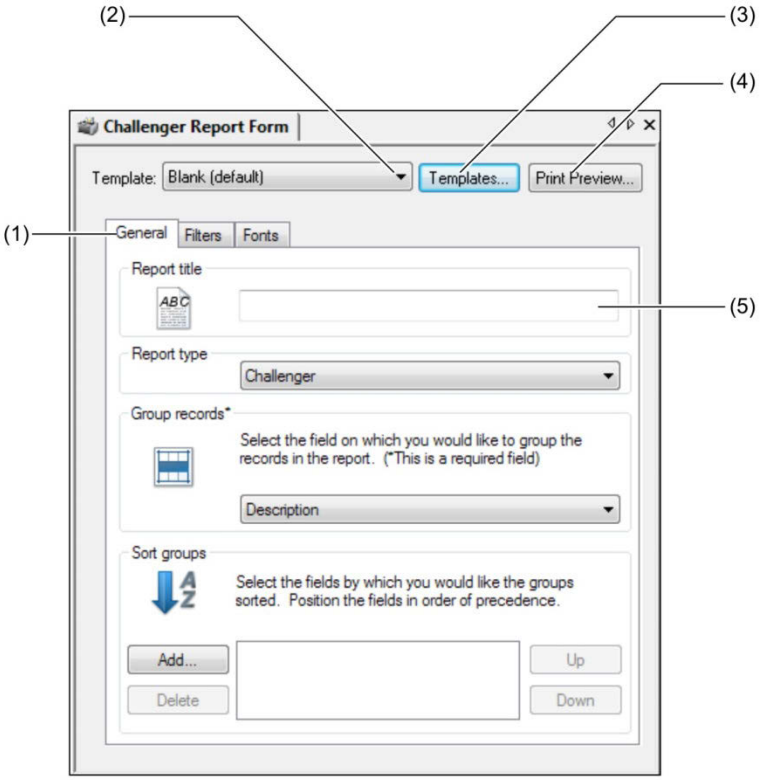
You can enable or disable Photo ID on a client without disconnecting it. You may have more Photo ID stations set up than you have licenses. However, if not all the clients require the license at the same time, you can enable and disable the license for the appropriate clients.

Reports and templates

This chapter discusses reports and templates for the reports. Security Commander provides extensive reporting capabilities based on your system configuration. All reports are selections of the Reports menu.

Reports use a number of common elements, as shown in Figure 13 below.

Figure 13: Challenger Report form (example)



(1) Tabs for defining the report

(2) Template field displays currently selected template (optional). To select a template, click the Template arrow and then select the required template from the list of templates that have been created for this report type.

(3) Click the Templates... button to rename, save, delete a template, or to make a selected template the default for the report type

(4) Click the Print Preview... button to preview a report before printing it. Same as “Print Preview Report” on page 79.

(5) Type the title to be printed at the start of the report.

For complete details of fields and capabilities of each Report, refer to the *Security Commander Help*.

Notes:

- Reports are filtered so that supplied information pertains only to the selected facilities of the current user.
- Be careful when selecting font styles and sizes. Some styles may not appear as desired when printed and some sizes may be too large for the page. Use the Print Preview command to check how the font style and size will print on a page.

Standard reports

Person

On the Reports menu, click Person to create a report on some or all persons in the database. Reports may include personal information, such as address, department, badge, access rights, and user fields of persons in the system. Also provides information for reports regarding badges assigned and regions.

Badge

On the Reports menu, click Badge to create a report on some or all badges in the system. Includes a report to relate Security Commander badges to Challenger users.

Persons in Regions

On the Reports menu, click Persons in Regions to create a report on the persons that currently are in particular regions.

Persons in Door Groups

On the Reports menu, click Persons in Door Groups to create a report on the persons assigned to selected Door Groups.

Persons in Floor Groups

On the Reports menu, click Persons in Floor Groups to create a report on the persons assigned to selected Floor Groups.

Persons in Alarm Groups

On the Reports menu, click Persons in Alarm Groups to create a report on the persons assigned to selected Alarm Groups.

Administration

On the Reports menu, click Administration to create a report on the administrative aspects of the program. Report types include alarm instruction, archive, client, facility, host parameter, operators, permission, and response.

Generates reports about the administrative options of the system. Report types include alarm instruction, archive, client, facility, host parameter, operators, permission, and response.

Challenger

On the Reports menu, click Challenger to create a report on the Challenger control panel devices in the system.

Floor Access

On the Reports menu, click Floor Access to create a report on the floors defined in the system and the access granted to each one.

Door Access

On the Reports menu, click Door Access to create a report on the persons in the system that has access to any of the specified doors or readers.

Area Access

On the Reports menu, click Area Access to create a report on persons' levels of control over areas (the ability to secure, disarm and/or reset), listed by areas and by last name. A person’s level of control is determined by the options selected in the alarm groups assigned to the person.

Challenger Groups

On the Reports menu, click Challenger Groups to create a report about the door groups or floor groups in the system, for a selected Challenger control panel or for all Challenger control panels.

Roll Call

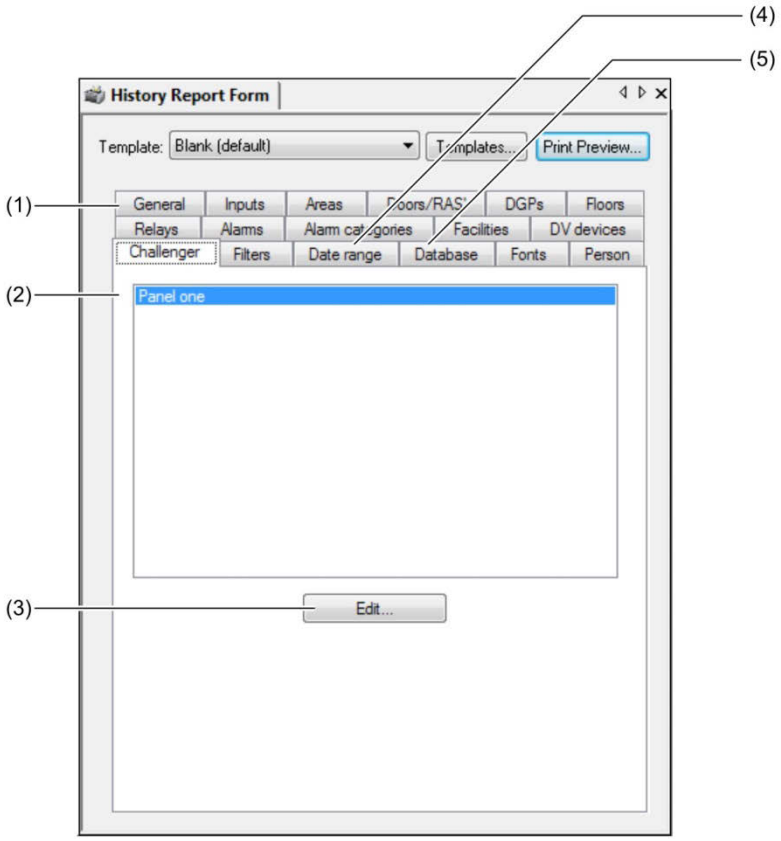
On the Reports menu, click Roll Call to create a report on the people who last entered one of the specified readers. The report provides a list of the last access granted to any or all persons in the system and each of their badges; that is, who last went where.

History reports

History

On the Reports menu, click History to create a report on events reported to Security Commander.

Figure 14: History Report form (example)



(1) Tabs for defining the report. Use General, Filters, and Fonts tabs as per standard reports. Use other tabs to further define (limit) the events to be included in the report.

(2) Example of limiting the report to events related to specific Challenger panel(s). Other commonly used tabs are Person and Doors/RASs.

(3) Click the Edit... button to open the assignment dialogue box. Use the assignment dialogue box to add or remove items from the tab.

(4) Specify a date and time range on which to report. Refer to *Security Commander help* for details of using this tab.

(5) By default both history and archive databases are used in history reports. The history database contains only records for the past day, week, or month as specified in “Archive Database” on page 41 (the default archive period is daily). All others are contained in the Archive database until cleared.

Badge History

On the Reports menu, click Badge History to create a report on the history of badge transactions.

Time and Attendance History

Note: This option is not available in Security Commander Lite.

On the Reports menu, click Time and Attendance History to create a report on the history of time and attendance activity.

The use of time and attendance transactions in producing meaningful reports depends on the following:

- An Intelligent Access Controller must be used for time and attendance transactions.
- Doors reporting time and attendance transactions must have Time Attendance Reader selected on the Challenger Doors Setup form > Reader Options tab.
- Doors reporting time and attendance transactions must have their clock on reader set to an IN reader address; and their clock off reader set to an OUT reader address.
- Readers or keypads designated for time and attendance transactions must be used for entry to and exit from the workplace, and no other purpose (for example, accessing other parts of the workplace during work time).
- Badges or PIN codes used for time and attendance transactions must be used by only one person (however, a person may have multiple badges or PIN codes).
- A time interval beginning with an IN transaction is deemed to be “on site”.
- A time interval beginning with an OUT transaction is deemed to be “off site”.
- The difference between an IN transaction and the next following OUT transaction is deemed to be “work time”.
- Time and attendance transactions are records of badge or PIN use at specified readers. Such transactions are not necessarily records of work or absence from work by a person.

Note: See “Using time and attendance readers” on page 61 for details.

Operator History

On the Reports menu, click Operator History to create a report on the history of operator activity.

External Reports

Note: This option is not available in Security Commander Lite.

On the Reports menu, click External Reports to access an executable program or report that was not created within Security Commander. Navigate to the program or folder, select the file, and click Open.

For example, you may wish to access a report created by a third party report generator such as Crystal Reports or Microsoft Access. Refer to “Using Microsoft Access 20” on page 80 for instructions to create a project, connect with Security Commander, and create reports.

Templates

Templates are not required to run reports: they are only a tool to help you save time and to produce consistent results. If you don't need to use a template, select "Blank (default)" as the template.

Security Commander provides templates that allow you to enter report parameters. These can be saved and then recalled to run a report.

When you select a specific Report from the Security Commander menu, a Template list box displays the name of the currently loaded template, if there is one. To select a template, click on the arrow at the right end of the field, which displays a list of the available templates. Select the desired template and it will be loaded.

Report templates are useful when a certain report will be run frequently. Once the desired report is configured, it can be saved as a template and revised by loading it from the template combo box.

If a date or time is specified, the date and time selections are saved as part of the template. You may need to change these areas each time you run the report. Verify that the template reflects the appropriate information and update as necessary.

Print Preview Report

On the File menu, click Print Preview Report to preview a report before printing it. Alternatively, click the Print Preview… button on the report form (Figure 13 on page 74, item 4).

A printer must set up in Windows and added to your system in order for this feature to work.

Print Report

On the File menu, click Print Report to send the current report to the currently defined printer.

Using Microsoft Access 2010

Note: This section is used with the External Reports option. It is not available in Security Commander Lite.

This section details the advanced procedures for creating database projects in Microsoft Access 2010 (Microsoft Access) and connecting to Security Commander databases.

The use of Microsoft Access is not required for using Security Commander, it is only necessary to perform further maintenance on the databases or to create custom reports.

A user named "exreport" with a default password "exreport" exists by default for use with the External Reports option. The "exreport" user has read-only permissions to the databases. We recommend that you use the Database Maintenance application to change the default password (see "Changing the "exreport" password" on page 110).

Creating Microsoft Access projects

You will need to create a project for each of the three Security Commander databases:

- Alliance8300
- Alliance8300Archive
- Alliance8300History

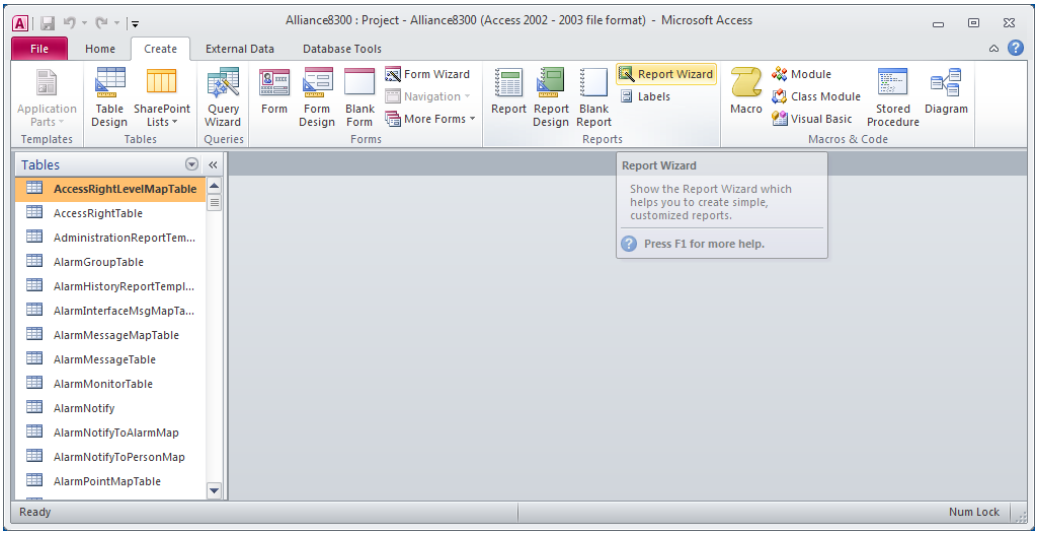
Begin by creating the Alliance8300 project and storing the project in the Security Commander Database folder.

To create a new Alliance8300 project:

1. In Access, select File > New. The Getting Started with Microsoft Office Access window opens.
2. Click the folder icon at the right-hand side of the File Name field. The File New Database dialogue box opens.
3. Navigate to Security Commander database location (for example, C:\Program Files (x86)\UTC Fire & Security\Security Commander\Database).
4. Click the "Save as type" arrow, and then select Microsoft Office Access Projects (*.adp).
5. Name the file, for example, "Alliance8300.adp", and then click OK.
6. In the Getting Started with Microsoft Office Access window, click the Create button. When asked "Do you want to connect to an existing SQL Server database?", click Yes. The Data Link Properties dialogue box opens.
7. Click the "Select or enter a server name" arrow, and then click the name of the computer where the Security Commander database is located.

8. Click to populate the “Use a specific user name and password” radio button, and then type a valid user name and password combination (either the “sa” user or the “exreport” user will work).
9. Click to populate the “Select the database on the server” radio button, click the arrow, and then select the appropriate database (for example, “Alliance8300”).
10. Click the Test Connection button. The Test connection succeeded message displays (if not, go back and check the user name and password).
11. Click OK. The Alliance8300.adp project is created and a list of tables displays

Figure 15: Microsoft Access 2010 project and Report Wizard



Setting up Microsoft Access Reports

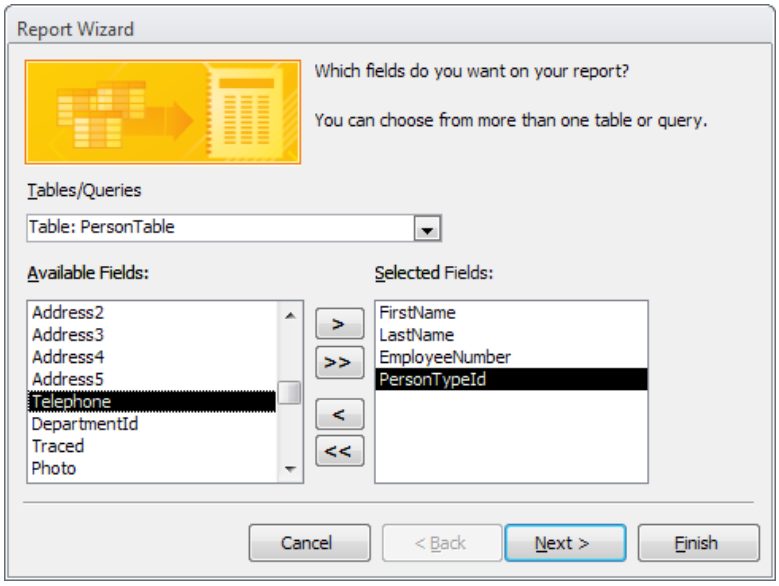
Note: Microsoft Access can be installed on the Security Commander Server computer and/or any Security Commander client computer.

Creating a Microsoft Access report

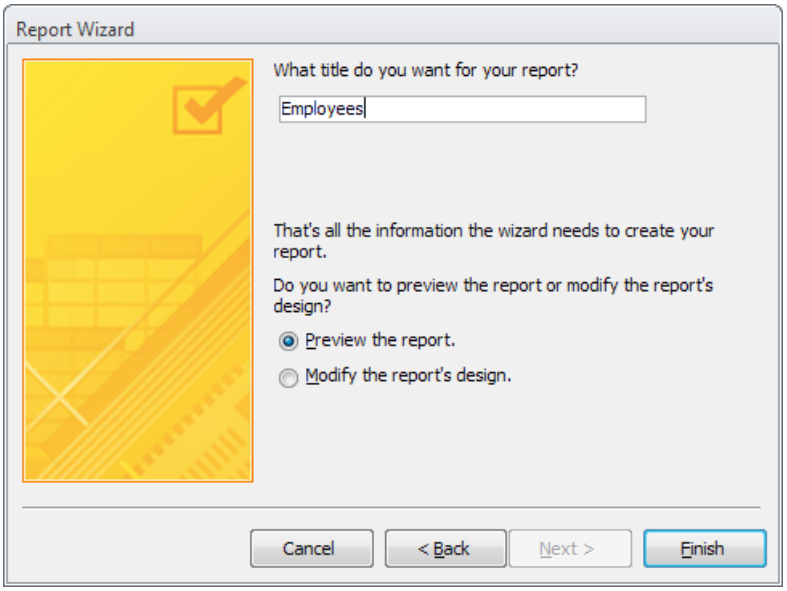
In this section, you will create a Microsoft Access report by using the Report Wizard, and then use drag-and-drop to automatically create a shortcut to the report for use by Security Commander.

To create and link a report to Security Commander:

1. In Access, click the Create tab, and then click Report Wizard (Figure 15 above).
2. Follow the Report Wizard prompts to define a report. In the following steps, we’ll create a sample personnel list.

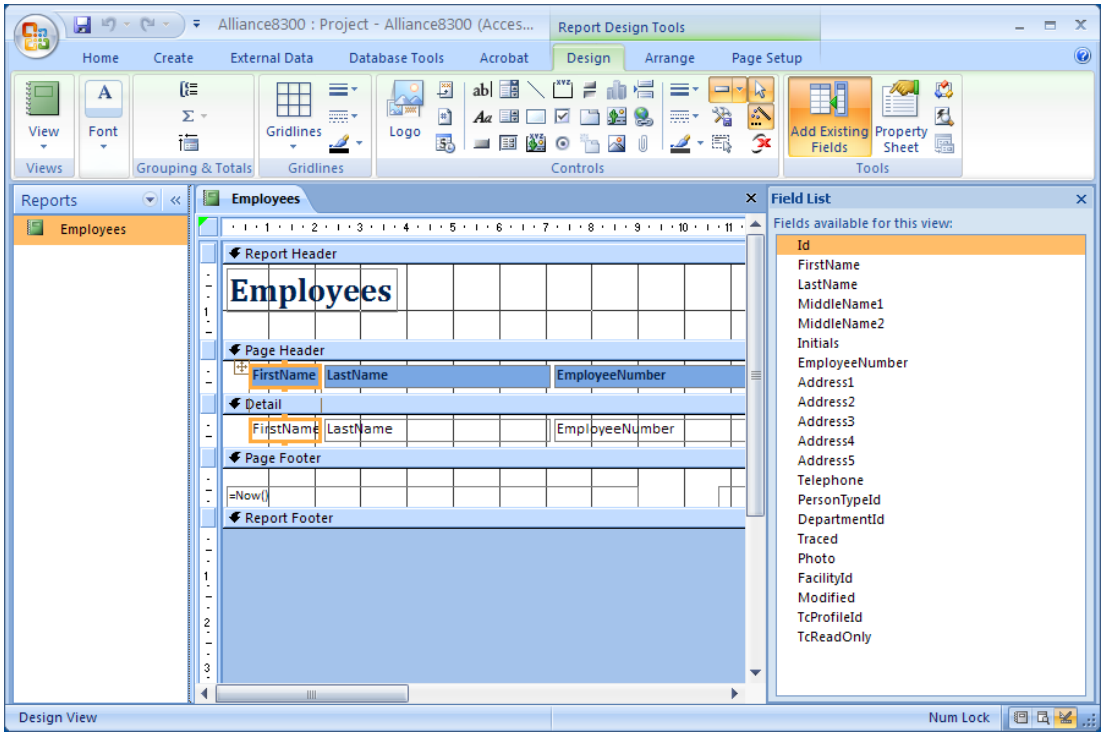


3. Click the Tables/Queries arrow and select a table from which you want data.
4. Select fields from the Available Fields list and then click the right-facing arrow > to populate the Selected Fields list. Selected fields will be used in the report.
5. Subsequent steps in the Report Wizard allow you to group and sort the report data, layout the report format, select from pre-defined styles, and give it a title.



6. Click Finish.

7. Use the print preview and design views, if needed, to further customize the report. The report is listed in the Reports list.

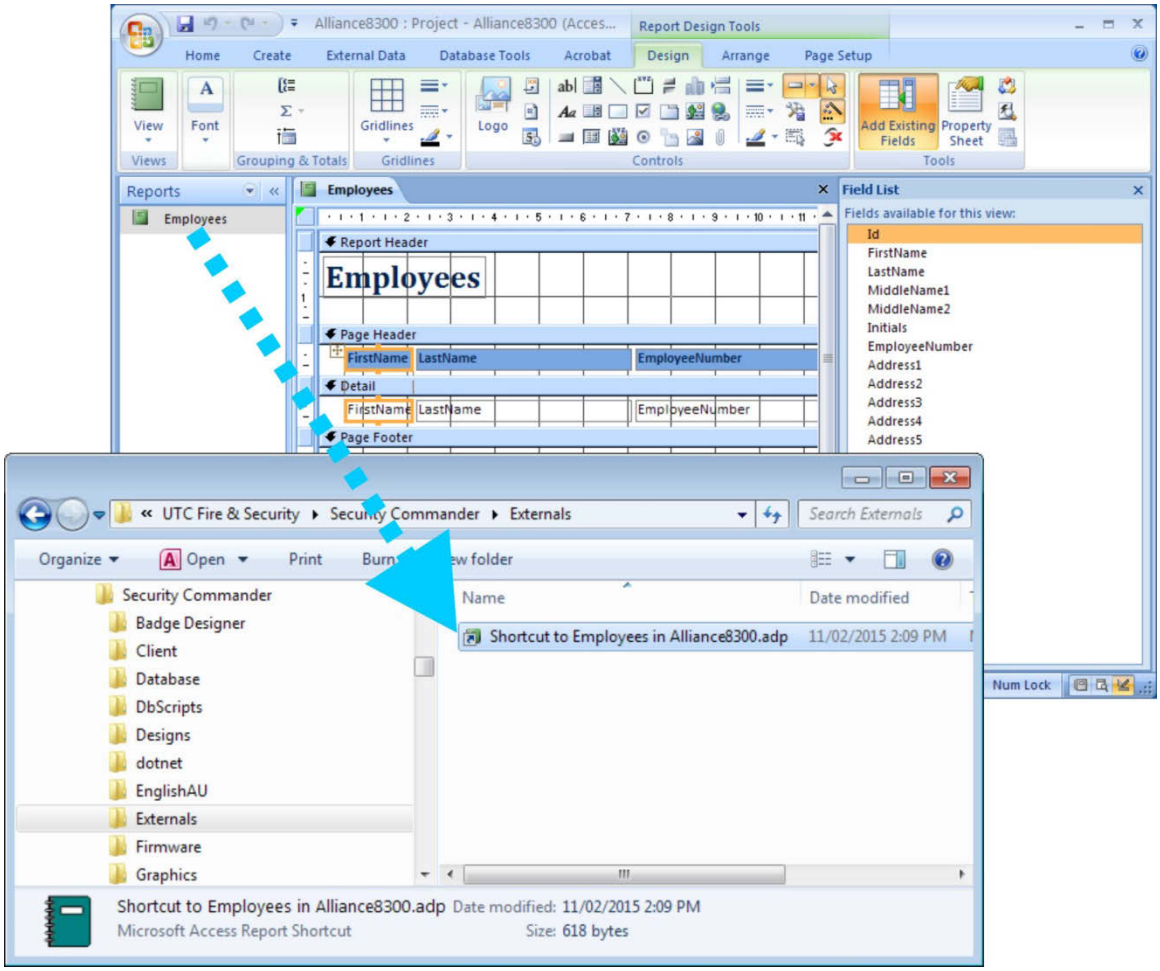


Do not close Access for now. You will use the Reports objects view in the next section (reduce the Access window size so that it does not occupy the entire Windows desktop).

Linking a Microsoft Access report to Security Commander

Security Commander has been designed to allow you to quickly add Microsoft Access reports to the External Reports command by means of Windows drag-and-drop functionality (see Figure 16 on page 84).

Figure 16: Drag-and-drop method of creating a shortcut



To automatically create a shortcut to the report for use by Security Commander:

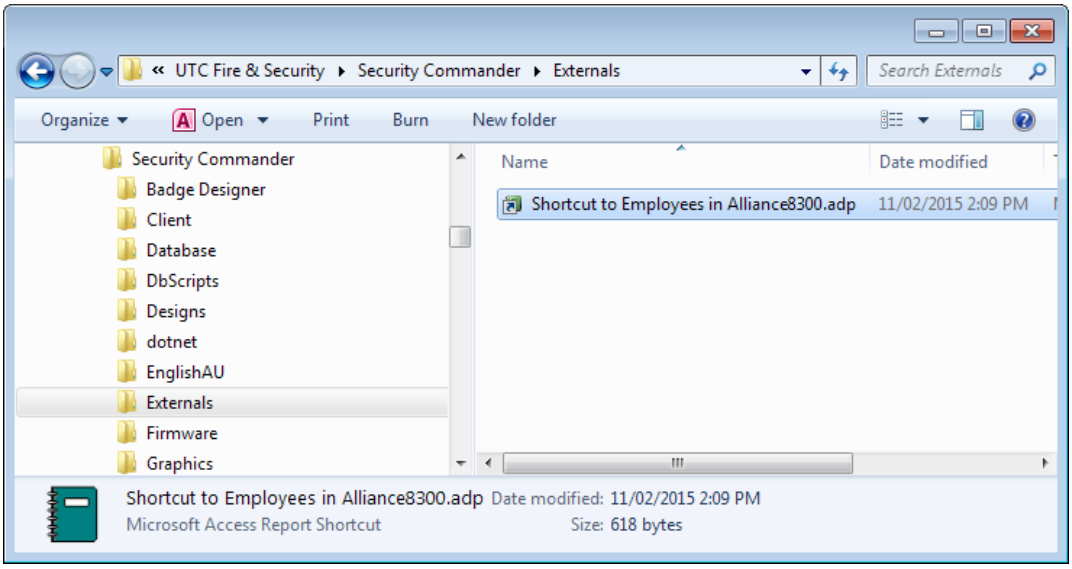
1. Open a Windows Explorer view of the Security Commander Externals folder on the server computer.

   Note: If you are creating the report from a client computer, navigate in Windows Explorer to the Server computer in Network Neighbourhood to display the Externals folder.

2. Position Windows Explorer and Microsoft Access on the Windows desktop so that both are visible.

3. Drag the report from the Microsoft Access project to the Security Commander Externals folder. See Figure 16 above.

Result: Windows automatically creates a shortcut to the Microsoft Access report “Employees”.



This shortcut is used in the Security Commander Reports > External Reports command (see “Launching External Reports from Security Commander” on page 86).

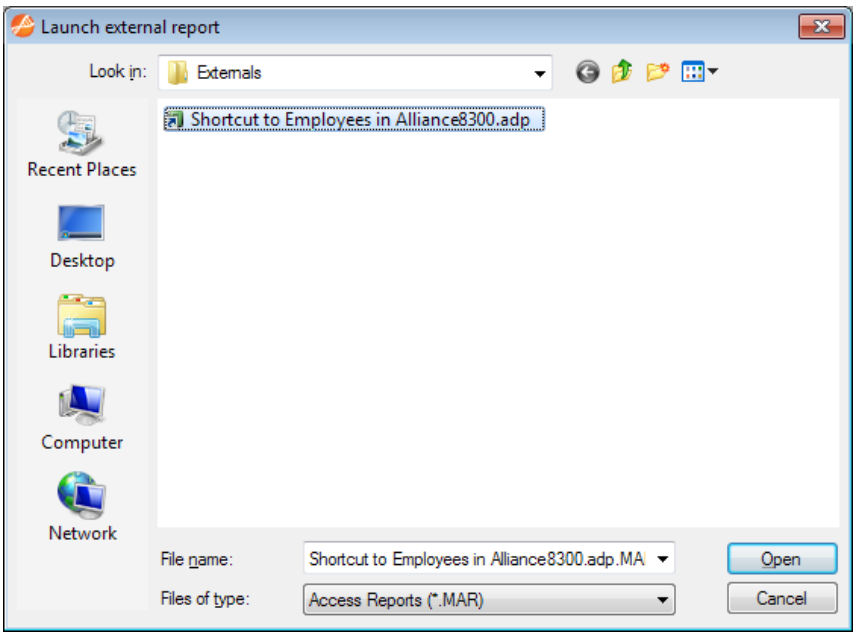
4. Close Microsoft Access and Windows Explorer when you are finished creating reports and dragging them into the Security Commander Externals folder.

Launching External Reports from Security Commander

To run a Security Commander external report:

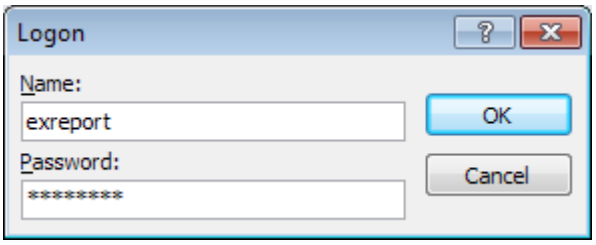
1. On the Reports menu, click External Reports.

   Result: The Launch External Reports window displays the report shortcuts that you've dragged into the Externals folder on the server computer. (The first time, you may need to browse to the C:\Program Files (x86)\UTC Fire & Security\Security Commander\Externals folder.)



2. Select the required report and click Open. A security notice displays.

3. Click Open, and the database logon window displays.



4. Enter “exreport” as user name. Enter the password as setup using the maintenance application and then click OK.

Result: Microsoft Access launches and opens the report in preview mode.

Note: Microsoft Access is required on all client PCs that will run this report.

Database and system management

This chapter discusses the various types of Security Commander files, and the tools available for maintaining, backing up, and restoring these files.

Maintaining databases

The Security Commander server computer has three databases:

- Alliance8300: Contains configuration data for items such as operators, badges, and Challenger control panels.
- Alliance8300History: Contains current history data (data that has not been archived) including badge transactions and operator history.
- Alliance8300Archive: Contains transaction history data that was previously stored in the Alliance8300History database and automatically moved based the Security Commander archive settings.

Maintenance operations for the Security Commander databases include:

- Archiving: Archiving does not protect data against loss: it only moves data from the current database to the archive database for the purpose of maintaining system performance and for managing the use of hard disk space. See “Archiving Security Commander history” below.
- Backing up: Backing up is used to protect data against loss by enabling you to move the data to another location, and in a manner that allows lost data to be recovered. The Auto Backup Utility and the Security Commander Database Maintenance utility are used to back up the Security Commander databases. See “Backing up databases” on page 91.

Archiving Security Commander history

The Alliance8300Archive database is created automatically by Security Commander based on the archive period (daily, weekly, or monthly) defined in the Parameters form (see “Archive Database” on page 41, and Figure 9 on page 42). The default archive period is daily.

Security Commander services must be running on the Security Commander server for a scheduled archiving operation to occur. If the services are not running, Security Commander attempts to perform the archiving operation the next time Security Commander is started and a transaction is received.

Archiving appends the daily, weekly, or monthly data from the history database to the archive database, and removes this data from the history database.

Note: When the archive process runs, new data is appended to the current file. You must monitor the size of the Alliance8300ArchiveDAT database file to ensure that it remains below 10 GB in size and to ensure that the Security Commander databases do not completely fill your hard drive. Depending on the use of archiving and diagnostic monitoring, you may need to reserve 20 GB of space free for use by Security Commander (archiving can create very large temporary files).

The factors in determining whether the archive database is too large can be:

- The database must remain less than 10 GB in size
- The amount of available hard disk space on the Security Commander server computer
- The performance you receive when running history reports
- The length of time you need to keep data
- Other factors specifically related to your installation

When you determine the archive database is too large:

1. Backup the data that you need to retain. See “Backing up databases” on page 91.
2. Assuming that Security Commander Database Maintenance utility displayed a message verifying that the backup was successful, delete the data from the Alliance8300Archive database. See “Deleting Security Commander archive history” below.

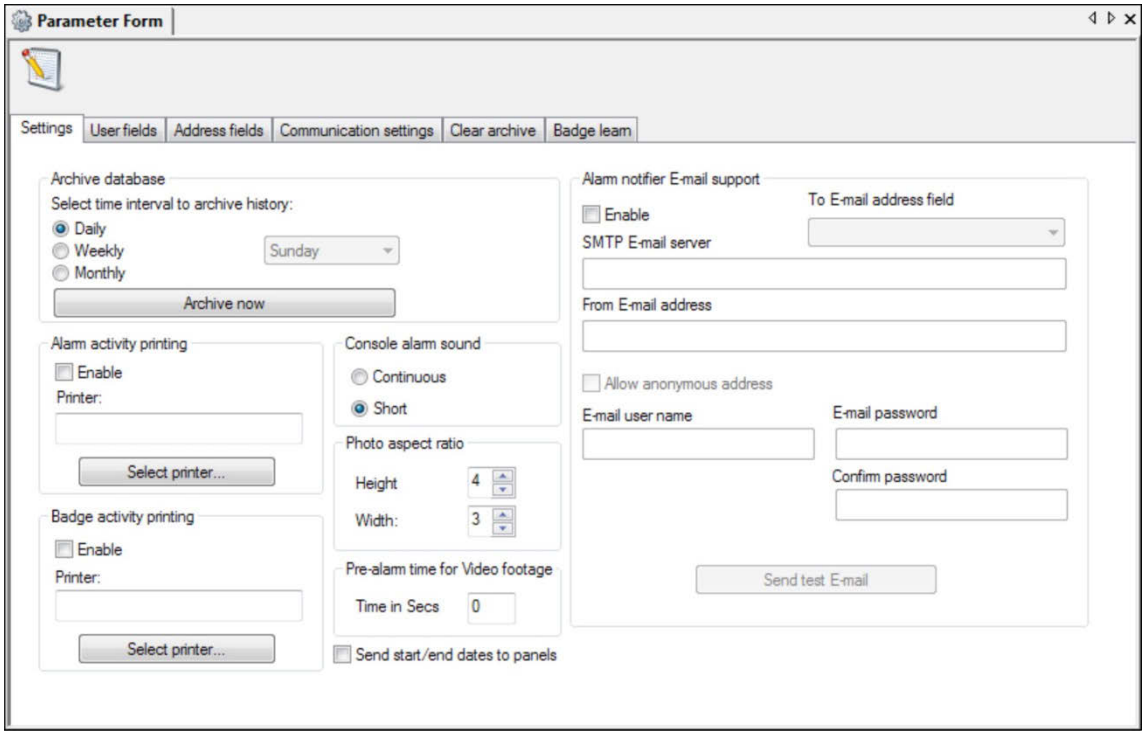
   Caution: If you do not back up the Alliance8300 Archive database, you could lose all the data stored in it.

   After you perform the backup, validate the quality of the backup file, then label and store the media in a safe place.

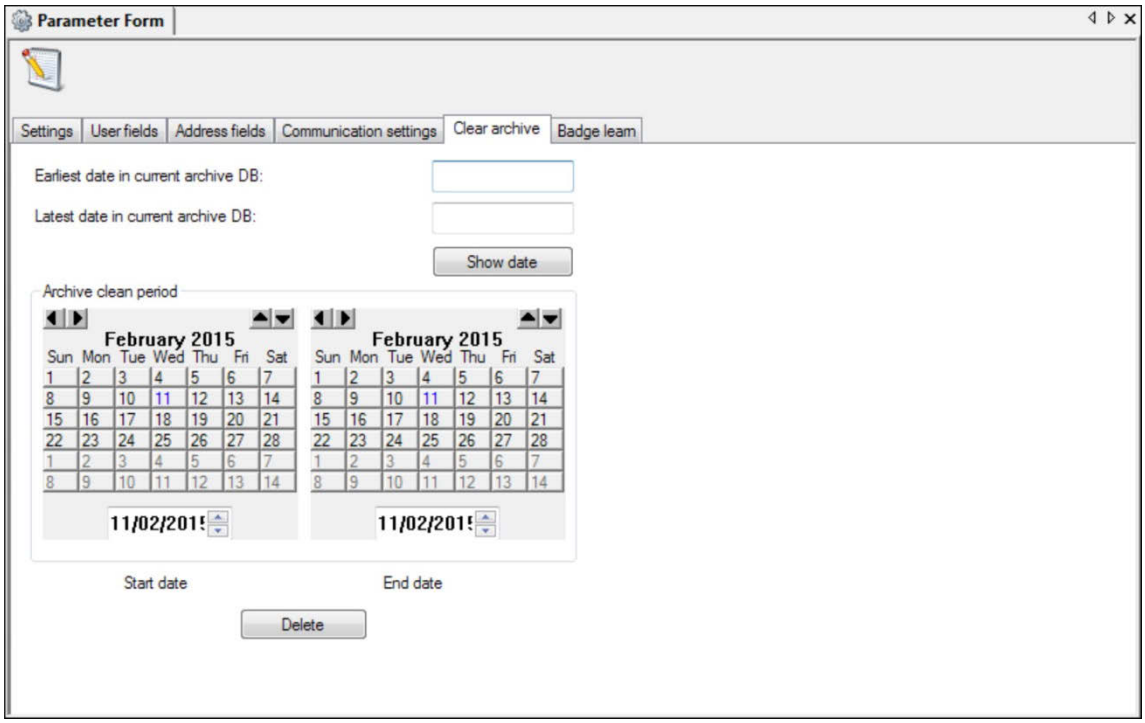
Deleting Security Commander archive history

To delete data from the archive database:

1. Start Security Commander and login.
2. On the Administration menu, click Parameters.
3. The Parameter form opens with the Settings tab displayed.

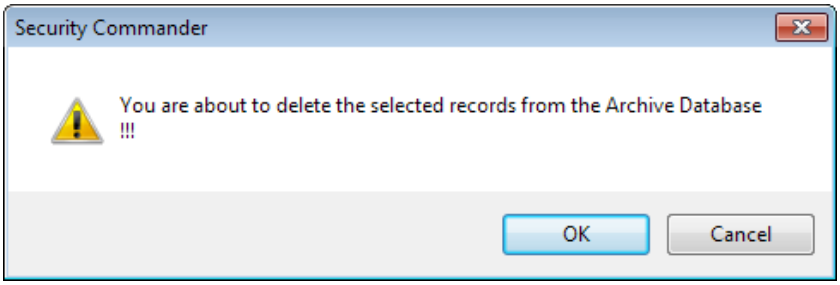


4. Select the Clear Archive tab.



5. Click Show Date to display the Earliest Date in Archive DB and Latest Date in Archive DB fields in MM/DD/YYYY format. If you do not have any records in your archive database, the two date fields display No Record.
6. Choose the Start Date of the data that you want to remove from your archive database by selecting the month, then the day to begin your archive.
7. Choose the End Date of the data that you want to remove from your archive database by selecting the month, then the day to end your archive.

8. Click Delete. A confirmation message displays.



9. Click OK.

   Result: The deletion of an archive database is taking place in the background. Background Tasks status is indicated on the status bar in the lower right side of the screen. The process may take hours to complete. The length of time is dependent on the size of the archive database and the hardware components of your computer.

   Upon completion, a window displays the message: The data from the Security Commander Archive database has been successfully deleted.

10. Click OK.

Backing up databases

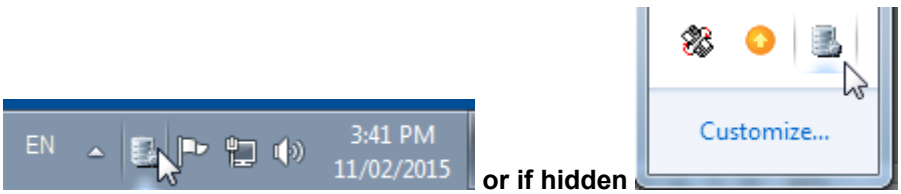
The following utilities can be used to back up Security Commander databases:

- Use the Auto Backup Utility to schedule database backups.
- Use the Security Commander Database Maintenance utility to back up the databases to .BAK files.

Using the Auto Backup Utility

1. Create a folder on your system or any where on the network using a mapped drive where the backup files will be stored.
2. Security Commander Auto Backup starts automatically when Windows is started and can be opened at any time from its icon in the Windows taskbar (Figure 17 below).

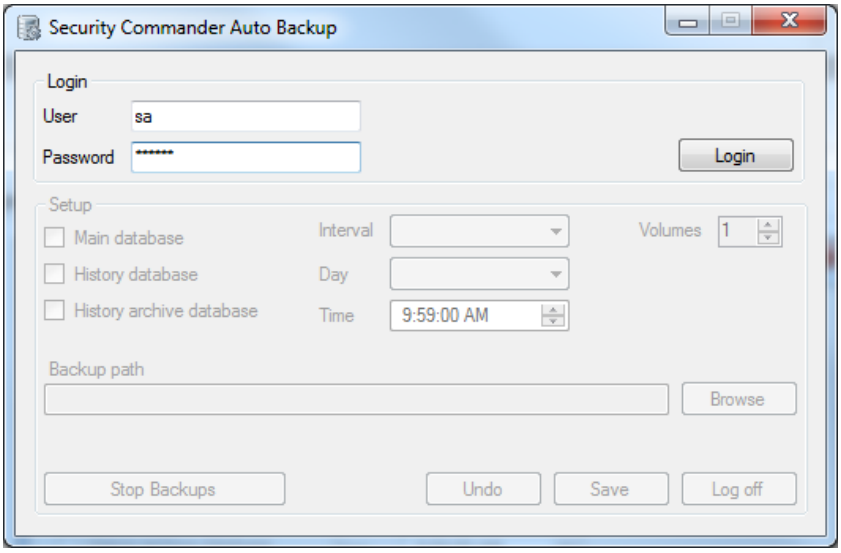
Figure 17: Auto Backup Icon



3. Right-click the icon and then select Configuration to open the Security Commander Auto Backup window (Figure 18 on page 92).

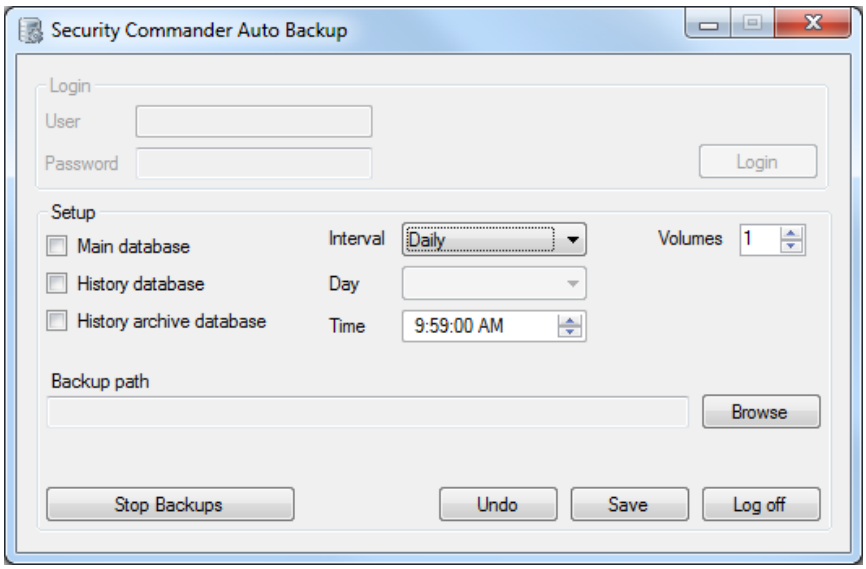
   Tip: If Security Commander Auto Backup isn't running (there is no icon in the Windows taskbar), you can start it from Start > All Programs > Tecom > Security Commander > Auto Backup Utility.

Figure 18: Auto Backup window login



4. Type the “sa” login and password, and then click Login.

Figure 19: Auto Backup window



After logging in, configure the backup options as follows:

- Select one or more databases to back up by checking the Main, History, and History archive check boxes.
- Click the Interval arrow and select whether the backups are to be done daily or weekly.
- For weekly backups, click the Day arrow and select the day on which to start the backups.
- Edit the hours, minutes, seconds, and AM/PM Time fields to configure the backup time.

- Click the Volumes up and down arrows to set a limit in the range 1 to 10 on the number of backup files (of each type) that will be retained in the backups folder. For example, select 1 if you want the folder to retain only the latest file prefixed with “Alliance8300History”; select 2 if you want two consecutive files to be stored, and so on.
- Click Browse and then navigate to the folder on your system where the backup files will be stored.
- Click Save to save the current configuration, and to schedule automated backups to begin at the programmed day and time.
- Click Log off to log off from the databases and leave the Security Commander Auto Backup window open.
- Click the Close button at top right-hand corner to close the Security Commander Auto Backup window. Security Commander Auto Backup continues to run as an icon in the Windows taskbar.
- Click Stop Backups to completely shut down Security Commander Auto Backup. No scheduled backups will run when Security Commander Auto Backups is shut down.

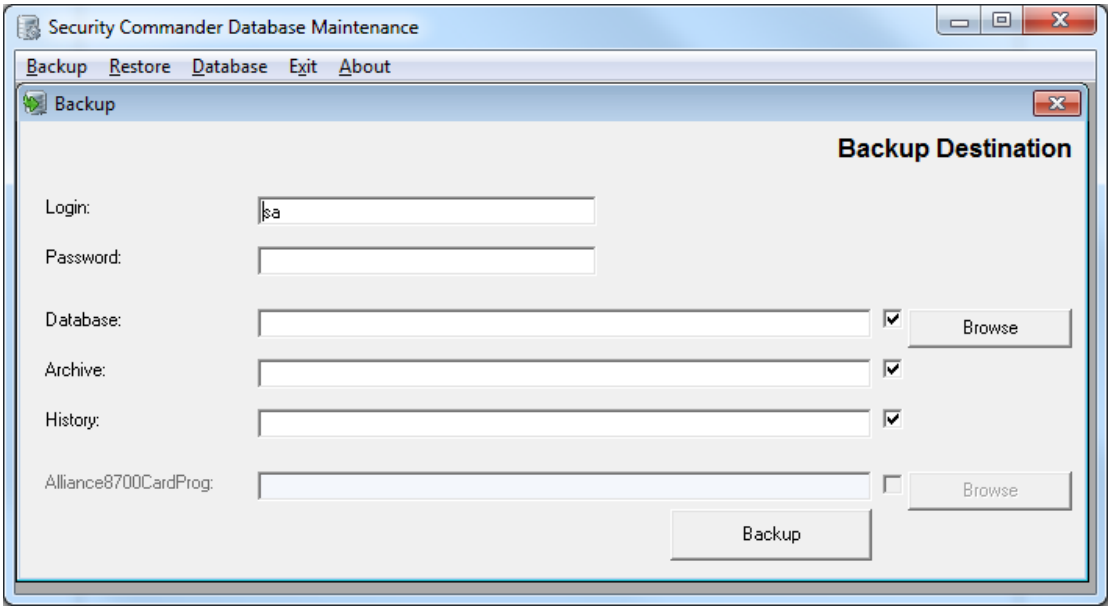
Backup files will be stored in your designated location in the format:

- Alliance8300_AutoBU_YYYY_MM_DD.bak for the main database.
- Alliance8300History_AutoBU_ YYYY_MM_DD.bak for the history database.
- Alliance8300Archive_AutoBU_ YYYY_MM_DD.bak for the history archive database.

Using the Database Maintenance Utility

1. Create a folder on your system or any where on the network using a mapped drive where the backup files will be stored.
2. Run the Security Commander Database Maintenance utility on the Security Commander server from Start > All Programs > Tecom > Security Commander > DB Maintenance.
3. The Security Commander Database Maintenance window displays.
4. Click Backup.

5. The Backup window displays.



6. Type the “sa” login and password.
7. Click Browse to choose where the backup files will be stored.

   Result: The .BAK files in each field will be named automatically, to include the directory path, file name, date, and time.
8. If you choose not to back up any of the three databases, clear the check box at the end of that field. If the check box is selected but no destination is entered in the database field, backup of that database file will not occur.
9. Click Backup.

   Result: The backup process begins. When backup is complete, a dialog box displays a message verifying the successful backup of the chosen databases.
10. Click OK.
11. Exit the Maintenance window.

Restoring data from a backup

You may need to restore data from a backup for a variety of reasons:

- To verify that a backup was successful
- To establish backup and restore procedures
- To recover lost data (accidental deletion or system failure)
- To recover a deleted archive database so that reports can be run using the data

Restoring Security Commander databases

Note: The backup files must be moved to the destination computer. The Security Commander Database Maintenance utility can only restore from a local machine (in this case the Security Commander server).

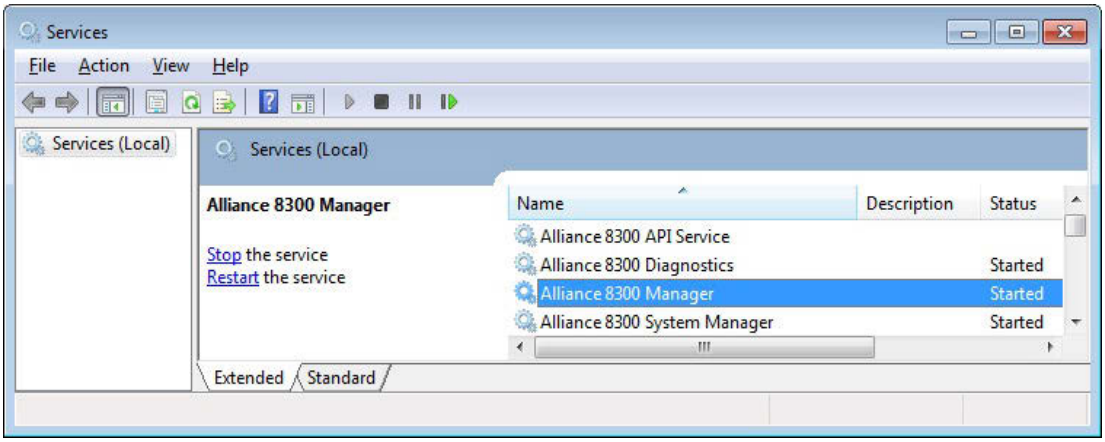
To restore a Security Commander database backup:

1. Stop the Security Commander services. Select Start > Settings > Control panel. Double-click Administrative Tools and then double-click Services.

   Alternatively, select Start > Run and enter services.msc. Click OK.

   Result: The Services window displays.

2. Find the Security Commander services and stop them in the following order: Alliance 8300 Manager, Alliance 8300 System Manager, Alliance 8300 Diagnostics.

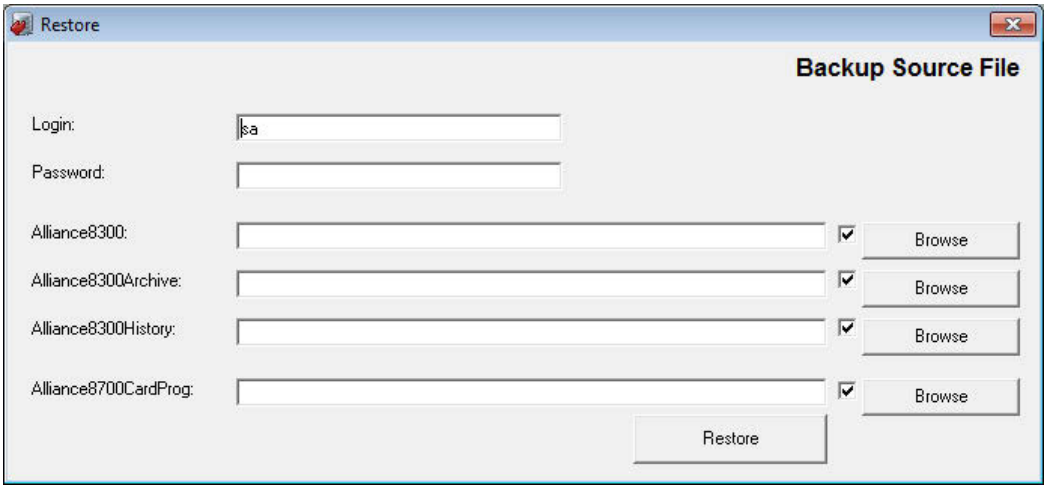


3. Run the Security Commander Database Maintenance utility on the Security Commander server from Start > All Programs > Tecom > Security Commander.

   Result: The Security Commander Database Maintenance window displays.

4. Click Restore.

   Result: The Restore window displays.



5. Type the “sa” login and password.

6. Click Browse to choose the Challenger database backup file. The program will then try to find all other backup files in this folder.
7. If you choose not to restore any of the three databases, clear the check box at the end of that field. If the check box is checked, but no destination is entered, the restoration will not occur.
8. Click Restore.

   Result: The restoration process begins. When restoration is complete, a dialog box displays a message, verifying the restoration of the chosen databases.

   Note: When you restore a database, you need to re-license Security Commander and all clients connected to it.
9. Click OK.
10. Exit the Alliance8300 Database Maintenance utility.
11. Re-register the Security Commander License using the license key initially provided. (If Security Commander does not accept the original license key, follow the complete license registration procedure described in the Security Commander Installation Guide.)

    Result: The database restoration is complete and your Security Commander application is ready to start.

System recovery

If your Security Commander server computer experiences severe errors while operating, you might need to rebuild the system and restore your databases. Follow the sequence of steps listed to recover your system.

The checklist below assists you in recovering your Security Commander system. Complete the steps in the order they appear:

- ❑ Repeat all the steps in the Security Commander Installation Guide from “Preparing the Operating System” to the end of “Installation Part 1”.
- ❑ Use the Security Commander Database Maintenance utility to restore the three Security Commander databases from your backup media. See “Restoring Security Commander databases” on page 95.
- ❑ Re-register the Security Commander License using the license key initially provided (if Security Commander does not accept the original license key, follow the complete license registration procedure described in the *Security Commander Installation Manual*).
- ❑ Restart the computer.

Diagnostics and troubleshooting

Using the diagnostic viewer

Security Commander provides an extensive diagnostic utility named DiagView. On the Administration menu, click Diagnostic Viewer to access DiagView. This utility is very flexible in that you can selectively activate the monitoring of Security Commander system components when needed.

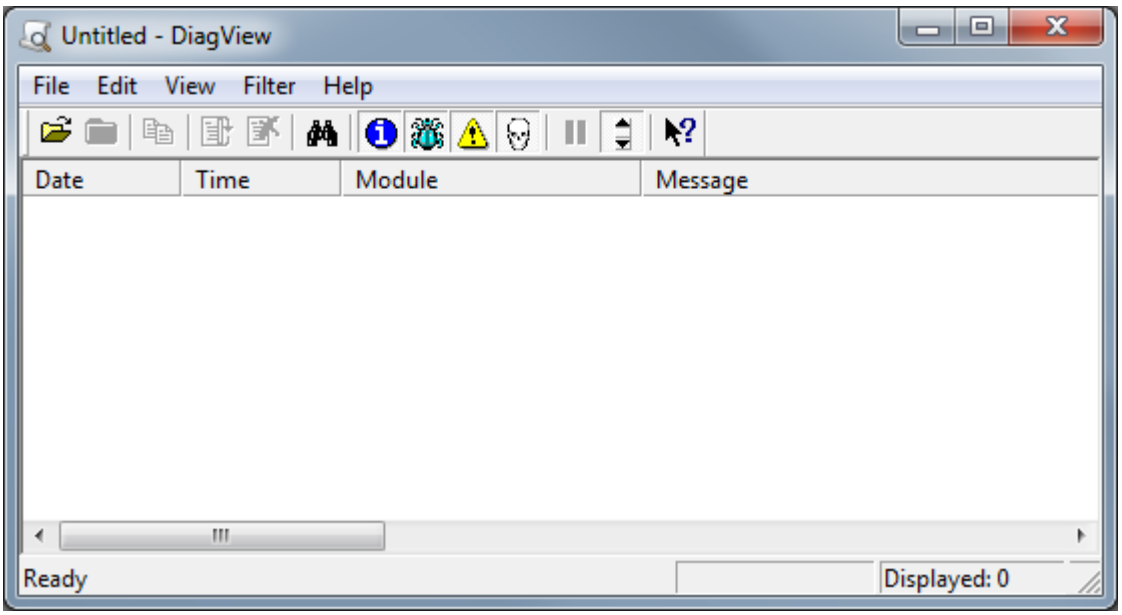
Note: The amount of data stored for diagnostics may make finding issues difficult. Activate diagnostics only when requested so be qualified support engineers.

This utility plus some common questions and answers are covered in this chapter.

To view diagnostics logs:

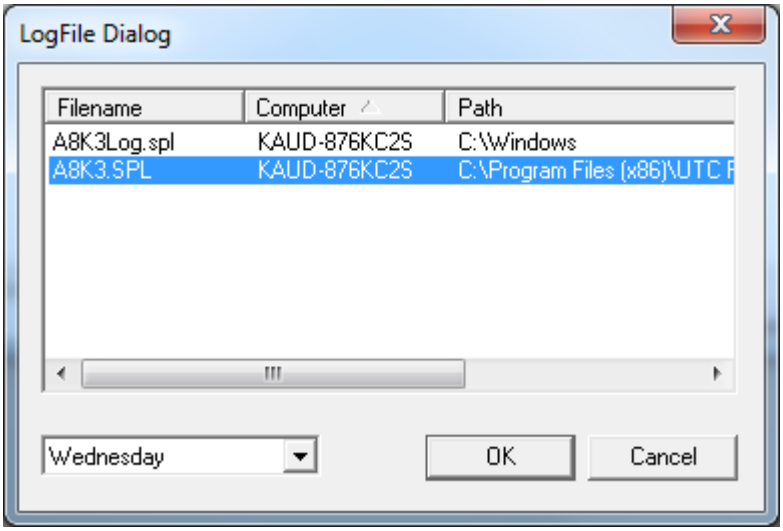
Select Start > All Programs > Tecom > Security Commander > Diagnostic Viewer. Alternatively, from Security Commander's Administration menu, select Diagnostic Viewer. The Diagnostic Viewer window displays (Figure 20 below).

Figure 20: Diagnostic Viewer window



Select Open from the File menu to display the LogFile selection dialogue box (Figure 21 on page 98).

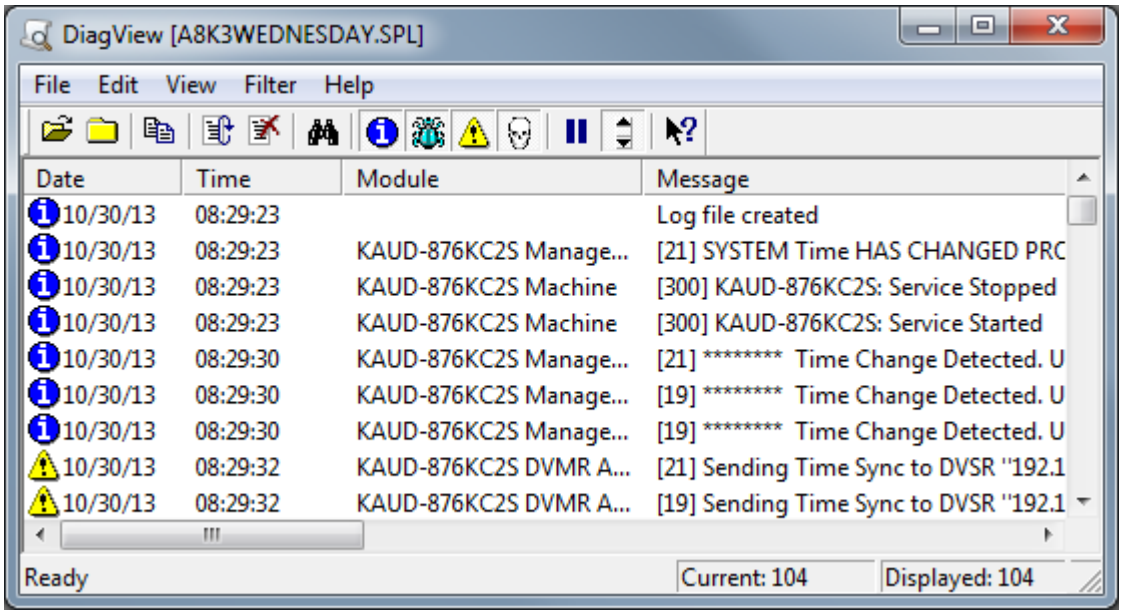
Figure 21: Opening a log file



Select the filename “A8K3.SPL” to open the log file corresponding to the day of the week shown at the bottom of the dialogue box (for example C:\Program Files (x86)\UTC Fire & Security\Security Commander\Logs\ A8K3WEDNESDAY.SPL). Click the day arrow to select a different day, if needed.

Click OK to open the log file in Diagnostic Viewer.

Figure 22: Diagnostic Viewer window populated



The Diagnostic Viewer window has menus plus an optional toolbar. You can toggle the toolbar display via the Toolbar option in the View menu.

If you want to display or hide a certain types of messages, click to toggle the filters in either the Filter menu (Figure 23 on page 99) or the corresponding toolbar buttons.

Figure 23: Diagnostic Viewer filters

Select Reload from the File menu or the corresponding toolbar button to refresh the Diagnostic Viewer window with the new filter selection.

Refer to *DiagView Help* for more information.

Turning on additional diagnostics

By default only a limited number of debug messages are stored and displayed. To store or display more debug messages in the Diagnostics Log within Security Commander, the diagnostics for that component you wish to monitor (COM port, Challenger control panel, or client) MUST be turned on.

Each client computer will have a set of diagnostic objects that represent what can be monitored on that machine. Diagnostic objects can be controlled remotely (turned on or off). All diagnostic objects can write messages to a common log file or any diagnostic object can write to a separate log file that can be defined by the user.

To create a log file:

1. On the Administration menu, click Logfile.

   Result: The Logfile form displays.
2. Click Add Record.
3. Your Computer name displays.
4. Enter a LogFile name to include an .spl extension.
5. Click Browse to navigate and select a folder in which to store the log file.
6. Click Save.

To enable diagnostics:

1. On the Administration menu, click Diagnostic Setting.
2. Click Search in the toolbar to display a list of components that you can monitor.
3. Select the desired component.

   Note: All diagnostic objects are prefixed with a machine name.
4. Select Enable debug messages check box and click Save.
5. When you are finished troubleshooting the system, don't forget to go back and DISABLE debug messages.

Caution: The more items you turn on for monitoring, the more the Security Commander system performance is compromised! This is even more important when monitoring port, communications, or Challenger control panel items.

There are many components available to monitor.

- The diagnostic objects, such as COM1, display the communications protocol between the Challenger control panel and its server as the information comes into the COM port.
- The diagnostic objects, such as Challenger control panel 1, display how information is being processed for that Challenger control panel.
- The remaining components are for client, manager service, system service, and other functional components.

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.

Alternatively, visit the Interlogix Support Portal at support.interlogix.com.au.

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

Appendix A. CCTV Support

Note: CCTV support in not available in Security Commander Lite.

Introduction

Security Commander interfaces with CCTV (Closed Circuit Television) systems via the Tecom Video Module.

Security Commander 2.1 (and later) DVR integration uses the following add-on video service applications (each with a corresponding brand-specific video plug-in module) to provide the interface between Security Commander and digital video devices.

- Video Status Manager (VSM) and the brand-specific VSM plug-in module, must be installed on the Security Commander server computer (one computer must have VSM).
- Video Presentation Client (VPC) and the brand-specific VPC plug-in module must be installed on each Security Commander computer that is used for controlling or viewing video. The VSM and VPC can be installed on the same computer.

Note: Any computer with VSM and/or VPC must also have Microsoft .NET Framework 4 installed.

The systems are CCTV control systems that operate separately from Security Commander and require their own hardware and software provided by the CCTV manufacturer. The interface between the CCTV system and Security Commander provides the capability to automatically control CCTV cameras based on alarms within Security Commander.

Setup and configuration

For the physical setup of the CCTV system that you purchased, refer to the documentation you received with the CCTV system.

Sources of additional details include the following:

- *Security Commander CCTV Interface Guide* covers setup and configuration of the CCTV system with Security Commander.
- *Security Commander Help* contains additional information on setting up CCTV alarms.

Digital Video Recorders (DVRs)

Security Commander has the ability to integrate with digital video recorders. Using your Security Commander system, you are able to set up, control, search, and view live and recorded video directly from your computer. Refer to the *Security Commander CCTV Interface Guide* for detailed instructions to setup and configure a DVR system with Security Commander.

Appendix B. Changing the server name

Introduction

The Security Commander Server computer holds the Security Commander databases, controls communications with Security Commander client computers, and controls the Security Commander licensing.

The need may arise to change the name of the Security Commander Server computer. This could typically be due to upgrading the computer or moving the Security Commander Server to a different computer (i.e. installing Security Commander, and restoring the Security Commander databases, to a computer with a different name than the original server's computer name).

Tip: If you need to move Security Commander Server onto a new computer, you may save time by changing the new server's computer name to be the same as the old server's computer name before installing Security Commander and restoring the Security Commander databases. However, after installing Security Commander you would still need to re-license the new server and all the clients.

If you have already installed Security Commander on the new server computer and you need to change the server's computer name, you must change it in four places:

- On the Windows operating system, Network Identification tab of your System Properties. See "Changing the name in Windows" below.
- In the Security Commander registry setting. See "Changing the name in Windows registry" on page 103.
- In the Security Commander database. See "Changing the name in the Security Commander database" on page 104.
- In the ODBC Data Source Administrator. See "Changing the name in ODBC" on page 104.

Note: Any Security Commander computer (server or client) that has had its computer name changed will lose communication with all controllers (Challenger control panels) hosted by that computer. In such a case, the Controller records for affected panels would have to be deleted and then recreated using the new computer name.

Changing the name in Windows

To change the name of the server computer in Windows:

1. Right-click the My Computer icon on your desktop.
2. Select Properties from the context menu.
3. Select the Network Identification tab from the System Properties.
4. Click Properties.

Result: The Identification Changes screen displays your Computer Name. Enter the new name of the Server computer. It should consist of a maximum of 15 alphanumeric characters with no spaces.

5. Click OK, and then click Apply. You will be asked to reboot your computer. Select OK.
6. When the computer reboots, you may receive an error message from MS SQL. Click OK to close the dialog. This error will be addressed later, as you change the server computer name in MS SQL.

Changing the name in Windows registry

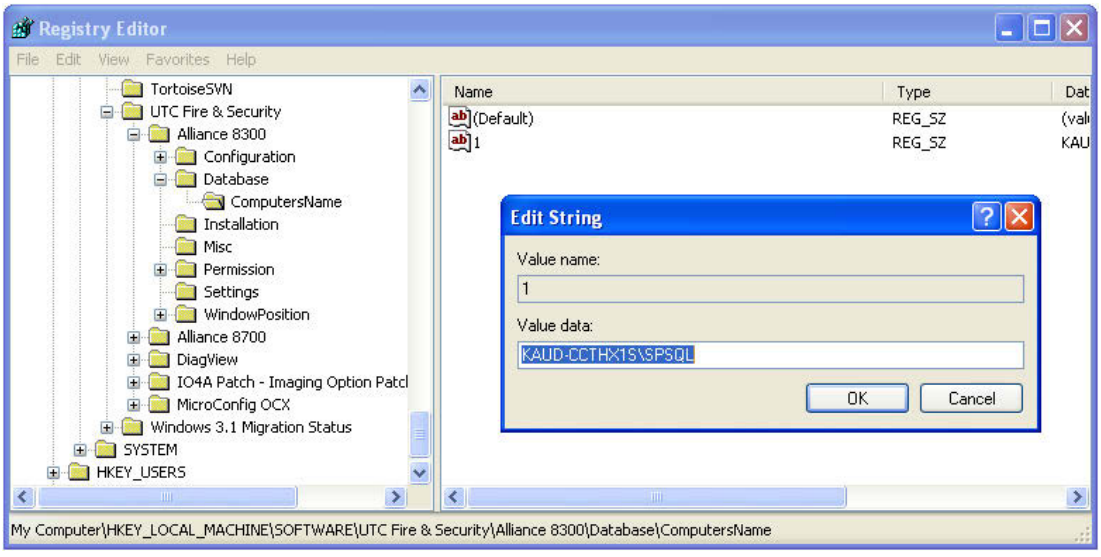
Caution: Always use extreme care when editing the Windows registry! Making a mistake while editing the registry can cause Windows to behave erratically. To fix this problem, you will need to reinstall your operating system.

To change the Security Commander Windows registry entry for the computer name:

1. Shut down the Security Commander client application.
2. Stop Security Commander services.
3. Click Start, then Run, type “regedit” and then click OK.

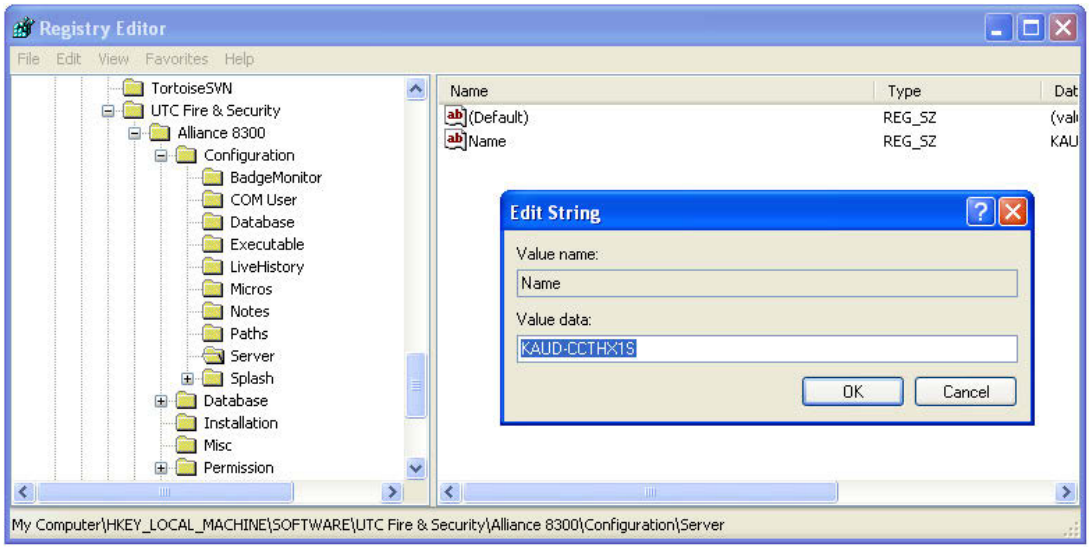
   Caution: Using the Registry Editor incorrectly can cause serious problems that may require you to re-install your operating system. Neither UTC nor Microsoft guarantees that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk!
4. Open the following by clicking “+” in front of HKEY_LOCAL_MACHINE, then SOFTWARE, UTC Fire & Security, Alliance 8300, Database, then ComputersName.
5. On the right side of your screen, double-click the key name 1 to open the Edit String dialog box.

   Result: The screen that displays should be similar to the following:



6. Type the new server name in front of \SPSQL, and then click OK.
7. Open the following by clicking “+” in front of HKEY_LOCAL_MACHINE, then SOFTWARE, UTC Fire & Security, Alliance 8300, Configuration, then Server.
8. On the right side of your screen, double-click the key name “Name” to open the Edit String dialog box.

   Result: The screen that displays should be similar to the following:



9. Type the new server name in front of \SPSQL, and then click OK.
10. Select Registry > Exit to close the Registry Editor.

Changing the name in the Security Commander database

Use the SPInitClient utility to update the server and client computers when the Security Commander server computer has its name changed or is moved to a different computer.

Refer to “Changing the server name” on page 120 for details.

Changing the name in ODBC

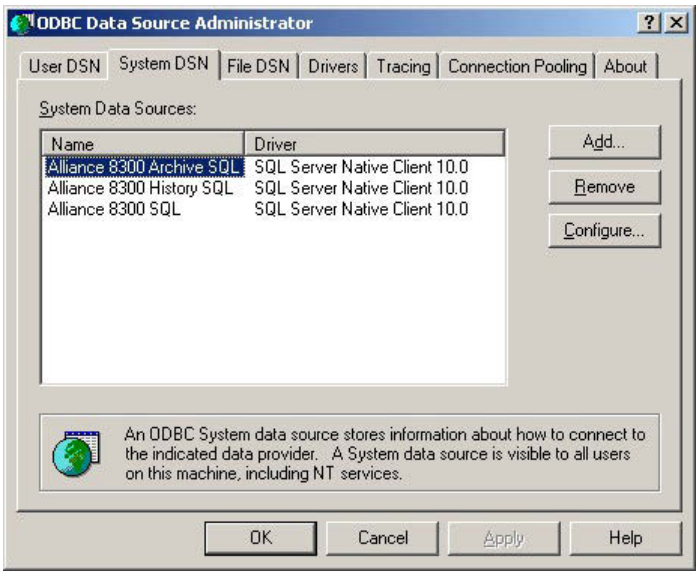
Open Database Connectivity (ODBC) is used to enable Security Commander (on the server and on clients) to connect with the Security Commander databases on the server computer.

If the name of the server computer is changed, then the new name must be applied to the Security Commander ODBC system data sources for the server and all client computers.

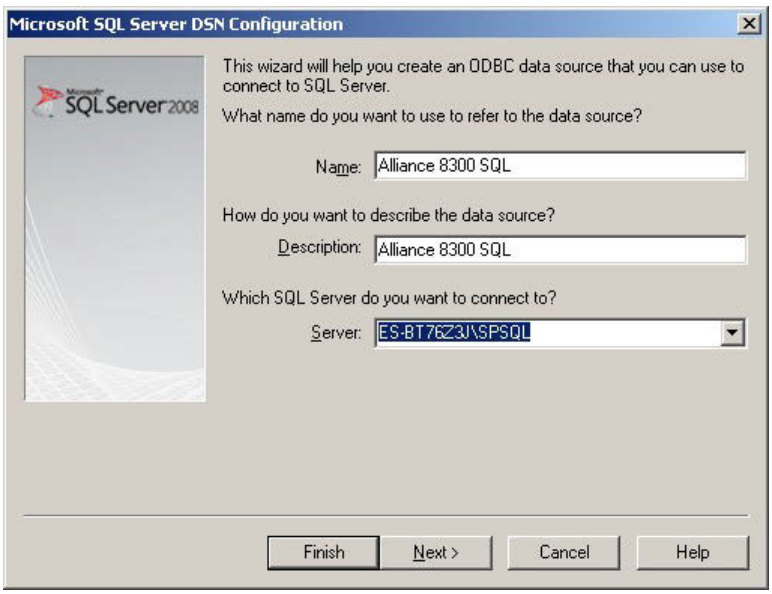
If performing this procedure on a Security Commander client computer, the Security Commander server must be running and connected to the network, and the client computer must also be connected to the network.

To change the name of the server computer in ODBC:

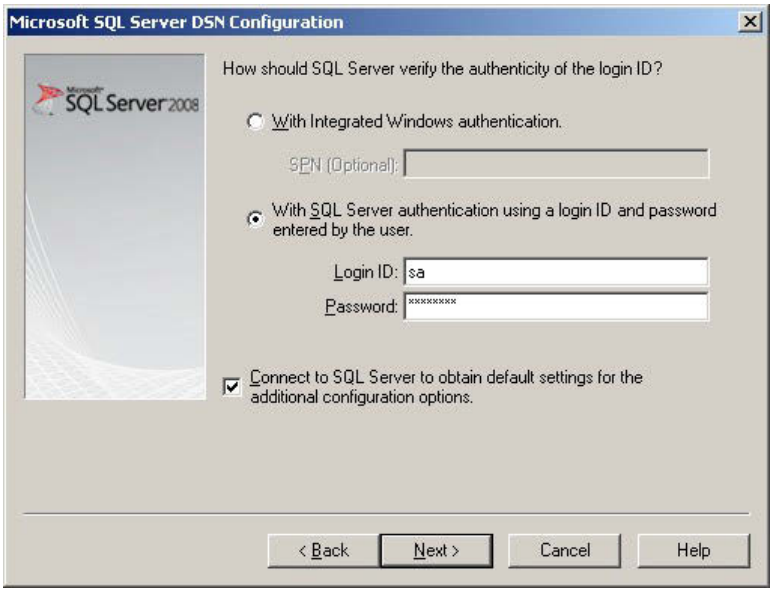
1. Select Start > Settings > Control panel. Double-click Administrative Tools and then double-click Data Sources (ODBC), and then click the System DSN tab on the ODBC Data Source Administrator window.



2. In turn, select each Security Commander item in the Name list, and then click Configure.
3. The Microsoft SQL Server DSN Configuration window displays.

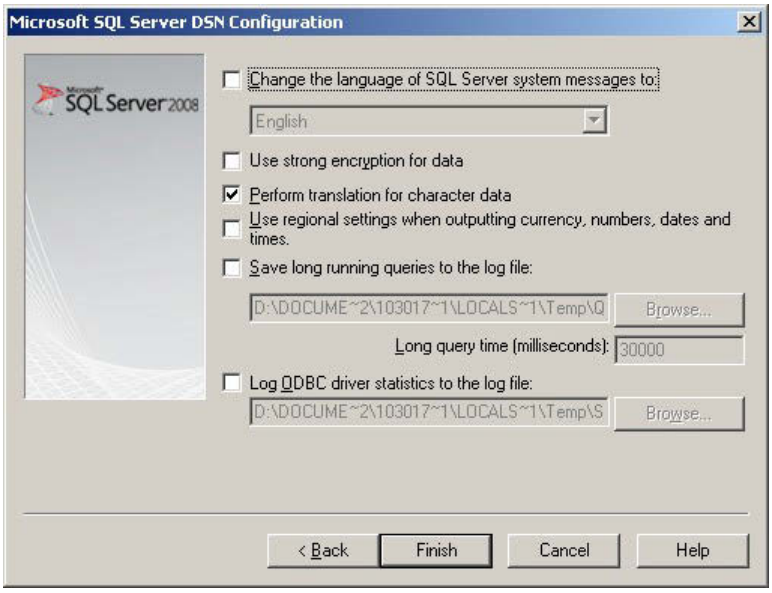


4. Click the Server arrow, select the Security Commander server from the list, and then click Next >.

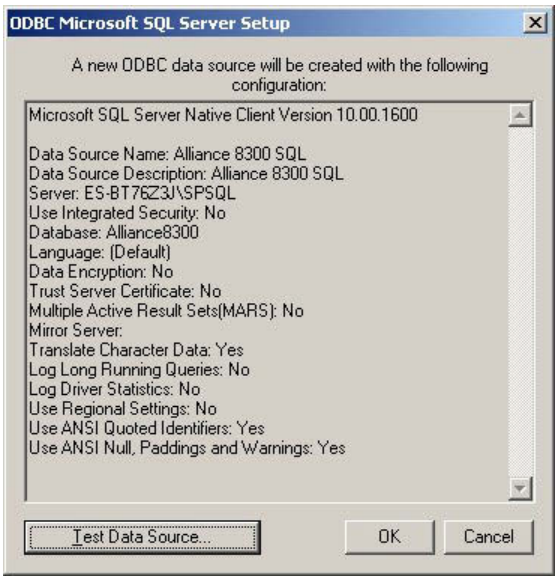


5. Type “sa” in the Login ID field, and password in the Password field, and then click Next >.
6. Accept the defaults and click Next >.

7. Accept the defaults and click Next >.



8. Click Finish.



9. Optional: Click Test Data Sources and then click OK to close the test results window.
10. Click OK to return to the ODBC Data Source Administrator window.

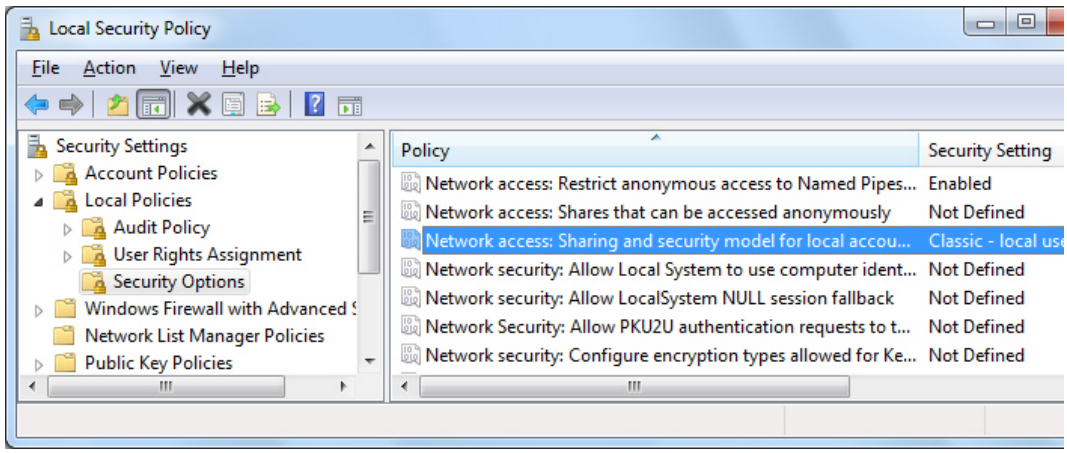
Appendix C. Configuring file sharing

Security Commander requires Classic model of the file sharing in the system.

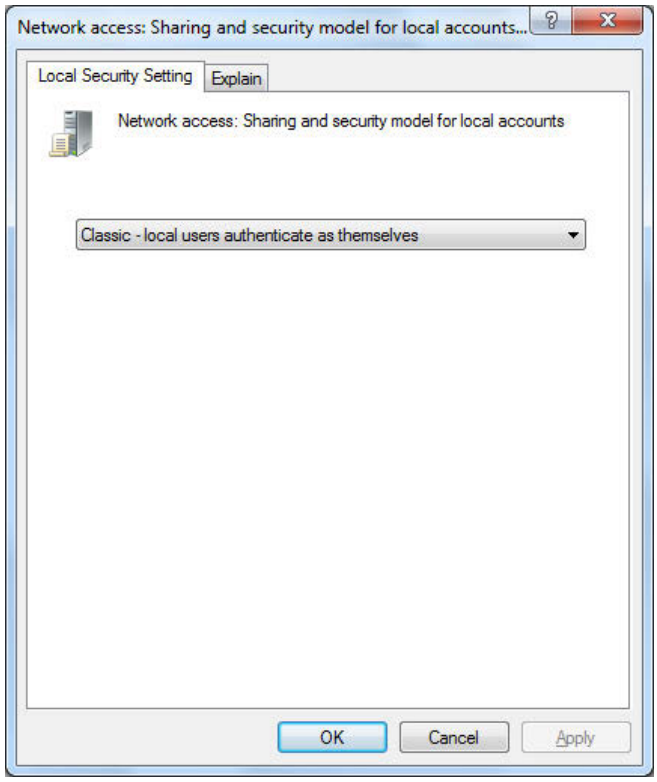
If there is another model set, the following error message will be displayed: “Simple File Sharing is not compatible with the application”.

To set Classic model:

1. Click Start > Settings > Control Panel.
2. Go to Administrative Tools > Local Security Policy.
3. Click Security Settings > Local Polices > Security Options.



4. Double-click Network Access: Sharing and Security Model for Local Accounts.



5. Choose value to “Classic - local users authenticate as themselves”. Apply changes.

Appendix D. Managing passwords

Introduction

Passwords appear in various places, and it's easy to get them confused. This section describes the various types of user name and password combinations that a Security Commander system administrator needs to know about:

- Database passwords (see "Database passwords" below).
- Security Commander operator passwords (see "Creating operators" on page 49).

Database passwords

This section describes the use of the Security Commander Database Maintenance utility for:

- Changing the "sa" password (see "Changing the "sa" password" below).
- Changing the "exreport" password (see "Changing the "exreport" password" on page 110).
- Resetting the application password (see "Resetting the application password" on page 111).

Security Commander uses MS SQL. During installation, an SQL user "sa" (system administrator) with password is created, and must not be changed until after installation has been completed.

Changing the "sa" password

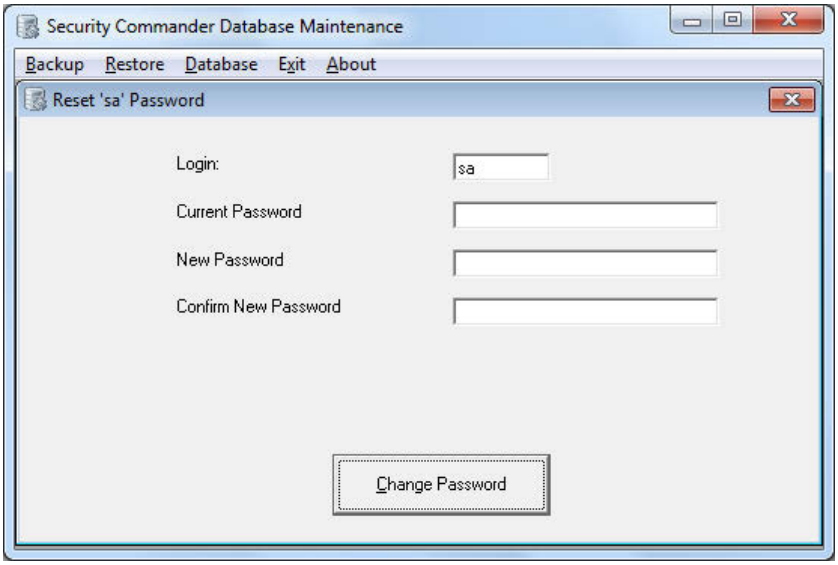
We strongly suggest that you assign a unique password of your choice for the MS SQL System Administrator ("sa") user, for increased security against database intrusion by computer software viruses and hackers.

The following procedure describes how to change the MS SQL password for user "sa" (system administrator) on a Security Commander server computer using the Maintenance utility.

To change the "sa" password:

1. Select Start > All Programs > Tecom > Security Commander > DB Maintenance.
2. From the Database menu, select Reset "sa" Password.

   Result: The Security Commander Database Maintenance [Reset "sa" Password] window displays.



3. Complete the Password fields with the appropriate entries for your current password and newly assigned password, and then click Change Password.
4. Exit the Maintenance utility.

Changing the “exreport” password

We strongly suggest that you assign a unique password of your choice for the MS SQL “exreport” user, for increased security against database intrusion by computer software viruses and hackers.

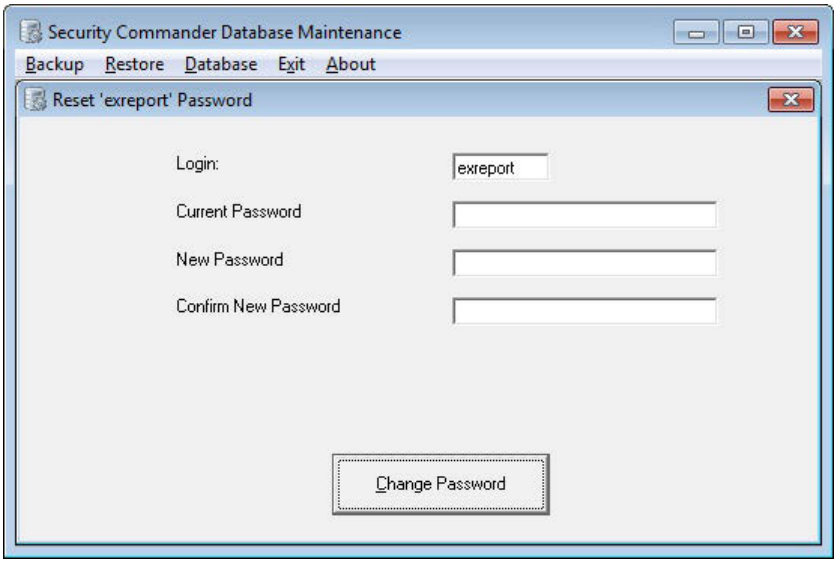
The following procedure describes how to change the MS SQL password for user “exreport” on a Security Commander server computer using the Maintenance utility.

To change the “exreport” password:

1. Select Start > All Programs > Tecom > Security Commander > DB Maintenance.

   Result: The Security Commander Database Maintenance utility window displays.
2. From the Database menu, select Reset “exreport” Password.

Result: The Security Commander Database Maintenance [Reset “exreport” Password] window displays.



3. Complete the Password fields with the appropriate entries for your current password and newly assigned password (default “exreport” user password is “exreport”), and then click Change Password.
4. Exit the Maintenance utility.

Resetting the application password

As applicable to Security Commander Server

Security Commander licensing uses the Security Commander server computer’s hardware configuration (among other things) when it generates the machine seed key, which is used for licensing.

You may need to reset the application password (and relicense Security Commander) as part of a troubleshooting process or to correct a problem when the following occurs:

- The Security Commander server computer’s hardware configuration has changed.
- One or more of the Security Commander services does not start.
- Security Commander on a remote client computer does not start or cannot connect with the Security Commander server computer.

Resetting the Security Commander application password does the following:

- Sets the application password to “devel”. The application user name and password are not normally seen by Security Commander operators, and no user action is required. This detail is for information only.
- Removes the current Security Commander license registration number.
- Puts the Security Commander system into “demo” (not “trial”) mode and will need to be relicensed. Refer to the Security Commander Installation Manual for details about licensing Security Commander.

Procedure

The following procedure describes how to reset the application password on a Security Commander server computer using the Maintenance utility.

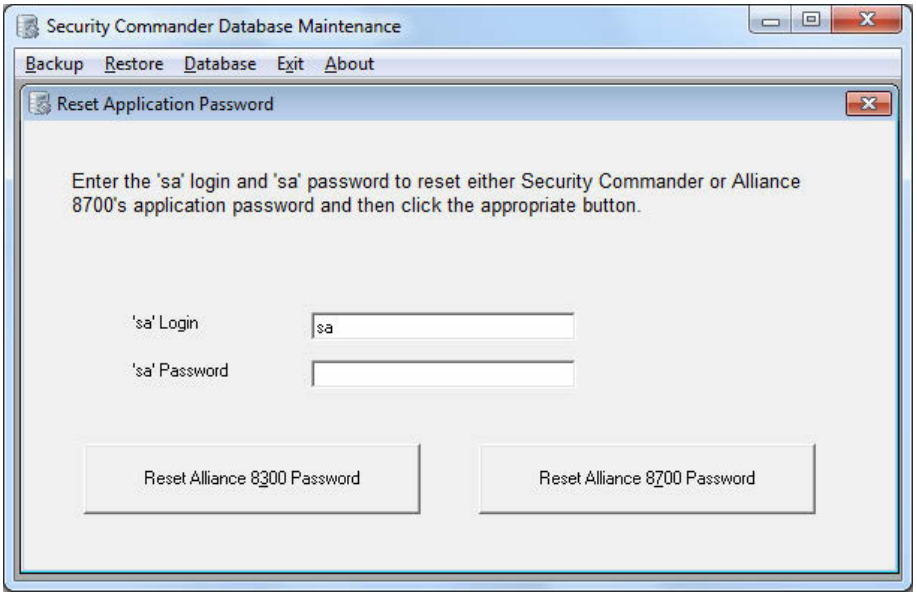
To reset the application password:

1. Select Start > All Programs > Tecom > Security Commander > DB Maintenance.

   Result: The Security Commander Database Maintenance utility window displays.

2. From the Database menu, select Reset Application Password.

   Result: The Security Commander Database Maintenance / Reset Application Password window displays.



3. Type the current system administrator password and login, and then click Reset Security Commander Password.
4. Exit the Security Commander Database Maintenance utility.

Note: Resetting the Security Commander application password puts the Security Commander system into demo mode and will need to be relicensed. Refer to the *Security Commander Installation Manual* for details.

Appendix E. Security Commander utilities

Titan migration utility

The Titan DB Migration utility is used to populate a new (blank) Security Commander database with data from up to 16 Challenger panels in a Titan system consisting of:

- Control panel programming settings only, or
- Control panel programming settings and users

The Titan DB Migration utility migrates data from a .zip file created from Titan's System Maintenance Utility (Export tab).

Notes:

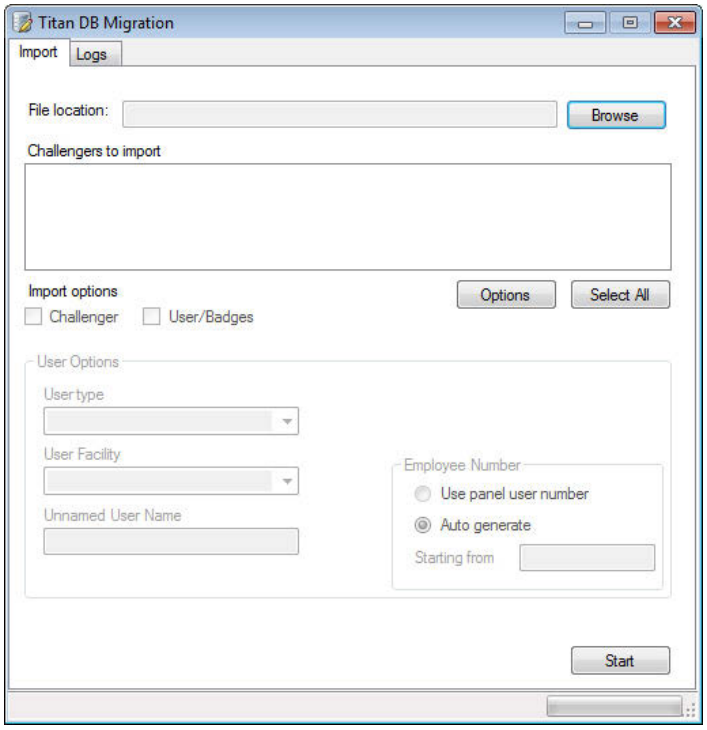
- Titan Photo ID is not migrated to Security Commander.
- Titan DB Migration may be used with Titan version 3.1.0.14 (or later) installed on the Security Commander server. If there is already an earlier version of Titan installed, then you must upgrade it before you can use this utility.
- You can download Titan from http://www.interlogix.com.au/downloads.
- Titan does not need to be registered in order for Titan DB Migration utility to work. However, the installation process requires a 12-digit serial number. If not registering Titan you can use any 12-digit number to proceed.

Importing a Titan system

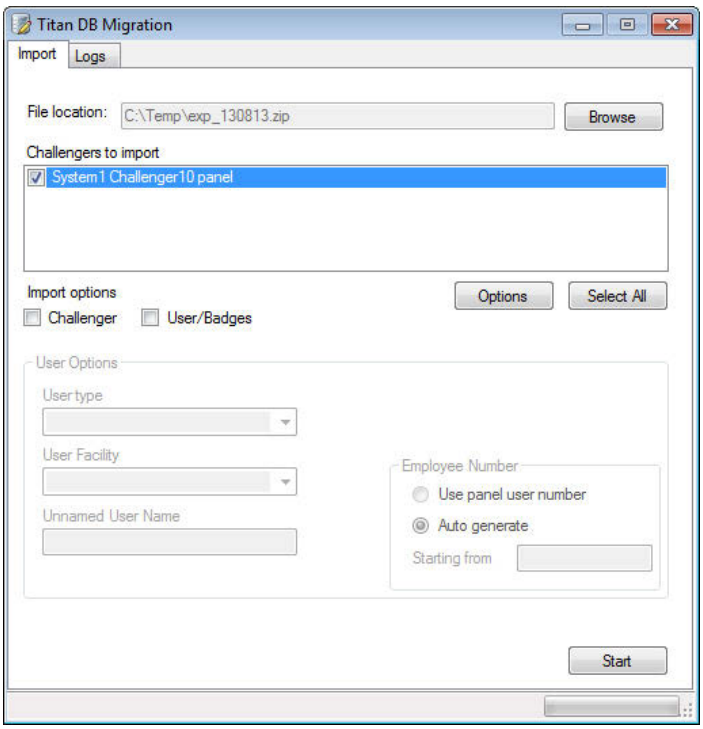
Security Commander must have been started at least one time before you run Titan DB Migration, otherwise you will receive an error message.

To use Titan DB Migration to populate a Security Commander database:

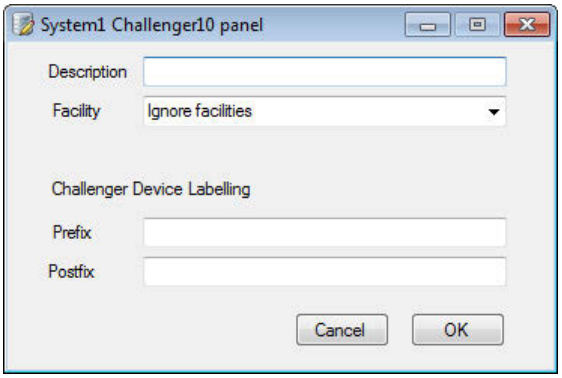
1. Run Titan DB Migration via the Start > All Programs > Tecom > Security Commander > Titan DB Migration command.



2. Click Browse to find the .zip file, and then click Open. All of the Challenger control panels contained in the .zip file are listed in the “Challengers to import” panel.



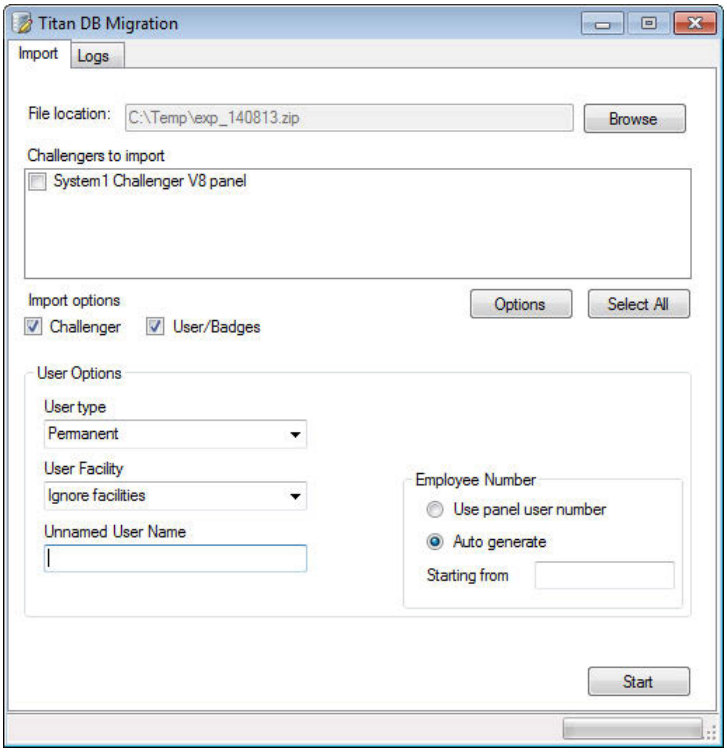
3. Click to select the Challenger control panels to be migrated (from one system only). The migration process can be performed only one time because you can only migrate into a blank Security Commander database.
4. Click the Options button if you want to modify some of the imported panels’ data.



- Type the name of the Challenger control panel in the Description field, or leave blank to use the name assigned in Titan.
- If one or more Facility records have been created in Security Commander, you can pre-assign a facility to the migrated Challenger control panel and all of its applicable programming settings. Click the Facility arrow, and then select the required facility.
- Type a prefix text label that will be added to the start of a device label (and followed by a space), or leave blank to not prefix the device name used in Titan.
- Type a postfix text label that will be added to the end of a device label (and preceded by a space), or leave blank to not postfix the device name used in Titan.

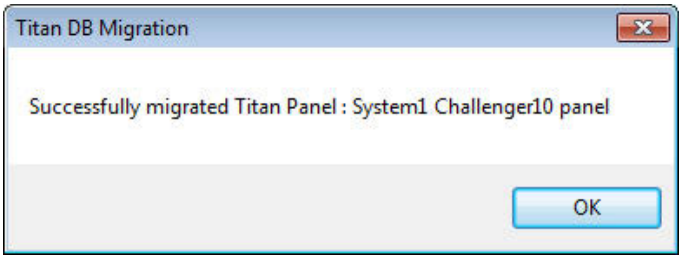
Click OK when finished defining options.

5. Click to select one of the following import options for all selected Challenger control panels to be migrated:
   - Click to select “Challenger” to migrate only Challenger control panel programming settings
   - Click to select “User/Badges” to migrate Challenger control panel programming settings and users



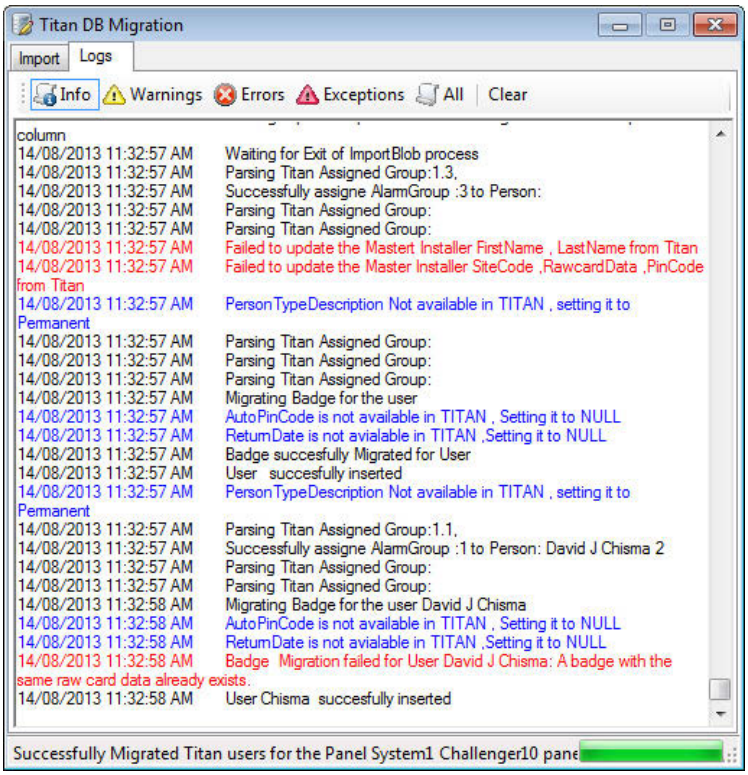
6. If you are migrating users/badges, select the following user options to apply to all migrated users:
   - Click the User type arrow and select a personnel type. All migrated uses will be assigned the selected type.
   - If one or more Facility records have been created in Security Commander, you can pre-assign a facility to the migrated users. Click the User Facility arrow, and then select the required facility.
   - Optionally apply a common name for any migrated users that don't have names in Titan. The common name is applied to any blank name fields. For example, if the common name is "Empty", then a user with no first or last name would be migrated as "Empty Empty".
   - Select the "Use panel user number" radio button to use the Challenger control panel's user numbers as the Security Commander's employee numbers.
   - Select the "Auto generate" radio button to create new employee numbers in Security Commander. You must also specify a starting number.
7. Click Start when finished defining import options and user options.

   For each Challenger control panel in sequence, Titan DB Migration displays a confirmation message after migrating's the panel's programming, and a second confirmation message after migrating's the panel's users until complete.



Troubleshooting

If any part of the migration fails, then the entire migration fails. After a failed migration, click the Logs tab to check for error messages.



Note: If you need to save the log for investigation, copy and paste the contents of the log into Wordpad (for example).

Database utilities

Refer to the following pages for database-related tasks:

- Creating: See “Creating the database” on page 118 for details about the Create Security Commander Database utility to create the databases.
- Removing: See “Removing the database” on page 118 for details about the Remove Security Commander Database utility.
- Backing up: See “Backing up databases” on page 91 for details about the Security Commander Database Maintenance utility.
- Restoring: See “Restoring Security Commander databases” on page 95 for details about the Security Commander Database Maintenance utility.

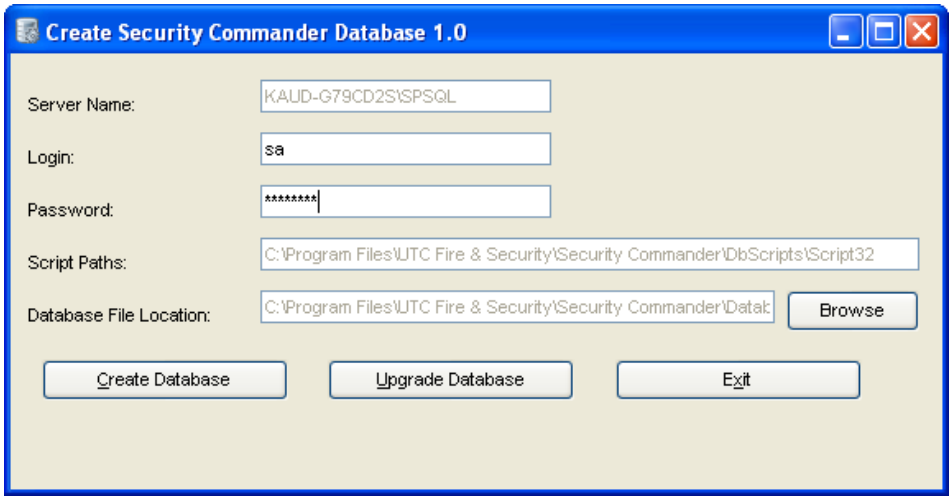
- Updating: See “Updating the database” on page 119 for details about using the Create Security Commander Database utility to update the databases.
- Changing passwords: See “Changing the “sa” password” on page 109 for details about changing the password for the SQL user “sa”.

Creating the database

The Create Security Commander Database utility (CreateA8K3DB10.exe) is used during the initial installation of Security Commander and is described in the *Security Commander Installation Manual*. If installing on a server computer, the Create Security Commander Database application runs automatically to create the database.

You can manually run the Create Security Commander Database application via the Start > All Programs > Tecom > Security Commander > Database Tools command.

Figure 24: Create Security Commander Database window

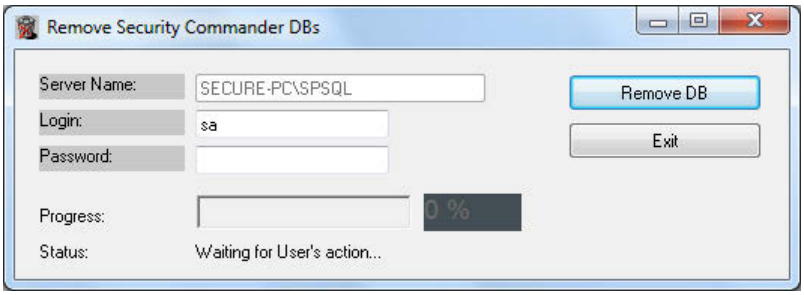


Removing the database

The Remove Security Commander Database utility (RemoveDB.exe) is used only when it is necessary to uninstall Security Commander and is described in the *Security Commander Installation Manual*.

Remove Security Commander Database may be launched via the Start > All Programs > Tecom > Security Commander > Remove Database command.

Figure 25: Remove database



Updating the database

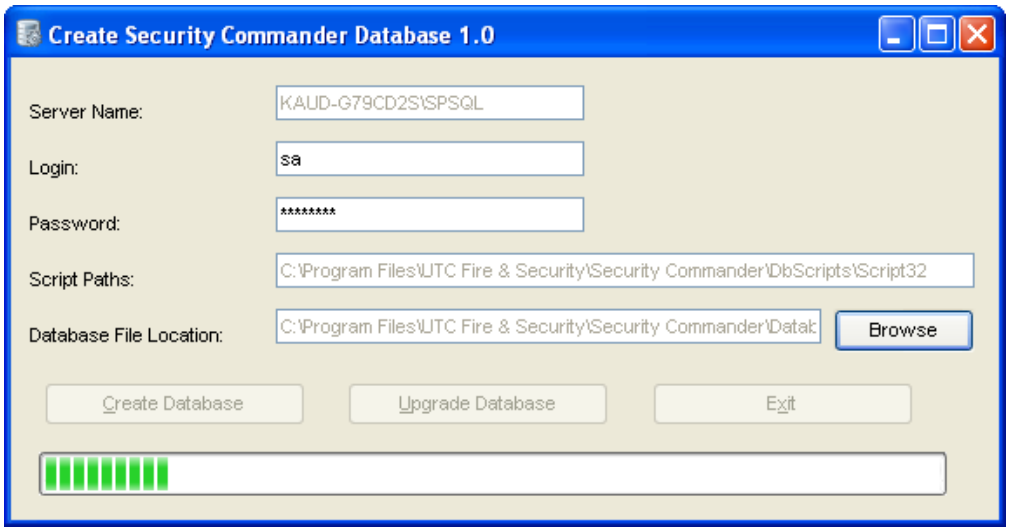
Later Security Commander releases may have different database schemas (different versions of one of more databases and their tables).

When updating Security Commander 1.85 or 1.91 without removing the databases, you can update the databases to the new version.

To convert the databases from an earlier version to a later version:

1. Run the Create Security Commander Database application via the Start > All Programs > Tecom > Security Commander > Database Tools command to open the Create Security Commander Database window (Figure 24 on page 118).
2. Type the database login “sa”, and then type the password (the password displays as *****). Click Upgrade Database to continue.
3. Create Security Commander Database creates the databases and defaults. This will take several minutes and progress may appear to stop. Please be patient.

Figure 26: Create Security Commander Database window



4. Create Security Commander Database displays a confirmation message.
5. Click OK to continue, and then click Exit to close the Create Security Commander Database window.

System administration utilities

Refer to the following pages for administration tasks:

- If you need to change the server name for the server or a client, use the SpInitClient utility (see “SpInitClient.exe” on page 120).

- If you have upgraded Windows on the server or a client, and you do not want to uninstall and reinstall Security Commander, you will need to reset the DCOM permissions and the Firewall exceptions, and then use the SpInitClient utility (see “SpInitClient.exe” below).
- For troubleshooting only, you may need to force shut down the Security Commander services — use the SPStop utility (see “SPStop.exe” on page 122).

SpInitClient.exe

Use the SPInitClient utility (SPInitClient.exe) to:

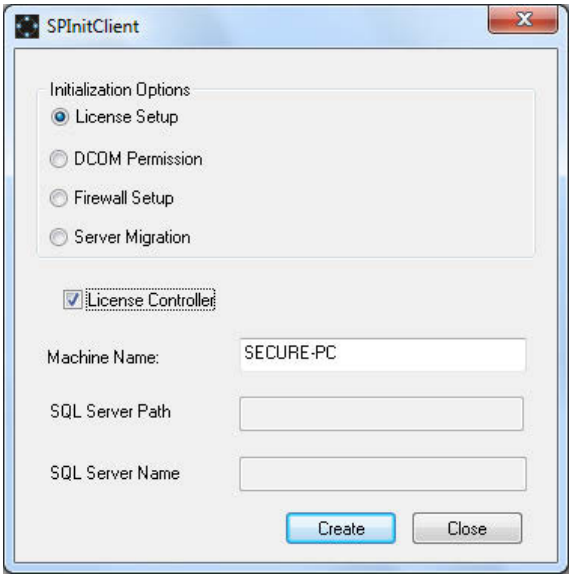
- Change the name of the Security Commander server computer on either the server or on a client (server computer name is normally corrected during Database restore).
- Create the required DCOM permissions and firewall exceptions to resolve connection problems.

Changing the server name

Use the SPInitClient utility when the Security Commander server computer has its name changed or when Security Commander server is moved to a different computer.

To change the name of the server computer in the Security Commander database:

1. Shut down the Security Commander client application.
2. Stop Security Commander services.
3. Run the SPInitClient utility located in (typically) C: \Program Files\UTC Fire & Security\Security Commander\.



4. Select License Setup.
5. Verify that the name of the Security Commander server computer is displayed in Machine Name.

Note: If the entered name is that of an existing registered Security Commander client, running this utility will not change it to the license controller.

6. Select License Controller and then click Create. This will update the Security Commander database, setting the entered name to be the current license controller server.

   Note: Clear License Controller and then click Create to reconfigure an existing Security Commander client computer when the Security Commander server computer has its name changed or when Security Commander server is moved to a different computer.

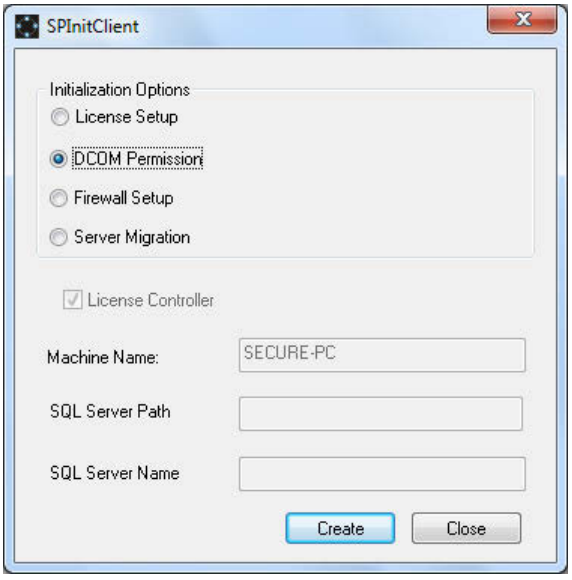
7. Click OK on the subsequent window and exit SPInitClient.

Setting the DCOM permissions

Use the SPInitClient utility to configure the required DCOM Services permissions for Security Commander.

To set up DCOM permissions:

1. Shut down the Security Commander user interface.
2. Stop Security Commander services.
3. Run the SPInitClient utility located in (typically) C: \Program Files\UTC Fire & Security\Security Commander\.



4. Select DCOM Permission and then click Create. This will ensure that the DCOM Services are correctly configured.
5. Click OK on the subsequent window and exit SPInitClient.

Resetting the Firewall exceptions

The process is similar to the previously described options, and adds the required rules and exceptions to Windows Firewall.

SPStop.exe

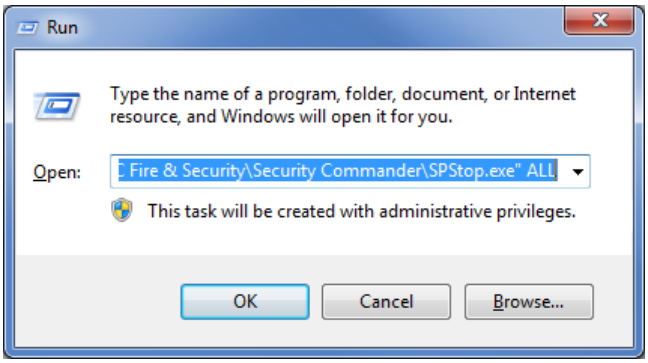
The utility SPStop.exe is used to shut down Security Commander services when they will not shut down from the Services window.

Note: Only use SPStop.exe to shut down Security Commander services when they do not shut down normally.

Click Start, and then click Run. At the Run window, browse to: Program Files\UTC Fire & Security\Security Commander\SPStop.exe

Click Open to display the file name in the command line of the Run window, add the argument All, and then click OK. Your display should look similar to the following.

Figure 27: Run window



Importing user data via CSV file

Select “Import Users” from the Personnel menu to import users, badges, and images, via a (comma separated values) file.

To import users:

1. Click “Browse...” to find and select a CSV file (the CSV file and the user image files must be stored in the same location).
2. Click “Start Import” to begin processing the CSV file.
3. Check the progress and look for errors in the Import log window.

Tip: Click the “ImportStatus” column heading to sort records into “Success” and “Fail” states.

The user data must be in one row per user and contain the following 28 fields, separated by commas, in the order listed below:

1. Facility
2. Last Name
3. First Name
4. Middle Name 1
5. Middle Name 2

6. Employee ID
7. Personnel Type
8. Department
9. Address 1
10. Address 2
11. Address 3
12. Address 4
13. Telephone
14. Profile Description
15. Photo (image file name)
16. User Field 1
17. User Field 2
18. User Field 3
19. User Field 4
20. User Field 5
21. Badge Group
22. Site Code
23. Badge Number
24. Card Data (required only for user-defined Badge Groups; same format as Titan and Forcefield, for example, 27.0.0.0.0.0.1).
25. PIN
26. Badge Status
27. Issue Date
28. Expiry Date

Glossary

24-hour alarm	Input types (5, 29, 33, and 59) that will generate an alarm regardless of area status (armed or disarmed).
Access	The condition of an area or building when it is occupied and when the security system has been set so that normal activity does not set off an alarm.
Access alarm	An input type where an unsealed state generates an alarm even though its area is in access (disarmed). For example, a holdup button.
Access control	The control of entry to, or exit from, a security area through doors.
Access groups	Alarm Groups, Door Groups, and Floor Groups assigned to a person.
Access rights	Determined by the access groups assigned to a person.
Access test	A defined interval during which specific inputs may be tested to see if they are operating correctly (without generating an alarm) when the area is in access (disarmed).
Access time	The time that a door will remain unlocked after a user has been granted access.
Acknowledge	To act on an alarm. In Security Commander, operator acknowledgments are recorded in both Operator and the Alarm History. See also reset.
Alarm	The state of a system when an input device is unsealed (activated) and the condition of the area is such that state should be signalled. For example, a PIR has detected a person in an area when the area is armed, causing a siren to sound, an alarm event to be recorded in the Challenger control panel, a message to be sent to management software, and a report to be sent to a remote monitoring company (central station). Defined via the Alarm form.
Alarm categories	Defined via the Alarm Category Setup form. Alarm categories are used in the Alarm form and the Alarm History Report to provide a means of filtering large numbers of alarms.
Alarm code	A user's full PIN code (used for alarm control) instead of a shorter door code.
Alarm code prefix	The alarm code prefix value in the range one to four enables users to enter a door code (a shorter PIN code) for access control. For example, if a user's full PIN code is six digits long (e.g. 123456), and the alarm code prefix value is two, then the first two digits are removed for access control, and the user can operate doors by entering only the last four digits of the PIN code (e.g. 3456). The PIN code must be at least five digits in length in order to use a door code. The smallest alarm code prefix value is one (the resulting door code must be at least four digits).
Alarm control	The control over alarm functions.
Alarm group	Alarm groups provide the means to control the system alarm functions (also called alarm control) for Person Profiles, Inputs, Doors, and Arming Stations. Alarm groups have areas and time zones, menu options, and panel options. Alarm groups are assigned to Person Profiles, and therefore to each piece of equipment the Person Profile uses to perform functions.

Alarm instructions	Defined via the Alarm Instructions form.
Alarm reporting	A procedure to transmit alarm events or other events to a remote monitoring company (central station) and a set of rules called a protocol.
Anti-passback	Anti-passback controls whether user credentials can be used to enter a defined region twice in succession. Entering a region twice in succession is either prohibited (hard anti-passback), or will only result in the anti-passback violation being reported (soft anti-passback). This functionality requires the use of an Intelligent Access Controller.
APB	See Anti-passback.
API	Application Program Interface. The interface between Security Commander and external applications.
Area	A section of a building which has specific security requirements. The Challenger control panel allows a building to be divided into 16 areas of differing security requirements. Each area is identified by a number and name, for example: 1. Office, 2. Workshop, 3. Boardroom.
Arm	See Secure.
Arming station	See RAS.
Auto reset	The auto reset function enables the Challenger control panel to automatically reset alarms. It is typically used for specified areas, and during specified times (for example, at night), each of which is determined by an alarm group.
Auto secure / access	Time zones are used to automatically arm and/or disarm areas. Areas being armed or disarmed automatically do not require any operator action.
Badge	A badge (card) identifies a person to Security Commander. A badge typically has a unique identity number consisting of a badge number and site code. The information to identify a user can also be available on a magnetic strip, a bar-code, a Wiegand card, or in a chip (smart card). In Security Commander, the term ‘badge’ also applies to a PIN because a badge does not have to be a physical device; it can be a PIN only.
Badge groups	Use the Badge groups tab on the Controller Setup form to add or remove badge groups that the controller will use. Defined via the Badge Groups Setup form
Badge learn	Using a badge learn device enables an unknown badge’s raw data to be entered into the Badge Setup form by presenting the badge to a badge learn device, and then clicking the Learn button to launch the Learn Badge Data form.
Battery	Backup power to prevent system failure in case of mains power trouble.
Battery test	Periodic test of the Challenger control panel’s or DGP’s battery to ensure proper functioning.
Burglar alarm	An alarm triggered by a security device like a PIR or door contact, indicating someone has entered without authorised access. May also be referred to as an intrusion alarm.
Camera	Defined via the Camera form.
Card	See Badge.
CCTV alarms	Defined via the CCTV Alarms form.
Central station	See Remote monitoring company.
CID	Ademco Contact ID reporting format.

Control (or controller) panel	An electronic device that is used to gather all data from inputs on the premises. Depending on programming and status of areas, it will generate alarm signals. If required, alarms and other events can be reported to a remote monitoring company. Defined via the Controller Setup form.
Deisolate	When used in relation to an input device: the input is no longer isolated and can report sealed, unsealed, or tamper conditions to the system. See also unsealed, sealed, isolate.
DGP	Data Gathering Panel. An electronic device that collects data from other security devices within a system, and transfers it to the Challenger control panel. Also includes Intelligent Access Controllers, as in “four-door DGP”.
Dial-up	See modem.
Disable	The equipment is set NOT to function as per its primary function. Events will NOT be reported as specified.
Disarm	See access.
Door	Defined via the Doors Setup form.
Door code	An optional version of the user’s PIN code shortened by the number of digits specified in the alarm code prefix digits. The door code is used for access control (for example, to open a door) without potentially revealing the entire PIN code used for alarm control. A door code must be four digits or more. See also alarm code.
Door contact	A magnetic contact used to detect if a door or window is opened.
Door control	The control of doors. Part of access control features.
Door group (access group)	A Challenger control panel feature, which assigns a group of doors or lifts to a user, in order to allow access at those doors/lifts. Access to each door in a group may be restricted via a time zone. Defined via the Door Groups form.
DOTL	Door Open Too Long. A DOTL alarm can be generated if a door is left open longer than the programmed shunt time. The system can be programmed to a sound a warning beeper before the DOTL alarm. This functionality requires the use of an Intelligent Access Controller.
Download	A download is defined as a method to send information to Challenger control panels.
Dual custody	A user may need to be accompanied by another user (or by a guard) before they can gain access to a door or lift. This functionality requires the use of an Intelligent Access Controller.
Dual custody programming	When this system option is enabled, two users must enter their PIN codes before access is granted to User menu 14, Program Users. (The master installer code does not require a second user.)
Duress	A situation where a user is being forced to breach the system security (e.g. forced at gunpoint to open a door). See also keypad duress.
DVMRs	Defined via the Digital Video Device form.
E/E alarms	Entry or exit alarm
Egress, Request to Exit (input)	An input that activates, or is programmed to activate, a Door Event Flag. For example, A button provided inside a door (egress button) to allow users to exit without using the door reader. Egress is also called Request To Exit (RTE).
Enable / disable doors	By default a door is enabled. When a badge is used on a card reader associated with the door, the door will open (depending on the settings in the door group). When disabled, the reader will not open the door.

Engineer	Personnel from an installer that is able to install and service the Challenger control panel.
Event flag	A signal activated by an input condition, an area condition, a macro logic output, an input shunt, or a system condition, and which activates a relay or a macro.
Event flag descriptions	This lists all Event flags programmed in the Challenger control panel, along with a description for each. Event flags are added to this list: during an Upload operation, if new Event flags are found when entering information in Security Commander, a new Event Flag will automatically be added to this list. Note: Adding descriptions to event flags improves the complete programming and maintenance process.
Extended access time	The time for the door to unlock when a user, with the "LONG ACCESS" flag enabled, presents a valid card or PIN at the door reader. This functionality requires the use of an Intelligent Access Controller.
Extensions (Challenger V8)	As of panel firmware version 8.128, the number of alarm groups, door groups, floor groups, and ‘hard’ time zones is automatically increased for panels fitted with TS0882, TS0883, or TS0884 memory expansion modules.
Facility	A grouping of database records typically used to indicate a building, location, function, and so on. Defined via the Facility form.
Floor group	A Challenger control panel feature, which assigns a group of floors to a user, in order to allow selection of those floors when accessing a lift reader. Access to each floor in a group may be restricted via a time zone. Defined via the Floor Groups form.
Floors	Defined via the Floor form.
Forced arm	Arms areas with unsealed inputs (the check for unsealed inputs is ignored). Depending on the input type, an unsealed input may cause an alarm. The option Auto-isolate unsealed inputs may be used to prevent unsealed inputs from generating alarms during forced arming.
Four-state inputs	The system’s input circuits are monitored for seal and unseal (normal and active) plus open and short conditions (reported as an input tamper alarm) based on the use of a pair of end-of-line resistors in the circuit.
‘Hard’ time zone	Clock-based time zones. ‘Hard’ time zones are valid between programmed start and end times. See also soft time zones. ‘Hard’ time zones are allocated to Challenger control panel functions to control the activity of that function by time and day and are primarily used to restrict access or to automatically arm/disarm areas.
Hardware IUM	4 MB or 8 MB memory expansion modules for a Challenger control panel and associated Intelligent Access Controllers.
History	A list of past alarm and access control events stored in memory which can be viewed on an LCD RAS (arming station), sent to a printer, or uploaded to a management software computer.
HLI	High Level Interface. An interface to control, for example, a DVR from a RAS.
Hold-up	A (silent) alarm that is triggered by a hold-up button. Normally it will not trigger any siren, only send a message to a remote monitoring company. Sometimes also referred to as Panic button.

Input	A Challenger control panel system can receive alarm signals from detection devices connected across input terminals on the Challenger panel or on DGPs. Alternatively, inputs can be logical inputs where a physical connection is not used. For example, an input can be activated by a macro logic equation. Each input device is identified by a number and text. For example, 14. Reception Holdup Button, 6. Fire Exit Door. Inputs are defined via the input Setup form.
Input shunts	An input shunt procedure isolates an unsealed input from generating an alarm during a certain time period.
Input tamper	In a system where input tamper monitoring is on, an input tamper alarm indicates that the system has detected that the input circuit has been in an open circuit or short-circuit condition. See four-state inputs.
Installer	A company that installs and services security equipment.
Intelligent Access Controller	Four-door or four-lift DGPs. Intelligent Access Controllers expand the Challenger system providing door relays, interlocking door functionality, greater system capacity, and advanced access control functionality such as anti-passback, DOTL, extended access time, and more.
Isolate	When used in relation to an input device: the input device has been isolated from indicating sealed, unsealed, or tamper conditions to the system. See also Unsealed, Sealed, Deisolate.
IUM	Intelligent User Memory. See hardware IUM and software IUM.
Key switch	A device using a switch to arm or disarm areas. The switch needs a key to switch.
Keypad	A remote arming station with keys to input data (keypad). Used to program the Challenger control panel, perform user options, view alarms, etc.
Keypad duress	When enabled, a duress code (user's alarm code + 1) can be entered on a keypad to activate a duress alarm. Keypad duress is enabled or disabled in Alarm Groups Keypad duress can be enabled or disabled for individual keypads connected to an Intelligent Access Controller.
LAN	The RS-485 data bus that connects RASs and DGPs to the Challenger control panel.
Latching alarms	When an input is programmed as a latching alarm type, alarms must be reset by an authorised user (typically via a RAS). Non-latching alarms automatically reset and report restoral when the alarm condition is no longer present.
LCD	Liquid Crystal Display. The part of a RAS (arming station) or fire panel/repeater where messages or programming details are displayed.
LCD keypad	A keypad with an LCD display.
LED	Light Emitting Diode. A light indicator on a RAS (arming station), detector, MCP, panel etc., which indicates a condition. For example: Area in alarm, communications fault etc.
Local alarm	An alarm which is transmitted only within a building, and occurs when an area is occupied. The circumstances which cause a local alarm can be checked and rectified by personnel on site and it is therefore unnecessary for the alarm to be transmitted to a remote monitoring company.

Local data bus	The local data bus (local LAN) connects DGPs and RASs to an Intelligent Access Controller. These devices are not visible to the Challenger control panel.
Lock / unlock doors	A door can be locked or unlocked. Unlocking a door will open the door until locked again by a lock command, either from Security Commander or an event that will lock the door (e.g. a time zone).
Log off	Logging off isolates the use of Security Commander. Operators need to log on before Security Commander can be used.
Log on	Logging on is required before Security Commander can be used. The default Login ID is “secure”, and there is no default password. Use the password that was entered during installation (or the new password for “secure”, if it was changed after installation).
Macro logic equation	A logic expression that combines event flags or relays in a specific manner. The result of a macro logic equation is an event flag or an input. A Challenger control panel can have 24 macro logic equations; an Intelligent Access Controller can have 48 macro logic equations.
Map relays	Map relays links relays to event flags and/or time zones. When mapped, the active event flag and/or time zone activate or deactivate the relay (which can also be an open collector output).
Mode time	The time limit for three-badge arming. For a RAS connected to a Challenger control panel, the mode time is 10 seconds. For a RAS connected to an Intelligent Access Controller, the mode time is programmable.
Modem	Modulator / demodulator. A modem enables communications between a Security Commander Client application and dial-up Challenger control panels. Modems on client Security Commander computers are allocated on the Parameters form. Control panel dial-up settings are specified on the Controller Setup form.
Normal	See Sealed.
Nuisance alarm	An alarm that is triggered by a security device, without any burglar. It could be caused by open windows, pets or incorrect projection of security equipment.
Offline	A device is not in communication with its controller. A device may be offline due to a malfunction in the device, a disconnection from the controller, or the device is not being polled by the controller. In some RAS applications, offline can mean that the RAS is connected to a controller’s Wiegand interface instead of the RS-485 data bus. Some devices, such as Intelligent Access Controllers, can continue to perform access control functions (such as granting door access to users) when offline (disconnected from the Challenger control panel).
Online	A device is considered to be online when it is connected to the controller’s RS-485 data bus and is responding to polling by the controller.
Operators	Operators are Security Commander users like installers or security personnel. Operators must be set up in Security Commander using the Operator form.
Person	A potential user of the security system. A person becomes a user when a badge is assigned via the Badge form. The Person record defines which Person Profile applies to a person.
Person	A record for a person. A person, with an assigned badge or PIN, may access the readers controlled by the system.

Person profile	Defines a set of access groups (Alarm Group, Door Group, and Floor Group), which determine the profile's access rights.
Person profile	The Person profile defines the set of access rights for a category of person. A profile is assigned to a person using the Access Rights tab of the Person form. The same profile might be assigned to many persons (for example, a 'Student' profile). When linked to a person's badge via the Badge Setup form, the profile becomes linked to a Badge Group.
PIN	Personal Identification Number. A 4 to 10 digit number given to, or selected by a user. It is necessary to enter a PIN on a system keypad as a prerequisite to performing most Challenger control panel functions. In the Challenger control panel programming the PIN is associated with a badge-person combination, which identifies the PIN holder to the system.
PIN code	A 4-10 digit number given to, or selected by, a user. It is necessary to enter a PIN code on an Advisor keypad as a pre-requisite to perform most Advisor Advanced options. In the Challenger control panel configuration the PIN code is associated with a user number, which identifies the PIN code holder to the system.
PIR	Passive Infrared detector. A security device used to detect intruders in a certain part of an area or premise. The technique used is based on infrared detection.
Poll	An inquiry message continually sent by the Challenger control panel to DGPs and RASs (arming stations). Polling allows the remote unit to transfer data to the Challenger control panel.
Privileged	A user may be assigned a user flag of privileged. A privileged user is not affected by anti-passback functionality for region numbers less than 200. This functionality requires the use of an Intelligent Access Controller.
PTZ camera	Pan-tilt-zoom camera
RAS	Remote Arming Station. A device that provides a user interface for security functions for areas or for access points (doors). The RAS may be a keypad, a reader, or other device which can be used to perform security function, such as arm/disarm, open doors, etc. Defined via the RAS Setup form.
Raw badge data	Same as raw card data (RCD)
Reader	A device used for access control that can read cards to allow access. Depending on the needs and the type of cards, the reader can for example be a magnetic swipe reader or proximity reader. May be integrated into a keypad. Also referred to as RAS, arming station, or door.
Relay	Relay or open collector output from the panel or a relay controller. Relays also refer to physical contacts that can be used to activate LED's, other relays, etc. Relays are available on all Challenger control panels, but also on many RASs, DGPs, etc. A relay can have two states: active or not.
Relay controller	A module that connects to the Challenger control panel or a DGP to provide relays or open collector outputs.
Remote monitoring company	Also called central station. A company that monitors whether an alarm has occurred in a security system. A remote monitoring company is located away from the building/area it monitors.
Reporting	See Alarm reporting.

Reset	To cancel an alarm in a Challenger control panel. A users who is authorised to arm or disarm the area in alarm, resets the alarm by arming or disarming the area. A Security Commander operator can send a Reset Ack command to the Challenger control panel. See also auto reset.
Sealed	When used in relation to an input device: the input device is NOT activated. For example: a reed switch indicates that a door is closed. See also Unsealed, Isolate, Deisolate.
Secure (arm)	The condition of one or more areas, when a change in the state of an input from sealed to unsealed will generate an alarm. Areas should be armed only when unoccupied.
Secure alarm	An input type where an unsealed state generates an alarm when its area is secure (armed) This is the default setting for inputs.
Secure test	A defined interval during which specific inputs may be tested to see if they are operating correctly (without generating an alarm) when the area is secure (armed).
SecureStream IP Receiver	SecureStream IP Receiver is an internet protocol (IP) alarm receiver designed for the Challenger system.
Shunt	A procedure which isolates an input from being activated when it is in an unsealed condition. For example, shunt stops a door generating an alarm when opened with a valid card within the time allowed.
Site number	See System code.
Smart Card	An electronic device in the form of a card or key fob that holds information to identify a user to the system. Smart cards are a type of proximity card.
Smart Card Programmer	An electronic device that is used to program smart cards. The Smart Card Programmer connects to the management software computer and enables cards (badges) to be programmed specifically for the system's users. The programmer provides a much higher level of security than can be achieved by only matching the card's serial number to a user.
Smart Card Reader	A type of RAS that communicates with a smart card presented to it.
Smart Door Controller	A single-door controller (polled as a RAS) that can operate online connected to a Challenger control panel or Intelligent Access Controller, or offline as a stand-alone device providing access for 20 users.
Soft time zone	Event-based time zones. Also called Time zone to follow relay.
Software IUM.	A programmable configuration for Challenger control panels using firmware versions 8.128 and above, that do not have 4 MB or 8 MB memory expansion modules. Software IUM enables all users to be IUM users (with 10-digit PIN codes and up to 48 bits of raw card data).
System	Can have different meanings, depending on the context. • Security Commander - A system in Security Commander is a set of one or more Challenger control panels that can be addressed all from the same system. Every Challenger control panel has a different ID, called the Computer Address. • Control panel - The Challenger control panel itself or all functions that are not related to a specific area or input.
System code	Also Site Code or Facility Code. This is a number identifying a certain batch of cards. The system code is available in the card data, together with the card number.
System data bus	The system data bus connects all DGPs and RASs to a Challenger control panel.
T&A	Time and attendance.

Tamper	A situation where an input, arming station, Challenger control panel, DGP or associated wiring are tampered with, or accidentally damaged. The Advisor Advanced tamper facility activates a signal when tamper occurs. Tamper alarms from inputs are called input tampers.
Tecom IP Receiver	Tecom IP Receiver is an internet protocol (IP) alarm receiver designed for the Challenger system.
Text variable	Used in conjunction with text words in Input Setup. A series of text words and text variables can be used to form phrases such as "Building 6 Area 4 Room 1 Door 6".
Text word	A word or phrase contained in the database and associated with a number from 1 through 999: Text words in the range 1 through 899 are predefined in the Word Library Text words in the range 900 through 999 are user-defined and added via Text Words, or automatically added by Security Commander when text is entered on a form such as Areas Setup.
Time zone (timezone)	If a Challenger control panel and the Security Commander computer are in different time zones, use the Timezone tab on the Challenger Setup Form to specify the Challenger control panel's time zone. If a Challenger Series control panel reports CID events via IP in SecureStream format, and the Challenger control panel and the central station are in different time zones, use the Time Zone selection on the Challenger System Options Setup Form to specify the Challenger control panel's time zone. See also 'hard' time zone and soft time zone.
Time zone to follow relay	A time zone to follow a relay is valid when the output is active and invalid when the output is restored. This is reversed if the output is inverted. Also called soft time zone.
Two-state inputs	The system's input circuits are monitored for seal and unseal conditions (normal and active). Open circuit and short circuit are detected as unseal. Two-state inputs use one end-of-line resistor in the circuit.
TZ (time zone)	See Time zone
Unsealed	When used in relation to an intrusion input device: the input device is activated. . For example, the state of a door's reed switch when the door is open. See also Sealed, Isolate, Deisolate.
Up/Download	A protocol providing means to view the status of the system or change parameters in the system either local or remote.
Upload	An upload is defined as a method to receive information from a controller panel.
User	Person with a badge used to gain access to places under the protection of the security system.
User authentication	The means by which a user is identified to the security system. Authentication may involve one or more of: presenting a proximity card, entering a PIN code, using a wireless remote device, or allowing appropriate hardware to read biometric factors, such as a fingerprint.
User category	User categories can be assigned to an alarm group to enable different types of users to use the timed access function on certain area/s, limit alarm control to "Arm/Reset only" on certain area/s or utilize the "User count for each area" or "Emergency" function.

User flags	When programming users in an access control system, user flags may be set for dual custody, guard, visitor, trace user, card only, privileged, and long access. This functionality requires the use of an Intelligent Access Controller.
User group	User groups define the options and permissions available to users.
User number	A controller-specific number. The same "user" (person with an assigned badge) could have a different user number at each Challenger control panel in a system.
Vault	Vault areas, when armed, are areas that will automatically arm other areas after a preset delay time.
Visitor	If a user’s record is designated as visitor, then the user’s PIN code or card must be followed by a guard’s PIN code or card in order to open a door or perform other functions. This feature applies only to doors controlled by an Intelligent Access Controller (doors 17 to 64).
Walk test	A test performed by a user or installer. To pass the test, the user or installer has to walk past detectors to activate these. The intention is to test the functionality of the security system.

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W