

Alliance 8300
EZ Edition 1.0
Professional Edition 1.0
User Manual



Copyright Copyright © 2005, GE Security Inc. All rights reserved.

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

Document number/ 1054415A (September 2005).

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

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

Trademarks and patents GE and the GE monogram are registered trademarks of General Electric.

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

Software license agreement IMPORTANT-READ CAREFULLY: This GE SECURITY End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and GE SECURITY for the software product identified in the Schedule heretoabove, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT").

By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA.

If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.

Software product license. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. Grant of license. This EULA grants you the following rights:

Application software. You may install and use one copy of the object code of the SOFTWARE PRODUCT, or any prior version for the same operating system, on a single computer. You shall pay to GE SECURITY the license fee specified in the Schedule hereto.

Storage/network use. You may also store or install a copy of the SOFTWARE PRODUCT on a storage device, such as a network server, used to install or run the SOFTWARE PRODUCT on your other computers over an internal network; however, you must acquire and dedicate a license for each separate computer on which the server SOFTWARE PRODUCT is installed or run from the storage device. The number of simultaneous logins of client SOFTWARE PRODUCTS will be limited by the server to the number stated at the time the license was purchased. A license for the server SOFTWARE PRODUCT may not be shared or used concurrently on different computers.

2. Description of other rights and limitations.

Not for resale software. If the SOFTWARE PRODUCT is labeled "Not for Resale" or "NFR", then, notwithstanding other sections of this EULA, you may not resell, or otherwise transfer for value, the SOFTWARE PRODUCT.

Limitations on reverse engineering. Decompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation

Separation of components. The SOFTWARE PRODUCT is licensed as a single product only. Its component parts may not be separated for use on more than one computer.

Support services. GE SECURITY may provide you with support services related to the SOFTWARE PRODUCT ("Support Services"). Use of Support Services is governed by the GE SECURITY policies and programs described in the user manual, in "online" documentation, and/or in other GE SECURITY-provided materials. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to the terms and conditions of this EULA.

Software transfer. You may permanently transfer all of your rights under this EULA, provided you retain no copies, you transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades, and this EULA), and the recipient agrees to the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade, any transfer must include all prior versions of the SOFTWARE PRODUCT. You must notify GE SECURITY in writing, of any transfer, and the name and address of the new recipient, as well as provide to GE SECURITY's satisfaction confirmation of the acceptance by the transferee of the terms of this EULA.

Termination. Without prejudice to any other rights, GE SECURITY may immediately by notice to you terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component Parts, and provide evidence to GE SECURITY's satisfaction of evidence that such copies have been destroyed.

3. Upgrades. If the SOFTWARE PRODUCT is labeled as an upgrade, you must be properly licensed to use a product identified by GE SECURITY as being eligible for the upgrade in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

4. Copyright. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, and text incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned exclusively by GE SECURITY or its suppliers, and no such rights are transferred to you. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material except that you may install the SOFTWARE PRODUCT on a single computer provided you keep the original solely for backup or archival purposes. You may not copy the printed materials accompanying the SOFTWARE PRODUCT.

EXCEPT AS EXPRESSLY PROVIDED ABOVE, THE LICENSED PRODUCT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND, EXCEPT AS EXPRESSLY PROVIDED ABOVE, YOU ASSUME THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LICENSED PRODUCT.

5. US government restricted rights. The SOFTWARE PRODUCT and documentation are provided with RESTRICTED RIGHTS. If you acquired this product in the United States, this EULA is governed by the laws of the state of Oregon. Any notices to be given by you in connection with this EULA are to be given as follows:

GE SECURITY
12345 SW Leveton Drive, Tualatin, OR 97062
Attention: Director of Legal Services

If this product was acquired outside the United States, then local law may apply.

6. Limited warranty. GE SECURITY warrants that (a) the SOFTWARE PRODUCT will perform substantially in accordance with the accompanying written materials for a period of one (1) year from the date of receipt, and (b) any Support Services provided by GE SECURITY shall be substantially as described in applicable written materials provided to you by GE SECURITY, and GE SECURITY support engineers will make commercially reasonable efforts to solve any problem issues in the most current release of the SOFTWARE PRODUCT and the prior major release of the SOFTWARE PRODUCT. Those reasonable efforts do not represent or warrant that such problem issues can or will be corrected or worked around. If the problem is determined by GE SECURITY to be of GE SECURITY's customer or your origin, the customer or you will pay GE SECURITY's then standard charge for work performed in responding to the problem. Modification or integration of other components not approved in writing by GE SECURITY voids or limits the warranty. To the extent allowed by applicable law, implied warranties on the SOFTWARE PRODUCT, if any, are limited to one (1) year.

7. Customer remedies. GE SECURITY's and its suppliers' entire liability and your exclusive remedy shall be, at GE SECURITY's option, either (a) return of the price paid, if any, or (b) repair or replacement of the SOFTWARE PRODUCT that does not meet GE SECURITY's Limited Warranty and which is returned to GE SECURITY. This Limited Warranty is void if failure of the SOFTWARE PRODUCT has resulted from accident, abuse, or misapplication. GE SECURITY does not warrant that the operation will be error free. Any replacement SOFTWARE PRODUCT will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Neither these remedies nor any product support services offered by GE SECURITY are available without proof of purchase from an authorized source.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, GE SECURITY AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT, WITH REGARD TO THE SOFTWARE PRODUCT, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES.

8. No other warranties.

9. Limitation of liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL GE SECURITY OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF GE SECURITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, GE SECURITY'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS EULA SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU TO GE SECURITY FOR THE SOFTWARE PRODUCT.

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

Regulatory



Contents

	Preface	1
	Conventions used in this document	2
	Safety terms and symbols	2
Chapter 1.	Introduction	3
	Product overview	4
	Key concepts	5
	Badge groups	5
	Controller setup	6
	Person profiles	7
	Persons	7
	Badges	7
	Facilities	7
	Event-triggered video	8
	References and related documentation	9
	Other manuals	9
	Online help	10

Chapter 2.	Setting up Alliance 8300	11
	Before you begin	12
	Tasks to be performed	13
	Starting Alliance 8300	14
	Accessing help	15
	Adding an operator	15
	Defining facilities	16
	Setting system parameters	18
	Control panel connections	18
	Setting up a network connection	19
	Prerequisite data — Alliance 8300 computer	20
	Prerequisite data — control panel	20
	Prerequisite data — universal interface	21
	Setting up the universal interface	21
	Setting up Alliance 8300	22
	Using encryption keys	23
	Setting up a direct connection	24
	Prerequisite data — Alliance 8300 Computer	24
	Prerequisite data — control panel	25
	Setting up Alliance 8300	25
	Setting up a dial-up connection	27
	Prerequisite data — Alliance 8300 computer	27
	Prerequisite data — control panel	27
	Setting up Alliance 8300	28
	Connecting and uploading data	29
	Completion	29

Chapter 3.	Operator interface	31
	Overview	32
	Starting Alliance 8300.....	33
	Main window.....	34
	Toolbar.....	35
	Status bar	36
	Forms	37
	Using search criteria	38
	Tab pages	38
	Shortcuts	38
	Online help	39
	Main menu command reference	40
	File menu.....	40
	Search menu	43
	View menu	44
	Operations menu	44
	Personnel menu	47
	Device menu	49
	Administration menu.....	59
	Reports menu.....	61
	Window menu	63
	Help menu.....	63
Chapter 4.	System parameters	65
	Overview	66
	Parameters form	67
	Settings tab.....	67
	User fields tab	68
	Address fields tab.....	69
	Communication settings tab.....	69
	Clear archive tab.....	70

Chapter 5.	Permissions, facilities, and operators	71
	Overview	72
	Creating Alliance 8300 permissions	73
	Permissions form	73
	Adding a permission	74
	Creating facilities	75
	Adding a facility	75
	Creating operators	76
	Adding an operator	76
	Managing facilities	78
Chapter 6.	Configuring devices	79
	Configuring alarms	80
	Configuring a control panel	81
	Standard alarm system programming	81
	Additional alarm system programming	83
	Using 4-door/elevator DGPs in access control system programming	83
	Configuring DVRs and cameras	87
Chapter 7.	Access rights, persons, and badges	89
	Access rights	90
	Person	90
	Person profile	91
	Badges	91
	Badge groups	92
	Master badge groups	93
	Assigning badge groups	94
	Control panel memory	95
	Learning badge data	97

Chapter 8. Controlling operations	99
Managing control panels	100
Controller utility.....	100
Monitoring badges	102
Monitoring alarms	103
Creating and using alarm maps.....	105
Alarm graphics editor	105
Alarm graphics viewer	105
Managing clients	106
Managing zones	106
Zone control	106
Zone status	106
Managing doors	107
Door/output control	107
Door/output status	108
Managing elevators	109
Elevator control	109
Elevator status	109
Managing areas	110
Area control	110
Area status	110
Managing arming stations	111
Arming station control	111
Arming station status	111
Managing DGPs	112
DGP controller control.....	112
DGP controller status	112
Managing digital video	113
Digital video viewer	113
Changing your password	113
Selecting facilities	113

Chapter 9.	Network client computers	115
	Client monitor form	116
	Client form	118
	Adding clients	118
	Modifying/removing clients	118
Chapter 10.	Reports and templates	119
	Reports	120
	Standard reports	120
	History reports	121
	External reports	123
	Templates	124
	Templates button	124
	Print preview report	124
	Print report	124
Chapter 11.	Using Microsoft Access	125
	Creating the exreport user	126
	Creating an MS access project	127
	Connecting to the database	129
	Creating a new user	131
	Setting up MS Access reports for Alliance 8300	134
	Creating an MS Access project	134
	Connecting to the database	136
	Creating an MS Access report	138
	Linking an MS Access report to Alliance 8300	142
	Launching external reports from Alliance 8300	144
	MS Access 2002 database utilities	145

Chapter 12. Database and system management	147
Overview	148
Alliance 8300 databases	149
Archiving Alliance 8300 history	150
Deleting Alliance 8300 archive history	151
Backing up Alliance 8300 and 8700 databases	154
Alliance 8300 files and settings	156
Backing up with MS Windows Backup	157
Backing up to your computer CD-RW drive	158
Restoring data from a backup	160
Restoring Alliance 8300 and 8700 databases	160
Restoring files	162
System recovery	163
Chapter 13. Diagnostics and troubleshooting	165
Turning on diagnostics	166
Creating a logfile	167
Viewing the diagnostics logs	168
Questions and answers	169
Installing Alliance 8300	169
Starting Alliance 8300	169
Using Alliance 8300	172
Hardware	177
Server-client communications	179
Uninstalling Alliance 8300	180
Appendix A. CCTV support	181
Setup and configuration	182
Digital video recorders (DVRs)	182
Appendix B. Changing the server name	183
Server name	184
Changing the name in Windows	185
Changing the name in the Windows registry	186
Changing the name in the 8300 database	187
Changing the name in ODBC	188

Appendix C. Managing passwords	193
Windows user passwords	194
Changing the secure password	194
Changing other Windows users' passwords	196
Database passwords	197
Resetting the application password	199
Procedure	200
Appendix D. Adding Windows users	201
Windows users and groups	202
Default Windows groups	202
Default Windows user secure	203
Adding Windows users	204
Assigning Windows users to groups	204
Appendix E. Alliance 8300 utilities	207
Database utilities	208
Creating the database	208
Removing the database	209
Updating the database	210
System administration utilities	212
SpInitClient.exe	212
SPDirShare.exe	215
SPShare.exe	216
SPStop.exe	217
Glossary	219
Index	221

Preface

The *Alliance 8300 User Manual* is a comprehensive guide to Alliance 8300 for both the system administrator and the installation technician to program, configure, and use the Alliance 8300 system. It supplements and expands the operator information contained in the Alliance 8300 online help and provides a level of detail required by advanced operator 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 Alliance 8300 in an existing security and access control system.

It is assumed that the security and access control system is in place and Alliance 8300 client and server computers have been installed and licensed in accordance with the *Alliance 8300 Installation Manual*.

It is further assumed that users of this manual have read and understood the *Alliance 8300 Installation Manual*.

Conventions used in this document

The following conventions are used in this document:

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

Safety terms and symbols

These terms may appear in this manual:



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



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

Chapter 1 Introduction

This chapter provides an overview of your Alliance 8300, including key concepts.

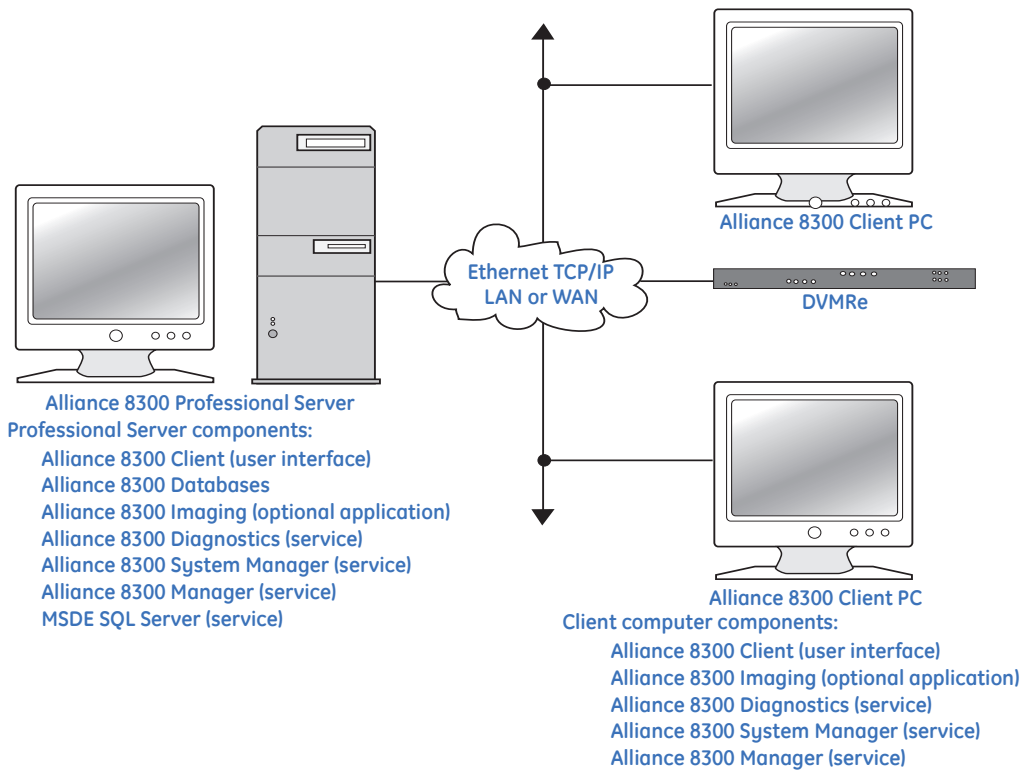
In this chapter:

<i>Product overview</i>	4
<i>Key concepts</i>	5
<i>References and related documentation</i>	9

Product overview

Alliance 8300 is a client-server security system management application with the ability to communicate over a LAN or WAN. *Figure 1* depicts the relationship between an Alliance 8300 server and remote Alliance 8300 clients.

Figure 1. Alliance 8300 Professional with two remote clients and a digital video recorder.



Key concepts

This section discusses the key concepts that you need to consider when using Alliance 8300, in particular the differences from other security management systems that you may be familiar with.

This section introduces the following concepts:

- *Badge groups* on page 5
- *Controller setup* on page 6
- *Person profiles* on page 7
- *Persons* on page 7
- *Badges* on page 7
- *Facilities* on page 7
- *Event-triggered video* on page 8

Badge groups

The purpose of *badge groups* is to provide flexibility in setting up multipanel 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).

Badge groups are based on *Badge Formats*, as listed in *Badge groups* on page 92, or custom formats. After creating a new badge group, assign the badge group to a control panel via the Badge Groups tab on the Controller Setup form.

Here's an example of how a combination of large and small control panels in the same system can be handled by managing badge groups:

- Control Panel A controls the building's main entrance and it has a memory size of **IUM large** (Intelligent User Module), which enables the control panel to handle up to 65,535 users.
- Control Panel B controls the building's administration offices and it has no memory expansion (up to 50 users). A special badge group has been created and assigned to Control Panel B named *Administration Staff*. Whenever a change occurs in Alliance 8300 to a person's record or access rights assigned to the Administration Staff,

Alliance 8300 automatically downloads (sends) the required user data to Control Panel B.

- Control Panel C controls the building's engineering offices and also has no memory expansion (up to 50 users). A special badge group has been created and assigned to Control Panel B named *Engineering Staff*. Whenever a change occurs in Alliance 8300 to a person's record or access rights assigned to the Engineering Staff, Alliance 8300 automatically downloads (sends) the required user data to Control Panel C.
- Control Panel A has been assigned the badge groups *Administration Staff* and *Engineering Staff* (among others). Whenever a change occurs in Alliance 8300 to a person's record or access rights belonging to either the *Administration Staff* or the *Engineering Staff*, Alliance 8300 automatically downloads (sends) the required user data to Control Panel A (as well as to Control Panel B or Control Panel C, as needed).

For more information see [Badge groups](#) on page 92 and [Control panel memory](#) on page 95.

Controller setup

All new Alliance 8300 control panel records are created with at least one *MASTER* badge group:

- **Master Installer** type (assigned Badge No. 50) enables a new control panel to be programmed initially.
- **Master User** type (assigned Badge No. 1) enables a new control panel to be used for access initially. The Master User type does not apply to Australian database defaults.

See [Master badge groups](#) on page 93 for details.

Before saving a new record for a control panel with *existing users*, remove the MASTER badge groups to avoid overwriting users 1 and 50. Refer to [Assigning badge groups](#) on page 94 for details.

Person profiles

Person profile records are defined in Alliance 8300 from the **Personnel | Person Profile** menu option. Person profiles control permissions. A person profile is the name given to a particular category of person (such as *Office Staff*) which share a set of access rights. Access rights are determined by up to three access groups (alarm group, door group, and floor group).

Persons

Person records are defined in Alliance 8300 from the **Personnel | Person** menu option. A *person* record contains details about a potential¹ user of the security system and assigns a *person profile* to provide the appropriate access rights.

Badges

In Alliance 8300, the term *badge* may 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 91 for more information.

Facilities

Facility records are defined in Alliance 8300 from the **Administration | Facility** menu option. We recommend 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.

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

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 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

Event-triggered video records are defined in Alliance 8300 from the **Administration | Event Trigger** menu option.

Event triggers 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.

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 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 *Alliance 8300 CCTV Operator's Guide* for more information.

References and related documentation

For more information, refer to the following documentation.

Other manuals

Alliance 8300 Installation Manual. Provides information for Integration Technicians to set up, install, and configure an Alliance 8300 system.

Alliance 8300 Imaging User's Guide. Provides instructions for users of the optional imaging package.

Alliance 8300 CCTV Operator's Guide. Provides interface instructions for CCTV equipment.

Alliance 8300 API Manual. Alliance 8300 API (Application Program Interface) provides the ability to import data from external applications such as a Human Resource Management System.

Alliance 8700 Installation Manual. Provides information for Integration Technicians to set up, install, and configure Alliance 8700 Smart Card Programmer software.

Kalatel DVMRe User Manual. Not supplied with Alliance 8300.

Online help

Alliance 8300 Online Help. Provides reference information, such as screen and field descriptions, along with instructions for system administrator duties, such as configuring Alliance panels.

Alliance 8300 License Setup Online Help. The Alliance 8300 License Setup application is used to register the Alliance 8300 License to enable communications with client computers and to enable the Image Capture and GuardDraw applications.

Alliance 8700 Online Help. Provides reference information, such as screen and field descriptions for the Alliance 8700 Smart Card Programmer software.

Image Capture Online Help. The Capture application is used to add an image or signature to a Person Form.

GuardDraw Online Help. The GuardDraw application is used to create and edit badge designs.

Digital Video Viewer Online Help. The Digital Video Viewer application is used to monitor digital video multiplexers/recorders and their associated cameras, control live video, as well as search and play back recorded video events

Digital Video Recorder Search Online Help. The Digital Video Search application is used to search for recorded video events triggered by reader and/or alarm transactions.

Diagnostic Viewer Online Help. The Diagnostic Viewer application is a diagnostic tool used to view the contents of Alliance 8300's diagnostic log files, apply filters to limit the information displayed, and search for a specific log entry.

Chapter 2 Setting up Alliance 8300

This chapter describes how to set up Alliance 8300 to a minimum degree in order to connect to a control panel and to upload data.

Once you have installed the Alliance 8300 software on the server and clients (if applicable), you will need to log onto the server computer and set a few parameters.

In this chapter:

<i>Before you begin</i>	12
<i>Starting Alliance 8300</i>	14
<i>Accessing help</i>	15
<i>Adding an operator</i>	15
<i>Defining facilities</i>	16
<i>Setting system parameters</i>	18
<i>Control panel connections</i>	18
<i>Setting up a network connection</i>	19
<i>Setting up a direct connection</i>	24
<i>Setting up a dial-up connection</i>	27
<i>Connecting and uploading data</i>	29
<i>Completion</i>	29

Before you begin

As part of the task of integrating Alliance 8300 into an existing security and access control system there are a number of issues that you'll need to consider. It will save time if you prepare or obtain this information **before** sitting down in front of Alliance 8300 and having to think about it as you come to it. The main issues are as follows:

- **Permissions** — In addition to the default, **System Administrator**, what operator permission categories will you need?
- **Operators** — In addition to the default Alliance 8300 operator login **Secure** what operators will you need? (The default Alliance 8300 operator has System Administrator operator permission.)
- **Access rights** — Access rights are defined by person profiles. In addition to the default, Master Installer Profile, what access rights definitions will you need?
- **Windows users** — See [Adding Windows users](#) on page 204 for information about setting up Windows users.
- **Facilities** — A facility is a way to organize records in the Alliance 8300 database by, for example, a location. See also [Defining facilities](#) on page 16.
- **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 are permanent and which are contractors. Alliance 8300 workstations require Imaging to be installed and licensed in order to edit badge designs.
- **Department** — Department names are used in person records and reports for sorting purposes.
- **Badge groups** — Alliance 8300 provides several default badge groups for use with control panels. It is recommended that you determine what badge groups are needed for each new control panel defined in Alliance 8300 and remove unneeded badge groups before you initially save the control panel record. Refer to the *Alliance 8300 Online Help System* for more information.

Tasks to be performed

Table 1 describes the Alliance 8300 tasks required to verify that the Alliance 8300 installation is complete and functioning correctly.

Table 1. Initial Setup of Alliance 8300

Task	Menu Form	Reference
1. Start Alliance 8300 and log on.	File Login	page 14
2. Add yourself as an operator in Alliance 8300.	Administration Operator	page 15
3. Program system parameters.	Administration Parameters	page 18
4. OPTIONAL: Create facilities.	Administration Facility	page 16 See also the <i>ALLIANCE 8300</i> online help.
5. Add the client computers to the Alliance 8300 server computer database.	Administration Client	See <i>Adding Alliance 8300 Clients</i> in the <i>Alliance 8300 Installation Manual</i> .
6. Set up client computers	Not applicable	<i>Table 1</i>
7. Connect to a control panel.	Operations Controller Utility	page 18
8. Retrieve data from the control panel.	Right-click Upload	page 29

For information on advanced setup topics see the Alliance 8300 online help.

Starting Alliance 8300

1. Select **Start | Programs | Alliance 8300 | Alliance 8300** to run the application. Alternatively, double-click the **Alliance 8300** desktop icon.



2. On the Alliance 8300 menu, select **File | Login**. Use the default Login ID *secure* and previously defined password to log on.

Note: In order to log onto Alliance 8300 from a client computer:

- You must have a valid Windows user name and password, which is part of the **AllianceGroup** local group on the Alliance 8300 server computer.
- You must have a valid Alliance 8300 operator login ID and password.
- Alliance 8300 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 Alliance 8300 running on the server computer).

Accessing help

To access the online Help, press the F1 key. Alternatively, select **Help | Help Topics**. from the menu bar.

Note: You do not have to be logged on to access Help.

Adding an operator

Add yourself as an operator in **Alliance 8300**. This will allow **Alliance 8300** to record the steps you take in setting up the system.

To add yourself as an operator in Alliance 8300:

1. Select **Administration | Operator**.
2. Select **File | New Record**. The Operator Form displays in edit mode (the Save Record command is enabled).
3. Add your details to the Operator Form. The only permission available initially is the default **System Administrator** permission.

For detailed information about setting up an operator, refer to the *Alliance 8300 Administrator's Guide* or the online help.

4. Save the Operator Form, log off, and then log on as the new operator.

Defining facilities

The Alliance 8300 database can be partitioned and related records can be grouped. In Alliance 8300, 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.

We recommend 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.

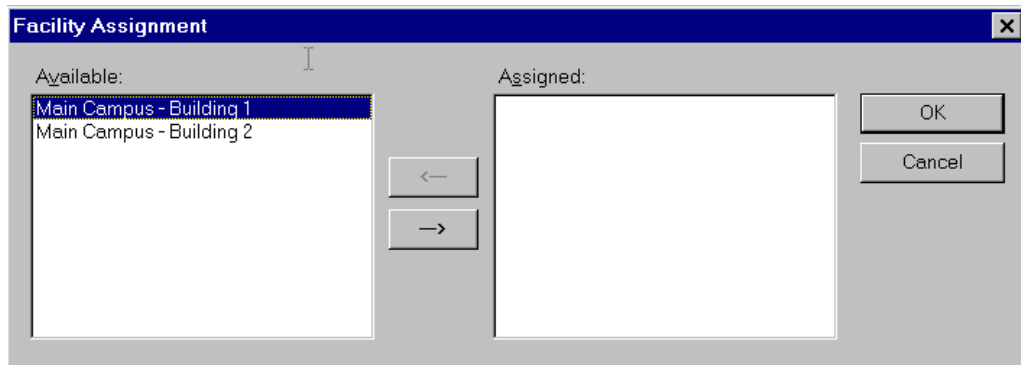
Operators can be assigned to one or more facilities and can choose which facilities to be active at any given time. Usually, the system administrator is assigned to all facilities. All records have the default *Ignore Facilities*, which means the records are not under facility protection; therefore,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

For more information about setting up a facility, refer to the *Alliance 8300 Administrator's Guide* or the Online Help.

You can assign more than one facility to an operator. To assign this operator to a facility, do the following:

1. Select **Administration | Operator**.
2. Select **Search | 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**. The Facility Assignment dialog displays (*Figure 2* on page 17).

Figure 2. Facility Assignment



In the example in *Figure 2*, 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 example in *Figure 2*, the facility **Main Campus – Building 1** now displays in the **Assigned** column.
9. Select **File | Save Record** to save the changes.

Setting system parameters

System settings for Alliance 8300 are determined by the Parameters Form. On the Parameters Form, you can specify:

- To archive history on a specific time interval, such as daily, weekly, or monthly.
- 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.
- To identify which modems will be used with Alliance 8300.

Note: For the changes on the Parameters Form to take effect, you MUST save the change and then stop and restart the Alliance 8300 services. The easiest way to do this is to restart the computer.

For more information on these items, refer to the *Alliance 8300 Administrator's Guide* or the online Help.

Control panel connections

When an Alliance 8300 computer is connected to a controller (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 an Alliance 8300 controller record.

Note: When creating controller records, it is recommended to avoid using a host computer that is likely to have its computer name changed. Any Alliance 8300 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 Alliance 8300 computer may be connected to a controller in the following ways:

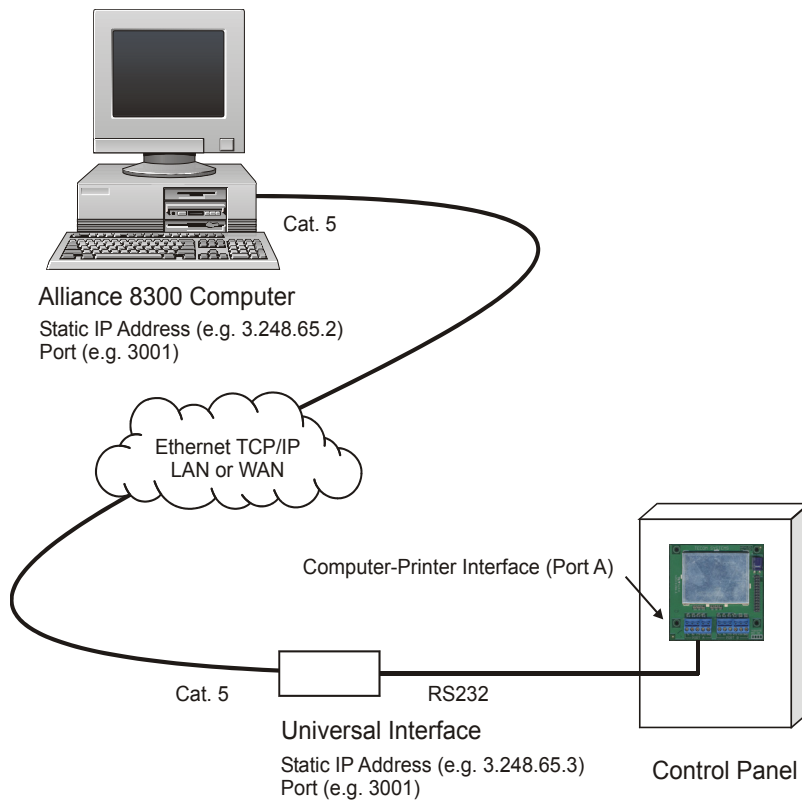
- Network (Ethernet) connection to 8- or 16-area control panels. See [Setting up a network connection](#) on page 19 for details.
- Direct connection. See [Setting up a direct connection](#) on page 24 for details.
- Dial-up connection via modem. See [Setting up a dial-up connection](#) on page 27.

Setting up a network connection

An 8- or 16-area Alliance control panel fitted with a suitable Ethernet adaptor such as the CA1806 Universal Interface can be connected via Internet Protocol (IP) to the Alliance 8300 computer via a LAN or WAN to provide control and upload and download capabilities.

Note: The CA1806 Universal Interface supports IP connection up to 10 Mbps. The Universal Interface cannot be used with a 4-area Alliance control panel.

Figure 3. Ethernet connection via CA1806 Universal Interface and CA1801 Computer-Printer Interface



The 8- or 16-area Alliance control panel must be fitted with the following devices to provide a network connection:

- AL-1801 Computer-Printer Interface is fitted to the Alliance control panel.
- AL-1806 Universal Interface connects to the RS232 port A on the AL-1801 Computer-Printer Interface. The AL-1806 Universal Interface has an RJ45 Ethernet port for network connection.

In addition to providing a network connection between the Alliance 8300 computer and an Alliance panel, the AL-1806 Universal Interface has a web interface to enable programming of the Alliance panel's communication settings. This web interface may be accessed via Internet Explorer on the Alliance 8300 computer.

Prerequisite data — Alliance 8300 computer

You need the following details about the Alliance 8300 computer:

- IP address.
- port number.

The network administrator may need to provide these details.

The Alliance 8300 computer must be connected to the network (for example, the network is visible to the Alliance 8300 computer's web browser).

Prerequisite data — control panel

You need the following details about the control panel:

- Model (for example, AL-40X7)
- Memory size (for example, IUM Large)
- Computer address (for example, 27)
- Password (for example, 0123456789)
- Encryption Key (if used). See *Using encryption keys* on page 23 for details.

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

If the password displayed in the Password field of the Controller Setup form is not correct, you must change the password in the Computer Connections Setup form. Refer to *Alliance 8300 Online Help* for details.

Prerequisite data — universal interface

You need the following details about the universal interface:

- Port number (for example, 3001)
- IP address
- User name
- Password

The Universal Interface must be connected to the network. You should see *Welcome to the Universal Interface* after you enter the Universal Interface's IP address at the browser's address bar (for example, <http://3.200.65.201/>) on the Alliance 8300 computer.

Setting up the universal interface

See the *AL-1806 Universal Interface Installation and Programming Guide* for details about installing and programming the Alliance panel's Universal Interface.

Use the following process to set up a network connection between the Alliance 8300 computer (the Universal Interface uses the term 'central station') and a Universal Interface connected to an Alliance control panel.

Configure the universal interface to accept commands from the Alliance 8300 computer.

1. Log onto the universal interface by entering its IP address in a web browser.
2. In **Central Station Parameters**, for one of the station numbers 4 through 10, specify a single Alliance 8300 computer's parameters for:
 - IP address
 - protocol (select **UDP**)
 - port number
 - data type (select **Event**)
 - Event type (select **Computer event only**)
 - Encryption key (if used).

Note: Station numbers 1, 2, and 3 are reserved for other uses such as SecureStream. Use only station numbers 4 through 10 for Alliance 8300.

3. Click the **Submit** button to save the changes.
4. Click **Restart Communications** to apply the changes.

Setting up Alliance 8300

Log on to Alliance 8300 and define the control panel.

1. In Alliance 8300, select **Device | Alliance | Setup**. The Controller Setup Form displays in search mode (the **Save Record** command is disabled).
2. Select **File | 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 [Defining facilities](#) on page 16 for details about facilities.
5. On the **Definition** tab, define the control panel. (For more information, press F1 for online 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 Alliance control panel.
8. Type the **Encryption Key** (if used) in the 16 encryption key fields. See [Using encryption keys](#) on page 23 for details.
9. If the control panel and the Alliance 8300 computer are located in different time zones, click the **Time zone** tab to select the control panel's time zone.
10. If the control panel already has existing users, click the **Badge Groups** tab, and then remove any badge groups named **MASTER Installer Type** or **MASTER Operator Type**.

Note: Failure to remove badge groups named **MASTER Installer Type** or **MASTER Operator Type** prior to saving a new control panel record may result in overwriting existing users 1 and 50 with the MASTER Installer or MASTER Operator types (as applicable).

11. Select **File | 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 29 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 Alliance 8300 and the Universal 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 Alliance 8300 and the Universal Interface. This is the more secure option because unencrypted control panel data is not transmitted over the network.

Setting up a direct connection

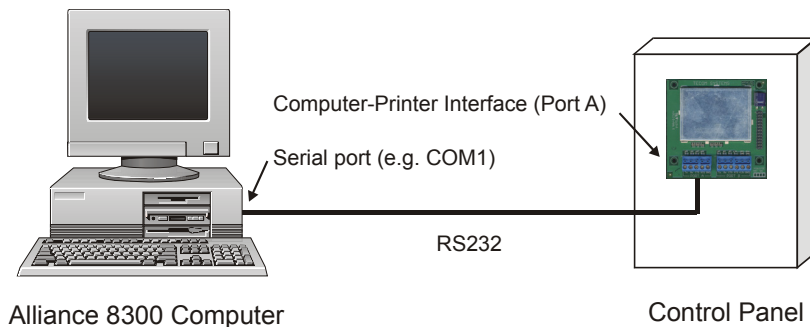
An Alliance 8300 computer may connect directly to an 8- or 16-area control panel fitted with an AL-1801 Computer-Printer Interface (not applicable to 4-area control panels). The Alliance 8300 computer's serial COM port connects to the RS232 port A on the Computer-Printer Interface.

Alternatively, a control panel's RS232 service port (J18) may be used for a temporary connection to the Alliance 8300 computer. Refer to the Alliance 8300 online help for details.

Multiple control panels may be connected to the same serial port (multidrop) by using a combination of RS485 LAN to Isolated RS232 Interfaces, such as TS0894. 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 Alliance 8300 computer.

Figure 4. Direct connection via CA1801 Computer-Printer Interface



Prerequisite data — Alliance 8300 Computer

You need to know the COM port number for the Alliance 8300 computer.

Prerequisite data – control panel

You need the following details about the control panel:

- Model (for example, AL-40X7)
- Memory size (for example, IUM Large)
- Computer address (for example, 27)
- Password (for example, 0123456789)

Use a RAS to interrogate the 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 direct connection between the Alliance 8300 computer and an Alliance control panel.

Setting up Alliance 8300

Log on to Alliance 8300 and define the Alliance control panel.

1. In Alliance 8300, select **Device | Alliance | Setup**. The Controller Setup Form displays in search mode (the **Save Record** command is disabled).
2. Select **File | 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 [Defining facilities](#) on page 16 for details about facilities.
5. On the **Definition** tab, define the control panel. (For more information, press F1 for online help.)
6. On the **Communications Settings** tab, click the **Communication Type** arrow and select **Serial**.
7. Under **Serial / Dial-Up**, click the **Com Port** arrow and select the port that will be used to connect to the control panel.
8. If the control panel and the Alliance 8300 computer are located in different time zones, click the **Time zone** tab to select the control panel's time zone.

9. If the control panel already has existing users, click the **Badge Groups** tab, and then remove any badge groups named **MASTER Installer Type** or **MASTER Operator Type**.

Note: Failure to remove badge groups named **MASTER Installer Type** or **MASTER Operator Type** prior to saving a new control panel record may result in overwriting existing users 1 and 50 with the MASTER Installer or MASTER Operator types (as applicable).

10. Select **File | Save Record**.

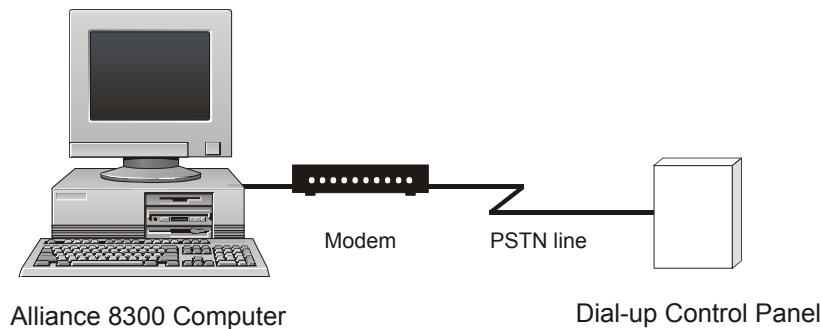
Note: Prior to connecting to a control panel for the first time you may wish to suppress the receiving of events. See [Connecting and uploading data](#) on page 29 for details.

Setting up a dial-up connection

An Alliance 8300 computer fitted with an approved modem may connect to a control panel via dial-up.

Note: If a modem is to be used to communicate with a control panel, you must manually lock the speed of the modem at 300 baud.

Figure 5. Dial-up connection via modem



Prerequisite data — Alliance 8300 computer

You need to know the telephone number of the modem that the Alliance 8300 computer will use for connecting with dial-up control panels.

Prerequisite data — control panel

You need the following details about the control panel:

- Model (for example, AL-40X7)
- Memory size (for example, IUM Large)
- Computer address (for example, 27)
- Password (for example, 0123456789)
- Phone number

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

Setting up Alliance 8300

To set up a dial-up connection between the Alliance 8300 computer and an Alliance control panel, do the following:

1. Log on to Alliance 8300 and define the Alliance control panel.
Note: You must program the modems to be used by the Alliance 8300 system in the **Parameters Form | Communications Setting** tab, and then restart the server for the settings to take effect. Refer to the *Alliance 8300 Online Help System* for details.
2. In Alliance 8300, select **Device | Alliance | Setup**. The Controller Setup Form displays in search mode (the **Save Record** command is disabled).
3. Select **File | New Record**. The Controller Setup Form displays in edit mode (the Save Record command is enabled).
4. Type a description (a name) to identify the control panel.
5. Click the **Facility** arrow and select the facility that the control panel will belong to. See [Defining facilities](#) on page 16 for details about facilities.
6. On the Definition tab, define the control panel. (For more information, press F1 for online help.)
7. On the Communications Settings tab, click the **Communication Type** arrow and select **Dial-Up**.
8. On the Dial Settings tab, type the phone number of the dial-up control panel.
9. Select other dial settings options as needed. (For details, press F1 for online help.)
10. If the control panel and the Alliance 8300 computer are located in different time zones, click the **Time zone tab** to select the control panel's time zone.
11. If the control panel has existing users, click the **Badge Groups tab** and remove any badge groups named *MASTER Installer Type* or *MASTER Operator Type*.
Note: Failure to remove badge groups named **MASTER Installer Type** or **MASTER Operator Type** prior to saving a new control panel record may result in overwriting existing users 1 and 50 with the MASTER Installer or MASTER Operator types (as applicable).
12. Select **File | 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 29 for details.

Connecting and uploading data

Use the following process to upload (retrieve) a database from a control panel for the first time.

1. Select **Operations | Controller Utility**. The Controller Utility Form displays with the new control panel listed.

Note: Suppress receiving events from the control panel until **after** uploading the full database. This enables Alliance 8300 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 control panel in the Controller Utility Form and **clear** the **Accept Events** option to suppress receiving events from the control panel.
3. Right-click the Alliance control panel in the Controller Utility Form and select **Set Online**. Alliance 8300 initiates communication with the Alliance control panel. After communication has been established, the status field displays **Connected**.
4. Right-click the Alliance control panel in the Controller Utility Form and select **Upload | Full Database** to copy the entire database from the Alliance control panel into Alliance 8300. (If the Alliance control panel is new, the panel default settings will be copied.)

Note: Badge records and person records are not uploaded.

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 control panel and uploading data, you have verified the operation of Alliance 8300.

This concludes the installation process.

Chapter 3 Operator interface

This chapter describes the Alliance 8300 work spaces and the methods of selecting operator commands.

In this chapter:

<i>Overview</i>	32
<i>Starting Alliance 8300</i>	33
<i>Main window</i>	34
<i>Toolbar</i>	35
<i>Status bar</i>	36
<i>Forms</i>	37
<i>Main menu command reference</i>	40

Overview

The Alliance 8300 login ID identifies an *operator*, and every operator has assigned permissions to use various Alliance 8300 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.

In addition to possible restriction over menu options, an operator's use of Alliance 8300 may be further restricted by the application of facilities. For example, an operator responsible for facilities A and B will not see control panels, devices, or various transactions associated with facility C.

The use of permissions and facilities enables an Alliance 8300 operator to work with **only** the items that may require the operator's attention.

Starting Alliance 8300

1. Select **Start | Programs | Alliance 8300 | Alliance 8300** to run the application. Alternatively, double-click the **Alliance 8300** desktop icon.



Alliance 8300

2. On the Alliance 8300 menu, select **File | Login**. Use the default Login ID *secure* and the assigned password to log on, or use your assigned login ID and password (if applicable).

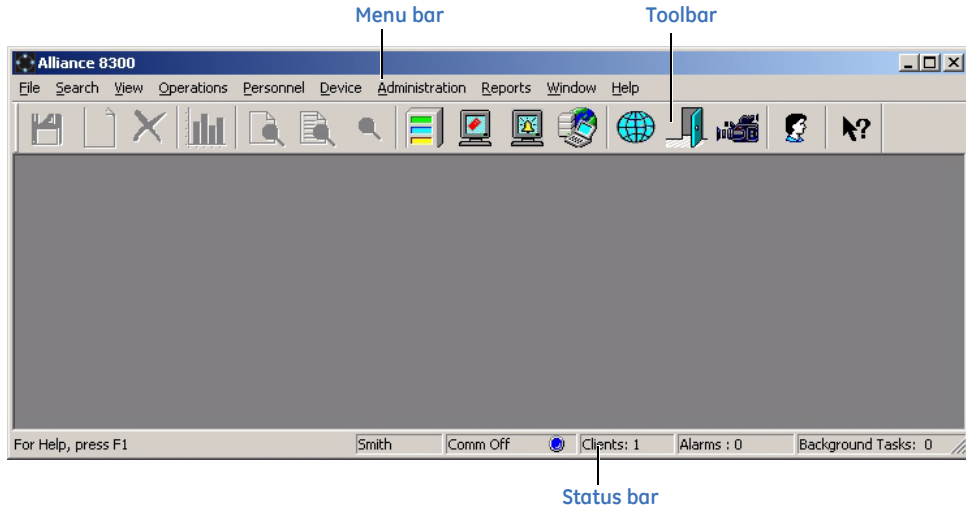
Main window

After starting Alliance 8300 and logging in, the main window displays the following items:

- Menu bar (see [Main menu command reference](#) on page 40)
- Toolbar (see [Toolbar](#) on page 35)
- Status bar (see [Status bar](#) on page 36)

The main window is shown in *Figure 6*.


Figure 6. Alliance 8300 Main Window



Toolbar

Toolbar buttons are a quick way to access commonly-used menu items. *Table 2* shows the toolbar buttons and their commands.

Table 2. Alliance 8300 main window toolbar buttons and commands

	Save record (Ctrl+S) on page 40		Badge monitor (Ctrl+B) on page 44
	New record on page 40		Alarm monitor (Ctrl+A) on page 45
	Delete record on page 41		Client monitor (Ctrl+C) on page 45
	Print preview report on page 41		Alarm graphics viewer (Ctrl+V) on page 45
	Clear search (F7) on page 43		Door/output control (Ctrl+D) on page 45)
	Recall search (F8) on page 43		Digital video viewer on page 46
	Search (F9) on page 43		Person (Ctrl+P) on page 47
	Controller utility (Ctrl+U) on page 44		Help button (click the Help button and then click the Alliance 8300 screen).

If you prefer to work without the Alliance 8300 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 Alliance 8300 system, restricted to the operator's assigned facilities.

Figure 7. Alliance 8300 Main Window Status Bar



The Alliance 8300 status bar indicates the following:

- For Help, press **F1**
- Current operator login ID (the operator in *Figure 7* is *Smith*)
- Communication port status
- Number of clients connected (for the facilities assigned to the current operator, see [Overview](#) on page 32 for details)
- Number of alarms (for the facilities assigned to the current operator, see [Overview](#) on page 32 for details)
- Number of background tasks taking place at the Alliance 8300 server computer. If the Status Bar indicates a background task is running, do not shut down the Alliance 8300 services until the task is complete.

If you prefer to work without the Alliance 8300 status bar, in order to provide additional workspace, use the **View | Status Bar** command to hide the status bar.

Forms

Many Alliance 8300 functions involve the use of forms that have a left-hand side and a right-hand side.

Figure 8. Operator Form.

The screenshot shows the 'Operator Form' window. On the left, there are input fields for 'Login ID' (Secure), 'Name' (Default Login), 'Password' (masked), 'Permission' (System Administrator), and 'Language' (English). On the right, a table displays search results. A label 'List of records (result of search)' points to the table. A label 'Details of selected record' points to the input fields on the left. The table has three columns: Login ID, Name, and Language. The first row is selected.

Login ID	Name	Language
Secure	Default Login	English
Green	Mr. Green	English
Smith	Mr. Smith	English

Records: 3

The right-hand side of the form displays:

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

Note: 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 8* has two tabs:

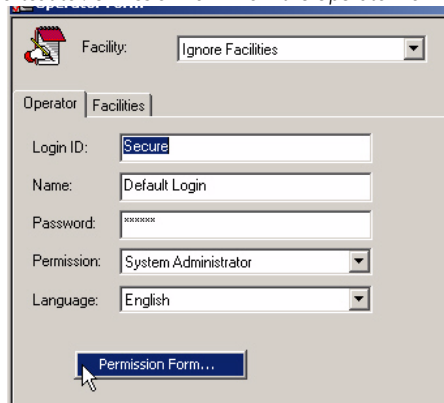
- **Operator** tab where the operator's details are recorded.
- **Facilities** tab where particular facilities are assigned to the operator.

Shortcuts

Right-click

Alliance 8300 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** has a right-click shortcut to the **Permission** form.

Figure 9. 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 control panel's devices and configuration settings.

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

Online 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 online 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 Alliance 8300 menu bar provides access to most commands.

This section is a reference to the main menu commands, as described in the Alliance 8300 online help. This section contains only summary information, please refer to the online 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 online help when using Alliance 8300, press the F1 button on your keyboard.

File menu

Save record (Ctrl+S)

Use this option to save changes made to the current record. If you do not save the changes, they will be discarded.

The **Save record** option 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.

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

New record

Use this option to create a new record and enable 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** option 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

Use this option to delete the current record. BE CAREFUL when selecting this option as deleted records cannot be recovered! The **Delete record** option is available only when a form is open and contains records, such as the Badge Form, and you have been given all permissions.

Some forms do not have a delete option.

Notes

Use this option to open 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 Alliance 8300 directory.

Log off (Ctrl+L)

The **Log off** option allows you to log off the system without exiting Alliance 8300. While logged off, no one can enter data into Alliance 8300 but it continues to communicate with the 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

Use this option to select your printer, printer properties, paper source, and orientation.

Print preview report

Use this option 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. The zoom% value will always read 100% regardless of the zoom used.

Print report

Use this option to send the current report to the currently-selected printer.

Export

Use this option 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

Use this option to save the report template under a new file name.

Set as default template

Use this option 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 option 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 option to clear the current report template

Exit

Use this option to log out the operator and shut down the Alliance 8300 client application.

Search menu

Clear search (F7)

The **Clear Search** option clears all data in the current form. Use this option when the form has data and you wish to start a new search. Note that the option 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** option 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 (F8)

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

Search (F9)

Use the **Search** option to conduct 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.

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 option is available only when a form that contains records is open, such as the Badge Form.

View menu

Toolbar

Use this option to determine whether or not the toolbar is visible across the top of your Alliance 8300 screen. This is a toggle selection.

Status bar

The **Status bar** option displays the status of the Alliance 8300 system, restricted to the operator's assigned facilities. This is a toggle selection.

See also *Status bar* on page 36.

Split

Use this option to change the horizontal size of the search results window on a form using either the mouse or the keyboard.

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

Next pane

Use the **Next pane** option to move the cursor between the main form, the tabs and the search results window, if there is one.

Operations menu

Controller utility (Ctrl+U)

Use this option to monitor communications, control and program the control panel.

Badge monitor (Ctrl+B)

Use the **Badge monitor** option to monitor badge activity.

Alarm monitor (Ctrl+A)

Use the **Alarm monitor** option to monitor alarm activity.

Client monitor (Ctrl+C)

Use the **Client monitor** option to obtain client information such as client type, Imaging status, and connection status.

Alarm graphics editor

Use the **Alarm graphics editor** option to add icons on graphical map views to point out the location and type of incoming alarms. You cannot create a map using Alliance 8300; create it using the program of your choice and save it in a .WMF or .EMF format.

Alarm graphics viewer (Ctrl+V)

Use the **Alarm graphics viewer** option to view the maps of your facility that were created. These maps point out the location and type of incoming alarms.

Zone control

See [Zone control](#) on page 106 for details about this command.

Zone status

See [Zone status](#) on page 106 for details about this command.

Door/output control (Ctrl+D)

Use the **Door/output control** option to manually open or close doors, or turn on or off outputs.

See [Door/output control](#) on page 107 for details about this command.

Door/output status

See [Door/output status](#) on page 108 for details about this command.

Elevator control

See [Elevator control](#) on page 109 for details about this command.

Elevator status

See [Elevator status](#) on page 109 for details about this command.

Area control

See [Area control](#) on page 110 for details about this command.

Area status

See [Area status](#) on page 110 for details about this command.

Arming station control

See [Arming station control](#) on page 111 for details about this command.

Arming station status

See [Arming station status](#) on page 111 for details about this command.

DGP controller control

See [DGP controller control](#) on page 112 for details about this command.

DGP controller status

See [DGP controller status](#) on page 112 for details about this command.

Digital video viewer

Use the **Digital video viewer** option to open a video command and control application that allows you to monitor digital video multiplexers/recorders and their associated cameras, control live video, as well as search and play back recorded video events.

Change password

Use the **Change password** option to change your password.

Select facilities

Use the **Select facilities** option to change the facilities currently in use.

Personnel menu

Person (Ctrl+P)

The **Person** option opens the *Person Form* which allows you to enter a person record into the system. You will enter information such as the name and address, assign access rights for access control, assign a department or user fields and even capture a photo.

Person profile

The **Person profile** defines the set of access rights for a category of person:

- Alarm Groups determine the areas, control panel commands, and control panel menu options can be used by the person profile. There may be no more than one Alarm Group per control panel assigned to a profile.
- Door Groups determine the doors (readers) that can be accessed by the person profile, and within which times. There may be no more than one Door Group per control panel assigned to a profile.
- Floor Groups determine the floors that can be accessed from an elevator by the person profile, and within which times. There may be no more than one Floor Group per control panel assigned to a profile.

Personnel type

Use the **Personnel type** option 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

Use the **Department** option to create departments which can then be assigned to person records.

Badge

A badge typically has a unique identity number consisting of a badge number and site code. However, in Alliance 8300, the term *badge* also applies to a PIN (personal identification number): a number that is entered on a RAS keypad.

See also *Badges* on page 91.

Badge groups

Badge groups tell the Alliance 8300 system which badges need to be downloaded to which control panels. Badge groups are linked to control panels via the Controller Setup Form, Badge Groups tab.

See also *Badge groups* on page 92.

Badge design

Use the **Badge design** option to create a format or design that will print on the badge.

Badge programmer

The Badge Programmer option launches the external *Alliance 8700 Smart Card Programmer* application. Alliance 8700, used in conjunction with TS0870P Smart Card Programmer hardware may be used to program user badges and reader configuration badges.

Device menu

The Device menu provides access to forms that control the following categories of devices (listed in the order that they appear in the Device menu):

- Alarms
- Digital video recorders
- Cameras
- All devices associated with an Alliance control panel.

Alarms

Use the **Alarm** option to modify the records that are automatically generated when you define a control panel.

See also [Configuring alarms](#) on page 80.

Digital video recorder

Use the Digital video recorder option to define, configure, and request status of your DVR.

Camera

Use the Camera option to edit your camera database records.

Alliance | Setup

Use this option to open the Controller Setup Form to define or edit the details of a control panel.

Alliance | Door groups

Use this option to specify when access to a specific door will be granted. Door groups are assigned to person profiles. Each door within the group may have a different time zone when access to the door will be granted.

Alliance | Floor groups

Use this option to specify when access to a certain floor will be granted. Floor groups are assigned to users. Different floor groups can have different periods (time zones) when access to the floor can be granted.

Alliance | Holidays

Use this option to enter 24 different holidays for the control panel. The holidays recorded here may be used in conjunction with time zones to control access or alarm functions. For example, staff who are allowed access during normal weekdays can be denied access on weekdays declared a holiday.

Alliance | Installer menu options

The Alliance Installer menu options are organized in the menu structure in the same order that they appear in a control panel Installer menu, accessed via an LCD RAS (Remote Arming Station).

Note: In the following sections, the text **Installer |** in the heading indicates the menu structure begins with **Device | Alliance | Installer**. Further submenu structure is not mimicked here for reasons of brevity.

Installer | Zone database

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

Installer | Area database

Use this option to record information relating to an individual area and can be programmed with a number of options, such as the area name, entry and exit times, and event flags.

Installer | Arming stations

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.

Installer | DGP

This option 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.

Installer | Alarm groups

Alarm groups provide the means to control the alarm system (also called alarm control) for person profiles, zones, doors, and arming stations.

Alarm groups have areas, menu options, panel options and time zones.

Alarm groups are assigned to person profiles, and to each door/RAS to perform functions. This provides flexibility when determining a person's access to, and control of, the system.

Installer | Timers

The Timer Setup Form is slightly different from most other windows, it is a one-off record for each control panel, for example, every Alliance 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 systemwide timers in this section.

Installer | System options

The System options menu is slightly different from most other windows in that it is a one-off record for each Alliance, for example, every Alliance has only one System options record. This function is used to record options common to the whole system.

Installer | Custom LCD message

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

Installer | Next service

Use this option to set a date and text to appear for the next routine service call.

Installer | Autoreset

Use this option to program the 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.

Installer | Computer connection

Use this option to define the control panel's setting for communications and reporting.

Communication setting must also be defined for the control panel record in Alliance 8300 via the Controller Setup Form, Communications tab.

Installer | Central station

Use this option to program all the settings for a specific central station.

Installer | Central station reporting

Use this option to program all system wide (PSTN, ISDN telephone) communication options.

Installer | Text words

Use this option to add user-defined words to the predefined Alliance word library. All words in the library are identified by a reference number. The predefined word library uses reference numbers 001 to 899, additional user-defined words use reference numbers from 900 to 999.

Installer | Time zones

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

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

There are two main types of time zones. These have the same function, except for the following:

- Hard time zones are based on defined times and dates.
- Soft time zones are based on events.

Installer | Alarm group restrictions

Alarm group restrictions restrict alarm groups arming/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.

Installer | Event to output

Use this option to set all options to link event flags to outputs.

Installer | Auto arm/disarm

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

Installer | Vault areas

Vault areas, when armed, are areas that will automatically arm other areas after a preset delay time. By using a special programming procedure, an alarm group restriction timer starts when all of the vault areas are armed. When the timer expires, a nonvault area linked to the vault areas will automatically arm.

Installer | 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 a zone. This zone 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.

Installer | Zone shunts

A shunt procedure bypasses an active zone from generating an alarm during a certain time period.

- A zone shunt is initiated when an output is activated, for example, by a door unlocking or by a keypad entry.
- During the shunt time the zone is bypassed.
- If the zone is still active after the shunt time has expired, the zone will generate an alarm, depending on the zone type and the status of the area.
- The shunt timers (16 available), may be programmed individually to control each zone shunt.
- Before the shunt timer expires, a warning may be given.
- A zone shunt stops a door generating an alarm when it's opened.

Installer | TZ to follow output

Use this option to select a time zone to follow an output. When the output is active, the time zone is valid, and when restored, invalid. This is reversed if the output is inverted.

Time zones that follow outputs are also referred to as soft time zones. Hard time zones are valid between programmed start and end-times. For example:

- To prohibit the use of a keypad, unless a keyswitch on a zone is active.
- To allow an area to be disarmed only if another area is first disarmed.

Installer | Printer

Program the details for the printer attached to the control panel.

Installer | Battery test

This option contains details regarding the battery test to be run for any battery on the Alliance system databus. All batteries are tested sequentially to prevent power problems. If a battery is disconnected for more than 10 minutes, a warning will be given.

During the battery test, the 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.

Installer | Event flag descriptions

This option lists and describes all event flags programmed in the control panel.

Installer | System event flags

Use this option to program the values of system 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: Take care not to assign Event flag numbers which are predefined (Event Flags 1 to 16) or Event Flag numbers which have been assigned by the Installer in the Zone Database, Area Database, RAS Database, or Zone Shunts.

Installer | Macro logic

Use this option to activate an event flag or a zone under specific logic conditions.

Up to four outputs or event flags can be included in the logic equation. Each output 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 zone) 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 zone and/or event flags, before attempting to program.

Installer | Clock correction

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

Installer | Class database

Reporting of alarms depends on the settings in reporting code in the zone database. This setting is a reporting class. There are 8 classes containing 6 conditions that can be selected for reporting.

The order of programming after selecting the Alliance number is:

- select the class (medical, fire etc.)
- select the reporting condition (bypass, unbypass, etc.)
- enable or disable the reporting by selecting or deselecting the central station number.

Installer | Report test

This option holds all programming for test call reporting.

Installer | System event to channel map

This is the 200 Baud FSK French communication option.

Installer | Voice reporting

Use this option to assign a voice message number from the Voice Module (AL-7200) to specified event numbers.

Installer | DVMR configuration

Use this option to configure an 8-area or a 16-area control panel for connection to a DVMRe (digital video multiplexer recorder) via a serial computer and printer interface printer port installed on the control panel.

The serial computer and printer interface must be connected to the RS-232/1 port on the DVMRe. This connection is referred to as a high-level interface (HLI).

The HLI enables security staff to operate the DVMRe via permitted RAS keypads to search for and view recorded video.

Refer to the control panel programming manual for detailed instructions.

Installer | 4-door/elevator DGP

Use this option to program DGPs associated with Alliance 4-door/elevator controllers.

Note: You must use the **Installer | DGP Setup** Form to define the 4-door or 4-elevator DGPs before using this form.

Installer | 4-door/elevator DGP | Doors

Use this option to program individual doors associated with Alliance 4-door/elevator controllers.

Installer | 4-door/elevator DGP | Elevators

Use this option to set up all elevator options for Alliance 4-elevator controllers.

Installer | 4-door/elevator DGP | Floors

This option displays the details for a floor on an Alliance 4-elevator controller. This has to be programmed before floor groups can be assigned.

Installer | 4-door/elevator DGP | Regions

Regions are used by Alliance 4-door/4-elevator controllers in combination with antipassback. Alliance 8300 also uses regions to be able to report on which region users can be found.

Installer | 4-door/elevator DGP | 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 output 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 output which may be; a pulse, timed, on delay, off delay or latched when activated.

Installer | 4-door/elevator DGP | DGP card batches

Card batches are used to provide easier programming of a range of consecutive cards into the Alliance 4-door/4-elevator controllers, while also allowing for multiple system codes.

Each of the 40 available card batches provides:

- a system code
- a number of cards
- a starting user number

Card batches are used to provide easier programming of a range of consecutive cards into the Alliance 4-door/4-elevator controllers, while also allowing for multiple system codes.

Installer | IADS DGP

Use this option to program the mode and protocol for a particular IADS (intelligent addressable device system) DGP.

Note: You must use **Installer | DGP setup** to define an IADS DGP before using this form.

Installer | IADS DGP | IADS DGP devices

Use this option to program the address, type, and other defining parameters for individual IADS DGP devices.

Installer | Wireless DGP

Use this option to program the mode and other options for a particular wireless DGP.

Note: You must use **Installer | DGP setup** to define a wireless DGP before using this form.

Installer | Wireless DGP | Wireless DGP zone sensors

Use this option to program the label code, zone data, and other defining parameters for individual wireless DGP zone sensors.

Installer | Wireless DGP | Wireless DGP fob sensors

Use this option to program the label code, button assignment, and other defining parameters for individual wireless DGP fob sensors.

Administration menu

Operator

Use the Operator option to set up individuals as users for the Alliance 8300 system and assign the facilities to which they have access.

Permission

Use the Permission option to define Operator access to various forms within Alliance 8300.

Client

Use the Client option to define a client computer.

API connections

Use this option to define records to enable external applications to interface with Alliance 8300.

Instruction

Use the Instruction option to create instructions to link with alarms. The instructions will then appear on the Alarm Monitor when the alarm occurs.

Response

Use the Response option to create a predefined response to an alarm. These responses are used on the Alarm Monitor.

Parameters

Use the Parameters option to establish settings for the entire application, such as archive intervals and appropriate modems.

Override

Use the Override option to generate a T/A (time in attendance) transaction. This information is written to history.

LogFile

Use the LogFile option to select your computer and name the LogFile, and enter the path and directory in which to place your logfile.

Diagnostic setting

Use the Diagnostic setting option to define what debug information will go to the diagnostics log. This is a good place to start for troubleshooting.

Diagnostic viewer

Use the Diagnostic viewer option to view what is 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

Use the CCTV Alarm option to link a CCTV Interface and alarm to Alliance 8300 so that the CCTV alarms will display on the Alliance 8300 Alarm Monitor.

Camera preset

Use the Camera preset option to generically define camera presets.

Event trigger

Use this option 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.

Facility

Use this option to define the desired facility, such as Building One and Building Two.

Reports menu

Refer to *Chapter 10, Reports and templates* on page 119 for additional details about reports.

Person

Use the Person report option to create a report on the people in the database. Reports may include personal information, such as address, department, badge, access rights, and user fields on all or a subset of persons in the system.

Badge

Use the Badge report option to create a report on the badges in the system.

Administration

Use the Administration report option 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.

Alliance

Use the Alliance report option to generate reports about the Alliance control panel devices in the system.

Floor access

Use the Floor access report option to create a report on the floors defined in the system and the access granted to each one.

Door access

Use the Door access report option to create a report on the persons in the system who have access to any of the specified doors or readers.

Alliance groups

Use the Alliance groups report option to generate reports about the door groups or floor groups in the system, for a selected control panel or for all control panels.

Roll call

Use the Roll call report option 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.

Alarm history

Use the Alarm history report option to create a report on the history of alarm activity.

Badge history

Use the Badge history report option to create a report on the history of badge activity.

Time and attendance history

Use the Time and attendance history report option to create a report on the history of time and attendance activity.

Operator history

Use the Operator history report option to create a report on the history of operator activity.

External reports

Use the External reports option to access an executable program or report that was not created within Alliance 8300. Navigate to the program or folder, select the file, and click Open.

Window menu

Cascade

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

Tile

Use this option to control multiple windows or forms. If you have several forms open but not visible, select this option to view all forms tiled side-by-side on your display screen.

Arrange icons

Use this option to control multiple windows or forms. If you have several forms in progress, you can temporarily minimize a form from view. Select this option to arrange the minimized form icons across the bottom of your Alliance 8300 window.

Help menu

Help topics (F1)

Use this option to launch the Alliance 8300 online help.

About Alliance 8300

Use this option to display the software version, service pack number, copyright information, and contact information.

Chapter 4 System parameters

This chapter covers how to use the Parameters Form.

In this chapter:

<i>Overview</i>	66
<i>Parameters form</i>	67

Overview

The Parameters Form will be one of the first parts of Alliance 8300 you need to use. For example,

- Before you define a 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.

Note: For the changes on the *Parameters Form* to take effect, you **MUST** save the change and then stop and restart the Alliance 8300 services. The easiest way to do this is to restart the computer.

Systemwide (global) settings for Alliance 8300 are specified on the Parameters Form, including:

- The database archive settings (daily, weekly, or monthly).
- Whether to print badge and alarm activity and to which printers.
- 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.
- To identify which modems will be used to communicate with control panels.

Parameters form

The Parameters Form is divided into five tab pages:

- Settings
- User fields
- Address fields
- Communication settings
- Clear archive

These tab pages are described in the following sections.

Settings tab

Archive database

In the Archive Database section (*Figure 31* on page 151), select to archive history on a daily, weekly, or monthly basis.

Note: The default setting is to archive history on a daily basis. We recommend that you use the default setting. Whatever setting you choose, you must monitor the size of the Alliance 8300 history and archive databases to ensure that each database remains under 2GB 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 1 a.m.
- **Weekly.** The archive is created every week on the day you select sometime between midnight and 1 a.m.
- **Monthly.** The archive is created on the first day of the month some time between midnight and 1 a.m.

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 Alliance 8300 server is running. If it isn't, then the next time Alliance 8300 is started and a transaction is received, the archive is created.

Alarm activity printing

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 when alarms are detected. Alternatively, select Short to sound a short tone when alarms are detected.

Badge activity printing

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

Photo aspect ratio

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.

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 5 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 client computers for communicating with dial-up control panels.

Clients list

Select a client computer in the *Clients* list.

Available modems

Available modems lists all the registered modems for the selected client computer. Click to select one or more modems to enable them to be used by Alliance 8300 (running on the selected client) to connect to a 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 client 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 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 Alliance 8300 when idle.

Clear archive tab

The Clear Archive tab is depicted in *Figure 32* on page 152.

Earliest date in current archive DB

If you have an archive database, this date will display when you click **Show Date**.

Latest date in current archive DB

If you have an archive database, this date will display when you click **Show Date**.

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.

Chapter 5 Permissions, facilities, and operators

This chapter covers how to create permissions, facilities, and operators.

In this chapter:

<i>Overview</i>	72
<i>Creating Alliance 8300 permissions</i>	73
<i>Creating facilities</i>	75
<i>Creating operators</i>	76
<i>Managing facilities</i>	78

Overview

Before individuals can access, use, or administer the **Alliance 8300** program, they must be set up as operators. The setup sequence is as follows:

1. Alliance 8300 permissions and facilities must be created before operators.
2. When operators are set up, they must be assigned permissions and one or more facilities.
3. At any given time, an operator can choose which facilities to be active from the list of facilities available to that operator.

Note: Operators using an Alliance 8300 client computer and working over a network connection (via either a domain or a workgroup) must be logged onto the client computer's operating system using a login ID and password combination that provides appropriate access permissions to the shared folders on the Alliance 8300 server computer. Alliance 8300 installation DOES NOT create any users or permissions under the domain environment.

Creating Alliance 8300 permissions

Permissions are assigned to operators and define what operators can do within Alliance 8300. 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.

Alliance 8300 comes with a System Administrator permission that allows full action on all forms. You may wish to create more restrictive permissions and apply the System Administrator permission ONLY to those operators fully trained in Alliance 8300.

Permissions form

The Forms list on the Permissions 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, 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 Alliance 8300 program organized 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 submenus.

Four types of actions can be assigned to forms:

- **None.** No access is given to that form.
- **Read.** Read only access is given. The form and the associated records can be viewed but not modified.
- **Update.** The records on that form can be viewed and modified.
- **All.** The records on that form can be viewed, modified and deleted.
- **Mixed.** 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 Alliance 8300 in order to allow an operator to be assigned a permission other than System Administrator.

To add a permission in Alliance 8300, do the following:

1. Select **Administration | Permission.**
2. Select **File | 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 Alliance 8300 database can be partitioned and related records can be grouped. In Alliance 8300, 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.

Note: It is recommended 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.

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 Alliance 8300, do the following:

1. Select **Administration | Facility**.
2. Select **File | 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 Alliance 8300 software. An Alliance 8300 operator has a login ID and password for Alliance 8300. This login ID and password is independent of the operator's Windows account login ID and password.

Note: An Alliance 8300 operator **must** have a Windows user account before they can use the Alliance 8300 system. An identical Windows user account (with membership to the appropriate groups) must be created on **every** Alliance 8300 computer in the system (the server and all of the clients). This enables the Alliance 8300 server and client computers to communicate as a workgroup (regardless of whether an Alliance 8300 operator is logged on). Refer to [Adding Windows users](#) on page 204 for details of adding Windows user accounts.

Adding an operator

When using the Operator Form for 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 Alliance 8300. Click the Operator tab and then click the Permission arrow to select a permission from the list. Permissions are created on the Permission Form.
- Assign facilities to operator. Once assigned, the facility is added to the Facility list on various forms when that operator is logged on. Click the Facilities tab to assign a facility to a selected operator. Facilities are created on the Facility Form.

To add an operator in Alliance 8300, do the following:

1. Select **Administration | Operator**.
2. Select **File | 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 on to Alliance 8300).

4. Type the operator's name.
5. Type the operator's initial password (the operator can change this later using this form or the Operations | Change Password command). The password field displays each character as *.
6. Click the Permission arrow and select the operator's permission. The only permission available initially is the default **System Administrator** permission.
7. Click the Language arrow and select the operator's language.
8. 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.
9. Assign the required facilities to the operator.
10. 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.

Chapter 6 Configuring devices

This chapter covers how to configure devices using the forms provided by the Alliance 8300 Device menu.

In this chapter:

<i>Configuring alarms</i>	80
<i>Configuring a control panel</i>	81
<i>Configuring DVRs and cameras</i>	87

Refer to the *Alliance 8300 online help* for more details about these options.

Configuring alarms

Alarm records are automatically created by Alliance 8300 when various device records are created. For example, when a Digital Video Recorder record is created using the **Device Digital Video Recorder Form** and is given a description *Second DVR*, Alliance 8300 automatically creates alarm records for the DVR with the following attributes:

- The **Description** field displays the alarm description, for example, *DVR 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 contents of the description field for the Digital Video Recorder record.
- The **Owner type** field displays *DVMR*, which identifies the alarm owner (such as a control panel or DVR) by the generic type of device.
- The **Category** field displays the alarm category, such as *CCTV Alarm*.

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 *Forms* on page 37).

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, do the following:

1. Select the **Search | Clear Search** command 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. Select the **Search | Search** command 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 Alliance 8300 online help for further details.

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

Configuring a control panel

Note: Before saving a new record for a control panel with *existing users*, remove the MASTER badge groups to avoid overwriting users 1 and 50 in the control panel.

The process of setting up a control panel in Alliance 8300 is simplified when the control panel has previously been set up. In this case, all that's required is to define the control panel record in Alliance 8300, connect to the panel, set it online, and upload (retrieve) the panel's database for editing in Alliance 8300.

The uploaded database populates or updates the default values in the Alliance 8300 database, except for:

- User records
- Facility assignment
- Device descriptions

This process is described in the *Alliance 8300 Installation Manual*.

In cases where a new control panel is being set up, it is useful to know the most efficient sequence for programming and where in Alliance 8300 various steps are performed.

The following sections describe recommended basic and advanced setup sequences for initially programming a control panel.

Standard alarm system programming

Using the recommended programming order provides the most efficient programming and makes sure that no item is forgotten when setting up a system. It is assumed that the control panel and all required devices are connected and the database has been uploaded.

All options can be accessed via the **Device | Alliance | Setup** option (Configuration tab), except where indicated otherwise. To use the recommended programming order, do the following:

1. Gather all information like maps, where detectors are located, what areas are available, etc.
2. Set up Alliance 8300 and the control panel to communicate. This process is described in the *Alliance 8300 Installation Manual*.
3. Program control panel system options.

4. Program all names that are not in the standard word library using text words. (Alliance 8300 recognizes when new words are used and offers to create new text words automatically.)
5. Program all required time zones.
6. Program area details.
7. Program all required alarm groups.
8. Program/activate all connected RASs (arming stations).
9. Program/activate all connected DGPs.
10. Program all available or required zones.
11. Program all required communication settings and central stations for alarm reporting.
12. Set all reporting related issues in the class database.
13. In the Report Test option, program test call details.
14. Map events to outputs. Take care all event flags have a clear description.
15. Program required access rights, persons, and badges. This process is described in *Chapter 7, Access rights, persons, and badges* on page 89.

Additional alarm system programming

When the standard setup has been taken care of, additional options might be required. The following is a list of options, all of which can be accessed via the **Device | Alliance | Setup** option (Configuration tab):

- If common building entry is required for alarm control, assign more than one area to a zone, or use area linking.
- For special access (for example, cleaners) an alarm group may require restricted options.
- When timed disarm is selected in alarm group restriction, program the disarmed period.
- Program automatic arming/disarming.
- Program required system options.
- Program extensive battery testing (if required).
- Program printer settings if a printer is to be connected.
- Configure time zones that are activated by outputs.
- Program required macro logic.
- Enter the required custom message for LCD RAS.
- Program automatic reset of areas.
- Program any areas required to be vault areas.
- Program zone shunts.
- Enter the next service date details.
- Program standard access control using RAS 1 through 16 (see next section).
- Program a relay control group to each RAS (door).
- Program any required door groups (see next section).

Using 4-door/elevator DGPs in access control system programming

Using the recommended programming order for an access control system ensures efficient programming and that no item is forgotten while programming the Alliance 4-door/elevator DGP.

All options can be accessed via the **Device | Alliance | Setup** option (Configuration tab), except where indicated otherwise.

Standard 4-door/elevator DGP programming

1. On the Alliance DGP Setup Form, set the DGP address for the 4-door DGP (see *Numbering* in the Alliance 8300 online help).
2. Set addresses of RAS devices (readers or DGPs connected to the local databus of the 4-door/elevator DGP (see *Numbering* in the Alliance 8300 online help).
3. Activate polling for the 4-door/elevator DGP and set the DGP type.
4. Check in system options the dual zone setting and the number of prefix digits.
5. Program time zones required for access control functions (Request to Exit Options, Override Time Zone, and Door Groups).
6. Determine which areas will bypass Request to Exit or Access through a door when the areas are armed.
7. On the Alliance 4-Door/Elevator DGP Setup Form, program 4-door/elevator DGP options:
 - Output controllers
 - Card batches (on the DGP Card Batches form)
 - Alarm code prefix digits
 - Poll RAS devices (on local databus)
 - List RAS devices with LCD display
 - List RAS devices with Request To Exit input enabled
 - Poll DGPs (on local databus)
 - Set tamper monitoring (dual zone) option
 - Enter card to PIN time
 - Enter two card time
 - Enter multibadge time
 - Enter relock delay time
 - Enter region count limit
8. On the Alliance Doors Setup Form (Access Options tab), program the following:
 - Enter the door to program
 - Enter the unlock time
 - Enter the extended unlock time (if required)
 - Select the shunt option (if required)

- Enter the shunt time (if required)
 - Enter the extended shunt time (if required)
 - Enter the shunt warning time (if required)
 - Enter the low security time zone (if required)
 - Select if the IN or OUT reader requires badge and PIN
 - Select if PIN is required during time zone
 - Select if antipassback is required
 - Enter the IN & OUT reader region (if required)
 - Select if IN or OUT reader requires two card function
9. On the Alliance Doors Setup Form (Request To Exit Options tab), program the following (if required):
- Enter the Request To Exit time zone
 - Select the Request To Exit option
 - Select if IN or OUT Request To Exit should be disabled when armed
 - Select if Request To Exit should be reported
10. On the Alliance Doors Setup Form (Reader Options tab), program the following:
- Select the card format used
 - Select the override time zone (if required)
 - Select the LED function (if required)
 - Select if the door zone should keep the door unlocked
 - Select if the unlock time zone should only start after entry
 - Select if the door open/close should be reported
 - Select if forced opening is to be reported
 - Select if the door should be held unlocked until the door opens
 - Select if the door closed and locked is reported as locked
 - Select if DOTL (door open too long) has to be reported
 - Select if the reader is a time attendance reader.
 - Select if a pulsed lock/unlock is required
 - Select if duress is to be disabled
 - Select if closed and locked is to be reported as locked
11. On the Alliance Doors Setup Form (Hardware Options tab), program the following:

- Enter the unlock output number
 - Enter the forced output number (if required)
 - Enter the warning output number (if required)
 - Enter the DOTL zone number (if required)
 - Enter the DOTL output number (if required)
 - Enter the Request To Exit zone number (if required)
 - Enter the fault output number (if required)
 - Enter the (door) zone number
 - Select if the 2nd door zone should be monitored
 - Select the shunt zones (if required)
 - Select the interlock zones (if required)
 - Select the area/s assigned to the door (if required)
12. On the Alliance Door Groups Setup Form, program the required door groups.
 13. On the Alliance Person Profile Setup Form program the person profiles that require access control functions (door groups).
 14. Program zones available on the 4-door DGP

Additional 4-door/elevator DGP programming

Alarm control

To program alarm control functions, do the following.

1. Program time zones required for alarm control functions (used in alarm groups)
2. Program alarm groups (if required) for access control functions
3. Select the door to program (in Access options)
4. Select alarm control:
 - Enter the required alarm group
 - Select the required alarm control option
 - Select if the IN or OUT reader should deny access when the area is armed
 - Select the authorized RAS on the system databus (if required)
5. Program the alarm groups for the Person Profiles that should have alarm control.

Antipassback

For antipassback to function, readers are required to enter and exit. The reader address specifies if the reader is used as an IN (entry) or OUT (exit) reader (see *Numbering* in the Alliance 8300 online help).

To program antipassback facilities, do the following:

1. Make sure both IN and OUT readers are available and are polled.
2. Select the door to program (in Access options)
3. Program access options:
 - Select the required passback option (disabled, soft, or hard).
 - Enter the region number for the IN and OUT reader.
 - Select if the IN or OUT reader should not allow users from region 0.

Configuring DVRs and cameras

Refer to the *Alliance 8300 CCTV Operator's Guide* and the *Alliance 8300 online help* for details.

Chapter 7 Access rights, persons, and badges

A user (person with a badge) may gain access to areas, doors, or floors protected by the security system. Alliance 8300 uses a number of concepts to control access rights, persons, and badges. This chapter describes these concepts.

In this chapter:

<i>Access rights</i>	90
<i>Person</i>	90
<i>Person profile</i>	91
<i>Badges</i>	91
<i>Badge groups</i>	92
<i>Control panel memory</i>	95

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 control panel.

A **person profile** may be assigned no more than one alarm group, door group, and floor group per control panel.

For example, a department manager would require a particular set of access rights and these could be defined as a person profile record named *Department Manager*.

Alarm groups

Alarm groups provide the means to control the system alarm functions (also called alarm control). 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 that the person profile uses to perform functions.

Door groups

Door groups specify when access to a specific door or arming station will be granted. Door groups are assigned to users via the person profile.

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 users via the person profile.

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

Person

The **Person Form** is used to enter a person record into Alliance 8300 and assign access rights via a selected person profile.

Person profile

A set of access rights for a particular category of person is determined by a type of record called a *person profile*.

Note: A person profile might be used by many people, and may be linked by badge group to many control panels. As a result, any change in a person profile can result in lengthy download times.

Badges

Badge records are defined in Alliance 8300 from the **Personnel Badge** menu option.

A badge typically has a unique identity number consisting of a badge number and site code. However, in Alliance 8300, 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 control panel, the badge will be downloaded (sent) as a user to the control panel (and any associated 4-door/elevator DGP controllers), as long as the badge is *active*. As a result of this association between badges and 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 control panel.
- User numbers greater than 50 require a memory expansion module.
- User numbers above 11,466 require an IUM (Intelligent User Module) memory expansion module.
- In a system with 1 MB expanded memory, users numbers from 1,001 through 11,466 may have a badge only without a PIN.
- In a 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 control panel (although in Alliance 8300 all users can have names).

Every new control panel that you create will have default badge groups listed according to the *default types** selection that was made when the Alliance 8300 database was created.

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

Badge groups

Badge groups are defined in Alliance 8300 from the **Personnel | Badge group** menu option. See [Badge groups](#) on page 5 for introductory information.

Badge groups tell the Alliance 8300 system which badges need to be downloaded to which control panels. Badge groups are linked to control panels via the Badge Groups tab of the Controller Setup Form.

Alliance 8300 provides default badge groups to accommodate the following badge formats:

- ATS Wiegand 32-bit
- ATS Wiegand 30-bit
- Aritech magstripe
- Hughs 34-bit
- PIN code
- Raw data
- Tecom ASP
- Wiegand 26-bit
- HID C1000
- Master Installer Types (depending on the languages selected when the database was created)
- Master User Types (depending on the languages selected when the database was created)

Note: See [Master badge groups](#) on page 93 for information on MASTER Installers and MASTER Users.

Every new control panel that you create will have the default badge groups listed on the Badge Groups tab of the Controller Setup Form.

Master badge groups

All new Alliance 8300 control panel records are created* with at least one *Master* badge group:

- **Master Installer** type (assigned Badge No. 50) enables a new control panel to be programmed initially.
- **Master User** type (assigned Badge No. 1) enables a new control panel to be used for access initially. The Master User type does not apply to Australian database defaults.

* The *Master* badge groups may be removed from the new control panel record **prior to saving** the record. This is important for control panels with existing badge databases. See [Controller setup](#) on page 6.

Note: Failure to remove Badge Groups named MASTER Installer Type or MASTER User Type prior to saving a new control panel record for an existing control panel (with existing users) may result in overwriting users 1 and 50 with the MASTER Installer or MASTER User types (as applicable).

It is further recommended that the MASTER badge groups are removed from the panel's assigned badge groups as soon as they are not needed, for the following reasons:

- The master PINs may be used on the control panel, possibly resulting in unauthorized use.
- The existence of the master badges using badge numbers 1 or 50 (as applicable) 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 control panel until it is resolved.

If you wish to have your own special Installer or User PINs, then you must create PIN-only records using the Badge Setup form. Assign the appropriate badge numbers (1 or 50) to use the same locations in the control panel memory as previously used by the default badge groups.

Each type of Master badge group has associated read-only records for Person, Person Profile, and Badge. For example, the Badge Group *MASTER Installer Type (Australia)* is the owner of the badge named *MASTER Installer PIN (Australia)*.

Assigning badge groups

Control panels are defined in Alliance 8300 from the **Device | Alliance | Setup** menu option.

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

Note: Remove all unneeded badge groups before saving the new control panel record in Alliance 8300. See [Master badge groups](#) on page 93 for details.

There are three criteria, all of which must be met, for a badge to be downloaded to a control panel:

- The badge group must be assigned to the control panel.
- The person profile assigned to a person requires the use of the control panel (for example, to open a door).
- The badge is marked *Active* (not lost or expired).

Note: Before saving a new record for a control panel with existing users, remove the MASTER badge groups to avoid overwriting users 1 and 50.

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

When adding a control panel with the default badge groups, the default Master Installer and Master User will be downloaded to the 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.

Control panel memory

The use of memory expansion modules govern the number of users available to Alliance control panels and Alliance 4-door/elevator DGPs:

Panel memory	Quantity of users
Small (no expansion)	50
Expanded (1MB)	11,466
IUM small (4MB)	17,873
IUM expanded (8MB)	65,535
IUM tiny (software IUM)	50
IUM mini (software IUM)	2,000
IUM small (4MB hardware IUM)	17,873
IUM expanded (8MB hardware IUM)	65,535

Note: Alliance 4-door or 4-elevator DGPs must be fitted with the same memory expansion modules as the associated control panel.

In Alliance 8300 the closest counterpart to control panel users are *badges*. In fact, a badge represents a collection of users across multiple control panels.

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

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

In control panels without memory expansion (non-IUM), the badge number directly corresponds to the user number in the control panel (therefore, the user number refers to the physical badge number).

In control panels with expanded memory (IUM), the badge number may or may not correspond with the user number in the control panel (raw card data is used, not the badge number). For these control panels, Alliance 8300 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, Alliance 8300 selects the first available user number in the control panel starting from 1 and working up to the maximum permitted by the control panel's user memory.

Note: Use the **Badge to Users** report to identify the assignment between badges and user numbers on all applicable control panels.

Learning badge data

The Learn Badge Data form is used to search the Alliance history databases for unknown badge data from one or all badge learn devices (badges that are known to the system do not need to be learned).

The overall process for learning badge data is as follows.

1. Use the Badge learn tab on the Parameters form to specify the devices 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 Alliance 8300. 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 *Alliance 8300 Online Help*.

Chapter 8 Controlling operations

This chapter covers the tasks associated with the Alliance 8300 Operations menu. Refer to the *Alliance 8300 online help* for more details about these options.

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

In this chapter:

<i>Managing control panels</i>	100
<i>Monitoring badges</i>	102
<i>Monitoring alarms</i>	103
<i>Creating and using alarm maps</i>	105
<i>Managing clients</i>	106
<i>Managing zones</i>	106
<i>Managing doors</i>	107
<i>Managing elevators</i>	109
<i>Managing areas</i>	110
<i>Managing arming stations</i>	111
<i>Managing DGPs</i>	112
<i>Managing digital video</i>	113
<i>Changing your password</i>	113
<i>Selecting facilities</i>	113

Managing control panels

Controller utility

The Controller Utility allows you to issue commands to one or more selected 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 commands are as follows:

- **Edit.** Edit the properties of the selected control panel using the Controller Setup Form.
- **New.** Define a new control panel using the Controller Setup Form.
- **Change state.** Set the selected offline control panel online, or set the selected online control panel offline.
- **Dial/hangup.** Enabled only when the selected control panels are dial-up type, and have the same connection status (currently connected). A dial or hangup command applies to all selected control panels.
- **Download | Badges database.** Send the badges database to the selected control panels.
- **Download | Installer database.** Send the installer database to the selected control panels.
- **Download | Full database.** Send both the badges and installer databases to the selected control panels.
- **Upload | Installer database.** Receive the installer database from the selected control panels.
- **Upload | Door/floor groups, holiday database.** (Right-click shortcut) Receive the door groups, floor groups, and holiday database from the selected control panels.
- **Upload | Full database.** Receive the installer database and the door/floor groups, and holiday database from the selected control panels.

Note: Uploading of the badges database is not supported in the current release of Alliance 8300.

- **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 control panel are received by Alliance 8300. The control panel may still be connected but events are not processed by Alliance 8300. See [Accepting events](#) on page 101 for details.

- **Queue outgoing.** (Right-click shortcut) The default setting is **disabled**, and commands are transmitted from Alliance 8300 to the control panel. When selected, a tick appears next to the Queue Outgoing menu item. The control panel may still be connected but outgoing commands from Alliance 8300 to the control panel are suspended and queued until the **Queue outgoing** is set to **disabled**. See [Queuing outgoing events](#) on page 101 for details.
- **Date and time.** (Right-click shortcut) Opens the Date and Time Control Form for the selected control panels. Select multiple control panels to set the local date & time for all selected control panels simultaneously. This setting will be displayed on local RAS LCD displays and reported to management software.
- **Engineering reset.** (Right-click shortcut) Opens the Engineering Reset Control Form for a selected control panel.
- **Remove controller panels.** (Right-click shortcut) Hides the selected control panels from the list. To restore, close and reopen the Controller Utility Form.

Accepting events

Right-click the Controller Utility Form to clear the Accept Events setting. Clearing this setting causes Alliance 8300 to suppress receiving events from the control panel. Some reasons for suppressing events are:

- You might want to upload (receive) the full database from the control panel before accepting events. Doing so enables Alliance 8300 to learn details of the alarms to be reported.
- An installer may need to connect to a 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 Alliance 8300 to suppress sending data to the control panel. Some reasons for queuing outgoing data are:

- Allow operators to make configuration changes without the changes being sent prematurely by Alliance 8300.
- Allows installers to make all necessary configuration changes, and apply those changes during times of low risk.

Monitoring badges

The *badge monitor* option opens the Badge Monitor Form that allows the operator to monitor badge activity (according to the operator's facility assignment).

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

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 option 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 cameras associated with the door/RAS badge transaction, as defined by its event trigger (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 cameras associated with the reader's badge transaction, as defined by its event trigger (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 cameras associated with the door/RAS badge transaction, as defined by its event trigger (the DVR must be online and not in error condition or serving another request for playback of recorded video).

Note: 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

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. 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
- **Alarm graphics editor.** Right-click shortcut to the Alarm Graphics Editor Form.
- **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 cameras associated with the alarm's transaction, as defined by its event trigger (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

(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 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 (the DVR must be online and not in error condition or serving another request for playback of recorded video).

Note: An alarm activity must have a DVR association in order to enable video options on the right-click menu.

Creating and using alarm maps

Alarm graphics editor

The Alarm Graphics Editor allows an authorized 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) or Enhanced MetaFile (.EMF) format.

Applications such as Microsoft Visio, Microsoft PowerPoint, CorelDraw, Adobe Illustrator, and many other drawing applications can save images in either .WMF or .EMF format. 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

The Alarm Graphics Viewer 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

See *Network client computers* on page 115 for details about this topic.

Managing zones

Zone control

Select **Zone control** to display a list of zones by all controllers, or select to filter the list by controller.

Type up to 20 words 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.

Click the zone you want to control, and then select a function (Bypass, Unbypass, Reset, or Reset ACK). The command will be sent to the control panel.

Zone status

Provides the status of the selected zones by all controllers, or by controller. The lists may be filtered by your assigned operator facilities.

Click the **Get Status** button to get an updated status on the selected zone. This may take a few minutes if a dial-up control panel is not currently connected.

Managing doors

Door/output control

The *Door/output control* option allows you to manually open or close doors and turn on or off outputs.

You can list readers (these are also referred to as arming stations or doors) or outputs for all control panels (or per control panel), as listed in the Controller Utility Form.

The labels of the **Set state to** buttons change depending on whether **Reader** or **Other** is selected.

Reader commands

When the selected DO type is **Reader**, (arming stations or doors) the associated commands are:

- **Duration unlock.** Opens the **Timed Open** window. Enter the time in seconds for the duration unlock time, and then click **OK**.
- **Indefinite unlock.** Unlocks the highlighted door which will remain unlocked until you manually lock it by clicking **Lock**.
- **Open.** Immediately unlocks the highlighted door.
- **Lock.** Immediately locks the highlighted door.
- **Enable.** When the **Enable** button is clicked, the selected devices will be enabled and will respond to all valid commands such as **Open** or **Lock**.
- **Disable.** When the **Disable** button is clicked, the selected devices will be disabled and will not respond to commands such as **Open** or **Lock**.

Other commands

When the selected DO type is **Other** (outputs) the associated commands are:

- **On indefinite.** Activates the highlighted output, which will remain active until you manually turn it off by clicking **Off**.
- **Off.** Deactivates the selected device.

Door/output status

The *Door/output status* screen displays the current state of the selected door or output, as received from the control panel.

Click **Get Status** to send a request for updated information from the control panel.

Managing elevators

Elevator control

Use the Elevator Control Form to display a list of elevators for all of your assigned control panels, or for a selected control panel.

Click the **Select Elevator** arrow and select an elevator from the list. The associated elevator number, floor number and control panel description are displayed in the list.

Click the floor that you want to control, and then select a function (**Disarmed** or **Armed**). The command will be sent to the control panel.

Type up to 20 words in the Purpose text box to describe the reason for the command. These comments are written to your operator history file and appear in the purpose field of the Operator History report.

Elevator status

Use the Elevator Status Form to display a list of elevators for all of your assigned control panels, or for a selected control panel.

Click the **Select Elevator** arrow and select an elevator from the list. The state of the elevator and its floors are displayed in the list, as received from the control panel.

Click **Get Status** to send a request for updated information from the control panel.

Managing areas

Area control

Select **Area control** to display areas by all controllers, or by controller. The lists may be filtered by your assigned operator facilities.

Type up to 20 words 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.

Click the Area you want to control, and then select a function (Arm, Forced Arm, or Disarm). The command will be sent to the control panel.

Area status

Select **Area status** to display areas by all controllers, or by controller. The lists may be filtered by your assigned operator facilities.

The **Area Status** screen shows the current state of the selected Areas, as received from the control panel. Click **Get Status** to send a request for updated information from the control panel.

Managing arming stations

Arming station control

Select to display an arming stations list by all controllers, or by controller. The lists may be filtered by your assigned operator facilities.

Type up to 20 words 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.

Click the arming station you want to control, and then select a function (Bypass, Unbypass, or Door Open). The command will be sent to the control panel.

Arming station status

Select to display an arming stations list by all controllers, or by controller. The lists may be filtered by your assigned operator facilities.

The Arming Station Status screen shows the current state of the selected arming stations (RAS), as received from the control panel. Click **Get status** to send a request for updated information from the control panel.

Managing DGPs

DGP controller control

Select to display a DGP list by all controllers, or by controller. The lists may be filtered by your assigned operator facilities.

Type up to 20 words 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.

Click the DGP you want to control, and then select a function (Bypass, Unbypass, or Battery Test). The command will be sent to the control panel.

DGP controller status

Select to display a DGP list by all controllers, or by controller. The lists may be filtered by your assigned operator facilities.

The DGP Status screen shows the current state of the selected DGPs, as received from the control panel. Click **Get status** to send a request for updated information from the control panel.

Managing digital video

Digital video viewer

The Digital video viewer menu option under the Operations Menu opens a video command and control application that allows you to monitor digital video multiplexers/recorders and their associated cameras, control live video, as well as search and play back recorded video events.

Changing your password

The Change password option opens the Change Password Form which allows you to change your password.

Selecting facilities

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

Chapter 9 Network client computers

In order for your networked clients to connect to the server computer, the server computer must know who they are. Use the Client Monitor Form to obtain client type, Imaging status, and connection status. Use the Client Form to add, modify, and remove computers from the network.

In this chapter:

<i>Client monitor form</i>	116
<i>Client form</i>	118

Client monitor form

Open the Alliance 8300 Client Monitor Form from the **Operations | Client monitor** menu option or click the Client monitor toolbar button.

The Client Monitor option opens the Client Monitor Form which allows you to obtain client information such as client type (Alliance 8300 or CCTV), Imaging status, and connection status.

Figure 10. Client Monitor Form

Client	Client Type	Imaging status	Connection status	Description	Primary Com...	Secondary C...
BBN791S	A8300 Client App	Disabled	Connected	Client 2	NULL	NULL
JBN791S	A8300 Client App	Disabled	Not connected	Client 3	NULL	NULL
MELDSK0708A (DBServer)	A8300 Client App	Disabled	Connected	PCName	NULL	NULL
MELTEST01	A8300 Client App	Enabled	Connected	Client 1	NULL	NULL

Connection Information		Imaging Information	
Licenses used:	3	Licenses used:	1
Client licenses:	10	Imaging licenses:	5

The top of the Client Monitor Form displays all currently defined network clients, their imaging status, and their connection status.

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

The connection status is either **Connected** or **Disconnected**. If the network client is disconnected, it does not count toward the license; the license is only counted if the client is connected. To connect the client, log onto that computer. An application running on the Server computer counts toward 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.
- **Launch client.** Select this icon to enable a CCTV interface.
- **Client form.** Right-click shortcut to the Client Form to, for example, enable or disable Imaging for the particular Alliance 8300 client.

Note: When using the Launch Client command, you must restart the Alliance 8300 computer to enable the CCTV interface.

Client form

Use the Client Form to define a client computer. Open the Alliance 8300 Client Form from the **Administration | Client** menu option.

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 Alliance 8300 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 online 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 Imaging on a client without disconnecting it. You may have more Imaging 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.

Chapter 10 Reports and templates

Alliance 8300 provides extensive reporting capabilities based on your system configuration. All reports are selections of the Reports menu. This chapter discusses reports and templates for the reports.

Note: Reports are filtered so that supplied information pertains only to the selected facilities of the current user.

In this chapter:

<i>Reports</i>	120
<i>Templates</i>	124

Reports

For complete details of fields and capabilities of each report, refer to *Alliance 8300 Online Help*.

Note: 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 option to check how the font style and size will print on a page.

Twelve standard reports are provided. Four are history reports. In addition, Alliance 8300 has the ability to access reports you have created using a third party report generator. The following is a brief description of each report.

Standard reports

Person

Provides personal information, such as address and department, on all or a subset of persons in the system.

Badge

Provides information in areas you select on all or a subset of badges in the system.

Administration

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

Alliance

Generates reports about the Alliance control panel devices in the system.

Floor access

Lists the people who have access to floors.

Door access

Provides a list of persons who have access to the specified doors or RAS devices; that is, who has access where.

Area access

The area access report is a list of persons' levels of control over areas (for example, 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 for the alarm groups assigned to the person profile.

Alliance groups

Generates reports about the door groups or floor groups in the system, for a selected control panel or for all control panels.

Roll call

Provides a list of the last access granted to any or all persons in the system; that is, who last went where based on individual badge activity.

History reports

The default database for history reports is Alliance 8300 History. This database contains only records for the past day, week, or month as specified in *Archive database* on page 67 (the default archive period is daily).

Depending on the dates selected for the report and the archive database settings on the Parameter Form, you may need to create the report from the Alliance 8300 Archive database instead of the default Alliance 8300 History database, or you may need to run the same report for both databases (with dates selected accordingly).

Alarm history

Generates reports on alarm transactions. Select the required database and date range settings as described in *History reports* on page 121.

Badge history

Generates reports on badge transactions. Select the required database and date range settings as described in [History reports](#) on page 121.

Time and attendance history

Generates reports on time and attendance transactions. Select the required database and date range settings as described in [History reports](#) on page 121.

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

- An Alliance access controller must be used for time and attendance transactions.
- Doors reporting time and attendance transactions must have **Time Attendance Reader** selected on the **Alliance Doors Setup Form | Reader Options** tab.
- Readers or keypads designated for time and attendance transactions must be used for entry to and exit from the workplace, and no other purpose (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 *absent*.
- 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.

Operator history

Generates reports on operator actions. Select the required database and date range settings as described in [History reports](#) on page 121.

External reports

The **External reports** option opens the **Launch External Reports** window, allowing you to access an executable application or report that was not created within Alliance 8300.

For example, you may wish to access a report created by a third party report generator such as Crystal Reports or Microsoft Access 2000 or 2002. Refer to *Chapter 11, Using Microsoft Access* on page 125 for instructions to create a project, connect with Alliance 8300, and create reports.

Templates

Alliance 8300 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 Alliance 8300 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 selected, 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.

Templates button

The **Templates** button is for saving a template or making it a default.

Print preview report

The **File | Print preview report** command allows you to preview a report before printing it. A printer must be set up in Windows and added to your system in order for this feature to work.

Print report

The **File | Print report** command allows you to send the current report to the currently-defined printer.

Chapter 11 Using Microsoft Access

This chapter details the advanced procedures for creating database projects in Microsoft Access 2002 (MS Access) and connecting to Alliance 8300 databases.

The use of MS Access is not required for using Alliance 8300. MS Access is only necessary to perform further maintenance on the databases or to create custom reports.

The first thing that must be done is to create the required SQL user named *exreport*. Microsoft Access 2002 reports created using other SQL logins may not achieve the desired results.

In this chapter:

<i>Creating the exreport user</i>	126
<i>Setting up MS Access reports for Alliance 8300</i> . . .	134
<i>Launching external reports from Alliance 8300</i> . . .	144
<i>MS Access 2002 database utilities</i>	145

Creating the exreport user

The Alliance 8300 databases are initially installed with the system administrator user name *sa* and password *master*. The *sa* user name and password is used initially in MS Access 2002 **only** to create the required SQL user named *exreport*. The *exreport* user name (with a default password of *exreport*) is then used to set up the three Alliance 8300 database projects.

The *exreport* login has read-only permission to the three Alliance 8300 databases. This is the login that must be used to connect to the Alliance 8300 databases when using the Alliance 8300 **Reports | External reports** command.

The process of creating the *exreport* user involves the following sections:

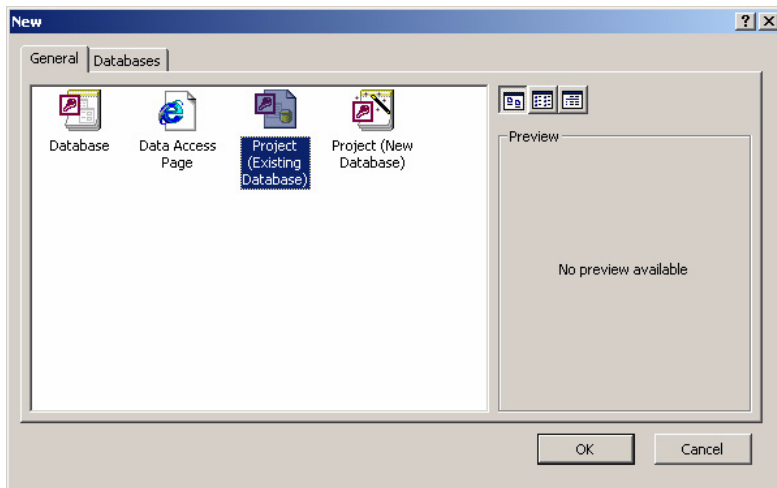
- [Creating an MS access project](#) on page 127.
- [Connecting to the database](#) on page 129.
- [Creating a new user](#) on page 131.

Creating an MS access project

Begin by creating the *Alliance 8300* project and storing the project in the Alliance 8300 Database folder. To create a new *Alliance 8300* project in MS Access, do the following:

1. In Access, select **File | New | Project (Existing Database)**.

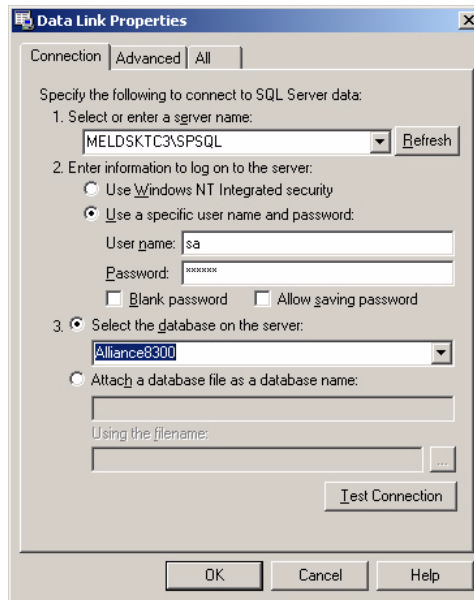
Figure 11. Existing project database



2. Click **OK**. A **File New Database, Save In** dialog box displays.
3. Name your project *Alliance8300.adp* and save in the Alliance 8300 Database folder (typically C:\Program Files\GE\Alliance 8300\Database\).

4. Click **Create**. The Connection tab of a Data Link Properties dialog box displays, enabling you to link the newly-created MS Access project to an SQL Desktop Engine (MSDE) database.

Figure 12. Data Link Properties window

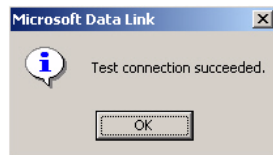


Connecting to the database

To connect the new project to Alliance 8300, do the following:

1. In the **Select or enter a server name** field of the **Data Link Properties, Connection** tab, select your server name from the list.
2. Select **Use a specific user name and password**, and type the user name *sa* and password *master*.
3. Do not select **Allow saving password**.
4. Select **Select the database on the server**. Click the arrow and select *Alliance8300*.
5. Click **Test Connection**. A **Microsoft Data Link** dialog box displays, informing you the link was successful.

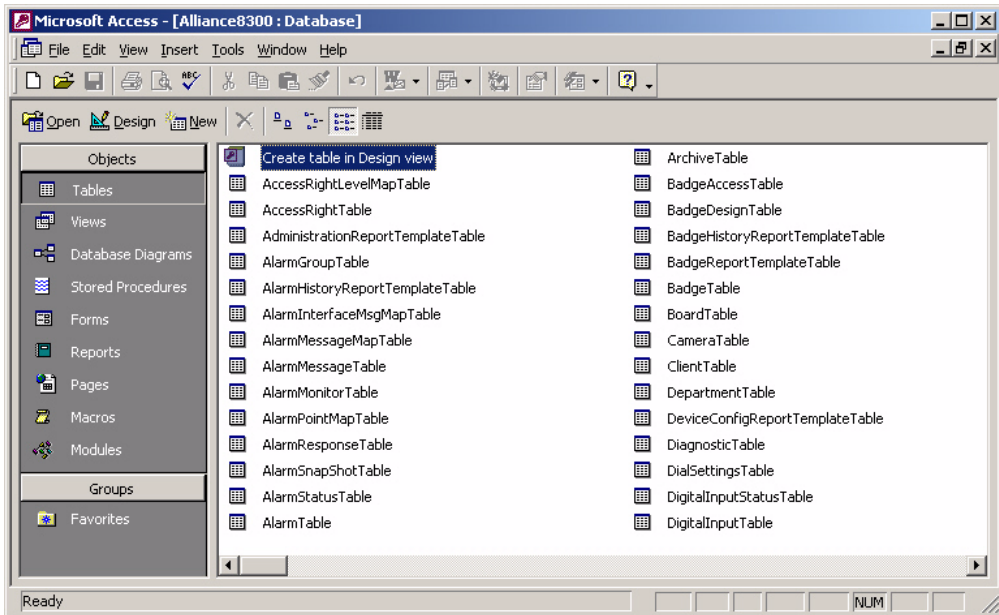
Figure 13. Microsoft Data Link dialog box



If the link was not successful, repeat these steps, verify your settings, and test the connection again.

6. Click **OK**. An *Alliance8300.adp* project is created and a list of the tables will display.

Figure 14. List of tables

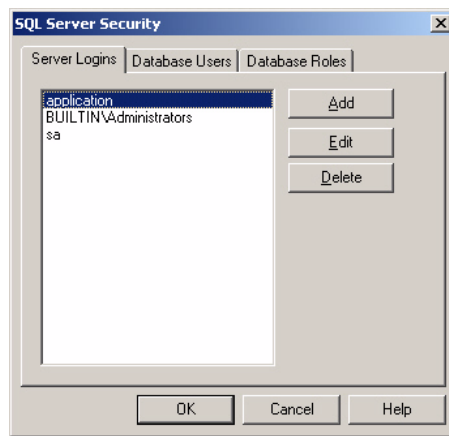


Creating a new user

To create a new user in MS Access, do the following:

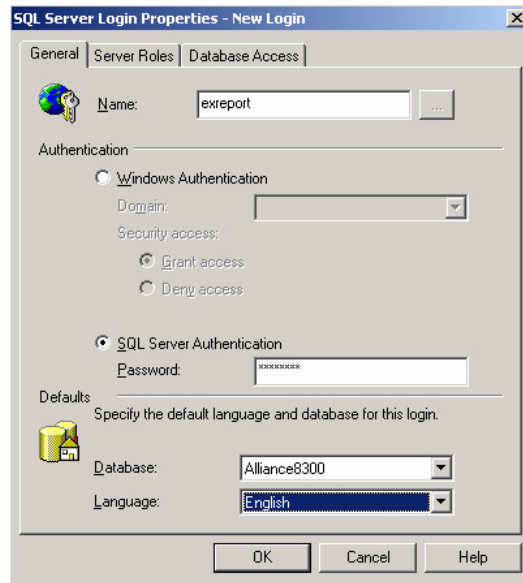
1. Select **Tools | Security | Database Security**. The **SQL Server Security** dialog box displays.

Figure 15. SQL Server Security box



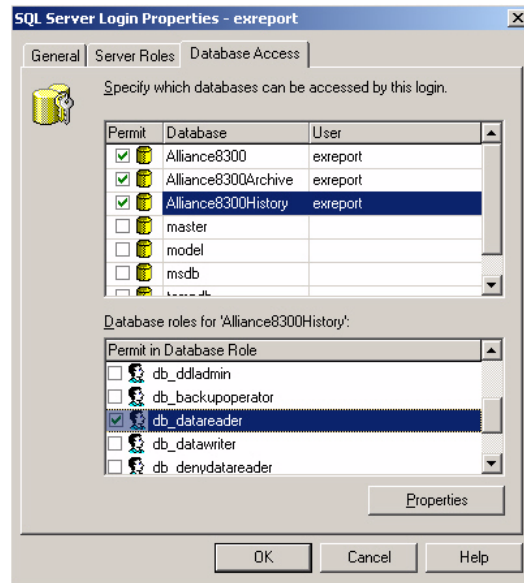
2. Click **Add**. The **SQL Server Login Properties -New Login** dialog box displays.

Figure 16. SQL Server Login Properties box



3. Type *exreport* in the **Name** and **Password** fields, and specify the default database and language.
4. Click the **Database Access** tab.

Figure 17. SQL Server Login Properties - exreport



5. Select **Permit** and select **db_datareader** for each of the Alliance 8300 databases.
6. Click **OK**.

Setting up MS Access reports for Alliance 8300

MS Access 2002 is required initially for creating the appropriate database user name and privileges (see [Creating the exreport user](#) on page 126).

Note: Use only MS Access 2002 to create the **exreport** user. It may be possible to use other versions of MS Access, such as Access 2000, for routine reporting tasks, however, some functionality may be lost or unavailable (depending on the version of MS Access and the Microsoft Service Release applied).

Creating an MS Access project

Note: MS Access can be installed on the Alliance 8300 Server computer and/or any Alliance 8300 client computer.

An MS Access project must be created for each of the three Alliance 8300 databases:

- Alliance8300
- Alliance8300Archive
- Alliance8300History

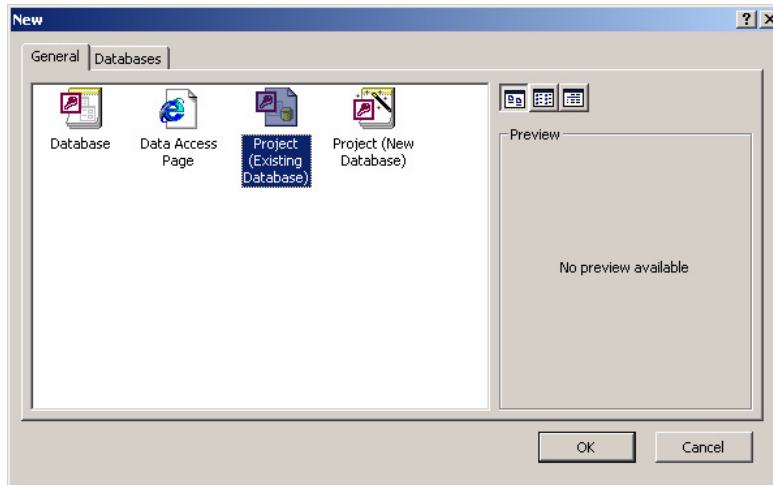
Begin by creating the *Alliance 8300* project and storing the project in the Alliance 8300 Database folder.

This may appear to be repetition of [Creating an MS access project](#) on page 127, however a different user name and password must be used in step 4.

To create a new Alliance8300 project in MS Access, do the following:

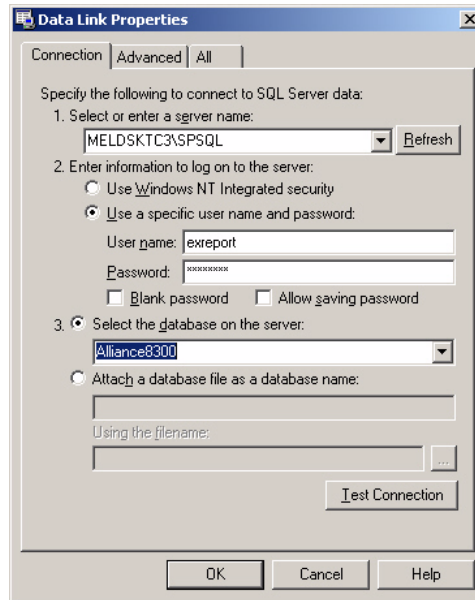
1. In Access, select **File | New | Project (Existing Database)**.

Figure 18. Project Database icon



2. Click **OK**. A **File New Database, Save In** dialog box displays.
3. Name your project *Alliance8300.adp* and save in the Alliance 8300 Database folder (typically C:\Program Files\GE\Alliance 8300\Database\). Overwrite the *Alliance8300.adp* database that you created in [Creating an MS access project](#) on page 127.
4. Click **Create**. The **Connection** tab of a **Data Link Properties** dialog box displays, enabling you to link the MS Access project to an SQL Desktop Engine (MSDE) database.

Figure 19. Data Link Properties window

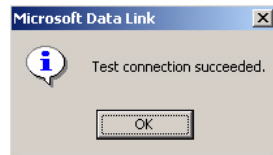


Connecting to the database

To connect the new project to Alliance 8300, do the following:

1. In the **Select or enter a server name** field of the **Data Link Properties**, **Connection** tab, select your server name from the list.
2. Select **Use a specific user name and password**, and type the user name *exreport* and password *exreport*.
3. Do not select **Allow saving password**.
4. Select **Select the database on the server**. Click the arrow and select *Alliance8300*.
5. Click **Test Connection**. A **Microsoft Data Link** dialog box displays, informing you the link was successful.

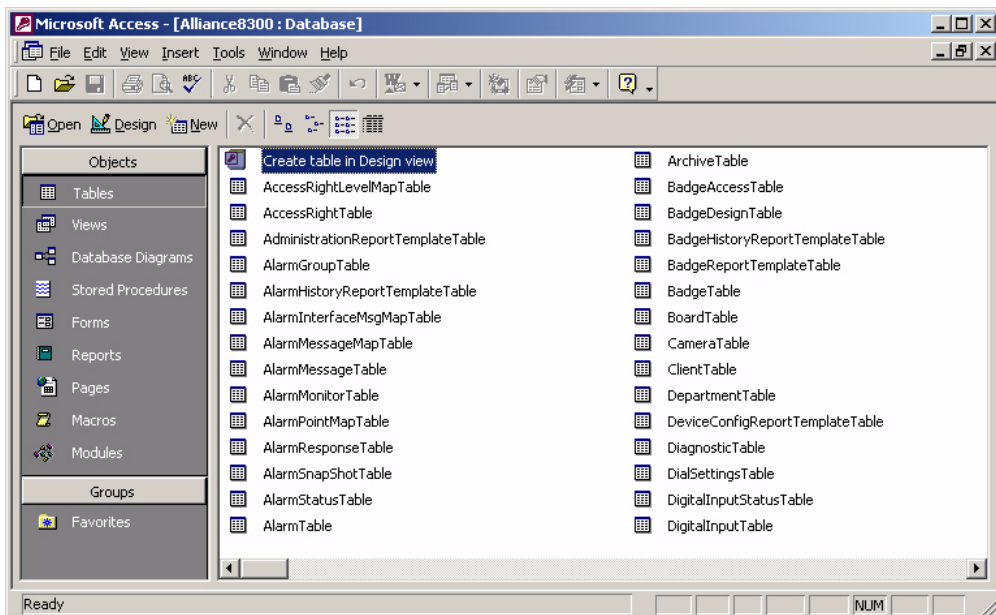
Figure 20. Microsoft Data Link



If the link was not successful, repeat these steps, verify your settings, and test the connection again.

6. Click **OK**. An *Alliance8300.adp* project is created and a list of the tables will display.

Figure 21. List of tables.



Note: Repeat the above steps to create all three projects, selecting at step 4 *Alliance8300Archive*, and again to select *Alliance8300History*.

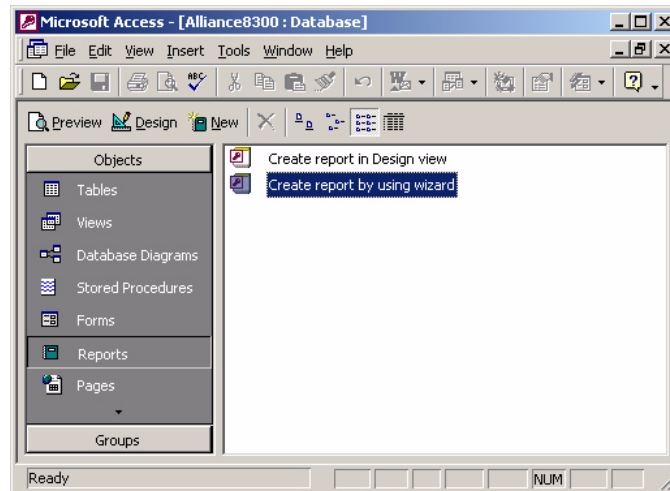
Creating an MS Access report

In this section, you will create an MS Access report using the **Create report by using wizard** utility, and then use *drag-and-drop* to automatically create a shortcut to the report for use by Alliance 8300.

To create and link a report to Alliance 8300, do the following:

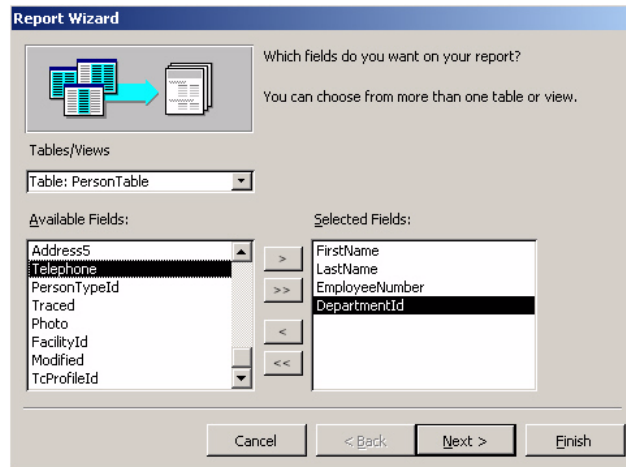
1. In Access, click **Reports** in the **Objects** panel and then double-click **Create report by using wizard**.

Figure 22. Create report by using wizard



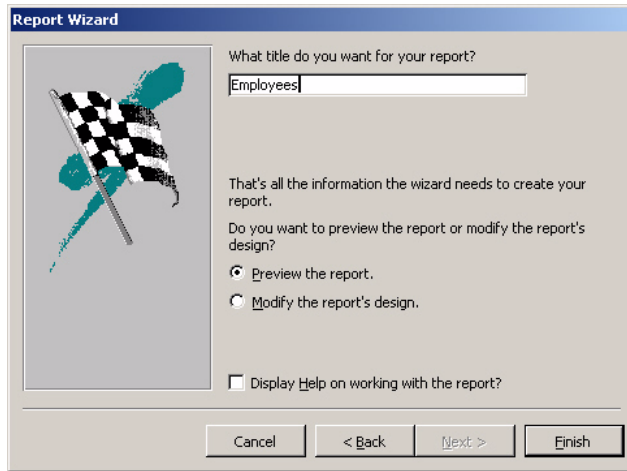
2. Follow the Report Wizard prompts to define a report. In the following steps, we'll create a sample personnel list.

Figure 23. Report wizard



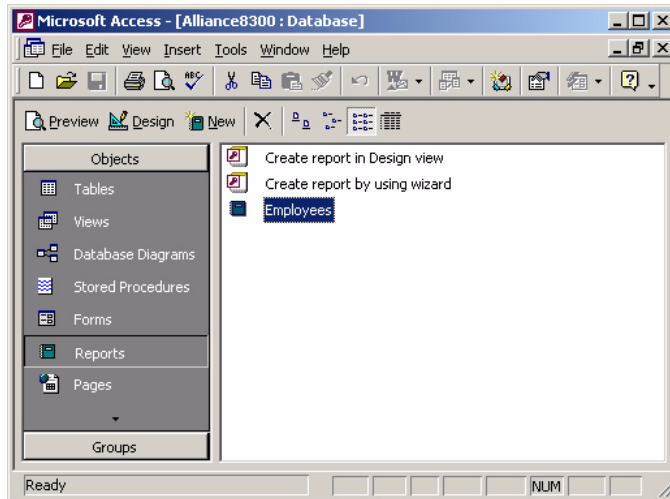
3. Click the **Tables/Views** arrow and select a table from which you want data.
4. Select fields from the **Available Fields** list and then click the right-facing arrow, to populate the **Selected Fields** list. Selected fields will be used in the report.
5. Subsequent steps in the Report Wizard allow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

Figure 24. Report wizard



6. Click **Finish**.
7. Use the print preview and design views, if needed, to further customize the report. The report is listed in the MS Access Reports list.

Figure 25. Employees icon



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

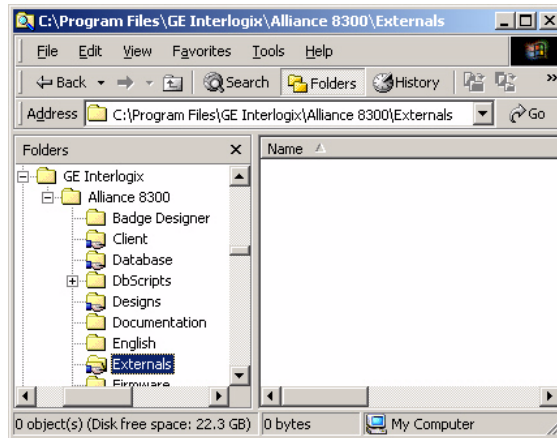
Linking an MS Access report to Alliance 8300

Alliance 8300 has been designed to allow you to quickly add MS Access reports to the **Reports | External Reports** command by means of Windows *drag-and-drop* functionality.

To automatically create a shortcut to the report for use by Alliance 8300, do the following:

1. Open a Windows Explorer view of the Alliance 8300 Externals folder on the server computer.

Figure 26. Program files



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

2. Position Windows Explorer and MS Access on the Windows desktop so that both are visible. Drag the report from the MS Access project to the Alliance 8300 Externals folder (see *Figure 27* on page 143). Windows automatically creates a shortcut to the MS Access report *Employees* (see *Figure 28* on page 143) which is accessible via the Alliance 8300 **Reports | External Reports** command (see *Figure 29* on page 144).

Figure 27. Drag the report to the folder

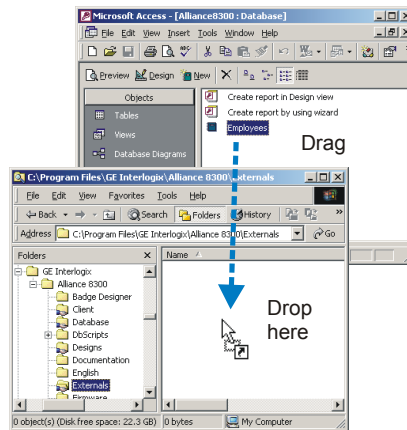
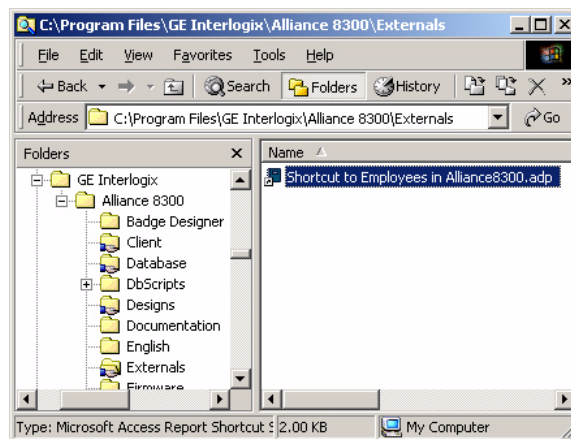


Figure 28. Shortcut created in the Alliance 8300 Externals folder



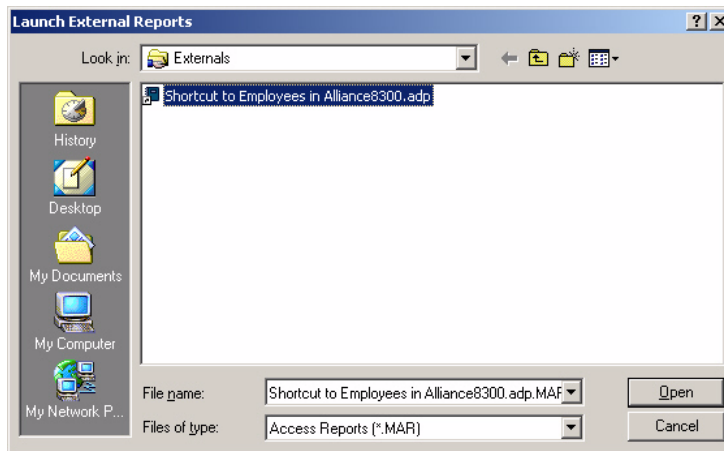
3. Close Microsoft Access and Windows Explorer when you are finished creating reports and dragging them into the Alliance 8300 Externals folder.

Launching external reports from Alliance 8300

To run an Alliance 8300 external report, do the following:

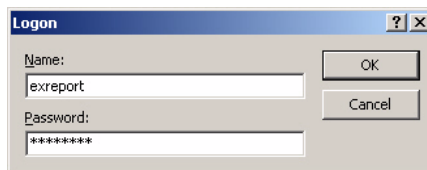
1. In Alliance 8300, select **Reports | External Reports**. The **Launch External Reports** window displays the report shortcuts that you've dragged into the Externals folder on the server computer.

Figure 29. View of shortcut in the Reports | External Reports command



2. Select the required report and click **Open**. The database login window displays.

Figure 30. Login



3. Type the user name *exreport* and password *exreport* and then click **OK**. MS Access launches and opens the report in preview mode.

MS Access 2002 database utilities

Once you have created an MS Access project for each database, select **Tools | Database Utilities | Compact and Repair Database**. Refer to the online Microsoft Access Help for details of the **Compact and Repair Database** process.

Note: Do not select any other options from the **Database Utilities** menu unless instructed by a System Support technician.

Chapter 12 Database and system management

This chapter discusses the various types of Alliance 8300 files, and the tools available for maintaining, backing up, and restoring these files.

In this chapter:

<i>Overview</i>	148
<i>Alliance 8300 databases</i>	149
<i>Alliance 8300 files and settings</i>	156
<i>Restoring data from a backup</i>	160
<i>System recovery</i>	163

In addition, the following sections apply to both Alliance 8300 and Alliance 8700 Smart Card Programmer:

<i>Backing up Alliance 8300 and 8700 databases</i> . . .	154
<i>Restoring Alliance 8300 and 8700 databases</i>	160
<i>Changing the name in ODBC</i>	188

Overview

The Alliance 8300 files stored on the server computer consists of the following types:

- **Databases** contained in the **Alliance 8300/Database** folder. See [Alliance 8300 databases](#) on page 149 for details.
- **Application files and related data** contained in the **Alliance 8300** folder and its subfolders (except for the Alliance 8300 databases in the Database subfolder), and Windows System State data such as the Registry. See [Alliance 8300 files and settings](#) on page 156 for details.

The overall process of backing up Alliance 8300 is as follows:

1. Run **Alliance 8300/8700 Database Maintenance** to backup the Alliance 8300 databases to create *BAK* files. See [Backing up Alliance 8300 and 8700 databases](#) on page 154.
2. Run **Microsoft Windows Backup** to backup the entire Alliance 8300 folder (including the *BAK* files created in step 1). See [Backing up with MS Windows Backup on page 157](#).
3. Run **Microsoft Windows Backup** a second time to backup the Alliance 8300 Windows Registry settings. See [Backing up with MS Windows Backup on page 157](#).

Alliance 8300 databases

The Alliance 8300 Professional server computer has three databases:

- **Alliance8300**. Contains configuration data for items such as operators, badges, and 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 Alliance 8300 archive settings.

Maintenance operations for the Alliance 8300 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 Alliance 8300 history](#) on page 150.
- **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 **Alliance 8300/8700 Database Maintenance** utility is used to back up the Alliance 8300 databases. See [Backing up Alliance 8300 and 8700 databases](#) on page 154. If the Alliance 8700 Card Programmer is installed there will also be an **Alliance8700CardProg** database, which you will also need to back up.

Archiving Alliance 8300 history

The **Alliance8300Archive** database is created automatically by Alliance 8300 based on the archive period (daily, weekly, or monthly) defined in the Parameters Form (see [Archive database](#) on page 67 and [Figure 31](#) on page 151). The default archive period is daily.

Alliance 8300 services must be running on the Alliance 8300 server for a scheduled archiving operation to occur. If the services are not running, Alliance 8300 attempts to perform the archiving operation the next time Alliance 8300 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 2 GB in size and to ensure that the Alliance 8300 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 Alliance 8300 (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 2GB in size.
- The amount of available hard disk space on the Alliance 8300 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, do the following:

1. Backup the data that you need to retain. See [Backing up Alliance 8300 and 8700 databases](#) on page 154.
2. Assuming that **Alliance 8300/8700 Database Maintenance** utility displayed a message verifying that the backup was successful, delete the data from the **Alliance8300Archive** database. See [Deleting Alliance 8300 archive history](#) on page 151.



CAUTION:

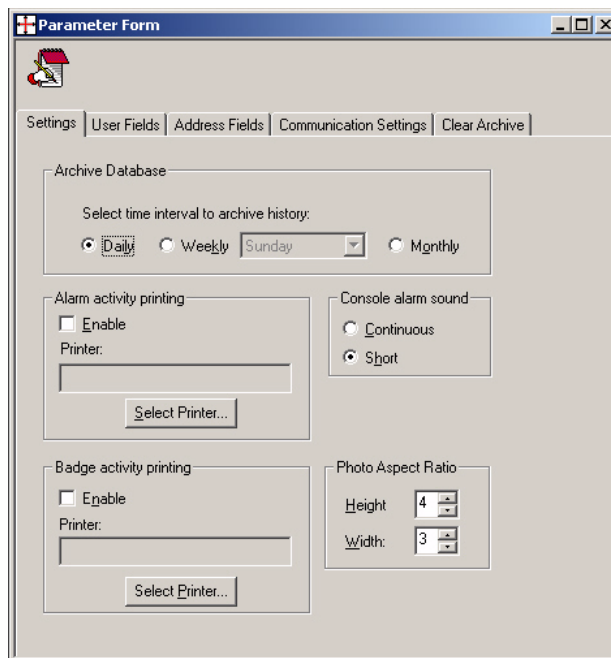
If you do not back up the Alliance 8300 Archive database, you will lose all the data stored in it. After you do the backup, validate the quality of the backup file, then label and store the media in a safe place.

Deleting Alliance 8300 archive history

To delete data from the archive database, do the following:

1. Start Alliance 8300 and login.
2. Select **Administration | Parameters**.
3. The **Parameter Form** opens with the **Settings** tab displayed.

Figure 31. Parameter form, Settings tab



The screenshot shows a window titled "Parameter Form" with a tabbed interface. The "Settings" tab is selected. The window contains the following sections:

- Archive Database:** A section with the label "Archive Database" and the instruction "Select time interval to archive history:". It includes radio buttons for "Daily" (selected), "Weekly", and "Monthly", and a dropdown menu currently set to "Sunday".
- Alarm activity printing:** A section with a checkbox for "Enable" (unchecked), a "Printer:" label, a text input field, and a "Select Printer..." button.
- Console alarm sound:** A section with radio buttons for "Continuous" and "Short" (selected).
- Badge activity printing:** A section with a checkbox for "Enable" (unchecked), a "Printer:" label, a text input field, and a "Select Printer..." button.
- Photo Aspect Ratio:** A section with "Height" and "Width" labels, each followed by a spin box. The Height is set to 4 and the Width is set to 3.

4. Select the **Clear Archive** tab.

Figure 32. Parameter form, Clear Archive tab

Parameter Form

Settings | User Fields | Address Fields | Communication Settings | **Clear Archive**

Earliest Date in Current Archive DB:

Latest Date in Current Archive DB: Show date

Archive clean period

February 2004 February 2004

Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7	1	2	3	4	5	6	7
8	9	10	11	12	13	14	8	9	10	11	12	13	14
15	16	17	18	19	20	21	15	16	17	18	19	20	21
22	23	24	25	26	27	28	22	23	24	25	26	27	28
29	1	2	3	4	5	6	29	1	2	3	4	5	6
7	8	9	10	11	12	13	7	8	9	10	11	12	13

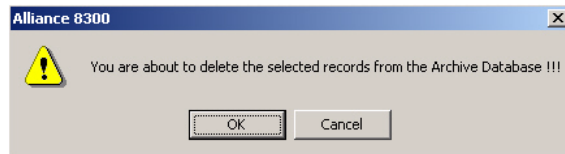
Start Date End Date

Delete

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 (*Figure 33*).

Figure 33. Message - Delete Data from Archive Database



9. Click **OK**. 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 Alliance 8300 Archive database has been successfully deleted.**
10. Click **OK**.

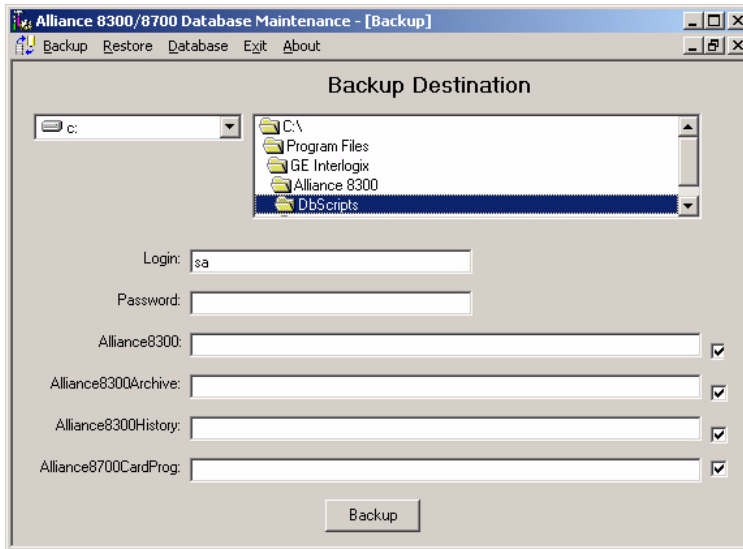
Backing up Alliance 8300 and 8700 databases

The **Alliance 8300/8700 Database Maintenance** utility is used to back up the Alliance 8300 and Alliance 8700 databases to BAK files, which can then be backed up using **Microsoft Windows Backup**. See *Backing up with MS Windows Backup on page 157*.

To back up the database files, do the following:

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 **Alliance 8300/8700 Database Maintenance** utility (Maintenance.exe) located in (typically) *C:\Program Files\GE\Alliance 8300\DbScripts*. The **Alliance 8300/8700 Database Maintenance** window displays.
3. Click **Backup**. An **Alliance 8300/8700 Database Maintenance - [Backup]** window displays.

Figure 34. .Alliance 8300/8700 database backup window



4. Type the **sa** login and password (the default password is **master**).
5. Navigate to the drive and folder on your system where the backup files will be stored. Double-click to open the **Destination** folder.

6. Holding down the left mouse button, drag and drop the destination folder onto each of the fields:
 - Alliance8300
 - Alliance8300Archive
 - Alliance8300History
 - Alliance8700CardProg (if the Alliance 8700 Card Programmer is installed)

The .BAK files in each field will be named automatically, to include the directory path, file name, date, and time.

7. 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.
8. Click **Backup**. The backup process begins. When backup is complete, a dialog box displays a message verifying the successful backup of the chosen databases.
9. Click **OK**.
10. Exit the **Maintenance** window.

Alliance 8300 files and settings

Alliance 8300's application files and related data are contained in:

- The Alliance 8300 folder and its subfolders (except for the Alliance 8300 databases in the Database subfolder).
- Windows System State data (including Windows Registry settings).

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.

Windows Registry settings may be backed up using the following methods:

- Use **Microsoft Windows Backup**. See *Backing up with MS Windows Backup on page 157*.
- Use the Windows Registry Editor (regedit) to export the Windows registry (or a portion of it) to a text file. See *Registry Editor* in the online help for details.

Note: Performing backup operations during busy periods may reduce the performance of the Alliance 8300 system.

You can use any backup program or media such as tape, zip disk, CD, or a network folder to produce a backup copy of selected data. The size of the files in the folder you want to back up will be a determining factor of which media to use.

If you have the **Alliance 8300 Imaging** option installed, the following additional folders will be stored in the Alliance 8300 folder:

- **Images.** Will only need to be backed up if you have **Imaging** installed. Contains the picture files of badge holders.
- **Signatures.** Will only need to be backed up if you have **Imaging** installed. Contains the signature files of badge holders.
- **Graphics.** Will only need to be backed up if you are using Alarm Graphics. Contains the alarm graphics maps.
- **Designs.** Will only need to be backed up if you have **Imaging** installed and previously created badge designs in the folder.

Backing up with MS Windows Backup

Microsoft Windows Backup enables you to backup:

- files and folders
- Windows System State data (including Windows Registry settings)

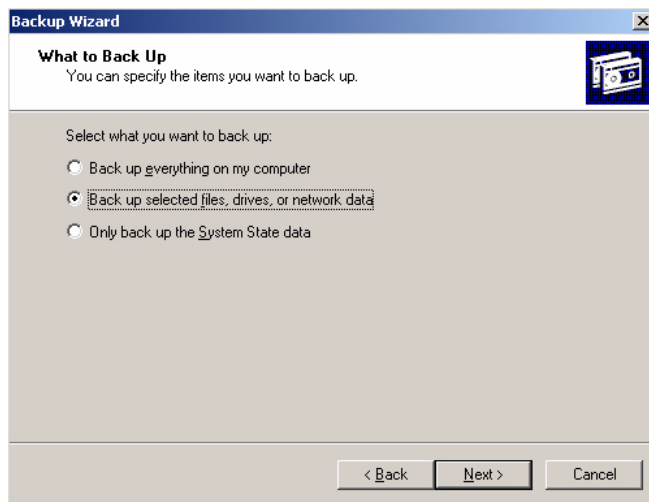
To backup both of these types of data, you would run Microsoft Windows Backup twice, selecting different options (see *Figure 35*).

If you use a tape drive for backup, typical instructions for using a tape drive are listed below. Similar procedures apply for using **Microsoft Windows Backup** to backup to other media.

To back up to the tape drive on the Windows 2000 Professional computer, do the following:

1. Insert the tape to which you want to back up.
2. Click on **Start, Programs, Accessories, System Tools**, then **Backup**. Microsoft Windows Backup will appear.
3. From the *Welcome to the Windows 2000 Backup and Recovery Tools* window, click **Backup Wizard**, then **Next**

Figure 35. Backup Wizard



4. Assuming you want to backup files, navigate to *C:\Program Files\GE\Alliance 8300* or wherever the installation of Alliance 8300 resides on your computer. Select the folder to back up. Click **Next**. The *Where to Store the Backup* window displays.

Note: Microsoft Windows Backup does not backup the Alliance 8300 databases in the Database subfolder. These must first be backed up using the Alliance 8300/8700 Database Maintenance utility, and then the resulting BAK files can be backed up using Microsoft Windows Backup. See [Backing up Alliance 8300 and 8700 databases](#) on page 154 for details about backing up these files.
5. Select the *Backup media type* and *Backup media or file name* and click **Next**.
6. The *Completing the Backup Wizard* window displays.
7. Click **Finish**. The *Backup Progress* displays.
8. Click **Close** and exit the Backup window.

Backing up to your computer CD-RW drive

If you use a CD-RW drive for backup, typical instructions for using a CD-RW drive are listed below (*Adaptec Easy CD Creator 4* is only an example).

To back up to the CD-RW drive on the Windows 2000 Professional computer, do the following:

1. Insert the blank CD to which you want to back up.
2. Click on **Start, Programs, Adaptec Easy CD Creator 4**, then **Create CD**. The Easy CD Creator 4 Welcome window displays.
3. From the Welcome window, click **Data**, then **Data CD**.
4. In the Easy CD Creator explorer window, navigate to the Alliance 8300 folder, then select the folder or folders to back up.

Note: Your Alliance 8300 database folder contains files with .mdf and .ldf extensions. DO NOT COPY, BACK UP, OR EDIT THESE FILES. See [Backing up Alliance 8300 and 8700 databases](#) on page 154 for details about backing up these files.
5. Drag and drop the files to the **CD Layout** window. This enables the **Create CD** icon on the main menu bar.
6. Click **Create CD** from the main menu. The **CD Creation Setup** window displays.

7. Select your **Target Device** from the drop-down list and click **OK**. A **CD Creation Process** window displays the progress of the creation procedure.
8. When a completion message displays in the progress window, the CD creation process is complete. Click **OK** to exit the **CD Creation Process** window.
9. From the **File** menu, select **Exit** to close the Easy CD Creator 4 application.

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.

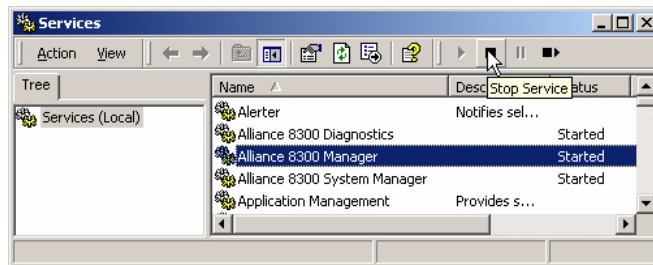
Restoring Alliance 8300 and 8700 databases

Note: The backup files must be moved to the destination computer. The **Alliance 8300/8700 Database Maintenance** utility can only restore from a local machine.

To restore an Alliance 8300 database backup, do the following:

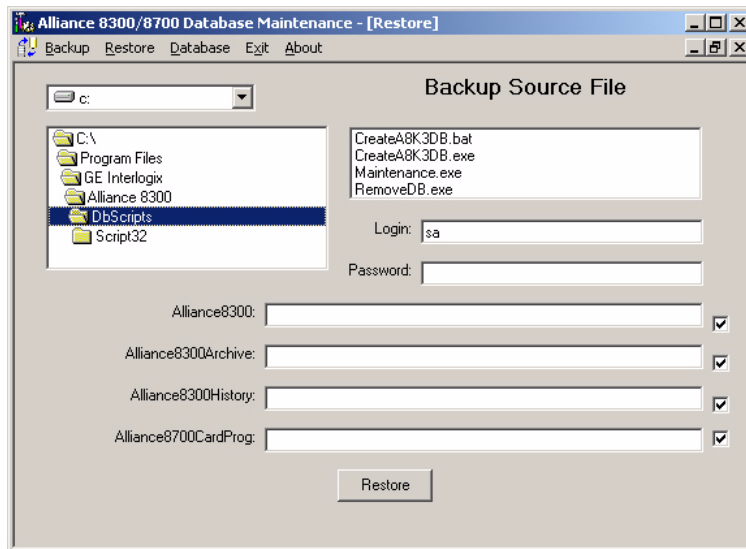
1. Stop the Alliance 8300 services. Select **Start | Settings | Control Panel**. Double-click **Administrative Tools** and then double-click **Services**. The **Services** window displays.
2. Find the Alliance 8300 services and stop them in the following order: Alliance 8300 Manager, Alliance 8300 System Manager, Alliance 8300 Diagnostics.

Figure 36. Select a service and then click Stop Service



3. Run the Alliance 8300/8700 Database Maintenance utility (Maintenance.exe) located in (typically) *C:\Program Files\GE\Alliance 8300\DbScripts*. The Alliance 8300/8700 Database Maintenance window displays.
4. Click **Restore**. An **Alliance 8300/8700 Database Maintenance - [Restore]** destination window displays.

Figure 37. Alliance 8300/8700 Database Maintenance (Restore) window

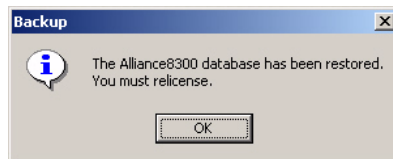


5. Type the **sa** login and password (the default password is **master**).
6. Navigate to the drive and directory folder on your system where the backup files are presently stored. Double-click to open the folder.
7. Holding down the left mouse button, drag and drop from the **Backup Source File** window onto each of the following fields:
 - Alliance8300
 - Alliance8300Archive
 - Alliance8300History
 - Alliance8700CardProg (if the Alliance 8700 Card Programmer is installed)
8. 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.

9. Click **Restore**. 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 may receive a message stating relicensing is required (this applies to only the Alliance8300 database, even if the message displays for another database).

Figure 38. Backup box



10. Click **OK**.
11. Exit the **Alliance8300 Database Maintenance** utility.
12. Reregister the Alliance 8300 license using the license key initially provided. (If Alliance 8300 does not accept the original license key, follow the complete license registration procedure described in the *Alliance 8300 Installation Manual*.)

Restoring files

If you used the **Backup Wizard** in **Microsoft Windows Backup** to backup your files (see [Backing up with MS Windows Backup on page 157](#)), then you can use **Restore Wizard** to restore your files.

Note: If you need to restore backed up files from the Alliance 8300 subfolders, restore the files and not the entire folder because the folder will not have the original share property as the original. Alliance 8300 depends on some folders being shared and having specific share properties.

System recovery

If your Alliance 8300 Professional System 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.

This checklist assists you in recovering your Alliance 8300 Professional system. Complete the steps in the order they appear.

- Repeat all the steps in the **Alliance 8300 Installation Guide** from *Preparing The Operating System* to the end of *Installation Part 1*.
- Use the **Alliance 8300/8700 Database Maintenance** utility to restore the three Alliance 8300 databases and the Alliance 8700 Card Programmer database (if applicable) from your backup media. See [Restoring Alliance 8300 and 8700 databases](#) on page 160.
- Restore the contents of the **Images, Signatures, Graphics, and Designs** folders from your backup media to the appropriate Alliance 8300 subfolders. See [Restoring files](#) on page 162.
- Reregister the Alliance 8300 License using the license key initially provided. (If Alliance 8300 does not accept the original license key, follow the complete license registration procedure described in the *Alliance 8300 Installation Guide*.)
- Restart the computer.

Chapter 13 Diagnostics and troubleshooting

Alliance 8300 provides an extensive diagnostic utility named DiagView. To access DiagView, select **Administration | Diagnostic Viewer**. This utility is very flexible in that you can turn the monitoring of many Alliance 8300 system components on and off.

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

In this chapter:

<i>Turning on diagnostics</i>	166
<i>Creating a logfile</i>	167
<i>Viewing the diagnostics logs</i>	168
<i>Questions and answers</i>	169
<i>Uninstalling Alliance 8300</i>	180

Turning on diagnostics

To display debug messages in the Diagnostics Log within Alliance 8300, the diagnostics for that component you wish to monitor (COM port, 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 logfile or any diagnostic object can write to a separate logfile that can be defined by the user.

Creating a logfile

To create a logfile, do the following:

1. Select **Administration | Logfile**. 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 logfile.
6. Click **Save**.

To enable diagnostics, do the following:

1. Select **Administration | 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.
6. The more items you turn on for monitoring, the more the Alliance 8300 system performance is compromised! This is even more important when monitoring port, communications, or control panel items.

There are many components available to monitor:

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

Viewing the diagnostics logs

Alliance 8300 provides a convenient way to view what's happening on the system. For each client, there is a default logfile (others can be created) for each day of the week such as *A8K3THURSDAY.SPL*. This file is overwritten each week, thus creating a new log for that day.

Additionally, for each client, there is a log located in the *WINNT\system32* folder. Under normal system operation, this log will be empty. It will be used to log messages if the server and the database cannot be reached.

During normal operation of Alliance 8300, information as well as debug messages are written to the daily log file. Under abnormal conditions, the log file may also contain warning and/or fatal messages.

Alliance 8300 has a log file viewer named DiagView, which can be used to open log files and display logged events in real time. To access DiagView, select **Administration | Diagnostic Viewer**. Every time Alliance 8300 writes an entry to the log file, DiagView displays the latest message. By default, DiagView displays only the latest 1000 messages. The number displayed can be changed in DiagView via the **File | Preferences** option.

All log files should be saved in the logs folder; it will be easier to locate for backups and upgrades. It is a shared folder which means other clients can gain access to the log files.

Questions and answers

This section provides answers to some common questions.

Installing Alliance 8300

- *What is the order of events during installation?*

The complete order of installation is detailed in the *Alliance 8300 Installation Manual*. A summary of the installation process follows:

1. Install Alliance 8300 on your Server computer (license domain and database server run on the Server computer).
2. Create the database on the server.
3. Register the Alliance 8300 license on the Server computer.
4. Start the Alliance 8300 application.
5. Use the Client Form to add and configure all your clients.
6. Install Alliance 8300 on your client computers.

- *What does this message mean: You must have Administrator Rights in order to install Alliance 8300 Server software*

You are logged on to Windows as a user who does not belong to the local Administrators group. The Alliance 8300 software can only be installed by a Windows user who belongs to the local Administrators group. Log off, then log on as a Windows user who belongs to the Administrators group or add the Windows user to the Administrators group.

Starting Alliance 8300

The Alliance 8300 server computer must be set up in a manner that the Alliance 8300 services start up automatically each time the server computer starts up. The Alliance 8300 services, running on the Alliance 8300 server computer, enable Alliance 8300 to run on remote Alliance 8300 client computers.

The process of setting up Alliance 8300 services to start automatically is described in the *Alliance 8300 Installation Manual*.

Alliance 8300 will not be able to run on a remote Alliance 8300 client computer in any of the following circumstances:

- If the Alliance 8300 server computer is not running.
 - If the Alliance 8300 services are not running on the Alliance 8300 server computer.
 - If the remote Alliance 8300 client computer cannot communicate with the Alliance 8300 server computer over the network because of network problems.
 - If the Windows login used on the remote client computer cannot access the Alliance 8300 shared folders on the server computer. To check this, log onto Windows on the remote client computer as user *secure* with the assigned password, and attempt to restart Alliance 8300 on the remote client computer.
 - If the Alliance 8300 client record (**Administration | Client**) for the remote Alliance 8300 client computer has not been set up in the Alliance 8300 server computer.
 - If the maximum number of clients permitted by the Alliance 8300 license is currently being used. On the Alliance 8300 server computer, check the bottom of the **Client Monitor** form and verify that there is at least one license available.
 - If Alliance 8300 was not correctly installed on the remote Alliance 8300 client computer (if the wrong Alliance 8300 server name was used during the client installation, or if the Alliance 8300 client wasn't licensed correctly).
- *I get a connection error when I try to start Alliance 8300 on a remote client computer. What do I do now?*
1. Make sure the Alliance 8300 server computer is running and connected to the network.
 2. On the Alliance 8300 server computer, go to the Services form and check Alliance 8300 services. If the Status column is blank for a service, then it is not running. Highlight the service , and click the **Start** button:
 - If the status changes to **Started**, then the service is now running. Try to start Alliance 8300 on the remote computer now.
 - If the status does not change to **Started**, use **DiagView** on the server computer to check the current day's log. It should display an error message providing a reason for shutting down.
 3. On the Alliance 8300 server computer, ensure that the Alliance 8300 client record (**Administration | Client**) for the remote Alliance 8300 client computer has been set up.

4. On the Alliance 8300 server computer, check the bottom of the **Client Monitor** form and verify that there is at least one license available for the client to use.
 5. On the Alliance 8300 client computer, verify that the currently logged on Windows user name and password has been set up by the network administrator with domain permissions to access the Alliance 8300 shared folders on the server computer. The network administrator must use the utilities described in *System administration utilities* on page 212 to set up users and groups.
 6. Verify that you are using TCP/IP or NetBEUI as your network protocol, that it is configured properly, and is used on both both the client and server computers.
- *What are some of the reasons the Alliance 8300 System Manager Service will not start?*

Possible causes include:

- Computer hardware has failed.
- Computer hardware has been replaced.
- The service cannot access the database.
- The client machine name is not in the client table.
- The services on the database server are not running.

Alliance 8300 licensing uses the server computer's hardware configuration (among other things) when it generates the machine seed key, which is used for licensing. A change in hardware may require Alliance 8300 to be relicensed. Reset the application password and relicense Alliance 8300. See *Resetting the application password* on page 199 for details.

- *What are some of the reasons the Alliance 8300 Manager Service will not start?*

Possible causes include:

- Computer hardware has failed.
- Computer hardware has been replaced.
- System service on the local machine will not start.
- The local machine did not receive a ping from the license domain machine within the ping timeout interval (check the license domain services are running).
- Client license count may have been exceeded.

Alliance 8300 licensing uses the server computer's hardware configuration (among other things) when it generates the machine seed key, which is used for licensing. A change in hardware may require Alliance 8300 to be relicensed. Reset the application

password and relicense Alliance 8300. See [Resetting the application password](#) on page 199 for details.

- *My services shut down unexpectedly. The log reports that the message database is down.*

This indicates a problem with connectivity to the database. In order not to lose any transactions, Alliance 8300 will save all badge and alarm messages by writing them to a file and read the file back in when the services start up again.

Correct the connectivity problem with the database and restart services.

- *What does this message mean: Maximum Number of Clients Limit Reached?*

The maximum number of clients permitted by the Alliance 8300 license are already connected to the server.

You may need to purchase additional Alliance 8300 client licenses from GE.

- *What does this message mean: “No security packages are installed on the machine, or the user is not logged on, or there are no compatible security packages between the client and server”?*

Communications may be blocked by DCOM Services permissions or by a firewall (in the case of Windows XP SP2). Use the **SpInitClient** utility (see [SpInitClient.exe](#) on page 212) to configure these items for the client computers and then restart the Alliance 8300 services.

More than one client computer may be involved. The client displaying the error message (affected client) may be unable to connect to a panel which is hosted by a different client (host).

After using the **SpInitClient** utility on both client computers, restart the services on the host before restarting the services on the affected client.

Using Alliance 8300

- *Can I customize the toolbar and add more buttons?*

No. The toolbar cannot be customized and buttons cannot be added to the toolbar.

You can, however, change the position of the toolbar. Simply click and drag the toolbar wherever you would like it to be on the screen.

- *How do I perform a search on a specific item?*

The **Search** button can be found on any form that provides search capabilities. If you click on this button and the current form is blank, all records will be returned. To specify a criteria, simply fill in the desired information. For example, if you want to find all badgeholders with the last name Smith, type Smith in the Last name field and click on the **Search** button.

You can also use the * character which allows you to search for patterns. For example, to search for badgeholders with the last name starting with Sm* would yield such names as Smith and Smithers.

- *Why can't I delete a record?*

Some forms, such as the Door/Output Status Form and the Door/Output Control Form, do not contain a Delete button because they display status information only.

Other forms, such as the **Alarm Form** or **Alarm Category** also do not contain a **Delete** button. To keep the system stable, NO ONE is given permission to delete these records, not even a System Administrator. These records are deleted when the associated control panel is deleted. However, on all other forms, you may be assigned the permission action **All**. (Permission actions are assigned using the Permission Form. Verify that the permission assigned to the operator on the Operator Form contains the desired permission actions by checking that permission on the Permission Form.) If you can't delete on those forms, you do not have permission to do so.

- *Why are there no alarms being displayed on the Alarm Monitor Form?*

Go to the **Alarm Form** and click on the **Alarm** tab. Make sure that the **Monitor** option is enabled.

- *How do I get into the Badge Design program?*

1. You must have the **Alliance 8300 Imaging** option installed. Refer to your *Alliance 8300 Installation Manual* for more information on installing this package.
2. The Alliance 8300 client you are using must have a license for Imaging. Select **Operations | Client Monitor**. The bottom section of the Client Monitor Form contains the section Imaging Information. (You may need to make the window larger to display the number of Imaging licenses presently in use and the number of Imaging licenses you are allowed, as purchased with your system.) Locate the name of your computer in the Client list. Then, look in the column **Imaging status** and verify that it reads **Enabled**.

(If **Imaging** status reads **Disabled** and the numbers indicate a license is available for

use, select **Administration | Client**. On the Client Form, Client tab, select **Enabled** in Imaging Status to enable **Imaging**. Return to the Client Monitor Form to check the Enabled status.)

3. If you have the **Alliance 8300 Imaging** option installed and your client has a license, you will need a badge design file. You should create your own and then save it in your Alliance 8300 Designs folder. The **Edit Badge Design** button becomes enabled allowing you to enter the Badge Design program.

- *When I run DiagView and try to open a file, only one logfile shows in the Logfile Dialog.*

This indicates the database cannot be accessed. Test the database connection.

- *Services shut down while DiagView is running. A dialog box pops up and displays the message Diagnostic Manager Service has Shutdown. After I restart services, no new messages are displayed.*

Communication has been lost with the services and the file needs to be reopened again when the services are up and running (refer to *Table 3*).

- *I do not understand the order in which the services should be shut down and started.*

Shutting down the Diagnostics Service will shut down the other Services. Note the service dependencies as described in *Table 3*.

Table 3. Service Dependencies

Service	Dependency
Alliance 8300 Diagnostics	MSDE 2000
Alliance 8300 System Manager	Diagnostics
Alliance 8300 Manager	Diagnostics, System Manager

- *I shut down my license domain server (cold boot). My clients are reporting database errors (that is, they have lost their network connection).*

This can occur when the network goes down for any purpose (common examples: hub loses power temporarily; network cable cut or broken).

It is best to either have clients use the **Client Monitor** form to force users off, or notify all clients to restart after a cold boot of the server is complete and after services have restarted on the license domain.

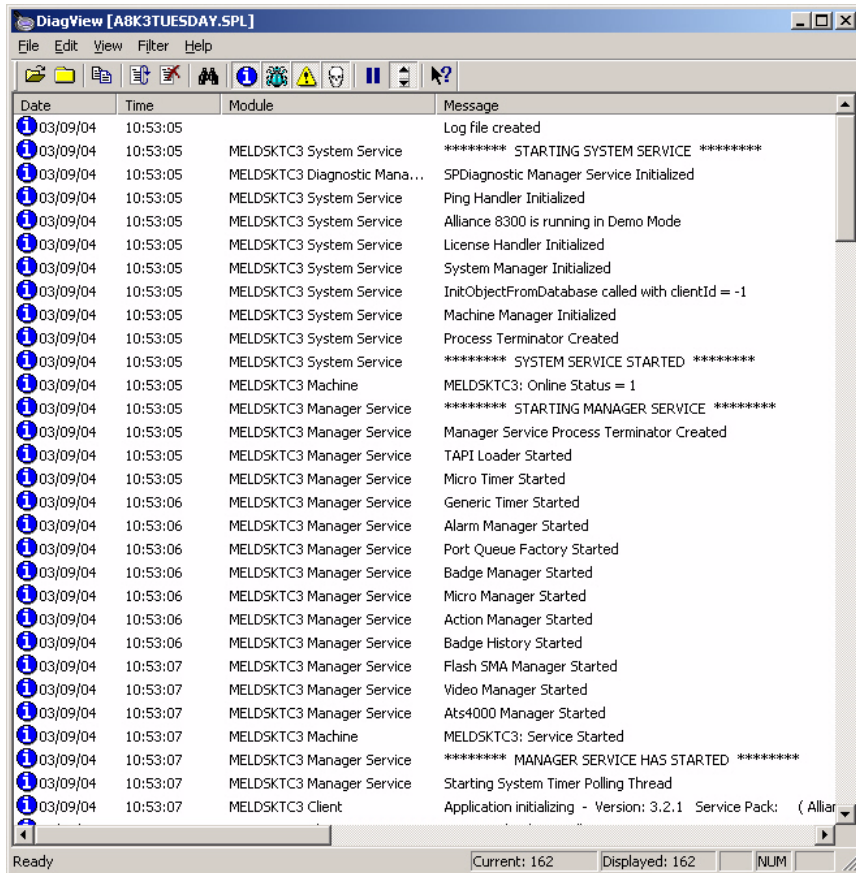
- *My services will not shut down from the Services window. Is there something I can do besides rebooting the system?*

Run the utility *SPStop.exe* found in the *Alliance 8300* folder. See [SPStop.exe](#) on page 217.

- *What should a normal startup of services look like in the logfile?*

It should look similar to the following with the exception of machine name and machine-encoded seed and control panels that may show up in the log. The following sample startup script displays a sequence of key events in the startup process. Note SYSTEM SERVICE STARTED, STARTING MANAGER SERVICE, etc.

Figure 39. Sample services startup



Hardware

- *My COM port is not working as expected. What should I do now?*

Use the **Controller Utility Form** to troubleshoot communications between the host and the control panel.

- Make sure the State field shows the control panel as *Online*. If it is *Offline*, right-click then select *Set Online*. If it is *Error*, then the host is not able to communicate correctly with the control panel.
- If this is a direct-connect control panel, make sure the Connection field shows **Connected**.
- Make sure the baud rate setting for the computer's COM port is 4800.
- Make sure the Comm. device field shows the proper communications port for this control panel, that is, COM1 for COM port 1.

Check the **Status** field to check the condition of the communications (status messages are **Idle** or **Normal**).

If everything looks OK on the Controller Utility Form, check the hardware settings:

1. Click **Start**, **Settings**, and then **Control Panel**.
2. From the Control Panel window, double-click **System**, then select **Device Manager**, then **Ports**.
3. Check that the baud rate setting for the computer's COM port is 4800.

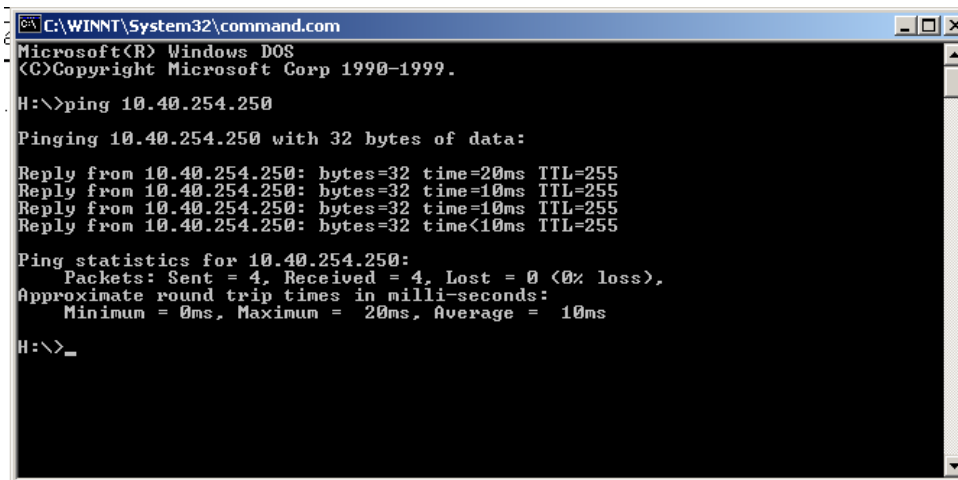
- *My network control panel is not working as expected. What should I do now?*

Follow the same steps as in *COM Port Not Working* (as discussed above). Verify the control panel's IP address from the **Comm Device** field. If no problems are identified on the **Controller Utility Form**, try pinging the control panel using the IP address shown in the **Controller Utility Form**.

For example: `C:\>ping 10.40.254.250`

If the **ping** command fails with a *Request timed out* message, verify that the host IP address is correct, that the host is operational, and that all the gateways (routers) between this computer and the host are operational. You should receive a reply screen display, similar to the following example:

Figure 40. Sample Ping Command Reply Screen



```
C:\WINNT\System32\command.com
Microsoft(R) Windows DOS
(C) Copyright Microsoft Corp 1990-1999.
H:\>ping 10.40.254.250

Pinging 10.40.254.250 with 32 bytes of data:

Reply from 10.40.254.250: bytes=32 time=20ms TTL=255
Reply from 10.40.254.250: bytes=32 time=10ms TTL=255
Reply from 10.40.254.250: bytes=32 time=10ms TTL=255
Reply from 10.40.254.250: bytes=32 time<10ms TTL=255

Ping statistics for 10.40.254.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 20ms, Average = 10ms

H:\>_
```

Server-client communications

- *A client computer is not able to remote-control a panel.*

Communications may be blocked by DCOM Services permissions or by a firewall (in the case of Windows XP SP2). Use the **SpInitClient** utility (see [SpInitClient.exe](#) on page 212) to configure these items for the client computers and then restart the Alliance 8300 services.

More than one client computer may be involved. The client displaying the error message (affected client) may be unable to connect to a panel which is hosted by a different client (host).

After using the **SpInitClient** utility on both client computers, restart the services on the host before restarting the services on the affected client.

Uninstalling Alliance 8300

Refer to the *Alliance 8300 Installation Manual* for details.

Appendix A CCTV support

Alliance 8300 interfaces with CCTV (Closed Circuit Television) systems. The systems are CCTV control systems that operate separately from Alliance 8300 and require their own hardware and software provided by the CCTV manufacturer. The interface between the CCTV system and Alliance 8300 provides the capability to automatically control CCTV cameras based on alarms within Alliance 8300.

In this appendix:

<i>Setup and configuration</i>	182
<i>Digital video recorders (DVRs)</i>	182

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:

- *Alliance 8300 CCTV Interface Operator's Guide* covers setup and configuration of the CCTV system with Alliance 8300.
- *Alliance 8300 Online Help* for additional information on setting up CCTV alarms.

Digital video recorders (DVRs)

Alliance 8300 has the ability to integrate with Kalatel digital video recorders.

Using your Alliance 8300 system, you are able to set up, control, search, and view live and recorded video directly from your computer. Refer to the *Alliance 8300 CCTV Interface Operator's Guide* for detailed instructions to setup and configure a DVR system with Alliance 8300.

Appendix B Changing the server name

The Alliance 8300 Professional Server computer holds the Alliance 8300 databases, controls communications with Alliance 8300 client computers, and controls the Alliance 8300 licensing.

In this appendix:

<i>Server name</i>	184
<i>Changing the name in Windows</i>	185
<i>Changing the name in the Windows registry</i>	186
<i>Changing the name in the 8300 database</i>	187
<i>Changing the name in ODBC</i>	188

Server name

The need may arise to change the name of the Alliance 8300 Professional Server computer. This could typically be due to upgrading the computer or moving the Alliance 8300 Professional Server to a different computer.

If you need to move Alliance 8300 Professional 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 Alliance 8300 and restoring the Alliance 8300 databases. However, after installing Alliance 8300 you would still need to relicense the new server and all the clients.

If you have already installed Alliance 8300 on the new server computer and you need to change the server's computer name, you must change it in the following places:

- On the Windows operating system, *Network Identification* tab of your system properties. See [Changing the name in Windows](#) on page 185.
- In the Alliance 8300 registry setting. See [Changing the name in the Windows registry on page 186](#).
- In the Alliance 8300 database. See [Changing the name in the 8300 database on page 187](#).
- In the ODBC data source administrator. See [Changing the name in ODBC](#) on page 188.

Note: Any Alliance 8300 computer (server or client) that has had its computer name changed will lose communication with all controllers (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**. 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**, then **Apply**. You will be asked to reboot your computer. Select **OK**.
6. When the computer reboots, you may receive an error message from MSDE 2000. Click **OK** to close the dialog. This error will be addressed later, as you change the server computer name in MSDE 2000.

Changing the name in the Windows registry

To change the Alliance 8300 Windows registry entry for the computer name:

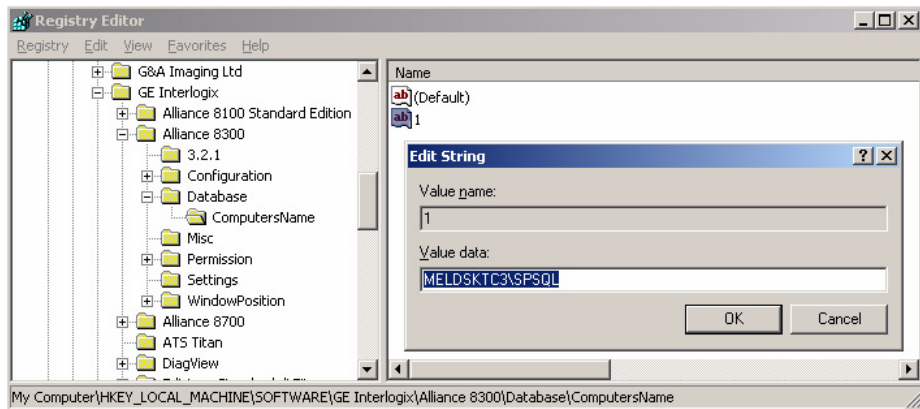
1. Shut down the Alliance 8300 client application.
2. Stop Alliance 8300 services.
3. Click Start, then Run, type *regedit* and then click OK.



CAUTION: Using the Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Neither GE nor Microsoft guarantee 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*, *GE*, *Alliance 8300*, *Database*, and *ComputersName*.
5. On the right side of your screen, double-click the key name **1** to open the *Edit String* dialog box. The screen that displays should look like *Figure 41*.

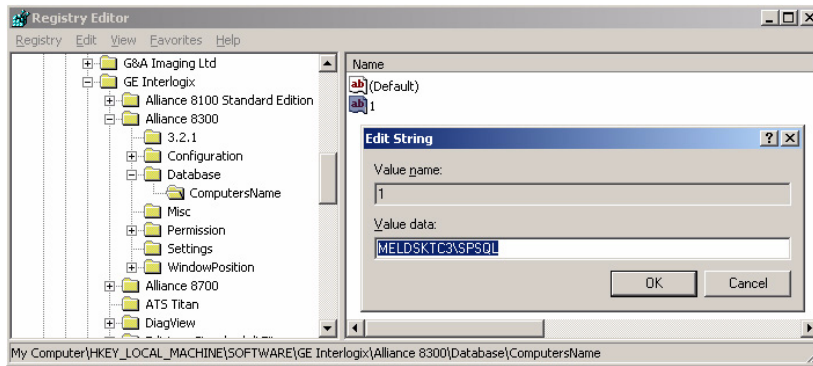
Figure 41. Sample screen



6. Type the new server name in front of *\SPSQL* then click **OK**.
7. Open the following by clicking + in front of *HKEY_LOCAL_MACHINE*, then *SOFTWARE*, *GE*, *Alliance 8300*, *Configuration*, and *Server*.

8. On the right side of your screen, double-click the key titled *Name* to open the *Edit String* dialog box. The screen that displays should look like *Figure 42*.

Figure 42. Registry editor



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 8300 database

Use the SPInitClient utility to update the server and client computers when the Alliance 8300 server computer has its name changed or is moved to a different computer. (Refer to [Changing the server name](#) on page 212 for details.)

Changing the name in ODBC

Open Database Connectivity (ODBC) is used to enable Alliance 8300 (on the server and on clients) to connect with the Alliance 8300 databases on the server computer.

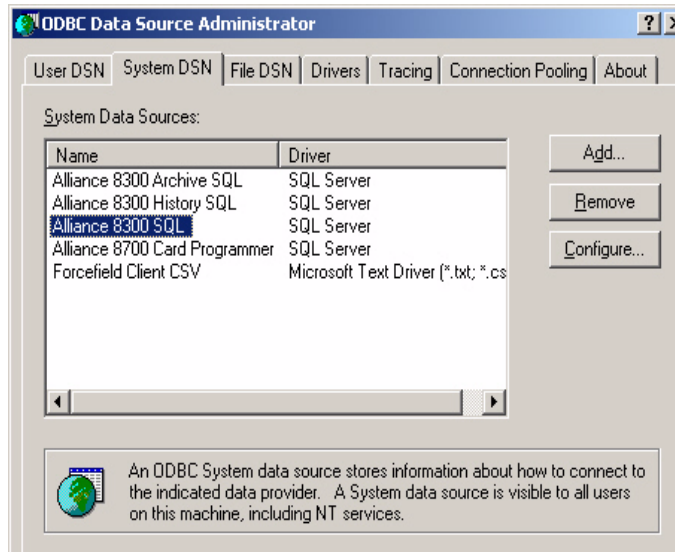
If the name of the server computer is changed, then the new name must be applied to the Alliance 8300 ODBC system data sources for the server and all client computers.

If performing this procedure on an Alliance 8300 client computer, the Alliance 8300 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, do the following:

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

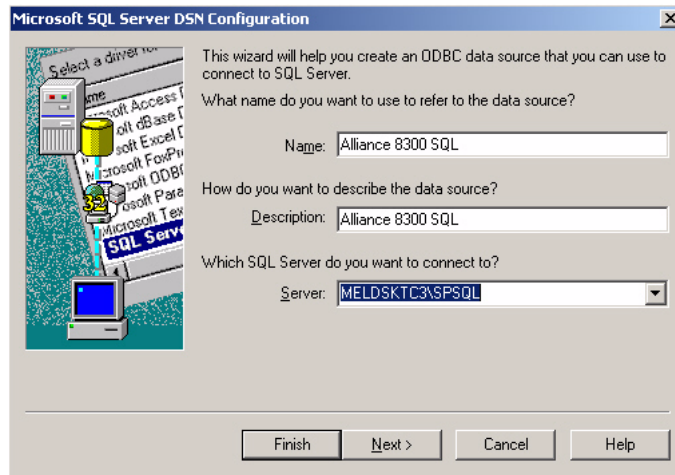
Figure 43. ODBC Data Source Administrator



2. In turn, select each Alliance 8300 item in the Name list (and the Alliance 8700 Card Programmer, if applicable), and then click **Configure**.

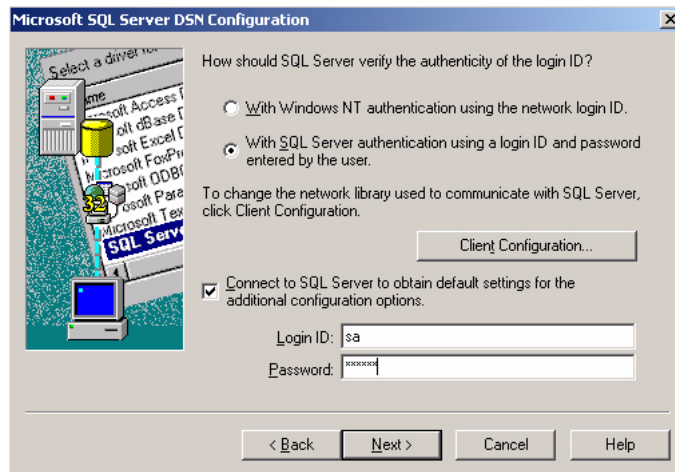
3. The Microsoft SQL Server DSN Configuration window displays (*Figure 44*).

Figure 44. Microsoft SQL Server DSN Configuration



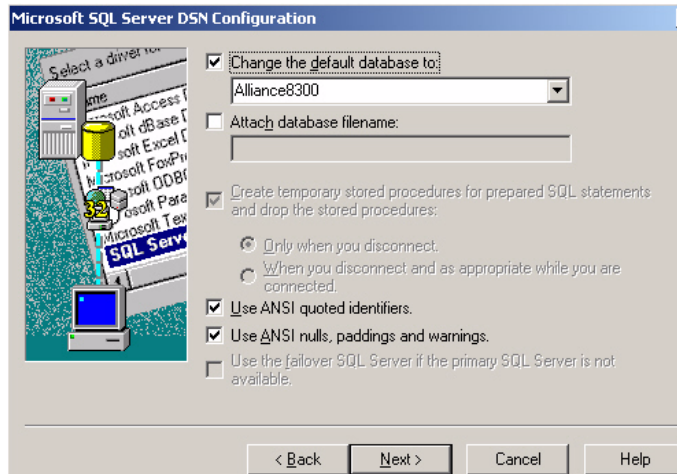
4. Click the **Server** arrow, select the Alliance 8300 server from the list, and then click **Next** (*Figure 45*).

Figure 45. Login ID and password



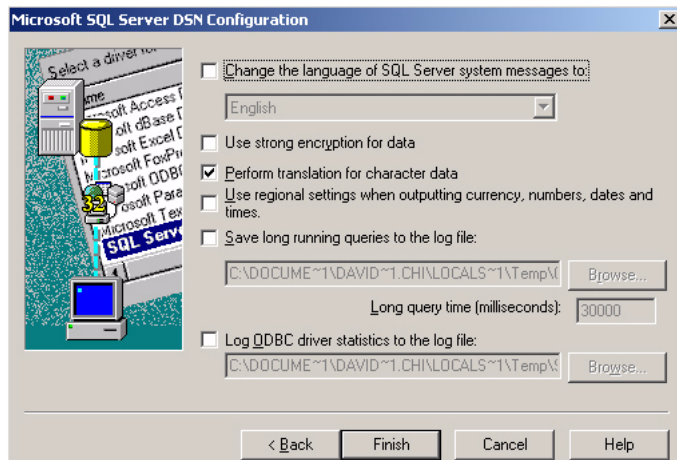
5. Type 'sa' in the **Login ID** field, and 'master' (or other password if it has been changed) in the **Password** field, and then click **Next**.
6. Accept the defaults and click **Next** (Figure 46).

Figure 46. Accept the defaults



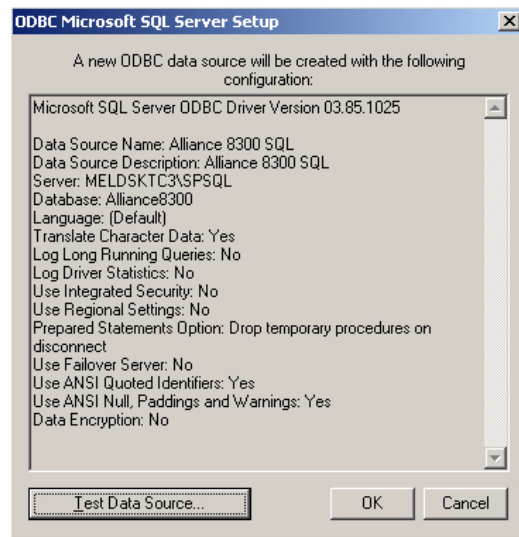
7. Accept the defaults and click **Next** (Figure 47).

Figure 47. Finish



8. Click **Finish** (Figure 48).

Figure 48. ODBC Microsoft SQL Server Setup



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

Appendix C Managing passwords

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 an Alliance 8300 system administrator needs to know about.

In this appendix:

<i>Windows user passwords</i>	194
<i>Database passwords</i>	197

Windows user passwords

Alliance 8300 has a default local Windows user account named **secure**. In addition to this account, each Alliance 8300 operator should have their own Windows user account (either a local or a domain account).

The procedures for changing Windows user passwords is described in the following sections:

- *Changing the secure password* on page 194.
- *Changing other Windows users' passwords* on page 196.

Changing the secure password

If the password for **secure** is changed on one Alliance 8300 computer, then it must be changed to the same password on all Alliance 8300 server and client computers.

The **secure** password is changed differently on the Alliance 8300 server and client computers:

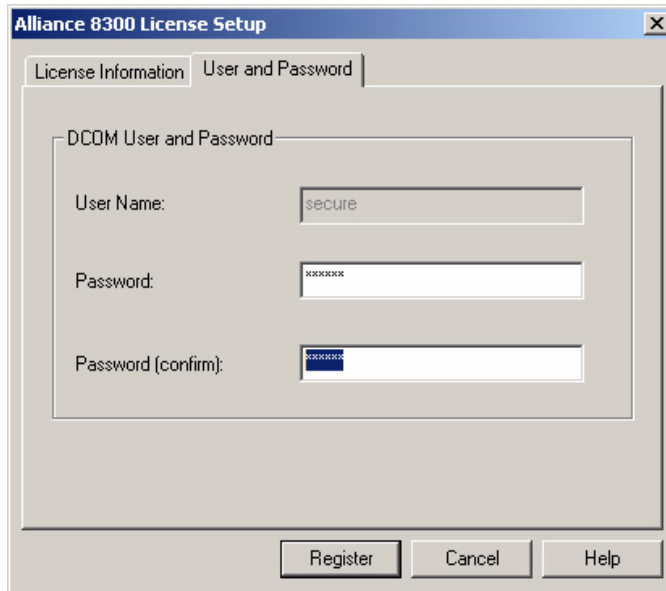
- On the Alliance 8300 server computer use *Server procedure* on page 194.
- On each Alliance 8300 client computer use *Client procedure* on page 195.

Server procedure

Use the following process on the Alliance 8300 server computer to change the password for the Window user account **secure**.

1. Click **Start | Programs | Alliance 8300 | Alliance 8300 License**. The *Alliance 8300 License Setup* screen displays.
2. Click the *User and Password* tab to display the *DCOM User Name and Password* fields.

Figure 49. Alliance 8300 license setup



3. Type the new password in the *Password* field, and then retype the new password in the *Password (confirm)* field. Click **Register** to apply the change. The *Alliance 8300 License Setup* screen closes.

Client procedure

The password for *secure* must be changed on the Alliance 8300 server before it can be changed on the clients. See [Server procedure](#) on page 194 for details.

1. Press **Ctrl+Alt+Del** to display the *Windows Security* dialog.
2. Click **Change Password**.
3. Type *secure* in the user name field.
4. Click the *Log on to* arrow and select the local computer name.
5. Type the current password in the *Old Password* field.
6. Type the new password in the *New Password* field.

7. Retype the new password in the *Confirm Password* field.
8. Click **OK**.
9. Relicense the client. Refer to *Preparing A Client Computer| Registering Alliance 8300 Clients* in the *Alliance 8300 Installation Manual* for details.

Changing other Windows users' passwords

The following procedure may be used to change the password of any Windows user account (other than *secure*). You must know the current password in order to change it.

The password for domain Windows user accounts may be changed domainwide (the server and all clients).

The password for local Windows user accounts must be changed at every Alliance 8300 computer.

Server and clients procedure

1. Press **Ctrl+Alt+Del** to display the *Windows Security* dialog.
2. Click **Change Password**.
3. Type the required Windows user name in the *user name* field.
4. Click the *Log on to* arrow and select the local computer name or domain name (depending on whether the Windows user is a local or domain user).
5. Type the current password in the *Old Password* field.
6. Type the new password in the *New Password* field.
7. Retype the new password in the *Confirm Password* field.
8. Click **OK**.
9. For local Windows user accounts, you must repeat steps 1 through 6 at every Alliance 8300 computer, ensuring that the new password is identical in each instance.

Database passwords

This section describes the use of the *Alliance 8300/8700 Database Maintenance* utility for:

- *Changing the sa password* on page 197
- *Resetting the application password* on page 199

Both the Alliance 8300 and Alliance 8700 applications use MSDE. During installation, an SQL user *sa* (system administrator) with password *master* is created, and must not be changed until after installation has been completed.

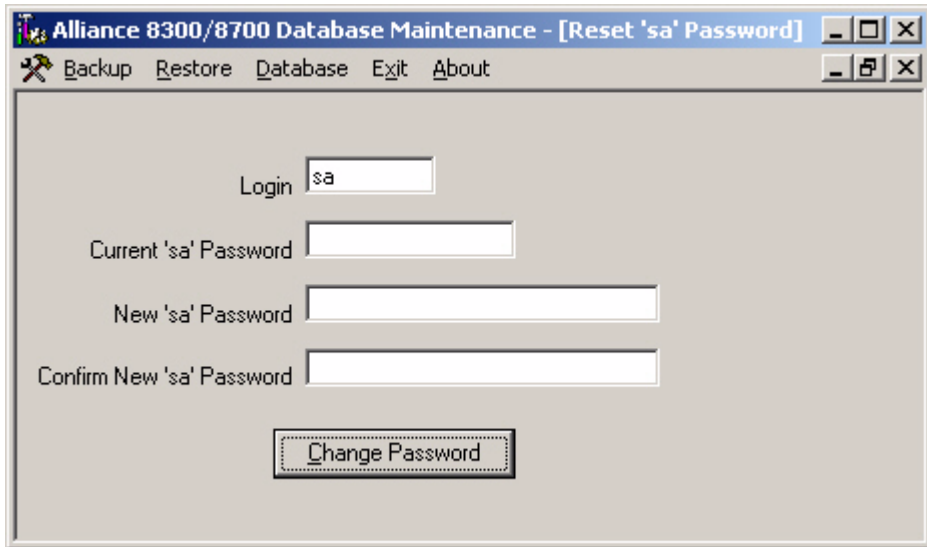
Changing the sa password

We strongly suggest that you assign a unique password of your choice for the MSDE 2000 system administrator (*sa*), for increased security against database intrusion by computer software viruses and hackers.

To change the MSDE 2000 password for user *sa* (system administrator) on an Alliance 8300 Professional Server computer (or on a standalone Alliance 8700 computer) using the Maintenance utility:

1. Navigate to the *DbScripts* folder of your computer (in either the *Alliance 8300* or *Alliance 8700*, folder as applicable) and double-click the *Maintenance.exe* file. The *Alliance 8300/8700 Database Maintenance* utility window displays.
2. From the **Database** menu, select **Reset 'sa' Password**. The **Alliance 8300/8700 Database Maintenance [Reset 'sa' Password]** window displays.

Figure 50. Reset sa Password Window



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.

Note: If a computer has **both** Alliance 8300 and Alliance 8700 installed, changing the *sa* password for one application will also change the *sa* password for the other application.

Resetting the application password

As applicable to Alliance 8300

Alliance 8300 licensing uses the Alliance 8300 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 Alliance 8300) as part of a troubleshooting process or to correct a problem when the following occurs:

- The Alliance 8300 server computer's hardware configuration has changed.
- One or more of the Alliance 8300 services does not start.
- Alliance 8300 on a remote client computer does not start or cannot connect with the Alliance 8300 server computer.

Resetting the Alliance 8300 application password does the following:

- Sets the application password to **devel**. *The application user name and password are not normally seen by Alliance 8300 operators, and no user action is required. This detail is for information only.*
- Removes the current Alliance 8300 license registration number.
- Puts the Alliance 8300 system into 'demo' mode and will need to be relicensed. Refer to the *Alliance 8300 Installation Manual* for details about licensing Alliance 8300.

As applicable to Alliance 8700

You may need to reset the application password if:

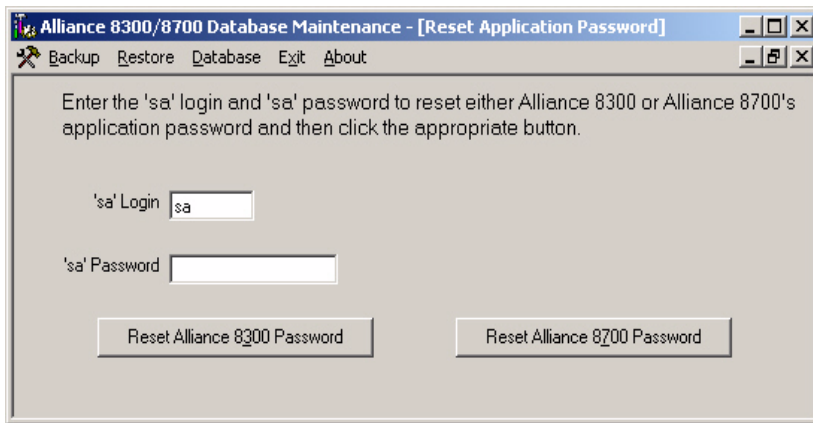
- The Windows registry entry was deleted or corrupted.
- You wish to change the encrypted application password as a security precaution.

Procedure

To reset the application password on an Alliance 8300 Professional Server computer (or on a standalone Alliance 8700 computer) using the Maintenance utility:

1. Navigate to the DbScripts folder of your computer (in either the Alliance 8300 or Alliance 8700, folder as applicable) and double-click the Maintenance.exe file. The Alliance 8300/8700 Database Maintenance utility window displays.
2. From the **Database** menu, select **Reset Application Password**. The **Alliance 8300/8700 Database Maintenance [Reset Application Password]** window displays.

Figure 51. Reset Application Password Window



3. Type the current system administrator password and login, and then click **Reset Alliance 8300 Password** or **Reset Alliance 8700 Password** (as required).
4. Exit the **Alliance 8300/8700 Database Maintenance** utility.

Note: Resetting the Alliance 8300 application password puts the Alliance 8300 system into demo mode and will need to be relicensed. You will need to contact GE during business hours to complete the relicensing process. Refer to the *Alliance 8300 Installation Manual* for details.

Appendix D Adding Windows users

This section describes Window users and groups and how to add user accounts for Alliance 8300 operators.

In this appendix:

<i>Windows users and groups</i>	202
<i>Adding Windows users</i>	204

Windows users and groups

Windows impose certain rules for user accounts in order to permit access to computers (either locally or remotely). It is required that Alliance 8300 operators have Windows user accounts that are correctly created and have the correct permissions (as provided by group membership).

This section does not describe how to create Windows user accounts. Please refer to your Windows documentation.

Windows user accounts are used by the Alliance 8300 server and each of the Alliance 8300 clients in order to provide security credentials. Security credentials enable the Alliance 8300 system and Alliance 8300 operators to access files and folders across the network, and to remotely control the security system, regardless of the network location. These security credentials are provided by membership to the default groups named *AllianceGroup* and *AllianceAdmin* (see [Default Windows groups](#) on page 202).

Windows users may be:

- Local users (communicating as a workgroup).
- Domain users (communicating within the domain).
- The Alliance 8300 server and each Alliance 8300 client communicate as a workgroup via the default local Windows user account named **secure**.

Default Windows groups

During the Alliance 8300 installation, default local groups named *AllianceGroup* and *AllianceAdmin* are automatically created.

These groups are then used by the default local Windows user account named *secure*, and are available for use by any other local or domain Windows users.

By assigning a user to a group, you give the user all the permissions and rights required to operate Alliance 8300. For example, an Alliance 8300 operator would typically be a member of *AllianceGroup*, and an Alliance 8300 administrator would typically be a member of *AllianceAdmin*.

Default Windows user *secure*

During the Alliance 8300 server installation, a default local Windows user account named *secure* is automatically created. The account details are:

- A login ID *secure*
- A password defined during installation (the default password is *master*).
- Membership of local groups *AllianceGroup*, *AllianceAdmin*, and *Administrators*.

This login ID and password combination is also the default Alliance 8300 operator login ID and password.

If during installation, the Windows user *secure* was given the default password *master*, we recommend that you change the password on all Alliance 8300 client and server computers. Use the same password for each computer, record the password and keep it in a secure location. See [Changing the *secure* password](#) on page 194.

The default local Windows user account *secure* is used by Alliance 8300:

- As the DCOM (Distributed Component Object Model) account.
- To access shared folders over the network.
- For authentication purposes. Authentication enables the Alliance 8300 client to access the databases on the server (through a firewall, if applicable) and for the Alliance 8300 services to communicate between clients and the server.

The same *secure* user name and password combination must be used on all Alliance 8300 client and server computers. Alliance 8300 clients automatically adopt the *secure* password on the server when the clients are relicensed.

Adding Windows users

We recommend that you set up additional Windows user accounts for Alliance 8300 operators. Additional Windows user accounts are required so that operators do not log on to Windows as *secure* with full administrative privileges.

The process of adding Windows users depends on whether the user accounts are local or domain accounts:

- Local users — The Windows user account must be created (with identical user name and passwords) on each Alliance 8300 computer (server and clients).
- Domain users — The Windows user account must be created by the domain administrator.

In either case, once the Windows user account has been created, it must be assigned to a group on each Alliance 8300 computer (server and clients). Refer to [Assigning Windows users to groups](#) on page 204 for details.

Assigning Windows users to groups

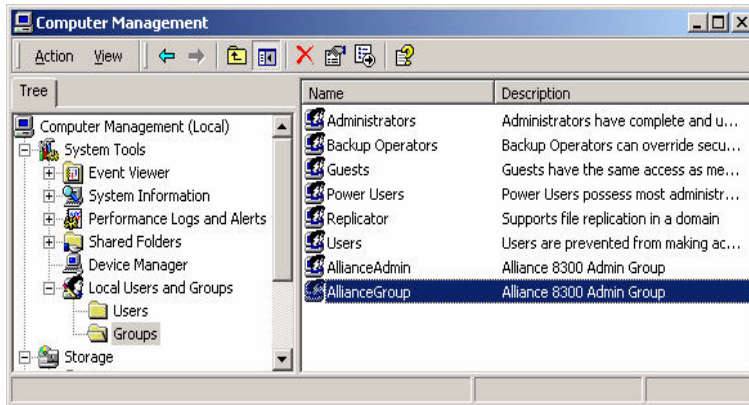
Every Windows user account must be assigned to at least one of the local user groups **AllianceGroup** or **AllianceAdmin** on every Alliance 8300 computer in the system (the server and all of the clients).

This section describes how to add a Windows user to the local group named **AllianceGroup**. The steps for assigning a Windows user to **AllianceAdmin** would be similar.

To assign a Windows user to a group, do the following:

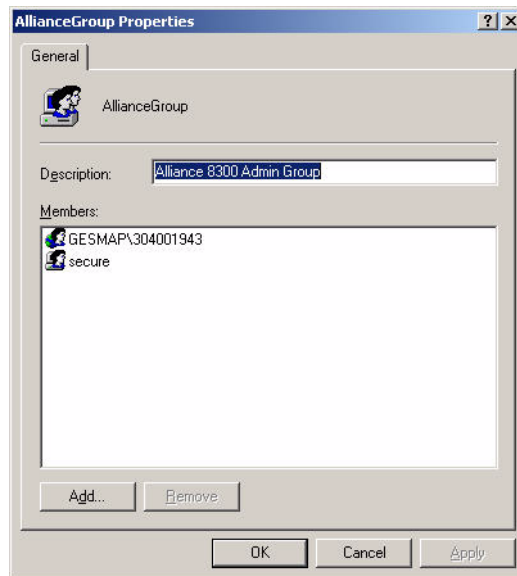
1. Click **Start | Settings | Control Panel**.
2. In **Control Panel**, double-click **Administrative Tools**, and then double-click **Computer Management**.
3. Expand **Local Users and Groups** then click **Groups**. Your screen should look similar to *Figure 52*.

Figure 52. alliance admin group window



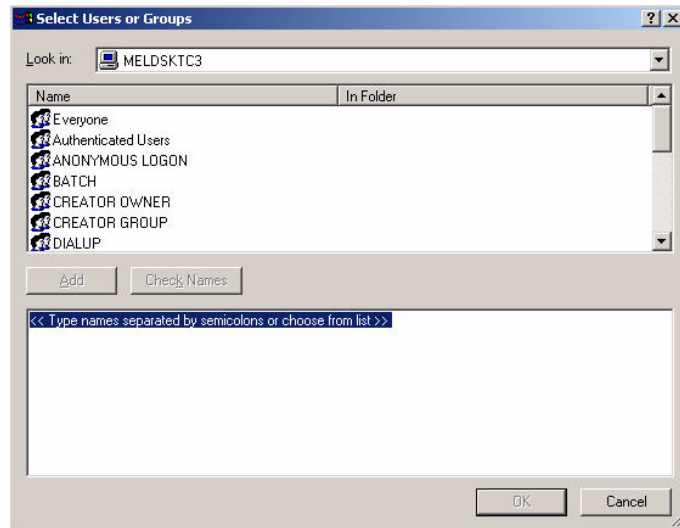
4. Double-click the name **AllianceGroup**. Your screen should look similar to *Figure 53*. Note the default Windows user name of *secure*.

Figure 53. Alliance group properties



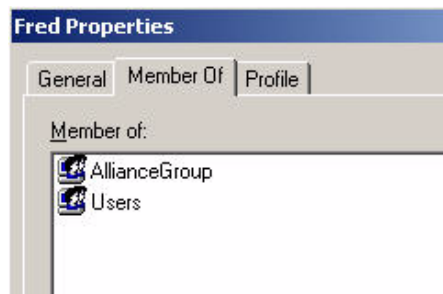
5. Click the **Add** button. The *Select Users or Groups* window displays.

Figure 54. .Select users or groups



6. Click the *Look in* arrow and select either the local computer name or the domain name, as required.
7. Type the name of the Windows user or select from the list.
8. Click **OK**. The window should look similar to the following properties of the Windows user Fred.

Figure 55. Fred properties?



Appendix E Alliance 8300 utilities

Alliance 8300 has a number of utilities that are used for a variety of tasks. This Appendix is a summary of these utilities, ordered by functional area as follows:

Database utilities on page 208

System administration utilities on page 212

Database utilities

Refer to the following pages for database-related tasks:

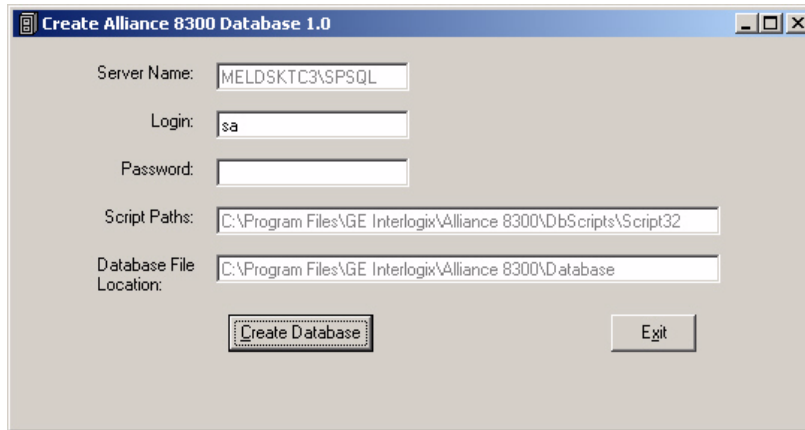
- **Creating** — See *Creating the database* on page 208 for details about the Create Alliance 8300 Database utility (CreateA8K3DB.exe).
- **Removing** — See *Removing the database* on page 209 for details about the Remove Alliance 8300 Database utility (RemoveDB.exe).
- **Backing Up** — See *Backing up Alliance 8300 and 8700 databases* on page 154 for details about the Alliance 8300/8700 Database Maintenance utility (Maintenance.exe).
- **Restoring** — See *Restoring Alliance 8300 and 8700 databases* on page 160 for details about the Alliance 8300/8700 Database Maintenance utility (Maintenance.exe).
- **Updating** — See *Updating the database* on page 210 for details about the Alliance 8300 Database Converter utility (ConvertAlliance8300.exe).
- **Changing passwords** — See *Database passwords* on page 197 for details about changing password for the SQL user **sa**.

Creating the database

The **Create Alliance 8300 Database** utility (CreateA8K3DB.exe) is used only during the initial installation of Alliance 8300 and is described in the *Alliance 8300 Installation Manual*.

Create Alliance 8300 Database may be launched via the **Start | Programs | Alliance 8300 | Create Alliance 8300 Database** option.

Figure 56. Create Alliance 8300 database

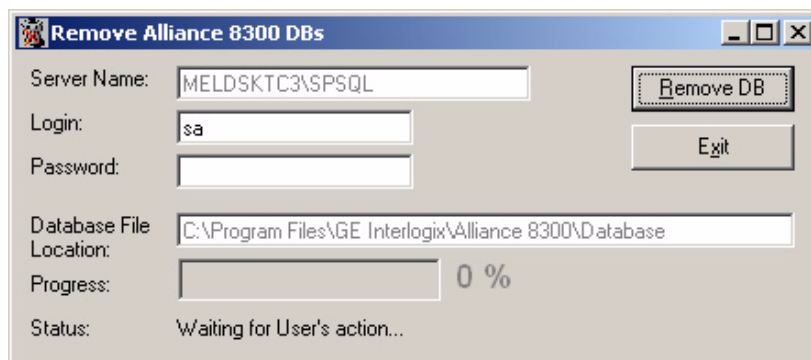


Removing the database

The **Remove Alliance 8300 Database** utility (RemoveDB.exe) is used only when it is necessary to uninstall Alliance 8300 and is described in the *Alliance 8300 Installation Manual*.

Remove Alliance 8300 Database may be launched via the **Start | Programs | Alliance 8300 | Remove Alliance 8300 Database** option.

Figure 57. Remove Alliance 8300 database



Updating the database

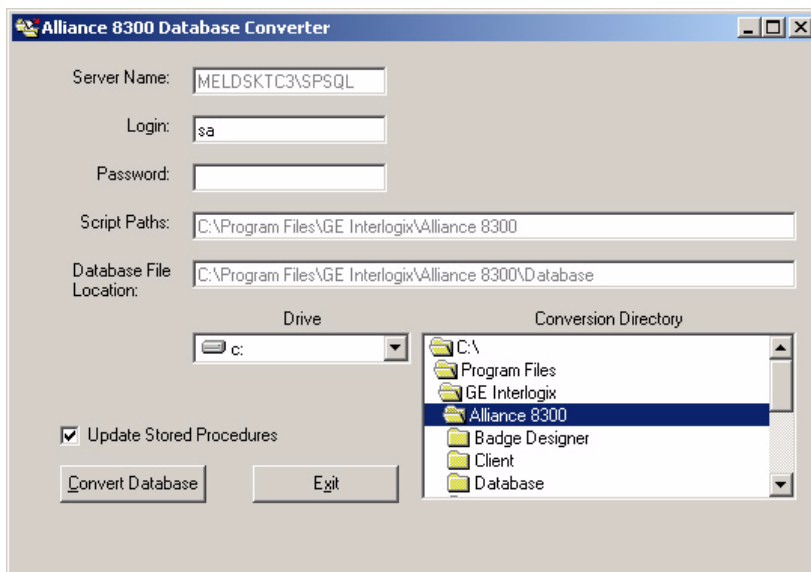
Later versions of Alliance 8300 may have different database schemas (different versions of one or more databases and their tables).

To accommodate changes in the Alliance 8300 databases, the **Alliance 8300 Database Converter** utility (ConvertAlliance8300.exe) converts the databases from an earlier version to a later version.

To convert the Alliance 8300 databases from an earlier version to a later version:

1. Stop Alliance 8300 services in the **following order**:
 - Alliance 8300 Manager
 - Alliance 8300 System Manager
 - Alliance 8300 Diagnostics
2. Run the Alliance 8300 Database Converter utility (ConvertAlliance8300.exe) located in (typically) *C:\Program Files\GE\Alliance 8300\DbScripts*.
3. The **Alliance 8300 Database Converter** window displays.

Figure 58. Alliance 8300 database converter



4. Type the password for the login 'sa'. The server name, login, script paths, and database file location edit boxes are completed automatically.
5. In the **Conversion Directory** window, navigate to the location that holds appropriate conversion files (supplied with the updated Alliance 8300 files) to update both the database structure and contents.
6. The **Update Stored Procedures** box is selected by default. This setting is appropriate for performing a single update, however, you might want to clear the box if you wanted to perform a series of updates as quickly as possible (in which case you would need to select the box for the last update in the series).
7. Click **Convert Database**.
8. Restart Alliance 8300.

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 *Changing the server name* on page 212).
- If you have upgraded Windows XP to Service Pack 2 on the server or a client, and you do not want to uninstall and reinstall Alliance 8300, you will need to reset the DCOM permissions and the Firewall exceptions — Use the **SPInitClient** utility (see *Setting the DCOM permissions* on page 214).
- If you have added a Windows user and need to manually set permissions — Use the **SPDirShare** utility (see *SPDirShare.exe* on page 215) and the **SPShare** utility (see *SPShare.exe* on page 216).

For troubleshooting only, you may need to force shut down the Alliance 8300 services — Use the **SPStop** utility (see *SPStop.exe* on page 217).

SplnitClient.exe

Use the **SPInitClient** utility (SPInitClient.exe) to:

- Change the name of the Alliance 8300 server computer on either the server or on a client.
- Create the required DCOM permissions and firewall exceptions when upgrading Windows XP to Service Pack 2.

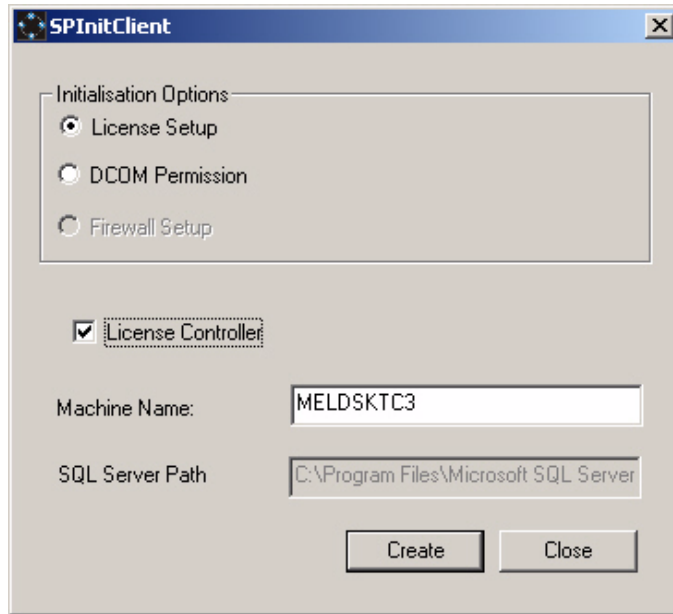
Changing the server name

Use the **SPInitClient** utility when the Alliance 8300 Professional Server computer has its name changed or when Alliance 8300 Professional Server is moved to a different computer.

To change the name of the server computer in the Alliance 8300 database:

1. Shut down the Alliance 8300 client application.
2. Stop Alliance 8300 services.
3. Run the SPInitClient utility located in (typically) *C:\Program Files\GE\Alliance 8300*.

Figure 59. SPInitClient utility



4. Select **License Setup**.
5. Verify that the name of the Alliance 8300 Professional Server computer is displayed in **Machine Name**.

Note: If the entered name is that of an existing registered Alliance 8300 client, running this utility will not change it to the license controller.

6. Select **License Controller** and then click **Create**. This will update the Alliance 8300 database, setting the entered name to be the current license controller server.

Note: Clear **License Controller** and then click **Create** to reconfigure an existing Alliance 8300 client computer when the Alliance 8300 Professional Server computer has its name changed or when Alliance 8300 Professional Server is moved to a different computer.

7. Click **OK** on the subsequent window and exit SPInitClient.

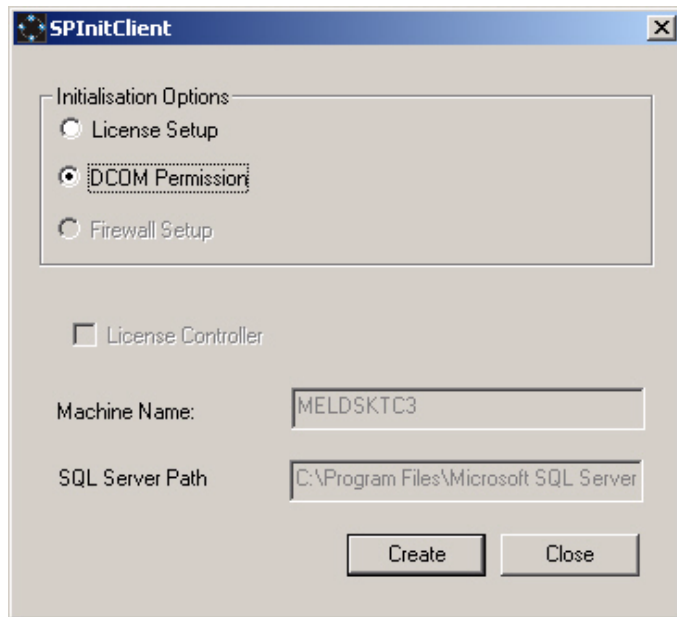
Setting the DCOM permissions

Use the **SPInitClient** utility to configure the required DCOM Services permissions for Alliance 8300.

To set up DCOM permissions:

1. Shut down the Alliance 8300 user interface.
2. Stop Alliance 8300 services.
3. Run the SPInitClient utility located in (typically) *C:\Program Files\GE\Alliance 8300*.

Figure 60. SPInitClient utility



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

This section applies only to Windows XP Service Pack 2.

The process is similar to the previously-described options, and adds the required rules and exceptions to Windows XP Firewall.

SPDirShare.exe

SPDirShare.exe is a command line utility that enables a specified folder to be shared by a specified Windows user group under a share name. If the specified Windows user group doesn't exist it will be created with the description "Alliance 8300 Admin Group".

Any Windows user with membership in the user group will be allowed full access rights to the folder.

Note: You must be logged onto Windows as an administrator to use this utility.

How to use SPDirShare.exe

1. Click **Start | Run**.
2. In the **Open** box, type **cmd** and then click **OK**.
3. In the command window, type *cd* followed by the path to the location of SPDirShare.exe. For example, type *cd Program Files\GE\Alliance 8300* and then press **ENTER**.
4. Type **SPDirShare dir share group**, where:
 - *dir* is the full path name of the specified folder
 - *share* is the share name
 - *group* is the user group

Note: Enclose the name in quotation marks if the path name, share name, or group name contains **spaces** (for example, "C:\Program Files\GE Interlogix\Alliance 8300\Images").

5. Press **ENTER**.
6. Type *EXIT* and then press **ENTER** to close the command window.

SPShare.exe

SPShare.exe is a command line utility that can be used on the Alliance 8300 server (or on a client with the server nominated) to:

- Modify the registry to set up permissions for Imaging.
- Modify the registry to allow a specified Windows user group to have remote access to the registry and to have full access to the *HKEY_LOCAL_MACHINE\Software\GE* registry key and all its subkeys.
- Create a Windows user group with the description “Alliance 8300 Admin Group”.
- Create a user name with the password *master* and the description *Alliance 8300 Default User*.
- Add a user name to a specified user group (and to the Administrators group).
- Create a folder share for a specified user group (full access rights are set for the group). You must be logged onto Windows as an administrator to use this utility.

How to use SPSHare.exe

1. Click **Start | Run**.
2. In the **Open** box, type **cmd** and then click **OK**.
3. In the command window, type *cd* followed by the path to the location of SPSHare.exe. For example, type *cd Program Files\GE\Alliance 8300* and then press **ENTER**.
4. Type **SPShare *dir share group user server***, where:
 - *dir* is the full path name of the specified folder
 - *share* is the share name
 - *group* is the Windows user group
 - *user* is the Windows user name
 - *server* is the server name (optional). If no server name is specified it is assumed that the currently used system is the server.

Note: Enclose the name in quotation marks if the path name, share name, group name, user name, or server name contains **spaces** (for example, "C:\Program Files\GE Interlogix\Alliance 8300\Images").

5. Press **ENTER**.
6. Type *EXIT* and then press **ENTER** to close the command window.

If you run SPShare without parameters, it only modifies the registry to set up permissions for Imaging (the same is true whenever the total number of parameters is less than four).

If the folder name, share name, group name, and user name are all entered, SPShare performs the following tasks in sequence:

1. If the specified user group doesn't exist it is created with the associated description *Alliance 8300 Admin Group*.
2. If the specified user name doesn't exist it is created with the password *master* and the associated description set to *Alliance 8300 Default User*.
3. The specified user name is added to the specified user group and to the Administrators group.
4. A folder share is created for the specified folder, share name, and user group name (full access rights are set for the group). If both the folder name and share name are blank no folder share will be created.
5. The registry is modified to allow the specified user group to have remote access to the registry.
6. The registry is modified to allow members of the user group to have full access to the HLM\Software\GE registry key and all its subkeys.

SPStop.exe

The utility **SPStop.exe** is used to shut down Alliance 8300 services when they will not shut down from the Services window (*Figure 36* on page 160).

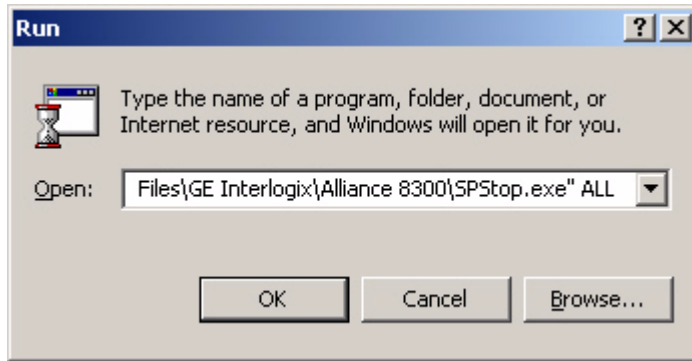
Only use **SPStop.exe** to shut down Alliance 8300 services when they do not shut down normally.

Click **Start**, then **Run**. At the Run window, browse to:

Program Files\GE\Alliance 8300\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 61. Run window



Glossary

This glossary lists a few key terms.

Term	Definition
Access groups	Alarm groups, door groups, and floor groups assigned to a person profile.
Alarm group	<p>Alarm groups provide the means to control the system alarm functions (also called alarm control) for person profiles, zones, doors, and arming stations.</p> <p>Alarm groups have areas and timezones, menu options, and panel options.</p> <p>Alarm groups are assigned to person profiles, and therefore to each piece of equipment the person profile uses to perform functions.</p>
Badge	<p>A badge typically has a unique identity number consisting of a badge number and site code. The term <i>badge</i> includes Smart Cards, magnetic stripe cards, card plus PIN, or PIN only.</p> <p>A badge record associates a badge with a person and a badge group.</p>
Badge group	Badge groups tell the Alliance 8300 system which badges need to be downloaded to which control panels. Badge groups are linked to control panels via the Badge Groups tab of the Controller Setup Form.
Operators	Alliance 8300 users such as installers or security personnel. Operators must be set up in Alliance 8300 using the Operator Form.
Person	<p>A potential user of the security system. A person becomes a user when a badge is assigned via the Badge form.</p> <p>The person record defines which person profile applies to a person.</p>
Person profile	Defines a set of access groups (alarm group, door group, and floor group) which determine the profile's access rights.
User	Person with a badge used to gain access to places under the protection of the security system.

C

cameras	
<i>configuring</i>	87
cards. See badges	
CCTV	
<i>event-triggered</i>	8
client modem pool	69
communication settings	69
control panel	
<i>configuring</i>	81
control panel badge groups	6
controller utility	100
conventions	2

D

database	
<i>backup</i>	148, 154
DCOM	203
debug messages	167
device	
<i>alarm</i>	49
<i>alarm group restrictions</i>	53
<i>alarm groups</i>	51
<i>Alliance installer</i>	50
<i>Alliance setup</i>	49
<i>area database</i>	50
<i>area links</i>	53
<i>arming stations</i>	50
<i>auto arm/disarm</i>	53
<i>auto reset</i>	52
<i>battery test</i>	54
<i>camera</i>	49
<i>central station</i>	52
<i>central station reporting</i>	52
<i>class database</i>	56
<i>clock correction</i>	55
<i>computer connection</i>	52
<i>custom LCD message</i>	51
<i>DGP macro logic</i>	57
<i>digital video recorder</i>	49
<i>door groups</i>	49

<i>DVMR</i>	56
<i>DVR</i>	49
<i>event flag descriptions</i>	55
<i>event to output</i>	53
<i>floor groups</i>	50
<i>holidays</i>	50
<i>IADS DGP</i>	58
<i>IADS DGP devices</i>	58
<i>macro logic</i>	55
<i>next service</i>	51
<i>printer</i>	54
<i>RAS</i>	50
<i>report test</i>	56
<i>system event flags</i>	55
<i>system event to channel mapping</i>	56
<i>system options</i>	51
<i>text words</i>	52
<i>time zones</i>	52
<i>timers</i>	51
<i>TZ to follow output</i>	54
<i>vault areas</i>	53
<i>voice reporting</i>	56
<i>wireless DGP</i>	58
<i>wireless DGP fob sensors</i>	58
<i>wireless DGP zone sensors</i>	58
<i>zone database</i>	50
<i>zone shunts</i>	54
<i>4-door/elevator DGP</i>	57
<i>4-door/elevator DGP card batches</i>	58
<i>4-door/elevator DGP doors</i>	57
<i>4-door/elevator DGP elevators</i>	57
<i>4-door/elevator DGP floors</i>	57
Diagnostic Viewer	165
diagnostics	
<i>turning on</i>	166
<i>viewing</i>	168
diagnostics log	168
DiagView	165
domain environment	72, 171
DSN configuration	189
DVR	49, 182
DVRs	
<i>configuring</i>	87

E	
event trigger	8, 60
events	
<i>accept, reject</i>	101
event-triggered video	8
external reports	
<i>launching</i>	144
F	
facilities	7, 16, 72
facility	
<i>adding</i>	75
<i>managing</i>	78
facility records	7
file	
<i>create default template</i>	42
<i>delete</i>	41
<i>exit</i>	42
<i>export</i>	42
<i>log off</i>	41
<i>new record</i>	40
<i>notes</i>	41
<i>print preview report</i>	41
<i>print report</i>	41
<i>print setup</i>	41
<i>save record</i>	40
<i>save template as</i>	42
<i>set as default template</i>	42
H	
help	39
<i>about Alliance 8300</i>	63
host parameter setup	18
I	
imaging	115, 156
<i>enable</i>	116
<i>license</i>	116
<i>permissions</i>	216
<i>status</i>	116
<i>users</i>	216
IUM	5, 95
J	
J18 port	24
K	
key concepts	5
L	
learn badge	97
logfile	
<i>creating</i>	167
<i>viewing</i>	168
M	
Manager Service	171
master	
<i>badge groups</i>	6
<i>installer</i>	6
<i>user</i>	6
memory expansion	5
memory expansion modules	95
Microsoft Windows Backup	157, 162
modem pool	69
modems	
<i>available</i>	69
<i>client</i>	69
<i>disconnect after idle</i>	69
<i>pool</i>	69
<i>reserved</i>	69
N	
network	
<i>adding share names</i>	215, 216
<i>adding users</i>	215, 216

<i>domain</i>	72, 171
<i>permissions</i>	72, 171
network control panels	
<i>modifying/removing clients</i>	118

O

ODBC	188
online help	39
operations	
<i>alarm graphics editor</i>	45
<i>alarm graphics viewer</i>	45
<i>alarm monitor</i>	45
<i>area control</i>	110
<i>area status</i>	110
<i>arming station control</i>	46
<i>arming station status</i>	46
<i>badge monitor</i>	44
<i>change password</i>	47
<i>client monitor</i>	45
<i>DGP controller control</i>	46
<i>DGP controller status</i>	46
<i>digital video viewer</i>	46
<i>door/output control</i>	45
<i>select facilities</i>	47
<i>zone control</i>	106
<i>zone status</i>	45
operators	72
<i>adding</i>	76
overview	
<i>system</i>	4

P

parameters	66
password	
<i>database</i>	197
<i>sa</i>	197
<i>system administrator</i>	197
permissions	72
<i>adding</i>	74
<i>form</i>	73
<i>viewing</i>	73

person profile	7
person records	7
personnel	
<i>badge</i>	48
<i>badge design</i>	48
<i>badge groups</i>	48
<i>badge programmer</i>	48
<i>card programmer</i>	48
<i>department</i>	48
<i>person</i>	47
<i>person profile</i>	47
<i>personnel type</i>	47
persons	89
ping	178
PIN-only records	93
printing	
<i>alarm activity</i>	68
<i>badge activity</i>	68

R

RAS	50
regedit	156
registry	
<i>permissions</i>	216
reports	120
<i>administration</i>	61
<i>alarm history</i>	62
<i>Alliance</i>	61
<i>Alliance groups</i>	62
<i>badge</i>	61
<i>badge history</i>	62
<i>door access</i>	62
<i>external</i>	123
<i>external reports</i>	63
<i>filters</i>	119
<i>floor access</i>	62
<i>Microsoft Access</i>	63
<i>MS Access</i>	123
<i>operator history</i>	62
<i>person</i>	61
<i>report templates</i>	124
<i>roll call</i>	62

<i>templates</i>	124
<i>time and attendance history</i>	62
restore	
<i>database</i>	160
<i>files</i>	162
<i>system</i>	163
restoring	
<i>Alliance 8300 archive</i>	160
<i>Professional database backup</i>	160, 162
<i>Professional Server</i>	160
S	
safety terms and symbols	2
search	
<i>clear search</i>	43
<i>recall search</i>	43
<i>search</i>	43
setup	
<i>initial steps for Alliance 8300</i>	13
sharing folders.....	215, 216
smart	
<i>badge</i>	7
<i>card</i>	7
Smart Card Programmer. See Alliance 8700	
SPDirShare.....	215
SPInitClient.....	212
SPStop.....	217
System Manager Service	171
system overview	4
system parameters.....	66

T

templates	124
<i>specified date or time</i>	124
troubleshooting	
<i>questions and answers</i>	169

U

user fields.....	68
------------------	----

utilities

<i>Alliance 8300/8700 Database Maintenance</i>	200
<i>application password</i>	200
<i>backup database</i>	148, 154
<i>convert database</i>	210
<i>ConvertAlliance8300.exe</i>	208, 210
<i>create database</i>	208
<i>CreateA8K3DB.exe</i>	208
<i>maintenance.exe</i>	154, 160, 197, 200, 208
<i>remove database</i>	209
<i>RemoveDB.exe</i>	209
<i>sa password</i>	197
<i>server name</i>	187, 212, 214
<i>SPDirShare.exe</i>	212, 215
<i>SPInitClient.exe</i>	187, 212, 214
<i>SPShare.exe</i>	216
<i>spstop.exe</i>	175, 217
<i>update database</i>	210

V

video

<i>event-triggered</i>	8
------------------------------	---

view

<i>next pane</i>	44
<i>split</i>	44
<i>status bar</i>	36, 44

W

window

<i>arrange icons</i>	63
<i>cascade</i>	63
<i>tile</i>	63
Windows registry	156, 186
Windows user group	216
workgroup	202, 203

Numerics

4-door/elevator DGP

<i>advanced setup</i>	86
<i>basic setup</i>	84

