

E N T R A P A S S TM

SPECIAL EDITION



High Performance Access Control and Integrated Security System

Reference Manual

KANTECH

DN1420-0612/ Version 3.18

© 2006 Tyco Safety Products, Canada, Ltd. All rights reserved.
Specifications may be modified without notice.



SENSORMATIC ELECTRONICS CORPORATION KANTECH – TYCO SAFETY PRODUCTS END-USER LICENSE AGREEMENT

FOR KANTECH Software Provided With or Without Products or Components

IMPORTANT - READ CAREFULLY

KANTECH Software purchased with or without Products and Components is copyrighted and is purchased under the following license terms:

- This End-User License Agreement (“EULA”) is a legal agreement between You (the company, individual or entity who acquired the Software and any related Hardware) and Sensormatic Electronics Corporation (“KANTECH”), the manufacturer of the integrated security systems and the developer of the software and any related products or components (“HARDWARE”) which You acquired.
- If the KANTECH software product (“SOFTWARE PRODUCT” or “SOFTWARE”) is intended to be accompanied by HARDWARE, and is NOT accompanied by new HARDWARE, You may not use, copy or install the SOFTWARE PRODUCT. The SOFTWARE PRODUCT includes computer software, and may include associated media, printed materials, and “online” or electronic documentation.
- Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to You under the terms of that license agreement.
- By installing, copying, downloading, storing, accessing or otherwise using the SOFTWARE PRODUCT, You agree unconditionally to be bound by the terms of this EULA, even if this EULA is deemed to be a modification of any previous arrangement or contract. If You do not agree to the terms of this EULA, KANTECH is unwilling to license the SOFTWARE PRODUCT to You, and You have no right to use it.

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:
 - a Software Installation and Use - For each license You acquire, You may have only one copy of the SOFTWARE PRODUCT installed.
 - b Storage/Network Use - The SOFTWARE PRODUCT may not be installed, accessed, displayed, run, shared or used concurrently on or from different computers, including a workstation, terminal or other digital electronic device (“Device”). In other words, if You have several workstations, You will have to acquire a license for each workstation where the SOFTWARE will be used.
 - c Backup Copy - You may make back-up copies of the SOFTWARE PRODUCT, but You may only have one copy per license installed at any given time. You may use the back-up copy solely for archival purposes. Except as expressly provided in this EULA, You may not otherwise make copies of the SOFTWARE PRODUCT, including the printed materials accompanying the SOFTWARE.
- 2 DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS
 - a 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. You may not make any changes or modifications to the Software, without the written permission of an officer of KANTECH. You may not remove any proprietary notices, marks or labels from the Software Product. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA.



- b **Separation of Components** - The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one HARDWARE unit.
- c **Single INTEGRATED PRODUCT** - If You acquired this SOFTWARE with HARDWARE, then the SOFTWARE PRODUCT is licensed with the HARDWARE as a single integrated product. In this case, the SOFTWARE PRODUCT may only be used with the HARDWARE as set forth in this EULA.
- d **Rental** - You may not rent, lease or lend the SOFTWARE PRODUCT. You may not make it available to others or post it on a server or web site.
- e **Software Product Transfer** - You may transfer all of Your rights under this EULA only as part of a permanent sale or transfer of the HARDWARE, 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 provided the recipient agrees to the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade, any transfer must also include all prior versions of the SOFTWARE PRODUCT
- f **Termination** - Without prejudice to any other rights, KANTECH may 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.
- g **Trademarks** - This EULA does not grant You any rights in connection with any trademarks or service marks of KANTECH or its suppliers.

3 COPYRIGHT

All title and intellectual property rights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, and text incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT, are owned by KANTECH or its suppliers. You may not copy the printed materials accompanying the SOFTWARE PRODUCT. All title and intellectual property rights in and to the content, which may be accessed through use of the SOFTWARE PRODUCT, are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants You no rights to use such content. All rights not expressly granted under this EULA are reserved by KANTECH and its suppliers.

4 EXPORT RESTRICTIONS

You agree that You will not export or re-export the SOFTWARE PRODUCT to any country, person, or entity subject to US export restrictions.

5 CHOICE OF LAW

This Software License Agreement is governed by the laws of the State of New York.

6 LIMITED WARRANTY

- a **NO WARRANTY**
KANTECH PROVIDES THE SOFTWARE "AS IS" WITHOUT WARRANTY. KANTECH DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.
- b **CHANGES IN OPERATING ENVIRONMENT**
KANTECH shall not be responsible for problems caused by changes in the operating characteristics of the HARDWARE, or for problems in the interaction of the SOFTWARE PRODUCT with non-KANTECH SOFTWARE or HARDWARE PRODUCTS.
- c **LIMITATION OF LIABILITY; WARRANTY REFLECTS ALLOCATION OF RISK**
IN ANY EVENT, IF ANY STATUTE IMPLIES WARRANTIES OR CONDITIONS NOT STATED IN THIS LICENSE AGREEMENT, KANTECH'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS LICENSE AGREEMENT SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU TO LICENSE THE SOFTWARE PRODUCT AND FIVE US DOLLARS (USD\$5.00). BECAUSE SOME JURIS-

-
- DICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.
- d DISCLAIMER OF WARRANTIES
THIS WARRANTY CONTAINS THE ENTIRE WARRANTY AND SHALL BE IN LIEU OF ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED (INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE) AND OF ALL OTHER OBLIGATIONS OR LIABILITIES ON THE PART OF KANTECH. KANTECH MAKES NO OTHER WARRANTIES. KANTECH NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON PURPORTING TO ACT ON ITS BEHALF TO MODIFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE PRODUCT.
- e EXCLUSIVE REMEDY AND LIMITATION OF WARRANTY
UNDER NO CIRCUMSTANCES SHALL KANTECH BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES BASED UPON BREACH OF WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER LEGAL THEORY. SUCH DAMAGES INCLUDE, BUT ARE NOT LIMITED TO, LOSS OF PROFITS, LOSS OF THE SOFTWARE PRODUCT OR ANY ASSOCIATED EQUIPMENT, COST OF CAPITAL, COST OF SUBSTITUTE OR REPLACEMENT EQUIPMENT, FACILITIES OR SERVICES, DOWN TIME, PURCHASERS TIME, THE CLAIMS OF THIRD PARTIES, INCLUDING CUSTOMERS, AND INJURY TO PROPERTY.

WARNING: KANTECH recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this SOFTWARE PRODUCT to fail to perform as expected.





Table of Contents

Chapter 1 • Introduction	1
Entrapass Main Features	2
Entrapass Manual and Help	4
Using the Reference Manual	4
Getting Help	4
Technical Support	4
System Architecture	5
Chapter 2 • Software Installation	7
System Requirements	8
Additional Requirements	9
Installation Kit	10
Installation Steps	11
To Install Entrapass Software	11
System Installation	12
System Update	22
Before Updating Your Software	22
To Update your Software	22
Removing the Entrapass Software	26
Chapter 3 • Getting Started	29
Session Start and End	30
To Start the Entrapass Workstation	30
To Access Information on the Workstation Connection Status	31
To Modify Your Work Area Properties	32
To Retrieve Hidden Windows on the Desktop	33
System Stand-Alone Utilities	34
Entrapass Workstation Toolbar	35
Basic Functions	37
To Find Components	37
To Find a Card	39
To Use an Extended Selection Box	40
To Select Components	40
To Select a Specific Folder	42
To Select a Specific Site	43
To Print	43
To View Components Links	44
Chapter 4 • System Devices	47
Entrapass Applications Configuration	48
To Configure an Entrapass Application	48
Defining General Parameters	48
Defining Security Parameters	49
Defining Message Controls	50
Defining Alarm Controls	52
Defining e-Mail Report Options	53
Defining Host Modem and Keypad Delays	55
Sites Configuration	57
To Set Up Communication Timing	58



To Configure a Direct RS-232 Connection Type	58
To Configure an Ethernet Kantech IP Link Connection Type	59
To Configure an Ethernet Polling Connection Type	62
To Configure a Dial-Up (RS-232) Modem Connection Type	63
Controllers Configuration	66
To Configure General Parameters for KT Controllers	66
To Configure a KT-100 Controller	68
To Configure a KT- 200 Controller	69
Defining KT-200 Expansion Devices	70
Defining KT-200 auxiliary devices	70
To Program KT-2252 Elevator Controllers	71
To Program REB-8 Elevator Controllers	72
Defining REB-8 Relays	74
To Configure a KT-300 Controller	75
To Configure the KT-300 Combus module	76
To Define Controller Options for	78
Controller Event Buffer Overflow Message	80
Doors Configuration	81
To Define General Parameters for a Door	81
To Define Door Keypad Options	82
To Define Contact Options	83
To Define REX (Request to Exit) Options	85
To Define Miscellaneous Options	86
To Define Elevator Doors	87
Relays Configuration	90
To Define Relays	90
Inputs Configuration	91
To Define Inputs	91
To Define Relays and Inputs	92
To Define an Input for an Elevator Door	92
To Enable Remote Event Reporting	94
Output Devices Configuration	95
To Define General Options for an Output	95
To Associate Events with Auxiliary Outputs	96
Chapter 5 •Definitions	97
Schedules Definition	98
To Define a Schedule	98
Creating a 2-day Continuous Interval	99
Floors Definition	100
Graphics Definition	101
To Define Components of a Graphic	101
To Design the Background for the Graphic Window	103
To Assign System Components to Graphic Icons	104
Holidays Definition	105
Chapter 6 •Operations.....	107
The Operations Toolbar	108
The Operation Dialogs Toolbar	108
The Operations Contextual Menu	109
The Component Status Window	110
Manual Data Reload	111



Manual Operations on Sites	112
To Perform Manual Operations on a Site	112
Communication Options Available from the Toolbar	113
Manual Operations on Controllers	114
To Select a Controller	115
To Perform a Controller Soft Reset	115
To Perform a Controller Hard Reset	115
To Manually Reload a Controller	116
To Calculate the Number of Cards In	116
To Reset the Cards In Counters	116
Manual Operations on Doors	117
To Select a Door or a Door Group	118
To Lock a Door Manually	118
To Unlock a Door Manually	118
To Unlock a Door Temporarily	119
To Reset a Door Schedule	119
To Enable a Door Reader	119
To Disable a Door Reader	119
Manual Operation on Elevator Doors	120
To Select an Elevator Door	121
To Lock Floors from Elevator Doors	121
To Unlock Floors from Elevator Doors	121
To Temporarily Unlock Floors from Elevator Doors	122
To Reset an Elevator Door Schedule	122
To Enable an Elevator Floor	122
To Disable an Elevator Floor	123
Manual Operations on Relays	124
To Select Relays	124
To Manually Deactivate a Relay	125
To Manually Activate a Relay	125
To Activate a Relay Temporarily	125
To Reset a Relay Schedule	126
Manual Operations on Inputs	127
To Perform Manual Operations on Inputs	127
To Manually Return an Input to its Normal State	128
To Stop Monitoring an Input	128
To Temporarily Stop Input Supervision (Shunt)	128
Chapter 7 •Users	129
Cards Definition	130
To Issue a New Card	130
To Create New Cards Using the "Save as" Feature	131
To Issue Cards Using the Batch Load Feature	131
To View and Verify PINs	132
To View Cards Assigned the Same PIN	133
Cards Handling	134
To Edit a Card	134
To Find a Card	134
To Delete a Card	134
To Customize Card Information Fields	134
Cardholder Access Levels Assignment	136
To Assign an Access Level to a Cardholder	136
Card Use Options Definition	137
To Add Comments to a Card	138



To Assign Pictures and Signatures	138
Assigning a Picture from a File	139
Assigning a Picture Using a Video Camera	140
To Import a Signature from a File	141
To Add a Signature from a Signature Capture Device	142
To Work with Photos and Signatures	143
Extracting Part of an Image	143
Editing a Picture/Signature	146
To Print Badges	147
Selecting a Badge Printer	147
Previewing and Printing Badges	148
Badges Designing	150
To Create a Badge Template	150
Specifying Properties for a Badge Layout	151
Editing a Badge Layout	152
Modifying the Number of Sides	152
Modifying the Background Color	154
Adding Objects to a Badge Layout	156
Incorporating Card Information Fields	156
Aligning Objects in the Template Layout	158
Modifying Card Fields Properties	158
Modifying Picture Properties	160
Adding Static Text Objects	162
Adding Bar Codes	163
Setting Up Barcode Properties	165
Adding The Current Date	165
Adding An Image	168
Placing Other Design Objects	170
Placing a Rectangle	172
To Validate Card Access	172
Cards Printing	174
To Print Cards	174
Last Transactions Display	178
To View the Last Transaction	178
Card Access Groups Definition	180
Access Levels Definition	181
To Create a New Day Pass Using the "Save as" Feature	182
CSV Files Import and Export	184
To Use a Predefined Pattern	184
To Create a New Import/Export Pattern	185
To Export Cards	186
To Import Cards	189
To Correct Import/Export Errors	191
Chapter 8 •Groups	195
Controller Group Creation	196
Door Group Creation	197
Relay Group Creation	198
Input Group Creation	199
Access Level Groups Grouping	200
Floor Group Creation	201



Chapter 9 •System Status	203
Text Status	204
To Display a Component Status	204
Numerical Status	206
To View the Numeric Status of a Specific Gateway	206
Graphic Status	207
To View a Controller Status	207
Database Status	209
To View Information About the Database	209
Server State	211
Chapter 10 •System	213
Operators Definition	214
To Create or Edit an Operator	214
Security Level Definition	217
To Create/Modify an Operator Security Level	217
To Define Login Options for an Operator	218
To Filter Controllers Available to an Operator	220
To Filter Doors Available to an Operator	220
To Filter Access Levels	221
To Filter Reports Available to an Operator	222
To Hide Card Information	223
Event Parameters Definition	225
To Define Events Parameters	225
To Create and View Associations	227
Creating an Association	227
Viewing an Association	228
Deleting and Restoring Associations	228
To Print Event Parameters	229
Instructions Definition	231
To Define an Instruction	231
Message Filters Definition	233
To Define Event for a Message Filter	233
Database Structure Definition	236
To View the Database Components	236
Chapter 11 •EntraPass Desktops	239
Work Area Customizing	240
To Change the Display Properties	240
Specific Desktop Customizing	241
To Customize a Desktop (Full Access Operator)	241
To Customize a Desktop for a "Read-Only" Operator	242
To Transfer a Customized Desktop	243
Message List Desktop	244
To View and Sort System Events	244
To Customize Event Display in the Message Desktops	245
To Perform Tasks on System Messages	247
Picture Desktop	250
To Modify Pictures Display Options	250
Filtered Messages Desktop	252
To Configure a Filtered Messages Desktop	252



Historical Report Desktop	253
To Configure a Historical Reports Desktop	253
To Create and Edit Historical Reports	254
To Display Historical Report State in Real-Time	254
Alarms Desktop	256
To Define an Alarms Desktop	256
To View System Alarm Messages	257
To Display Alarm Desktops Automatically	259
To Acknowledge Alarms/Events	261
Acknowledging an Alarm Message	261
Acknowledging Alarms from the Alarms Desktop	262
Instruction Desktop	263
To View an Instruction about an Alarm Message	263
Graphic Desktop	265
To View Graphics in the Graphic Desktop	265
Chapter 12 •Reports	267
Quick Report Definition	268
To Define a Quick Report	268
Historical Reports Definition	271
To Define a Default “All Events” Report	271
To Define a Custom Historical Report	272
Defining Components for an Historical Report	273
Defining Card Options for an Historical Report	274
To Define a Card Use Report	275
To Define Automatic Report Schedules	276
Specifying Additional Options for an Automatic Report	278
To Define a Report Output Format	279
To Request Historical Reports	281
To Request an Event Report	283
E-mailed Reports	284
To Define a Report to Send by e-Mail	284
Time and Attendance Reports Definition	286
To Define Time and Attendance Reports	286
Time and Attendance (T & A) Reports Request	288
To Request a T and A Report Manually	288
Operations On Time and Attendance	289
To Add Transaction in the Time and Attendance Database	289
Report State	292
Reports Viewing	293
To Display a Report	293
To Preview Historical Reports	294
To Preview Time and Attendance Reports	295
Chapter 13 •EntraPass Options	297
Card Format Modification	298
To Define a Display Format	298
System Language Selection	300
To Change the System Language	300
Printers Selection and Configuration	301
To Select and Set Up a Log Printer	301
To Select and Set Up a Badge Printer	302



System Date & Time Modification	303
Multimedia Devices Configuration	304
To Select an Alarm Sound	304
To Define Video Options	305
To Set Up the Signature Capture Device	306
System Options	307
Server Parameters	307
Schedule	307
Disk Space	307
Icon Status	308
Firmware Parameters	309
KT-300	309
KT-100	309
KT-IP	310
Image Parameters	310
Picture and Badging	311
Graphic	312
Report Parameters	312
CSV	313
Disk Space	313
User Name Format	314
PIN Parameters	314
Custom Messages	316
To Set Up Custom Messages	316
Database Integrity Verification	317
To Perform a Quick Verification of the Database Integrity	317
Chapter 14 •The Server Module	319
Backups	320
To Create Backups of Type D, A, and T	320
To Restore Data (D, A and T)	322
Chapter 15 •System Utilities	323
Database Utility	324
To Verify the Database Integrity	324
To Update Database Fields	325
Vocabulary Editor	327
To Install the Vocabulary Editor	327
To Translate the System Language	327
To Integrate your Custom Language in Entrapass	331
To Distribute the New System Vocabulary	333
To Update the Server Vocabulary	333
To Upgrade the System Vocabulary	335
Express Setup Program	336
To Configure a Controller Using Express Setup	338
Defining Relays	339
Defining Inputs	340
Defining Auxiliary Outputs	340
Quick Viewer	341
Chapter 16 •Animated Icons	343
Controllers	344
Doors	346



Relays	350
Inputs	352
Sites and Gateways	354
Gateway (Gateway Software Interface):	356
EntraPass Application	357
Others	357

Chapter 1 • Introduction

Welcome to EntraPass, a powerful multi-user access control system that provides all the features required in the most demanding applications.

What Is EntraPass? EntraPass is a comprehensive, menu-driven access control software package. Among the many features EntraPass offers, you will find:

- Kantech IP Link module
- KT-200, KT-100 and KT-300 compatibility
- Express setup
- Local anti-passback, interaction between door controllers, DayPass for temporary visitors
- Elevator control
- Integrated Badging capability
- Interactive floor plans
- Configurable desktops by operator
- Multiple reader technology
- External alarm system interfacing
- Time and Attendance reporting
- e-mail reports capability
- Visual diagnostics
- Vocabulary editor included

What Is Access Control? Access control consists of a set of components (door readers, exit detectors, motion detectors, etc.) that are professionally installed and electronically controlled. System workstations are used to receive event messages, acknowledge alarms, modify the system database, etc. A supporting advantage of access control is that all system events are carefully archived and can be easily retrieved for inspection purposes.

Entrapass Main Features

Kantech IP Link Module. Entrapass is compatible with the Kantech IP Link module that provides a secure ethernet connection that serves as a polling device that will control the excess bandwidth by communicating to the gateways only when necessary. The Kantech IP Link module's main function is to relay information between the controllers and the gateway.

KT-100, KT-200, KT-300 Controllers. Entrapass is compatible with Kantech's KT-100, KT-200 controller and KT-300. This has an added benefit when upgrading existing sites that require more flexibility and improved user interfaces. It also allows installers to select the controller that best suits their customers' needs and budget.

Express Setup. The Express Setup utility enables installers to automatically define and configure the most standard system components. This saves installation time and prevents setup errors. With Express Setup, the system is fully functional and ready to test the hardware and wiring before the installer makes the customized changes necessary for a particular site.

Elevator Control Capability. Entrapass allows installers to program up to 64 floors per elevator cab using expansion devices such as KT-PC4216, KT-PC4204 or REB-8 (16 floors maximum). This indispensable feature in a multi-tenant building allows facility managers to restrict specific floor access to authorized cardholders.

Integrated Badging. The Integrated Badging feature was added to Entrapass to allow users to design and print badges. Pictures and signatures can be imported or, with the necessary devices, captured and incorporated into cards for printing badges.

Interactive Floor Plans. Entrapass can import and display high-resolution graphics created on CAD-type systems, allowing you to design a graphic-based system that operators can use with minimal training. Interactive icons can be added to floor plans to display component status and offer full manual operation of the component in real-time.

Configurable Desktops by Operator. With Entrapass, each Operator can be assigned up to 4 configurable desktops. These desktops display selected windows featuring message events, user photos, filtered events, alarm instructions, high-resolution graphics, and global alarms. Desktops can contain any combination of windows.

Interfacing with External Alarm Panels. KT-100 and KT-300 controllers allow users to arm, disarm, and postpone the arming of an external alarm panel through. This allows Entrapass to easily integrate with an external alarm system.

Time and Attendance Feature. The Time and Attendance feature is a low-cost alternative to high-priced dedicated Time and Attendance systems. It enables operators to print or download time sheets in a CSV format to a payroll system.

Visual Diagnostics. Entrapass offers on-screen real-time visual representation of the system devices, with conditions updated in real-time, including high resolution floor plans that can be imported and displayed on screen. Interactive system icons can be added to the graphic to display component status in real-time. Manual operations may be performed from the real-time system graphic.

Vocabulary Editor. The system is multilingual. It is available in English, French, Spanish and German. It can also be translated in up to 99 languages.

Entrapass Manual and Help

Using the Reference Manual

The *Reference Manual* is designed for Entrapass system installers, administrators and users. You may refer to the hard copy of the manual or to the on-line version in pdf format.

To download an updated version of Acrobat Reader, browse to <http://www.adobe.com>.

Getting Help

Our window-level help will provide you with immediate and context-related help. Press [F1] on your keyboard to display the help related to the active window or select [Help] [Contents] from the Entrapass menu.

For **immediate** help, use the **Help** button, found in all the system window. You may also use the right-click option; it may either display a shortcut menu or the help file of the active window.

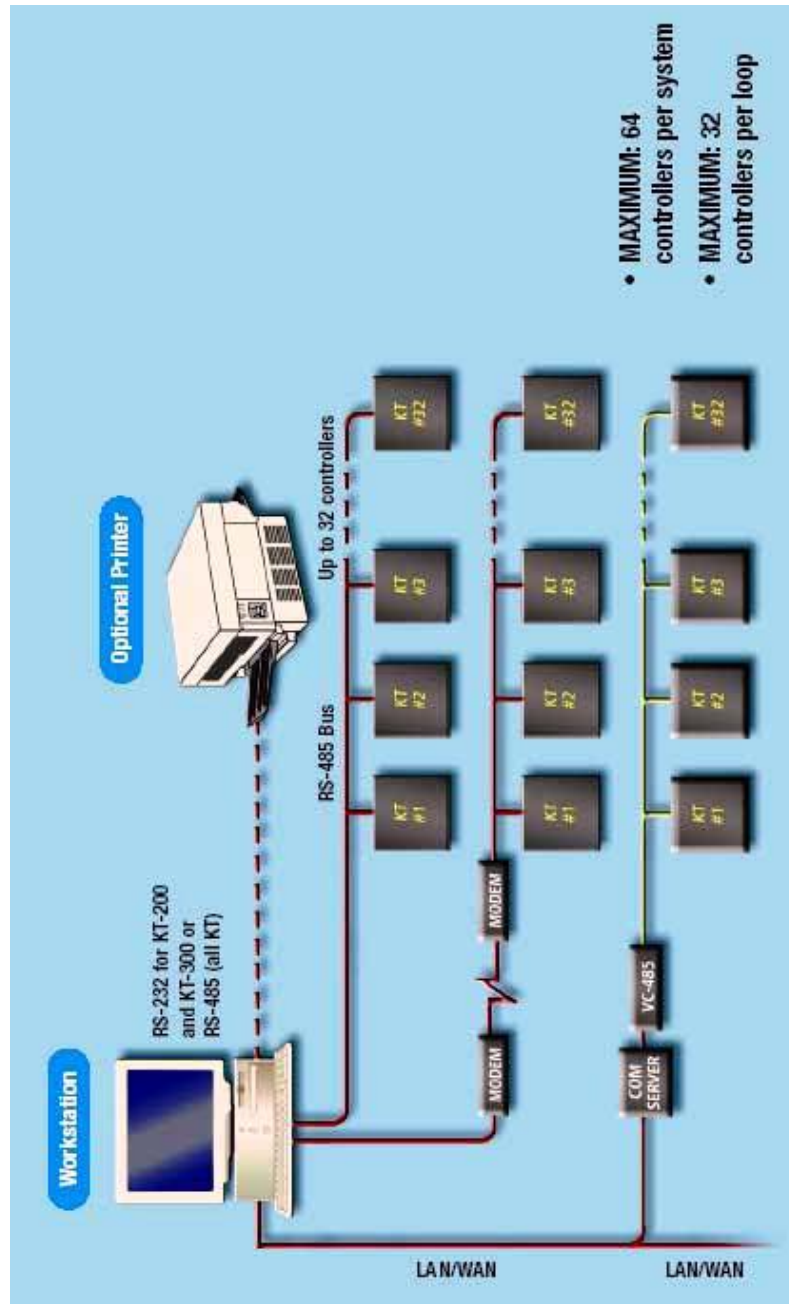
Technical Support

If you cannot find the answer to your question in this manual or in the Help files, we recommend you contact your system installer. Your installer is familiar with your system configuration and should be able to answer any of your questions.

Should you need additional information, please call our Technical Support Help desk, Monday to Friday 8:00 AM to 8:00 PM E.S.T. (GMT -5:00)

Phone	+1 (450) 444-2030
Fax	+1 (450) 444-2029
US & Canada	1 888 222-1560 (Toll Free Number)
Internet	http://www.kantech.com
E-mail	kantechsupport@tycoint.com

System Architecture





Chapter 2 • Software Installation

Before any installation takes place, make sure that the computers on which the software will be installed meet the necessary requirements.

For information concerning hardware equipment installed with the software, refer to the documentation supplied with the hardware.

This chapter contains information related to the EntraPass software. You will find:

- System requirements
- Software installation and upgrading

Depending on the system configuration, there are different system hardware requirements for the installation of the EntraPass software.



System Requirements

Make sure that the computer on which you are installing the software meets the following requirements:

- Operating Systems: Windows® 98 (Second edition)/NT/2000/XP/2003 Standard and Enterprise Server Editions
- Processor: Pentium III at 800 MHz (minimum)
- RAM: 128MB RAM minimum
- Minimum free hard disk space: 4 GB
- Screen resolution: 800 x 600
- Graphic adapter: 4MB
- 48X DVD/CD-ROM drive
- Network Interface card: 10 Base-T network adaptor

Additional Requirements

For several applications, you can use the following devices:

- **A video capture card**—to capture user images for card identification
- **A sound card**—to use warning sounds when an alarm is reported
- **A badge printer**— to print badges (Badging)
- **A signature capture device**— to capture signatures (Badging)
- **A log printer**—(dot-matrix or laser) to print events (messages and alarms)
- **A Report printer**—(laser) to print reports



Installation Kit

The EntraPass installation package contains EntraPass software CD as well as the *Reference Manual* DN1420. It also contains a CBLK-10 kit including 100-foot cable, 2 connectors from KT-200/ KT-300 and a DB9 to DB25 adaptor.

Your installation CD allows you to install the basic components of your EntraPass:

- 1 single-workstation application
- Report Viewer
- Vocabulary Editor

Installation Steps

The InstallShield Wizard will guide you through the installation steps. All you need to do is to enter the **System Installation Code** (located on the software CD) and follow the instructions displayed on the screen.

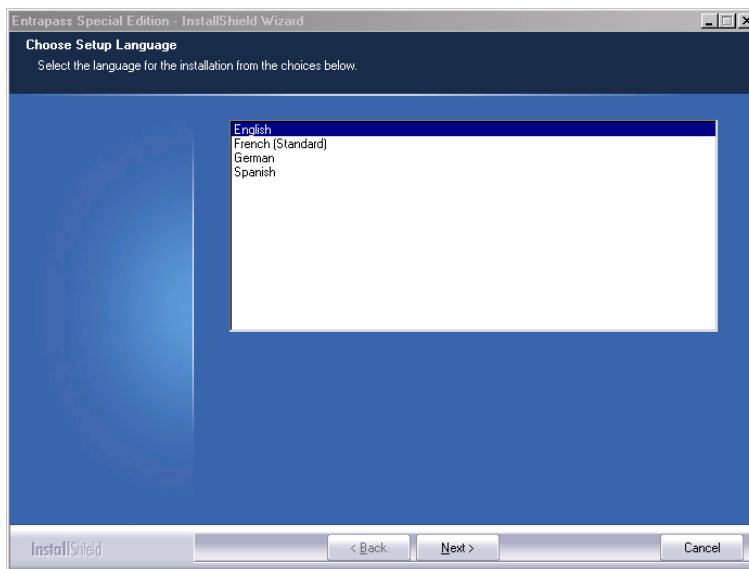
To Install EntraPass Software

The system will be up and running in three steps! Installers need to:

- 1 Install the software using the **System Installation Code** located in the CD pocket.
- 2 Install the workstation.

System Installation

- 1 Before you begin the installation, make sure that no EntraPass application is running.
- 2 Insert the software CD into the CD-ROM drive. The installation program should start automatically if your computer is configured to autorun. If the installation program does not start automatically, click **Start > Run**, then enter `d:\Setup.exe` (where `d:` is the CD-ROM drive) in the displayed field. The system displays the installation setup window.

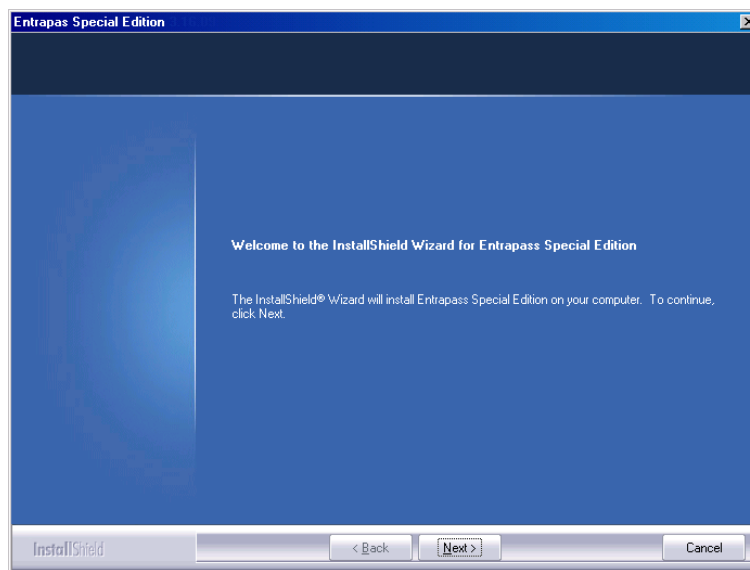


- 3 Before you go any further, you must select which language you wish to install the system in. English is selected by default.



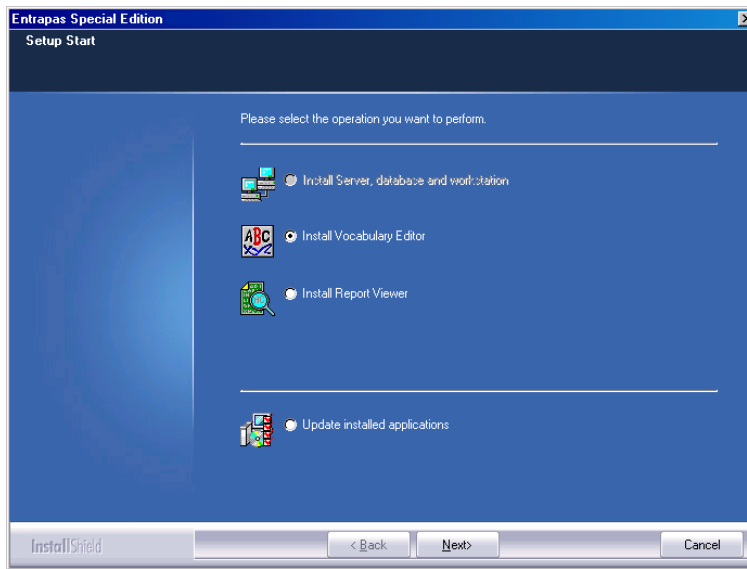
NOTE: The system language depends on the language you select when installing the software. For example, if you select “French”, it will be the system default language at start up.

- 4 Click **Next**. The Welcome screen will be displayed.



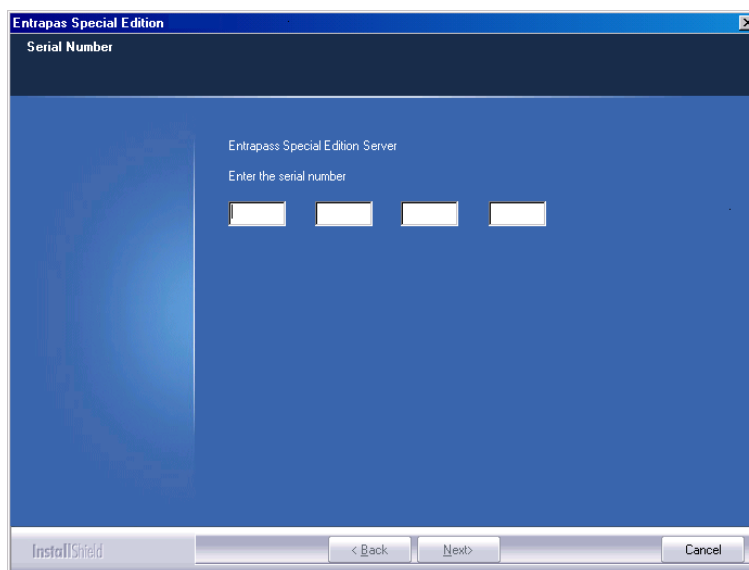
- All the installation windows look the same as the Welcome window.
 - You will notice the software version you are about to install is located at the top left.
 - The middle section of the window contains the instructions you will follow throughout the installation process. The instructions will be updated automatically when you click **Next**.
 - **Back** and **Next** buttons are available at the bottom of the screen to allow navigating back and forth within the installation screens if you wish to verify or modify a parameter you previously setup.
 - You can **Cancel** the installation at any time.

- 5 Click **Next** to continue the installation. The Setup Start window will be displayed.



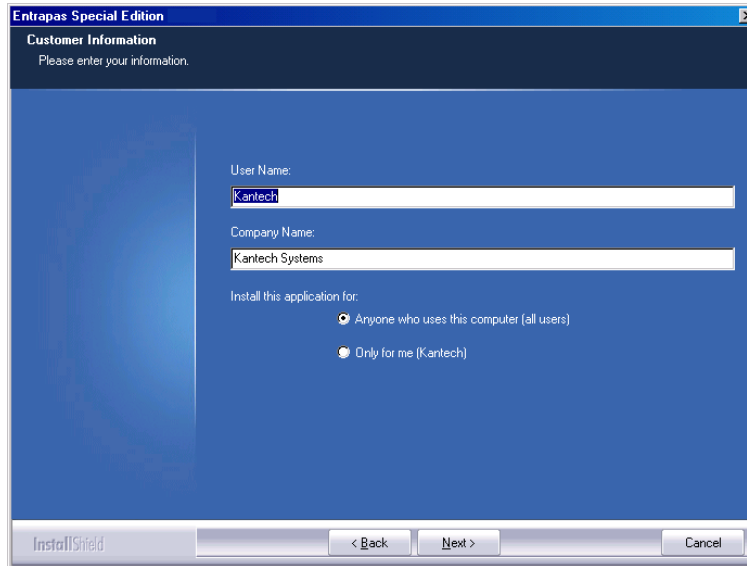
- 6 Select the operation(s) you wish to perform. The first set of options are for new installs and the last option is for updates. During the first installation, you will only be able to select one of the install options. We suggest that you install the first option in the list.
- **Install Server, Database and Workstation:** This option will install the EntraPass Specialsystem. It will be grayed out if the application is already installed on the machine.
 - **Update Installed Applications:** This option will be grayed out if the system has not been installed previously. To update your EntraPass system, see *"System Update"* on page 22.

- 7 Click **Next**. The Serial Number window will be displayed.



- 8 Enter the **Serial Number** for the EntraPass Special Server or Software. The information is located in the CD pocket. Make sure to enter the correct digits. The **Next** button is only enabled if the serial number is valid.

- 9 Click **Next**. The Setup window will be displayed, indicating the installation progress. Once completed, the system displays the software End-User License Agreement.

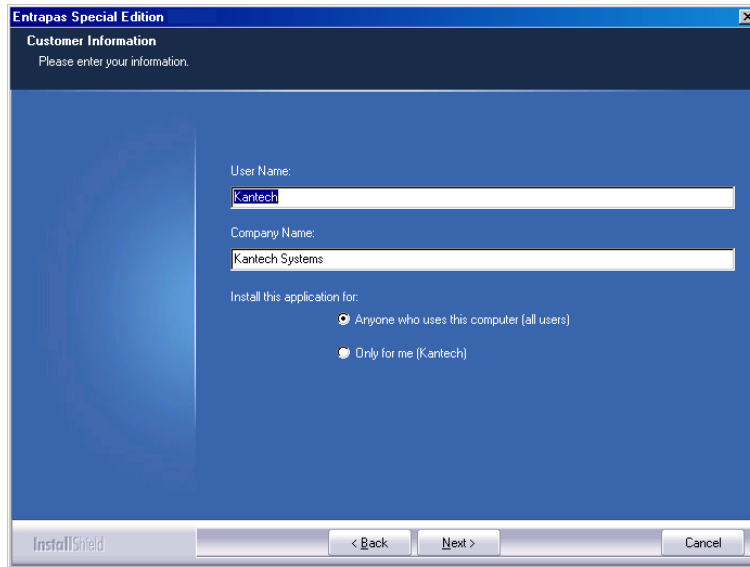


- 10 Click **I accept...** if you understand and agree with the conditions described in the end-user license agreement or click **I do not accept...** to cancel the installation.

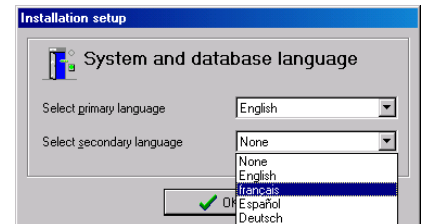


NOTE: You will not be able to complete the installation if you refuse the terms of the license agreement. The **Next** button will remain grayed out until you select **I accept...**

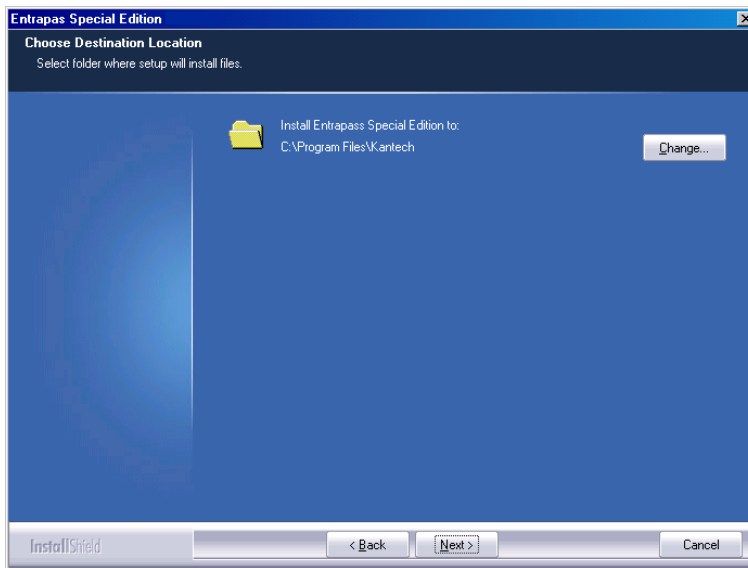
- 11 Click **Next**. The Customer Information screen will be displayed.



- 12 Enter the **User Name** and the **Company Name**.
- 13 Select the user type: **Anyone** who will use this computer or **Only** the person currently logged in and registered in the system.
- 14 Click **Next**. You will be prompted to select the system and database language.
- 15 Select the primary language. You can select a secondary language or leave the selection to None.

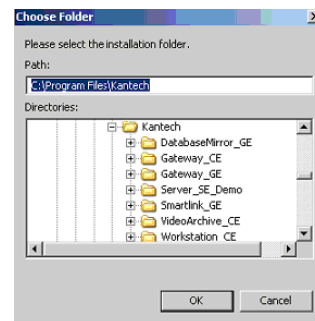


16 Click **OK**. The Choose Destination window will be displayed.

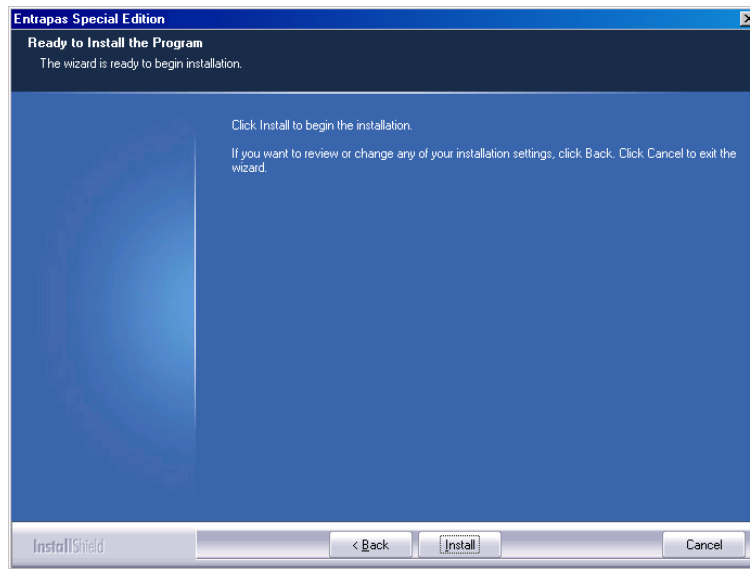


17 Click **Next** to accept the default installation folder indicated in the window.

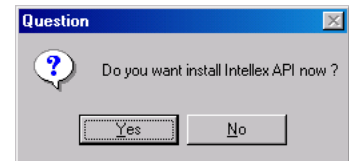
- If you want to change the directory where to install the application, click **Change**. The Choose Folder dialog will pop up where you can select the new installation directory.
- Type in the destination directory where you want to install EntraPass or double-click the directory structure all the way down to the destination directory. Then, click **Ok**. The path will be indicated in the Choose Destination Location window.



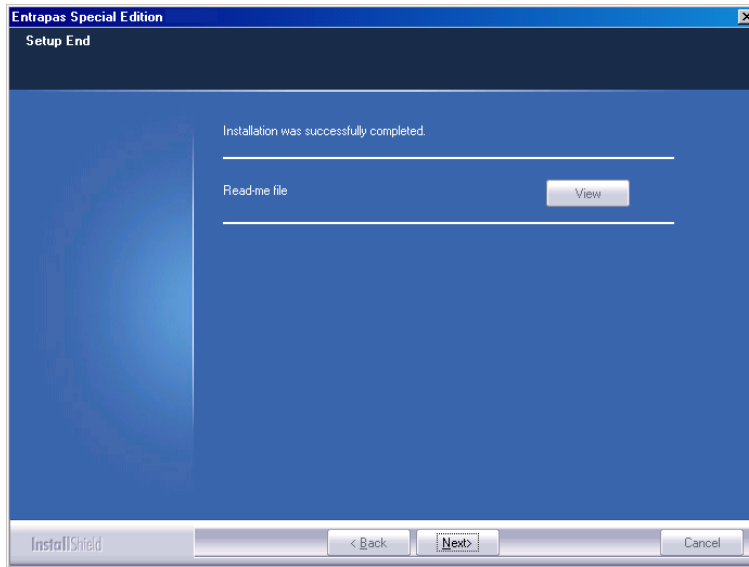
- Click **Next**. The Ready to Install window will be displayed.



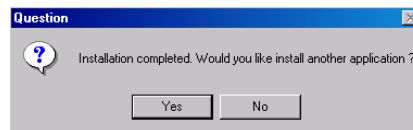
- 18 If you need to review the parameters you've setup, click **Back**. If everything is ready for the installation, click **Next**. The system starts the installation and displays the installation setup window.
- 19 During the installation process, you will be prompted to **Install the Intellex API now?**
 - If the API is not already installed, click **Yes**.
 - If the API is already installed, click **No**.



- 20 Once the first option installation is completed, the system will prompt you to consult the **Read Me** file.

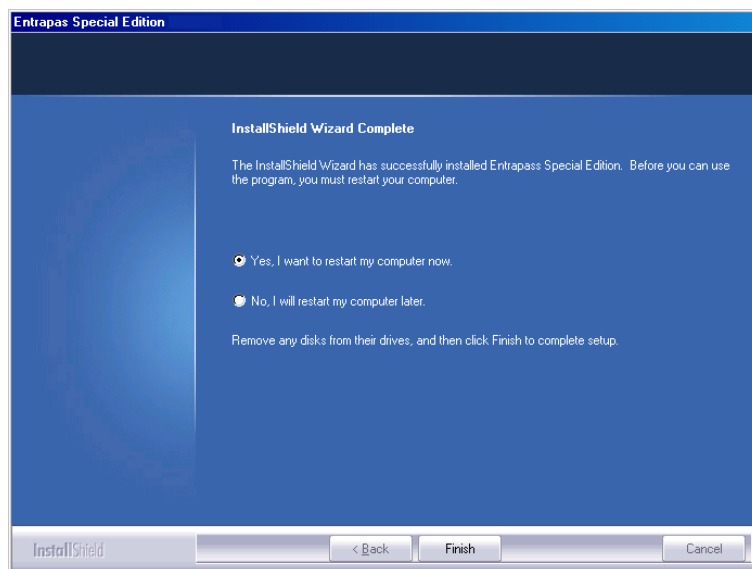


- 21 Click **Next**. The system will verify if there are any other applications or utilities you can install. If this is the case, the following message will popup on screen:



- If you want to install other applications, click **Yes** and start over at number 4.

- If the installation is completed and you do not wish to install other applications, click **No**. The InstallShield Wizard Completed window will popup:



- 22 You can select to restart your computer at this time or do it later.
- 23 Remove the cd from the cd drive.
- 24 Click **Finish** to complete the installation.



NOTE: You must restart the computer after the installation.

System Update

When you update your software, the system automatically detects the components that are installed and updates them.

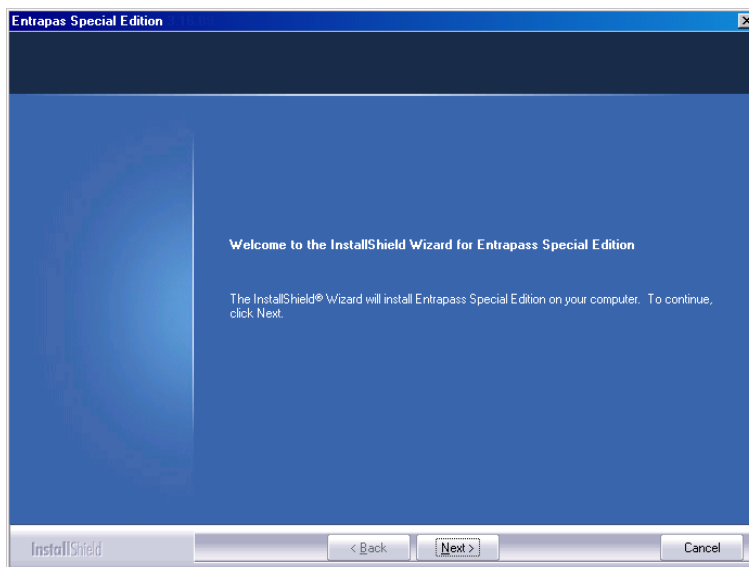
It is highly recommended to update your system when the system is at its minimum use (Friday night, for example.)

Before Updating Your Software

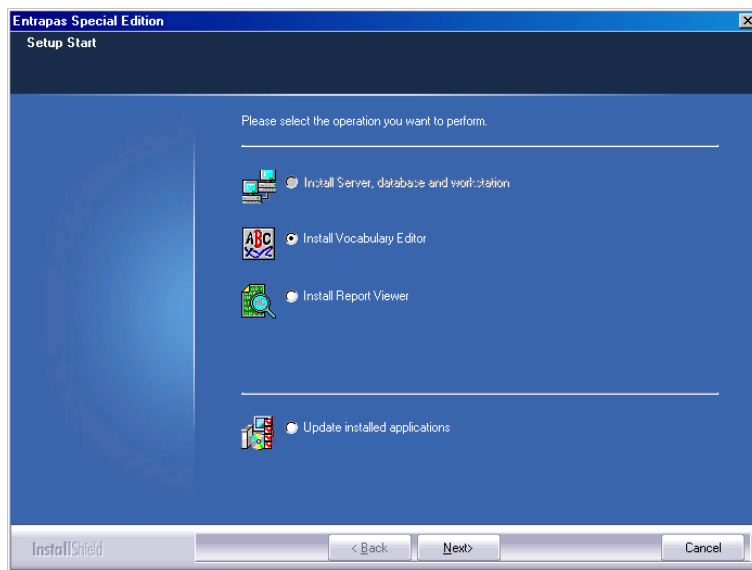
- 1 Perform a **complete backup of your system database**. For more information on how to perform a backup, see *"Backups"* on page 320.
- 2 Verify the system database (see *"Database Utility"* on page 324) to make sure that no errors are detected.
- 3 Once all applications have been updated, we strongly recommend that you reload the gateways to ensure that all data will be refreshed and sent to controllers (**Operations > Gateway reload**).

To Update your Software

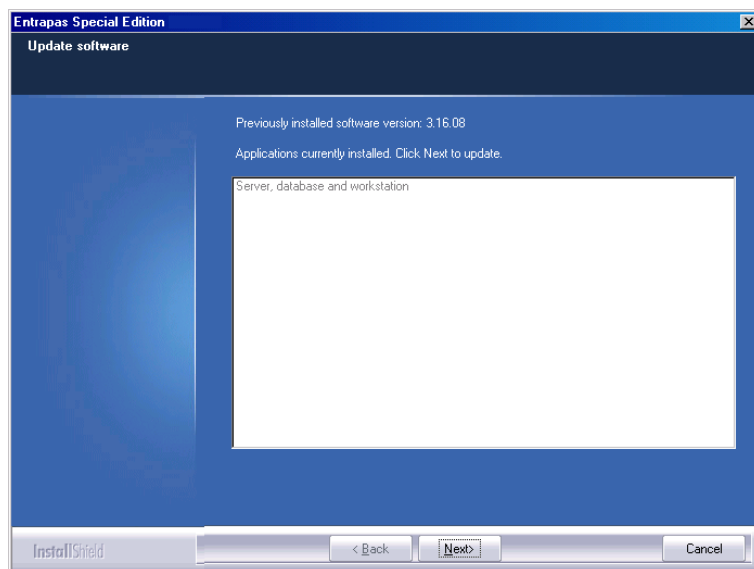
- 1 Insert the software installation CD into the CD-ROM drive. The installation program should start automatically if your computer is configured to autorun. If the installation program does not start automatically, click **Start > Run**, then enter d:\Setup.exe (where d: is the CD-ROM drive) in the displayed field. The system displays the installation setup window.
- 2 Click **Next**. The Welcome window will be displayed.



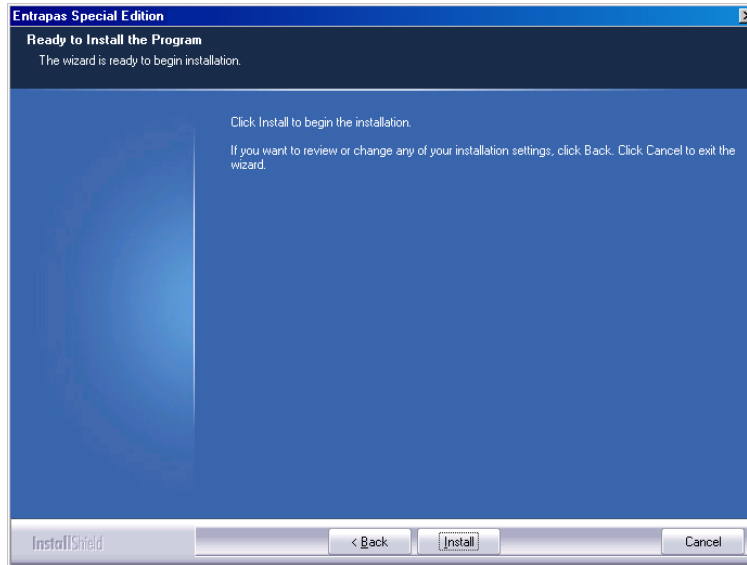
- 3 Click **Next**. The Setup Start window will be displayed.



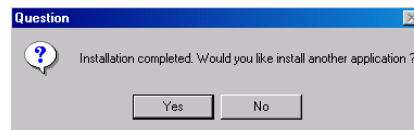
- 4 Select **Update Installed Applications** and click **Next**. The Previous Software window will be displayed, listing all the software that are currently installed on your machine.



- 5 Click **Next** to continue. The update will start and all programs currently installed on your machine will be updated.



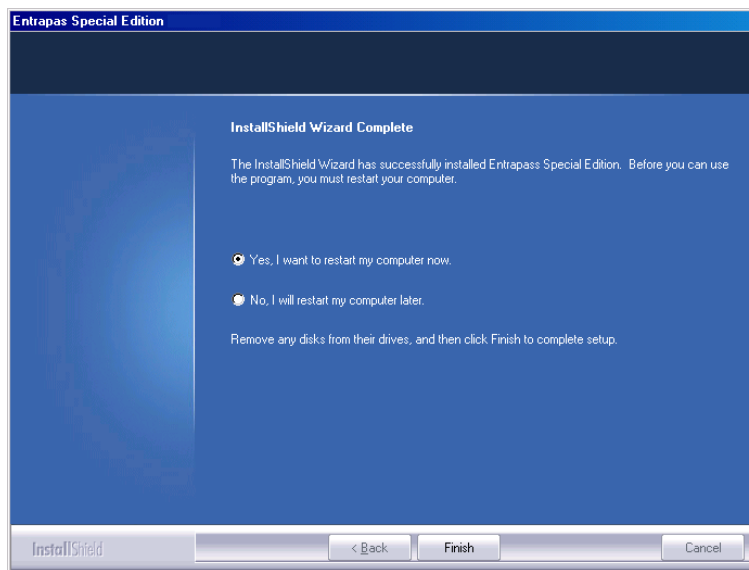
- 6 Click the **View** button to read the Read-Me File that contains information on the updates that were done to the different applications. When you are done with this file, close it. You will automatically return to the Setup End window.
- 7 Click **Next**. The system will verify if there are any other applications or utilities you can install. If this is the case, a message will popup on screen:



- If you want to install other applications, click **Yes** and start over at number 2.



- If the installation is completed, click **No**. The Maintenance Completed window will popup:



- 8 You can select to restart your computer at this time or do it later.
- 9 Remove the cd from the cd drive.
- 10 Click **Finish** to complete the installation.

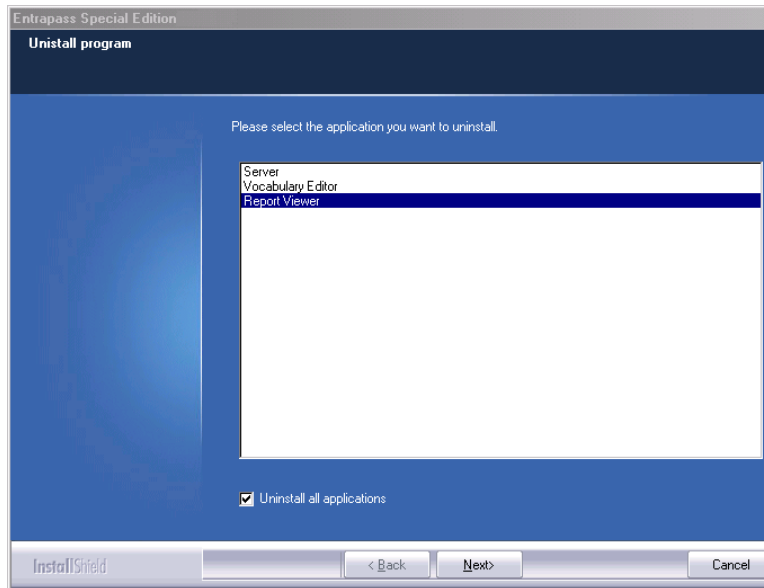


NOTE: After the update, you must restart the computer in the order prescribed at the beginning of this chapter, see "Before Updating Your Software" on page 22.

Removing the EntraPass Software

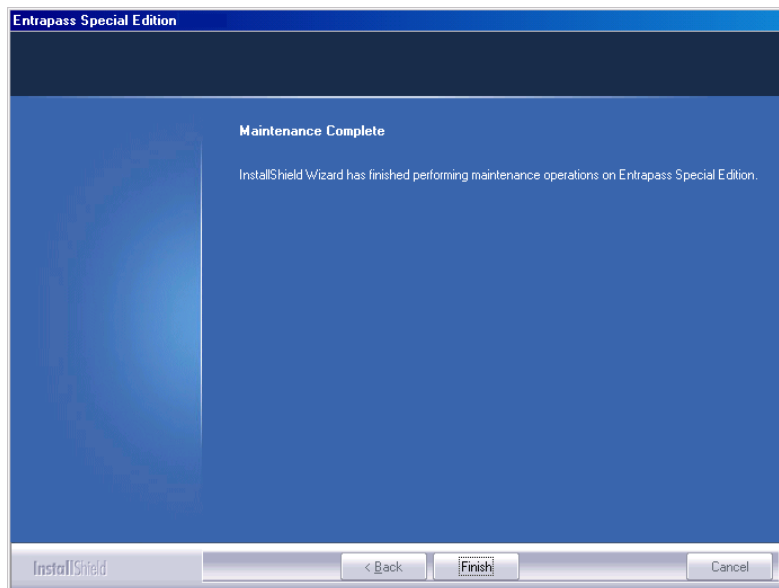
If you need to remove the EntraPass software from the computer, you will use the **Add/Remove Programs** option in the Control Panel.

- 1 Click **Start > Settings > Control Panel**.
- 2 When the Control Panel is opened, click **Add/Remove Programs** to open the dialog.
- 3 Select the program you want to delete from the list and click **Remove**. The EntraPass Uninstall program dialog will display on the screen.



- 4 Select the application you want to uninstall. If you want to uninstall EntraPass completely, check the **Uninstall all applications** box.
- 5 Click **Next**. The process will begin.

- 6 When the uninstall process is completed, the Maintenance completed dialog will display on the screen.



- 7 Click **Finish** to exit the wizard.
- 8 Restart your computer.



Chapter 3 • Getting Started

This chapter introduces operators to the EntraPass system graphical user interface and basic functions.

To start an EntraPass session, you only have to start the Entrapass Workstation



NOTE: *All authorized system operators must have a unique and confidential login name and password that should be assigned by the system installer/administrator. It is very important to restrict access to the EntraPass workstations to authorized personnel only.*

Session Start and End



NOTE: The system keeps the last five usernames, allowing operators to select their username from the drop-down list. To delete a username from the list, simply select it, then press **Delete** on the keyboard.

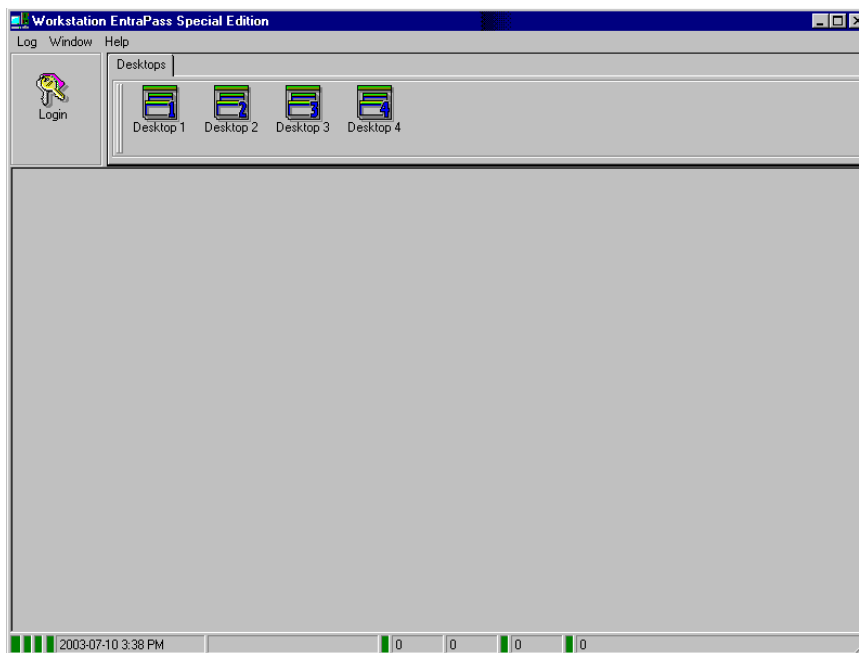
To Start the EntraPass Workstation

An EntraPass workstation is a computer where the EntraPass monitoring application has been installed. It enables operators to access and program the system database and components.

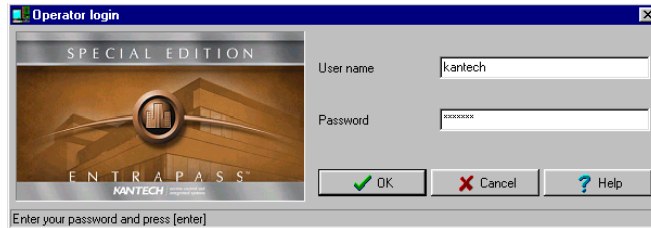
- 1 Start EntraPass workstation (from Windows® Start menu or from the desktop).



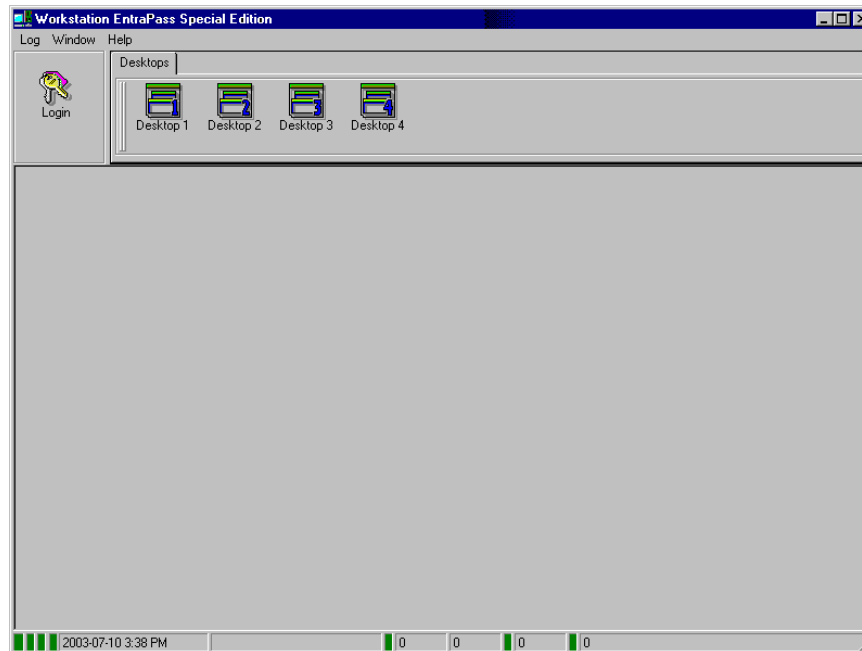
- 2 Click the **Login/logout** button on the toolbar.



- 3 Enter your Operator **User name** and **Password**. The password is case sensitive. The default **User name** is kantech. It is not case sensitive. The default **Password** is kantech, in lower case; it is case sensitive.



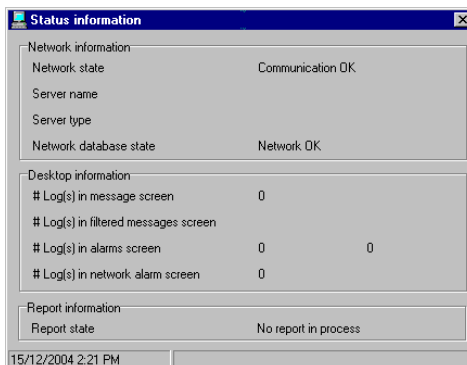
NOTE: If you cannot log on properly, check if the Caps Lock key is activated. When proper login data have been entered, the system menu, toolbar and status bar are enabled.



To Access Information on the Workstation Connection Status

- 1 Click any tab to access the system toolbar or select a menu item to access the system menu. In the lower part of the window, color-coded flags indicate the communication status: Green, communication is OK; Red: communication problems; Blue: a report is pending.
- 2 Move the cursor over the colored rectangles to show details about the network status, the network database status and the workstation application report status.

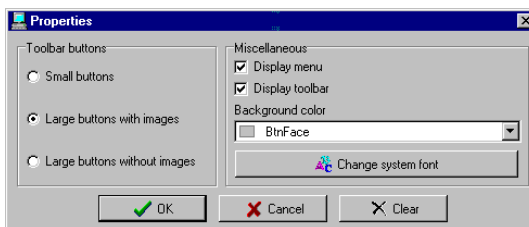
- 3 Move the cursor over the displayed numeric values to show details. It will indicate, in order, the system date and time, the operator's name, items in the Alarms desktop, alarms to be acknowledged, etc.
- 4 Double-click (or single click, depending on your system settings) any number in the status bar to display the Status information window.



NOTE: It is recommended to use the **Login/logout** button when you exit EntraPass programs. This ensures that the system databases are shutdown properly.

To Modify Your Work Area Properties

- 1 Right click anywhere in the main window to display the Properties window. It allows you to customize the window buttons as well as the background color.



- 2 To modify the size of the toolbar buttons, select one of the following:
 - **Small buttons:** small buttons are displayed below menu items
 - **Large buttons with images:** components icons are displayed on large buttons
 - **Large buttons without images:** no icons are displayed
- 3 In the Miscellaneous section, make the appropriate choice:
 - **Display menu:** only the menu bar appears. No icons are displayed. Right-click the work area to modify the properties.
 - **Display toolbar:** the menu bar and the toolbar are displayed.
- 4 Select a background color for the work space.

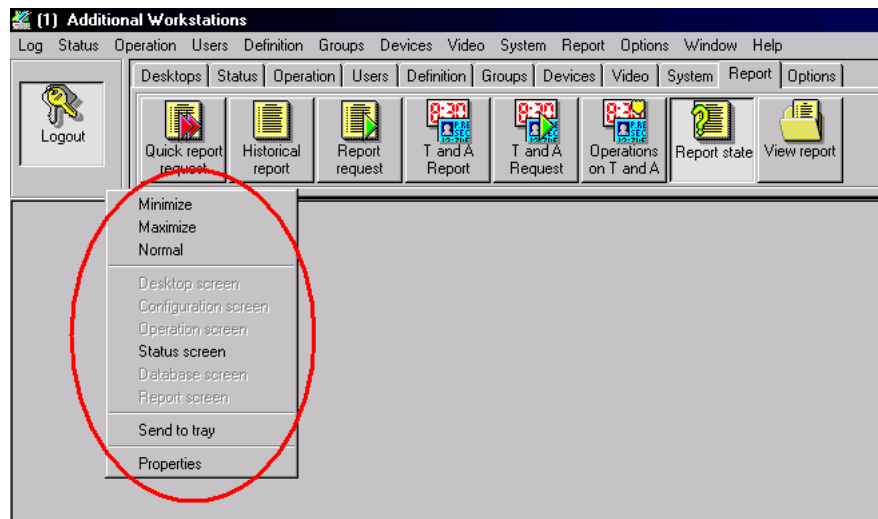
To Retrieve Hidden Windows on the Desktop

Entrapass allows you to work with multiple windows opened in the Desktop area. When a window is minimized or sent to the background, it completely disappears from the screen. A command in the workstation contextual menu can help you retrieve the dialogs.

- If the window was minimized, the command in the menu will bring it at the front of the screen where you will be able to maximize it.
- If the window was sent to the background, the command in the menu will bring it to the foreground.

This command applies for desktop screens, configuration screens, operation screens, status screens, database screens and report screens.

- 1 Right-click the background area of the workstation window. A contextual menu will popup.



- 2 In the example above, the Status screen was sent to the background. Clicking the **Status screen** command in the menu will bring it back to the foreground.



System Stand-Alone Utilities












Entrapass includes a number of stand-alone utilities that allow operators to perform a variety of tasks including verifying the system database or changing the system language. The following is a list of Entrapass stand-alone utilities:

- **Database Utility:** This program is intended to re-index archived files, update database fields, verify archived files, verify the database integrity, verify the database index, verify the database links and verify the database hierarchy.
- **System Report Viewer:** Program used by the operator to view reports without having to start a Workstation. When this utility is installed, operators can view reports sent by other workstations using the Entrapass e-mail feature.
- **Vocabulary Editor:** Simple and easy program used to translate the software in the language of your choice.

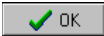




These utilities may be launched from the Windows® Start menu of any computer where Entrapass installed. For details on Entrapass stand-alone utilities, see "*System Utilities*" on page 323.

EntraPass Workstation Toolbar

EntraPass windows display most of the following buttons. They are an easy way to access the system functions. Usually, a “hint” is displayed when you move the cursor over an icon. You may access the EntraPass toolbar from any EntraPass workstation window. Icons vary according to the window that is open. Most of the icons are similar to icons you are familiar with and that are used in the computer industry.

Button	Description
	The New button is used to insert new information in the system database. This may be adding a site, a card, a schedule, a controller, etc.
	The Save button saves all the information you have entered since the last save. Information is saved directly in the system.
	The Save As button allows operators to save all of the information of an existing component under a new name without affecting the original component. When using this option while issuing a card, it allows you to create a new card or save under a new card number without having to modify the information of the original card.
	The Delete button is used to delete the currently selected record. As a security against accidental deletion, a warning is displayed prompting you for confirmation. When a component is erased, all links with other items are erased as well. However, the records (archives) are kept in the database after an item is erased.
	The Print button: depending on which menu you are working in, the Print button can be used to print reports, card lists, event parameters, etc.
	The Parent button allows operators to display their search in a hierarchy or to divide searches by gateways, site and controller (according to the menu). This button becomes useful when the system database increases in size; you can find a specific item by selecting its parent items.
	The Link button enables operators to see all instances of an item in other menus. For more information, see <i>"To View Components Links" on page 44</i> .
	The Find button allows operators to find a specific item or component in the system database by using a specific character string. For more information, see <i>"To Find Components" on page 37</i> .
	The Close button is used to close a menu or a sub-menu. If you forget to save your information before closing a menu, the system displays a window prompting you to confirm the “save” operation before closing the menu.
	The Cancel button is used to cancel all modifications that were made since the last time a valid save was performed. The system will prompt you to confirm the operation.
	Use the Help button to view the help content on a specific subject.



Button	Description
	<p>The OK button is used to save and accept the modifications, additions or deletions made to a record in the database of the system.</p>
	<p>The Select all button is used to select all the items or components displayed in a list.</p>
	<p>The Unselect all button is used to unselect all the items or components that were previously selected in a list of choices.</p>
	<p>In several system windows, operators have access to graphic and animation buttons. These buttons are particularly useful when you want to display the status of a component before performing an operation on that component.</p> <p>The Enable graphic button is used for example in the Status menu and in the Operations menu. When enabled, this button displays the image related to the selected component (i.e.: door) and displays also the associated components (i.e.: reader). To display components in real-time, this button must be used with the Enable animation button.</p>
	<p>The Enable animation: when enabled, this button automatically enables the Enable graphic button. This activates the current component (i.e.: door) and displays its status in real-time. For example, if you wish to lock a door which was previously unlocked, the reader's image (also visible) will be modified; the green dot will change to red.</p>
<p>Right-click</p>	<p>The Right-click shortcut menus allow operators to enable a shortcut menu from which they can choose a specific command depending on the active menu.</p>

Basic Functions

Following are the basic system operations:

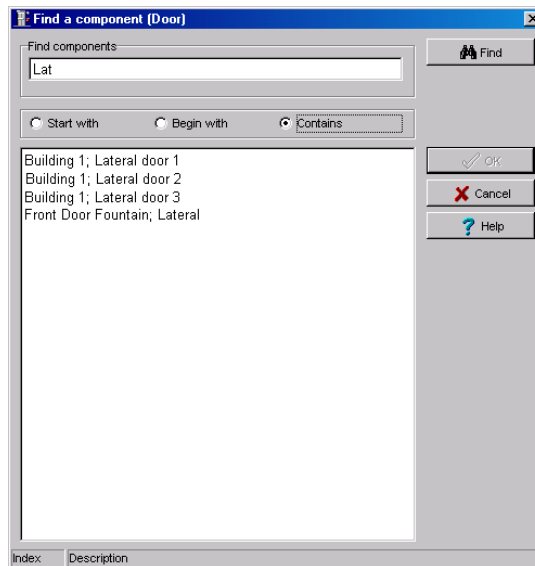
- Find components
- Select components
- Print lists or reports
- View links between components

To Find Components

The Find Components function allows operators to find a specific item or component in the system database by using a specific character string.

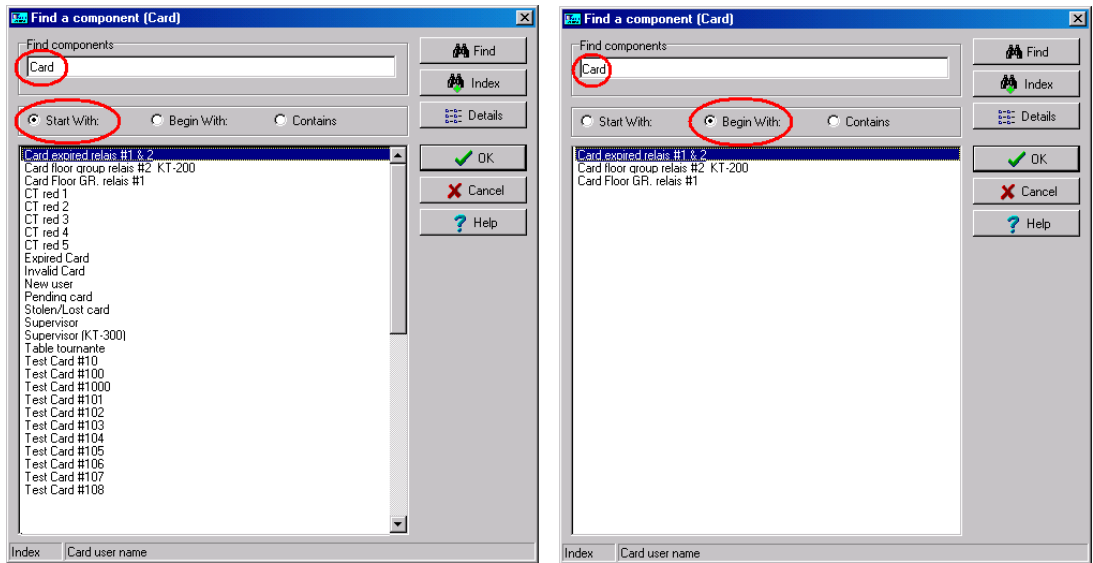
There are two types of Find Components dialogs: One that can be accessed from any EntraPass window toolbar; One that will be accessed through all the dialogs that pertain to users.

- 1 From any EntraPass window toolbar, click the binoculars button.



- 2 Enter a keyword to start the search. To reduce the search results, check one of the boxes:
 - **Start with:** Results will list all components that start with the text you specify, in alphabetical order, and will include the rest of the list of components available in the database.
 - **Begins with:** Results will list only components that start with the text you specified.

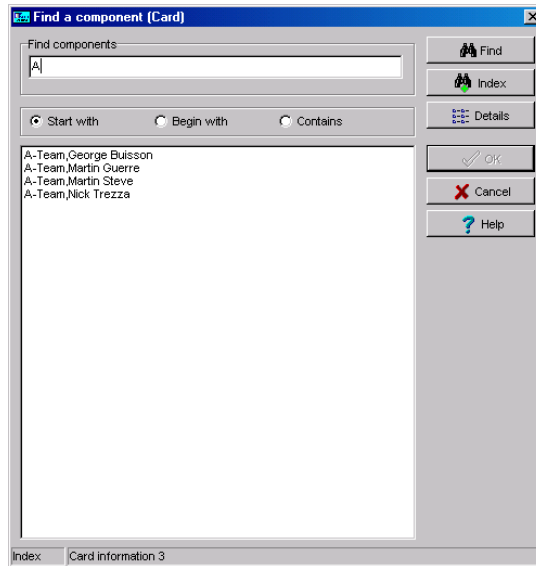
- **Contains:** Results will list all components that contain the text you specify.



- 3 Click **OK**. The system displays the list of the components found according to the search string.
 - To cancel a search in progress, click the **Cancel** button.

To Find a Card

- 1 From any EntraPass window that pertains to users, click the binoculars button in the toolbar.



- 2 Enter a keyword to start the search. To reduce the search results, check one of the boxes:
 - **Start with:** Results will list all components that start with the text you specify, in alphabetical order, and will include the rest of the list of components available in the database. (refer to the screen on the left in the example below.)
 - **Begins with:** Results will list only components that start with the text you specified. (Refer to the screen on the right in the example below.)
 - **Contains:** Results will list all components that contain the text you specify.
- 3 To display the contents of one of the Card Information field with the results of the search, click the **Index** icon and select which field you want to display.

- To view the picture that corresponds to the entry selected in the list, click **Details**. This will open a picture window next to the current dialog.



- Click **OK**. The system displays the list of the components found according to the search string.
 - To cancel a search in progress, click the **Cancel** button.



NOTE: When you select one of the three search options, (**Start with**, **Begin with** and **Contains**), the selection will be selected by default the next time you open this dialog.

To Use an Extended Selection Box

An extended selection box allows you to view all components of a drop-down list by right-clicking on the list. This option is available where a drop-down list exists for components such as applications, controllers, and doors. If the option is available, a hint box is displayed when the cursor is placed over the drop-down list.

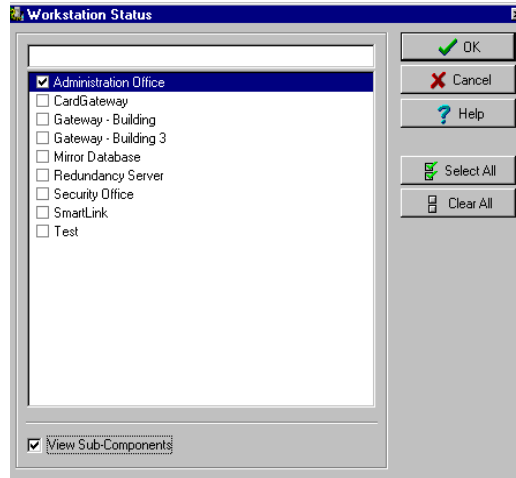
Available text filters in the extended selection box:

- Contains
- Starts with
- Ends with
- Exact word
- Selected

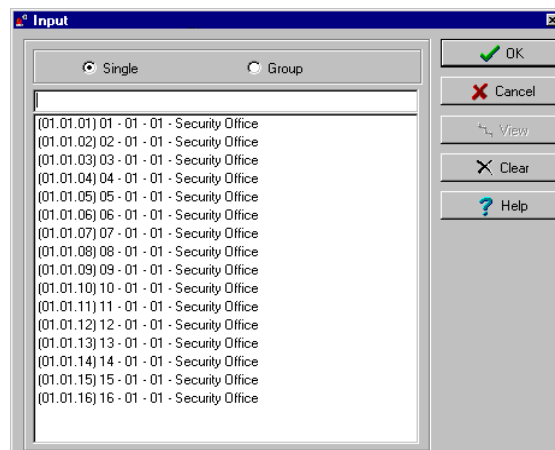
To Select Components

The **Component selection** function allows operators to select one or more system components. The method employed may be context sensitive.

- 1 From the active window, click the **Select Components** button. It opens a secondary window from which you may select appropriate options.
- 2 You may need to check options that are displayed or use the **Select All** button (left) to select all the displayed options. You may also select **Single** to view components that are not grouped or select **Group** to view the existing groups.

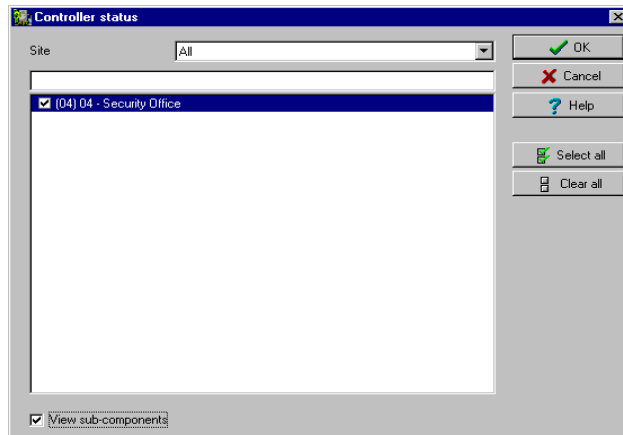


- 3 From the displayed list, select the component/group you want to display. You may check the **View sub-components** option to display the components associated with the selected components.
- 4 Where available, use the **Select all** button to select all the components, or use the **Clear all** button to remove the check marks from the selected components. Click **Cancel** to return to the previous window without any selections or changes.

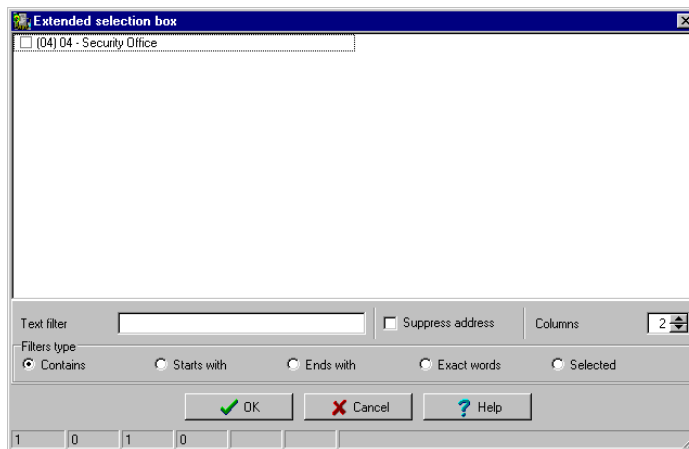




- Another selection method may be used as displayed in the following Controller Status window. Right click inside the window to display an Extended Selection Box with a complete listing of components.



- Set the required number of columns in the Extended Selection box window to display all components as required. A **Text Filter** may be employed to limit the listing.



- Click **OK** to apply selections and return to previous window.

To Select a Specific Folder

You may need to browse through the hard drive to locate a specific folder for backups, for example.

- 1 From the active window, click the **Select** button (it is identified by "..."). It opens a secondary window from which you may select a specific folder.
- 2 To change the destination folder, browse the Drives drop-down list (lower part of the window). You may click the **Refresh drive** list to make sure that the displayed list is up-to-date.
- 3 Once you locate the folder you are searching, click **OK** to go back to the active window.

To Select a Specific Site

EntraPass offers you the ability to associate a specific component with a specific gateway/site. For example, you can define a specific holiday for a specific site or gateway.

- 1 From an active window, click the New icon. The system displays the Select Gateway/Site window.
- 2 Double-click a Site/Gateway from the displayed list then click **OK**.
- 3 Assign a meaningful name to the component being defined.
- 4 Follow the steps to complete the task.

To Print

Operators may need the Print function to:

- Print a list of cards
 - Print event parameters
 - Print event-relay association
 - Setup a report for printing
- 1 From any EntraPass window, click the **Print** icon.
 - 2 Select the components you wish to include in your list. You can use the **Select all** button (if available) to include all the displayed components in the list.
 - 3 When you select **Print empty fields** option (if available), the list will include the titles of the fields even if they are empty.
 - 4 When you have finished selecting the fields, you can preview your list before you actually print it. When you preview the list, you can:
 - Define the printer setup
 - Print a hardcopy of your report or list
 - Save the report or list for later use with the **Quick Viewer** program or load an existing report. For more information on this program, see *"Quick Viewer" on page 341*.
 - 5 If you want to modify the settings, close, modify and print your list.
 - 6 You can use the **Font** button to select a specific font and font size for your list.
 - 7 To select or modify a font selection:
 - Select the font type from the Font menu. A preview of your selection will be displayed in the Sample box.
 - Choose the formatting attribute from the **Font Style** menu (regular, italic, bold or bold italic).
 - Enter the font size from the Size menu (10 or 11 is a default). The smaller the font, the more items appear on your list.

- You can also select a color from the **Color** menu (black is a default). The changes appear automatically in the sample box. Click on **OK** when you are done. Use the **Preview** button from the Print window to preview your output before printing.



NOTE: If there is no printer configured for the computer, an error message appears.

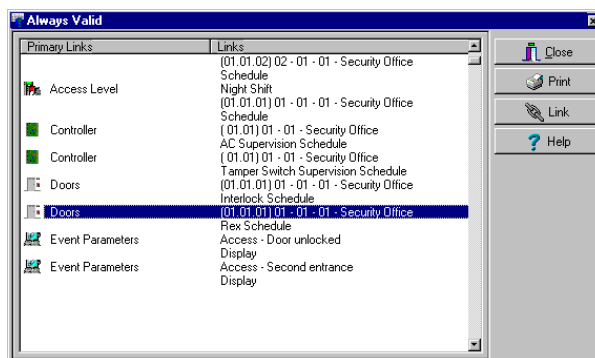
To View Components Links

The **View links** function allows you to view all instances of an item within other menus. Therefore, it is possible to see all links an item has with other items.



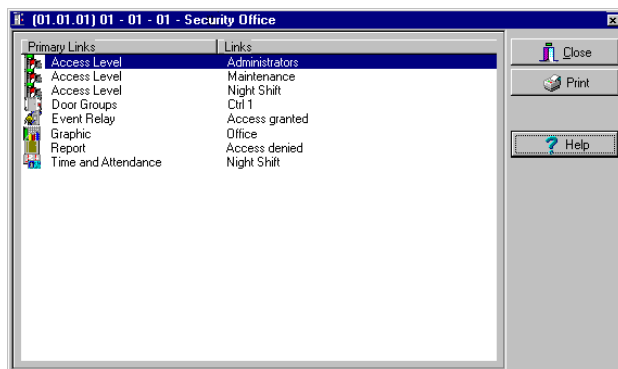
NOTE: You can use the **View links** button before you delete a component from the database in order to see which menus will be affected by the deletion. You can also print the links of a selected component.

- From any menu window, select a component and click the **Link** button. All the components that are associated with the selected component are displayed.
- The icons that are located on the left side of the components indicate the component type. For example, if you select the **Always valid** schedule (in the Schedule definition menu) and click the **Link** button, the system will display a list of all the menus in which this schedule is used.



NOTE: In the highlighted example, the **Always valid** schedule is used as the REX (Request to EXit) schedule in the Door definition menu. You can right-click an item to select a category. For example, if you right-click and select Access levels, only the access levels in which this schedule is defined are displayed.

- 3 To view the links of the selected door with other components of the system, select the door, then click the **Link** button again:



- 4 All system components that are associated with the selected door appear. In this example, the “door” is used in the Administrator access level; users granted this access level are allowed access to the selected door.
- 5 Click the **Print** button to print the information displayed on the screen.



Chapter 4 • System Devices

After the installation of the system hardware and software, you have to configure the access system devices. These include software components (EntraPass applications) and physical components (controllers, relays, doors, etc.).



NOTE: *It is recommended to use the Express Setup utility to save configuration time and to prevent setup errors. In addition, using Express Setup allows you to test the hardware and wiring immediately after the installation.*

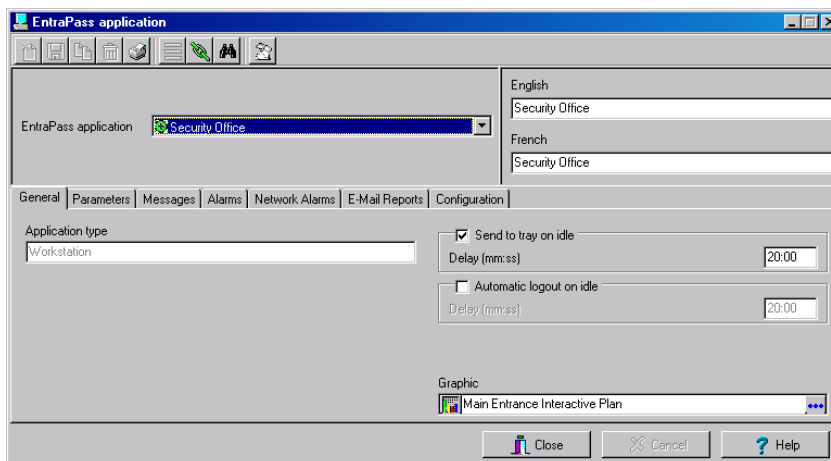
You run the **Express Setup** utility when you are configuring sites or controllers for the first time. You may run the Express set up utility by clicking its icon in EntraPass windows. For detailed information about using the Express Setup utility, see *"Express Setup Program"* on page 336.

EntraPass Applications Configuration

EntraPass Special Edition application is a single-workstation software.

To Configure an EntraPass Application

- 1 From the EntraPass main window, select the **Devices** tab, then click the **EntraPass applications** icon. The EntraPass applications main window appears.



- 2 From the **EntraPass application** drop-down list, select the application you want to configure. This list displays all EntraPass applications that have been installed. The **Application type** drop-down list displays the type of the selected item. Assign a name to the selected EntraPass application. If you are running the software in two languages, for example in English and French, you may assign a name in English and in French.
- 3 Click the save button to activate the new application.

Defining General Parameters

The **General** tab allows you to specify the system behavior when the operator is inactive, that is when there is no action on the keyboard (idle time).

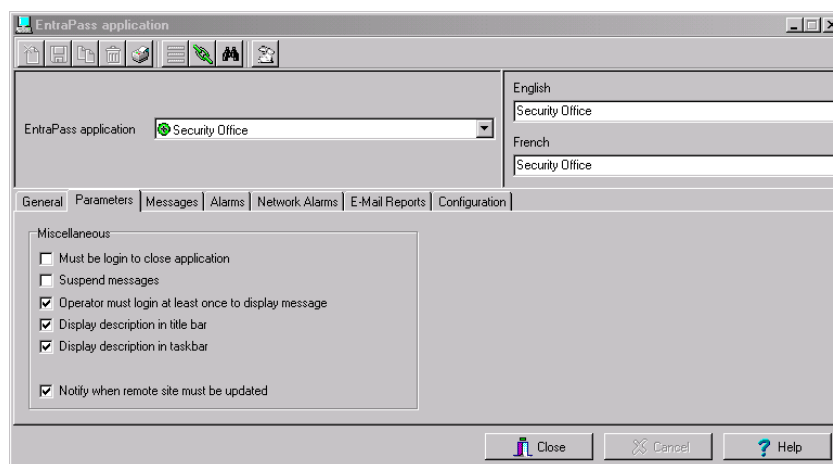
- 1 For added security, specify the system behavior when the operator is inactive. This feature provides additional security to prevent access to the system by an unauthorized person. The default delay is 20 minutes. You may keep the default delay or change it.
 - Select the **Send to tray on idle** if you want the EntraPass applications to be minimized when there is no action on the keyboard. If you do this, you have to specify the period after which the application will be minimized if there is no action on the keyboard: in the Send to tray on idle, enter the delay after which the EntraPass applications will be minimized and sent to the task bar.
 - Select the **Automatic Logout on idle** option if you want the EntraPass applications to logout when there is no action on the keyboard. If you do this, you have to specify the period after



- which the application will be minimized: in the Automatic logout on idle enter the delay after which the Operator will be automatically logged out, (the option has to be checked).
- From the **Graphic** list, you may select the graphic to which the EntraPass applications is assigned, if applicable. For details on defining graphics, see *"Graphics Definition" on page 101*.

Defining Security Parameters

- This section applies to all EntraPass applications (EntraPass Workstations). From the EntraPass applications window, select the **Parameters** tab.

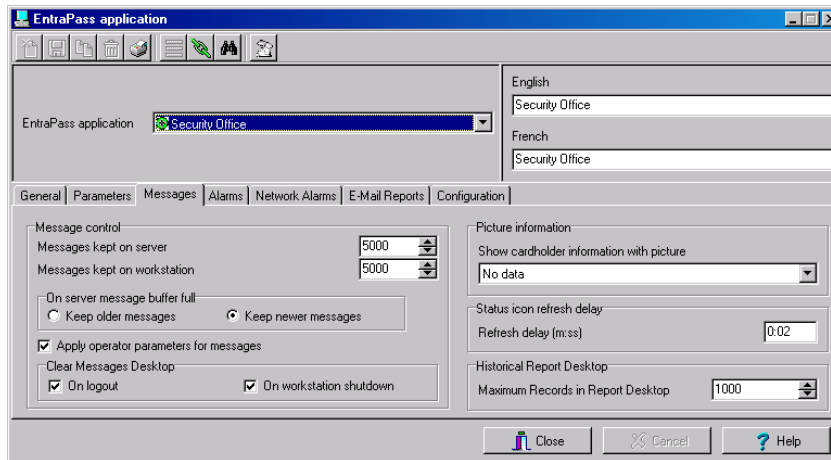


- Make the appropriate choices:
 - Must be login to close application:** checking this option will oblige operators to login before they exit an EntraPass program.
 - Suspend messages:** if this option is selected, all incoming messages for this EntraPass applications will be suspended. Use this option for an EntraPass workstation that is used only to configure components or when messages are not required.
 - Operator must login at least once to display messages:** checking this option will oblige the operator to login at least once with a valid username and password before system messages can be viewed.
 - Display description in title bar:** check this box to display EntraPass applications description in the window titlebar (top).
 - Display description in taskbar:** check this box to display EntraPass applications description in the window taskbar (bottom).
 - Notify when remote sites must be updated:** check this option to tell the system to send a notification before updating remote sites. When this option is enabled, operators will receive a notification before updating site communicating via a modem. If this option is selected, operators will receive a notification each time data related to sites (such as schedules, controllers, etc.) are modified. They will have the choice of updating remote

sites (**Yes**), refusing the change (**No**) or clicking **Details** so that they can select specific sites to be updated.

Defining Message Controls

- 1 Click the **Messages** tab to define how messages should be processed in the module



NOTE: Messages desktops are configured in the Desktop definition menu. For details, see "Entrapass Desktops" on page 239.

- 2 In the **Message control** section:

- Specify the number of messages that will be **kept on the server** when the Entrapass workstation is off-line, that is, when it is not connected to the module. The module buffers a maximum of 100,000 messages per Entrapass workstation (default: 5,000).
- Specify the number of messages that will be **kept on the workstation**. There is a maximum of 100,000 messages per Entrapass workstation. By default, it keeps 5,000 messages.



NOTE: The Entrapass workstation will always keep newer events. To view older events, you have to request a historical report. For details on requesting reports, see "Reports" on page 267.

- 3 Specify if the Server should keep newest or oldest messages when its buffer reaches the defined maximum number:
 - **Keep older messages:** the module will keep the oldest messages and archive the newest messages when the Entrapass workstation is off-line and when the Server buffer is full.
 - **Keep newer messages:** The module will keep the newest messages and archive the oldest messages when the Entrapass workstation is off-line and when its buffer is full. Messages are processed on a first in - first out basis.

- 4 You may want to create exceptions to the EntraPass workstation configuration by checking **Apply operator parameters for messages** options. When this option is enabled, operator settings have priority over EntraPass workstation settings.



NOTE: If the **Apply operator parameters for messages** option is selected all events will be filtered according to the EntraPass workstation configuration, and filtered again according to the security level of the operator who is currently logged on the EntraPass workstation. If the “Apply operator parameters for messages” option is selected and no operator is logged in, or the EntraPass workstation is off-line, events will NOT be buffered by the system.

- 5 In the **Clear Message Desktops** section, specify when messages should be cleared:
 - **On logout** (on a regular logout by an operator)
 - **On workstation shutdown** (when the EntraPass workstation is completely shutdown)
- 6 In the **Picture information** section, select the field content that will be displayed below the cardholder picture. The **Show cardholder information with picture** drop-down list contains 10 definable fields (Card information 1, Card information 2, etc.).

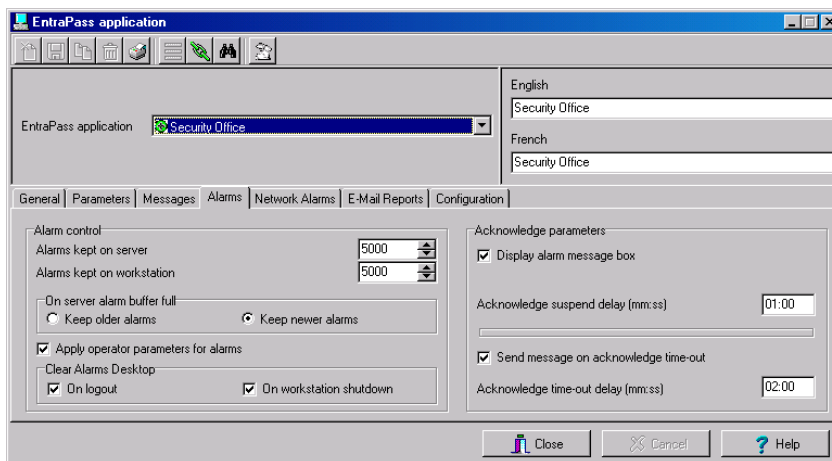



NOTE: By default, the field displays “card information #1” to “card information #10”. These labels may be customized. For more information on renaming card information labels, see “To Customize Card Information Fields” on page 134.

- 7 In the **Status icon refresh delay** section, specify the time interval at which the EntraPass applications refreshes the condition reported by the status icon visible in the status bar. Refresh delays range from 0.01 to 4.59 sec. in increments of 0.01 sec.
- 8 You can define the **Maximum Records in Report Desktop** that can be retrieved from archived files and displayed on screen. The maximum is 200,000.


Defining Alarm Controls

- 1 Click the **Alarms** tab to define how alarms should be processed.



 **NOTE:** Alarms desktops are configured in the Desktop definition menu. For details, see "EntraPass Desktops" on page 239.

- 2 In the **Alarm control** section:
 - Specify the number of alarms that will be **kept on the server** when the EntraPass workstation is off-line, that is, when it is not connected to the module. The module buffers a maximum of 100,000 alarms per EntraPass workstation (default: 5,000).
 - Specify the number of alarms that will be **kept on the workstation**. There is a maximum of 100,000 alarms per EntraPass workstation. By default, it keeps 5,000 alarms.

 **NOTE:** The EntraPass workstation will always keep newer events. To view older events, you have to request a historical report. For details on requesting reports, see "Reports" on page 267.

- 3 Specify if the Server should keep newest or oldest alarms when its buffer reaches the defined maximum number:
 - **Keep older alarms:** the module will keep the oldest alarms and archive the newest alarms when the EntraPass workstation is off-line and when the Server buffer is full.
 - **Keep newer alarms:** The module will keep the newest alarms and archive the oldest alarms when the EntraPass workstation is off-line and when its buffer is full. Alarms are processed on a first in - first out basis.

- 4 You may want to create exceptions to the EntraPass workstation configuration by checking **Apply operator parameters for alarms** options. When this option is enabled, operator settings have priority over EntraPass workstation settings.



NOTE: If the **Apply operator parameters for alarms** options are selected all events will be filtered according to the EntraPass workstation configuration, and filtered again according to the security level of the operator who is currently logged on the EntraPass workstation. If the **Apply operator parameters for alarms** options are selected and no operator is logged in, or the EntraPass workstation is off-line, events will NOT be buffered by the system.

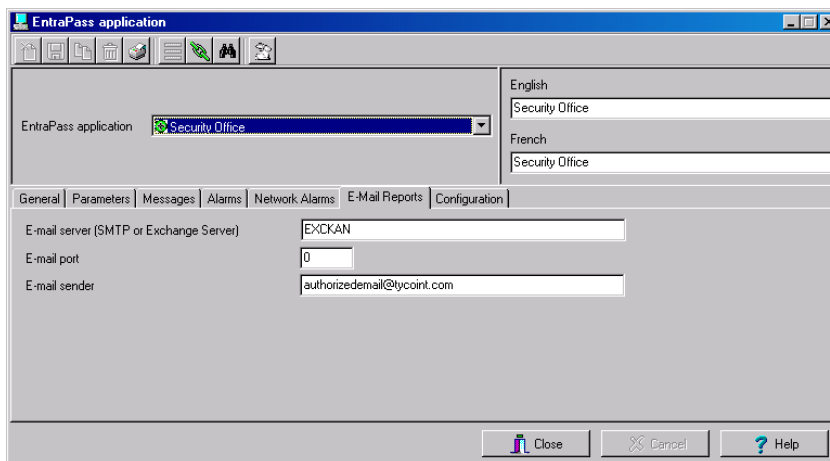
- 5 In the **Clear Message Desktops** section, specify when alarms should be cleared:
 - **On logout** (on a regular logout by an operator)
 - **On workstation shutdown** (when the EntraPass workstation is completely shutdown)
- 6 You may define the acknowledgement parameters. Checking **Display alarm message box** will send an acknowledgement message box even if the operator is working in another application. When this option is enabled, you have to enter the delay during which the acknowledgement message box will be suspended. At the end of the delay, an alarm message box will be displayed again requiring an acknowledgement from the operator.
- 7 You may check the option **Send message on acknowledge time-out** to generate an “acknowledge time-out” event when the operator fails to acknowledge an event during the time-out delay specified in the **Acknowledge time-out delay** field. The message will be sent to the Message desktop and the Alarms desktop. For more information on EntraPass desktops, see “*Entrapass Desktops*” on page 239.

Defining e-Mail Report Options

Entrapass offers users the ability to send and to view reports using e-mail capabilities. e-mails can be sent in two formats: report pack files (rpf) and comma separated values (CSV).

- **rpf files:** this file is a compressed report file. It can be opened with a double-click. To view rpf files, users must install a new version of EntraPass Workstation package or the Report Viewer (Set up window) utility found on the installation CD or on Kantech Web site (www.kantech.com).
- **CSV files:** these files can be viewed using Excel or any spreadsheet editor.

- 1 From the EntraPass applications main window, select the **E-mail** tab.



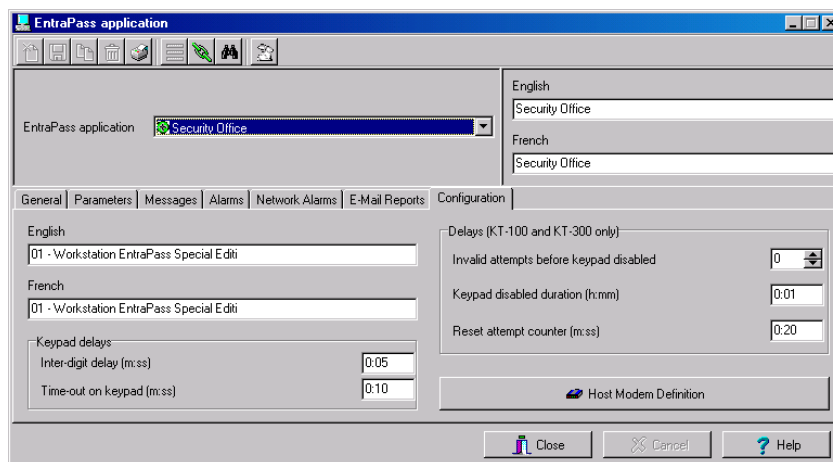
- 2 In the **E-mail server (SMTP or Exchange)** field, enter the name of the E-mail server that will be used for sending e-mails.
- 3 In the **Port** field, enter the number of the port that will be used for sending e-mails (usually 25).
- 4 Enter a valid E-mail address in the **From** field. This e-mail address will be used for authenticating the e-mail server.



NOTE: To view reports sent from EntraPass, the **Report Viewer** utility must be installed on computers where EntraPass is not installed. To install this utility: Installation CD > Setup window.

Defining Host Modem and Keypad Delays

The host modem and the keypad delays are defined in the **Configuration** tab.



- 1 In the **Keypad** delays section, enter the **Inter-digit delay** time (m:ss). It represents the maximum delay permitted between each selection of a keypad key by a user.
- 2 Enter the **Time-out on keypad** delay time (m:ss). It is set in seconds. It represents the maximum time allowed for users to begin entering their personal identification number at a keypad.



NOTE: The maximum time allowed for both the inter-digit and time-out on keypad delays is 4 minutes and 15 seconds.

- 3 In the Delays KT-100 and KT-300 only, use the up/down arrows, determine the number of **Invalid attempts before keypad is disabled**. Users have a maximum of 255 invalid attempts before the keypad is disabled.
- 4 Enter the **Keypad disabled duration** delay (h:mm). The maximum duration allowed is 4 hours: 15 minutes. When the counter reaches the maximum attempts counter, the keypad will be disabled for all cards. It is disabled for the delay specified in the **Keypad disabled duration** field.
- 5 Enter the **Reset attempt counter** delay (m:ss). When the delay specified in the **Reset attempt counter** field is expired, the system will set the attempt counter to zero. The maximum delay is 4:15 minutes. If the value entered is greater than the maximum allowed, then the system will use the previous correct value.



- 6 Click the **Host Modem Definition** button to configure the modem communication options if your gateway connects to the first controller of a remote site via modem.

Select a modem	English	Host Modem#1
Description	French	Host Modem#1
Host Modem#1	Modem connection type	Receive and transmit
	Serial Com port	18
	Host Baud Rate	19200
	Code to access an outside line	
	Host phone number	5
	Modem brand	US Robotics sportster 33.6
	Modem init settings	AT&F&D2&C1&H0&J0&R1&K0&M0&B1
	Phone line type	Tone
	Number of rings before answer	1

- Click on the **New** button to add a modem to the modem selection list.
- Configure the modem as per the example entries shown in the previous window and click **OK** to return to the **Device** definition window.



NOTE: For reliability and configuration consistency, Kantech currently supports the US Robotics Sportster external modem only. Moreover, the **Modem connection type** should be set to **Receive and transmit** while the **Modem settings** should not be changed. If you are uncertain about modem setup parameters, consult your network administrator for the settings which apply to your particular hardware configuration.

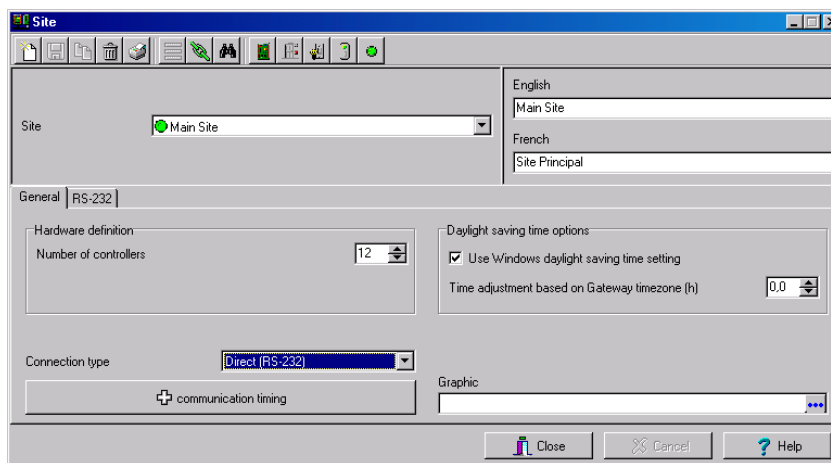
Sites Configuration

A site is composed of 32 controllers attached to the same serial port. EntraPass Special Edition supports 2 sites composed of KT-100, KT-200 or KT-300 controllers.

Items displayed in the EntraPass Site window vary depending on the selected connection type. For example, if the selected connection type is an RS-232, an **RS-232** tab will be displayed to configure the corresponding serial port and baud rate. If the connection type is dial-up, three extra tabs will be displayed for modem configuration.

Four types of connections are available: Direct (RS-232 and USB), Enhanced Ethernet (KT-IP), Ethernet (polling) and Dial-Up (RS-232) modem.

- 1 From the **Devices** window, click the **Site** icon.

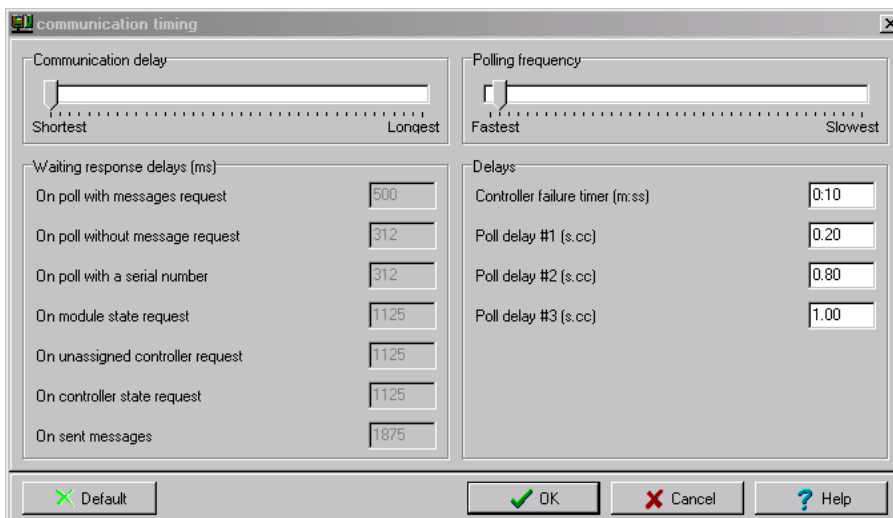


- 2 Select the **Gateway** where the site will be configured.
- 3 If you are defining a new site, assign a name to the new site and click the **Save** icon. The bullet next to the site name will turn green.
- 4 Under the **General** tab:
 - In the **Hardware definition** section, specify the number of controllers for the site. There may be up to 32 controllers per site. If the number specified is greater than the maximum allowed, the system will set the value to 32.
 - In the **Daylight saving time option** section, check the **Use Windows daylight saving time setting** box to automatically switch to daylight saving time according to Windows standard settings. Leave unchecked if you want to do it manually.
 - If you are communicating with a remote site by modem, enter the time difference between the remote site and the EntraPass location in the **Time adjustment based on Gateway timezone (h)** field. This setting will allow events from the remote site to be displayed at local gateway time on EntraPass workstations located in different timezones.

- Select a **Graphic** to which the gateway is assigned, if applicable. Use the scroll list to select the **Connection type** between the system. This will determine which tabs will be displayed for configuration.

To Set Up Communication Timing

Caution: Do not use the **Communication timing** option. If you need to set up the communication delay and polling frequency, call Kantech Customer Assistance. Inappropriate use of this option may cause serious problems to the system. The Communication timings window shows the actual default settings. They must be preserved unless advised otherwise by Kantech Systems.

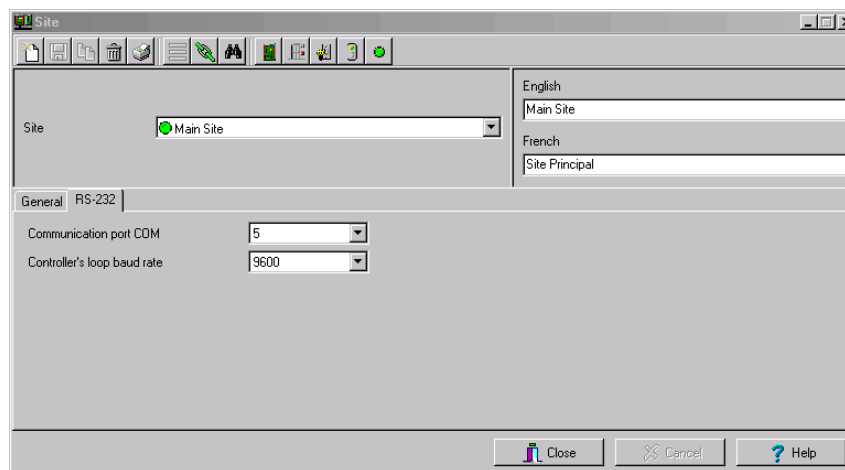


To Configure a Direct RS-232 Connection Type

This type of connection can be configured in EntraPass Special Edition to communicate via a RS-232 gateway.



- 1 When selecting the **Direct RS-232 connection type** option in the **General** tab, a **RS-232** tab will become available.



- Select the **Communication Port COM**.
- Select the **Controller's loop baud rate**. The default rate is 19200 baud.

To Configure an Ethernet Kantech IP Link Connection Type

This type of connection can be configured in EntraPass Special Edition to communicate via a Kantech IP Link module.



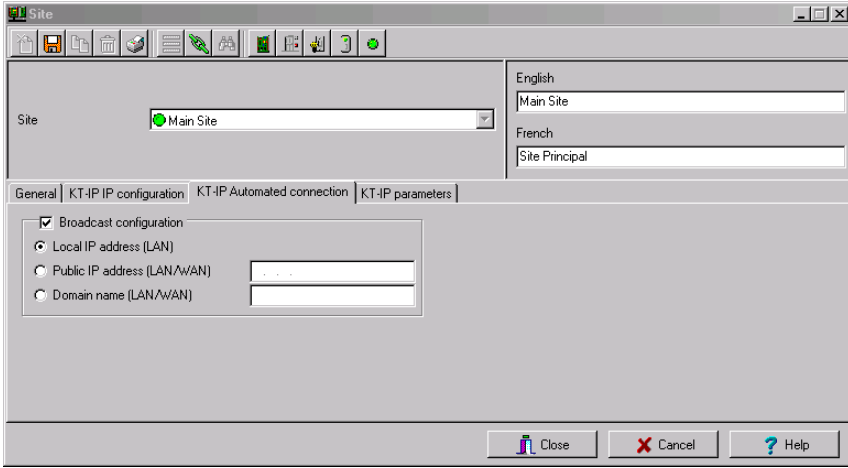
NOTE: For complete information on configuring the Kantech IP Link module, please refer to the Kantech IP Link Module Installation Manual, DN1670.



- 1 When you specify **Enhanced Ethernet (KT-IP)** from the **Connection type** drop-down list in the **General** tab, you will be able to access three extra tabs: **KT-IP IP configuration**, **KT-IP Automated connection** and **KT-IP parameters**.

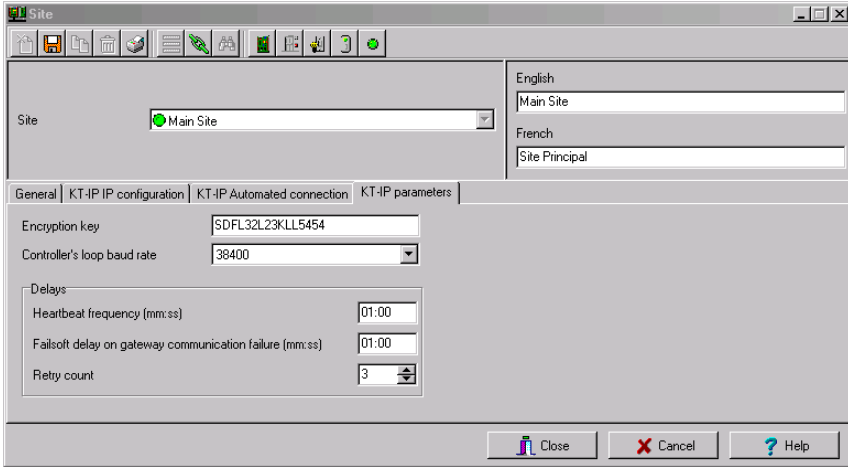
- **MAC address:** Enter the Kantech IP Link module MAC address. The first 6 numbers in the MAC address (00-50-F9) cannot be modified.
- The **Online** box must be checked at all time.
 - **Obtain IP address automatically:** Check this option when configuring a Kantech IP Link module with a DHCP or automatic address.
 - **Use the Following IP Address:** Check this option when you want to assign a static address to the Kantech IP Link module. When selected the next three parameters will become available.
 - **IP Address:** Kantech IP Link module static IP address that should have been provided by the System Administrator. Make sure that the IP address is unique and belongs to the same segment than the Kantech IP Link module segment (for example: 192.168.0.X, X being the number that differs from the Kantech IP Link module address).
 - **Subnet mask:** This address should have been provided by the System Administrator. Make sure that the subnet mask is the same as the Entrapass Special Edition system.
 - **Gateway (Router):** You will enter the computer gateway address.
 - Port **18810** is automatically assigned to the Kantech IP Link module by default. It is advisable not to modify it.
- The **Gateway address** will be used when in DHCP mode.
 - **IP address:** You will enter the computer gateway address.
 - **Domain name:** If necessary, you will enter the name provided by the System Administrator.

- 2 Move to the **KT-IP automated connection** tab if you are in a WAN environment.



The screenshot shows the 'Site' configuration window with the 'KT-IP Automated connection' tab selected. The 'Broadcast configuration' checkbox is checked. Under the 'Local IP address (LAN)' section, the 'Local IP address (LAN)' radio button is selected. The 'Public IP address (LAN/WAN)' and 'Domain name (LAN/WAN)' radio buttons are unselected, and their respective input fields are empty. The 'General' tab is also visible, showing 'Main Site' selected for the site and 'English' for the language.

- In a WAN environment, the **Broadcast configuration** box must be checked at all times.
 - **Local IP Address:** Will assign the Kantech IP Link module IP address automatically.
 - **Public IP Address (LA/WAN):** This IP address should have been provided by your internet provider.
 - **Domain Name (LAN/WAN):** This information should be provided by the System Administrator.
- 3 Move to the **KT-IP Parameters** tab to configure security and communication parameters.



The screenshot shows the 'Site' configuration window with the 'KT-IP Parameters' tab selected. The 'Encryption key' field contains the hexadecimal code 'SDFL32L23KLL5454'. The 'Controller's loop baud rate' is set to '38400'. Under the 'Delays' section, 'Heartbeat frequency (mm:ss)' is '01:00', 'Failsoft delay on gateway communication failure (mm:ss)' is '01:00', and 'Retry count' is '3'. The 'General' tab is also visible, showing 'Main Site' selected for the site and 'English' for the language.

- **Encryption key:** You will enter a 16-digit hexadecimal code to secure your site.

- **Controller's loop baud rate:** Enter the controller's loop baud rate.



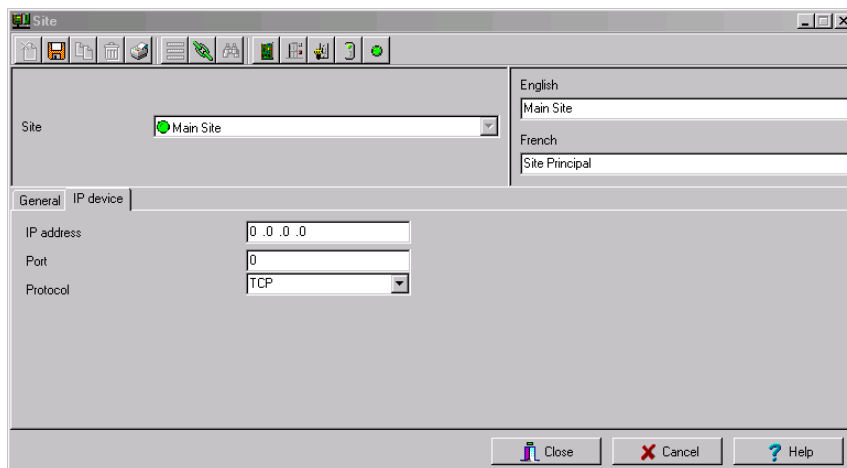
NOTE: For KT-200, the maximum baud rate is 19200.

- In the **Delay** section:
 - **Heartbeat frequency (mm:ss):** Enter the frequency to which you want the Kantech IP Link module to send a signal to the gateway to indicate it is online
 - **Failsoft delay on gateway communication failure (mm:ss):** Enter the delay before the gateway will consider the Kantech IP Link module has lost communication.
 - **Retry Count:** Enter the number of time the gateway should try communicate with the Kantech IP Link module before doing a hard reset.

To Configure an Ethernet Polling Connection Type

This type of connection can be configured in EntraPass Special Edition to communicate with the system via the network (Lantronix).

- 1 When selecting the **Ethernet (Polling)** option in the **General** tab, an **IP device** tab will become available.

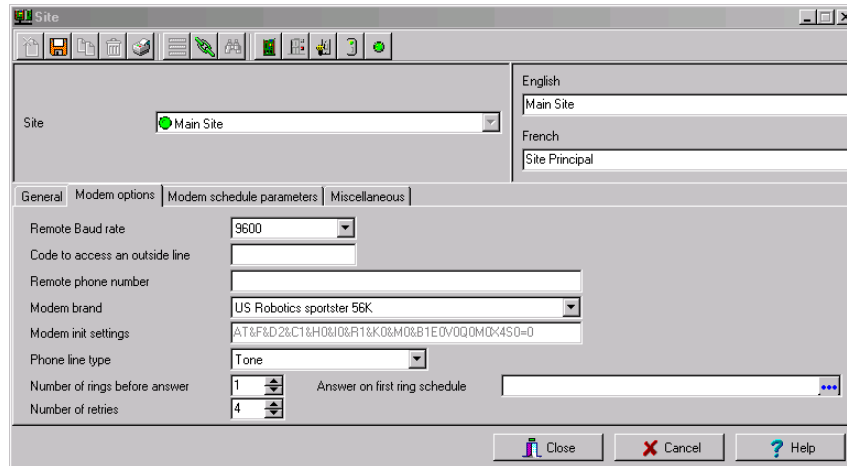


- Enter the terminal server **IP address** and **Port** number.
- Select the communication protocol:
 - **TCP** if the site communicates with the gateway through a terminal server using TCP protocol. In this case, you have to configure the terminal server. To do this, follow the manufacturer's instructions or refer to the Terminal server documentation.
 - **UDP** (User Datagram Protocol), a connectionless protocol that, like TCP, runs on top of IP networks. UDP offers a direct way to send and receive data over an IP network. It is used primarily for broadcasting messages over a network. Check this option if the site you are configuring uses this protocol.

To Configure a Dial-Up (RS-232) Modem Connection Type

If you specified **Dial-up (RS-232) modem** from the **Connection type** drop-down list in the **General** tab, you will be able to access three extra tabs: **Modem options**, **Modem schedule parameters** and **Miscellaneous**.

- 1 Select the **Modem Options** tab to set outgoing call behavior to site modem.



NOTE: The **Remote Baud rate** should not be changed. If you are uncertain about modem setup parameters, consult your network administrator for the settings which apply to your particular hardware configuration.

- Enter the **Code to access an outside line** (if applicable).
- Enter the **Remote phone number**.

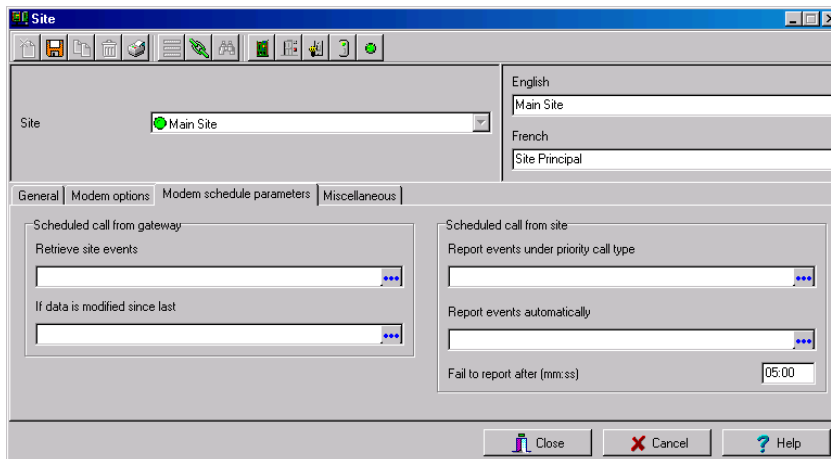


NOTE: For reliability and configuration consistency, Kantech Systems currently supports the US Robotics Sportster external modem only.

NOTE: The **Modem init settings** can not be changed.

- Select the **Phone line type**: **Tone** or **Pulse**.
- Set the **Number of rings before answer** that will define the number of rings before the modem picks up the call. This option is valid whenever ring schedules are not in effect.
- Set the **Number of retries**. This will set the number of calls the modem will attempt to make before giving up.
- Set the **Answer on first ring schedule** option to configure the time interval during which site modem will be allowed to answer on one ring.

- 2 Move to the **Modem Schedule parameters** tab to set time intervals during which the gateway or site connects to remote sites or gateways (through modem calls) in order to perform specific tasks.

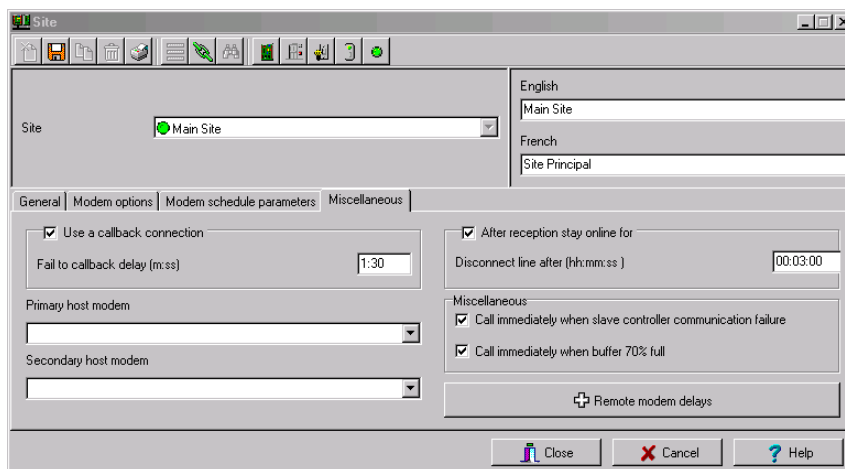


- Click on the **Retrieve site events** browse button to bring up the schedule selection window. Select the schedule that best corresponds to the time requirements set out for this task. For more information on defining schedules, see *"Schedules Definition" on page 98*
- Repeat this step for **If data is modified since last**, **Report events under priority call type** and **Report events automatically**.
- Define the delay before the system will **Fail to report after (mm:ss)**.



NOTE: To schedule the reporting of events under priority call types, first define **Priority call types** for items such as doors, inputs and controllers.

- 3 Click the **Miscellaneous** tab to configure how modems handle site incoming and outgoing calls.



- Check the **Use a callback connection** box to force the gateway modem to hang up after initial connection to the remote site modem and to stand by for an acknowledgement call from the remote modem. You may also want to customize the **Fail to callback delay**. Default is set to 1:30 (1min 30 sec.).
- Select the **Primary host modem** in the drop down list. If available, select a backup modem in the **Secondary host modem**. This setting is useful when the primary modem is busy or fails to take the call.
- Check **After reception stay online for** if you wish to limit in-call time to a predetermined amount of time which can be set to anywhere between 00.03.00 and 23.59.59.
- Check the **Call immediately when slave controller communication failure** to be alerted in the event that a slave controller fails to send data to the master controller (the one carrying the modem).
- Check the **Call immediately when buffer 70% full** to force download of a site controller's event buffer as soon as it reaches 70% capacity.



NOTE: Do not click the **Remote modem delays** button. All values are factory-set for optimum performances with the supported US Robotics modems. Settings **SHOULD NOT** be edited unless recommended by Kantech.

Controllers Configuration

Controllers provide audiovisual feedback on the access decision. Typically, a red/green light (LED) indicator on the reader informs the cardholder that the door is unlocked or that access has been denied. A local door alarm can be installed to provide an audible warning if the door is forced open or remains open after an access.

The controller definition tells the system how a controller is being used and what devices are associated with it: (doors, input zones, relays and output devices). Controllers may be defined during a gateway or site definition; or in the controller definition menu, by selecting either the controller icon (**Devices > Controller**) or by using Express Setup utility.

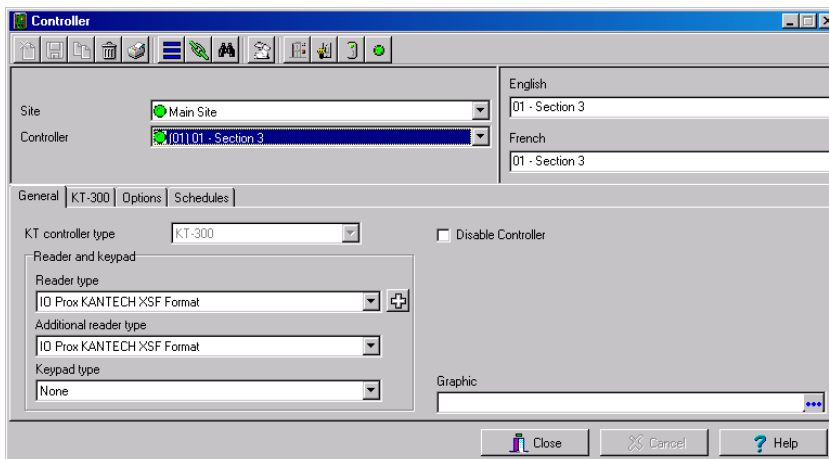
EntraPass supports three types of controllers: KT-100, KT-200 and KT-300. These provide the ability to activate local functions associated with a controller.

The number of devices associated with a controller varies according to the controller type. The following table summarizes the basic components associated with each type of Kantech controller:

Type	Doors	Relays	Input Zones	Auxiliary Outputs
KT-100	1	4	4	2
KT-200	2	2	16	4
KT-300	2	2	8	4

To Configure General Parameters for KT Controllers

- 1 From the **Controller** definition window, select the gateway associated with the controller site.
- 2 From the **Site** drop-down list, select the site where the controller is located.
- 3 From the **Controller** drop-down list, select the controller you want to define. Once selected, the language section is enabled. You may rename the selected controller.
- 4 In the **General** tab drop-down list, select the **KT Controller type**.



- Assign a meaningful name to the controller in the language section (English and French in our example), then click the **Save** icon. Once you save, the **Controller type** drop-down list becomes disabled.



NOTE: If you selected **KT-200**, a number appears next to the drop-down list. If you move your cursor above that number, a hint will popup to indicate the jumper setup for that **KT-200** controller.


- The system prompts you to use the Express Setup program. Click **Yes** to continue. If you select **No** you will have to manually configure these devices in their respective definition menus (doors, relays, inputs and auxiliary outputs).



NOTE: *Entrapass* offers you the ability to install two types of readers on the same controller (primary and secondary). The two readers must be of the same technology (Wiegand or ABA). This feature is only available with **KT-100**, **KT-300** under a Corporate Gateways.

- After configuring components associated with the controller, select the reader and keypad installed on your controller from the **Reader** and **Keypad type** drop-down lists.



NOTE: The **New reader driver** icon  allows you to install a custom driver for a specific controller. Moreover, using this button allows you to add the driver in the Read Driver table, making it available the next time you want to configure a new controller.

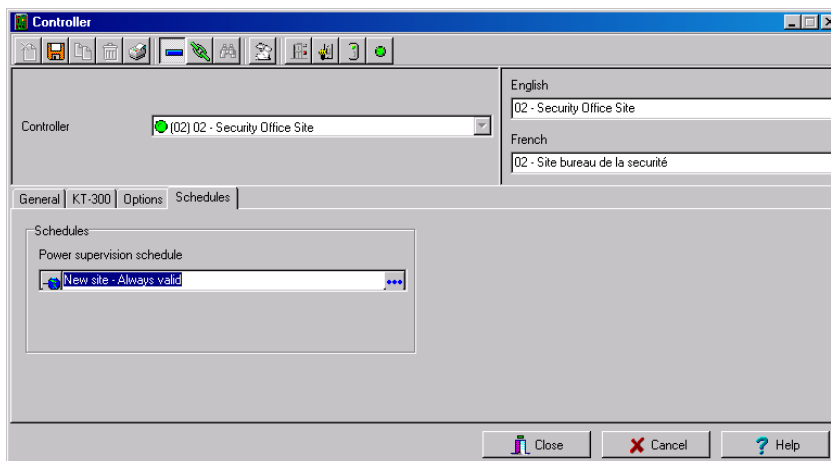
- Use the **Disable Controller** when you need to put the controller in disable mode. In disable mode, the controller will never be polled and all status requests from this specific controller will send a message that this controller is disabled.



NOTE: This option can be used when a controller is removed temporarily but must not be deleted (when under repair, for example). It also allows Operators to easily setup the software before the physical installation is completed.

- Select a **Graphic** to which the gateway is assigned, if applicable.

- 5 To define the schedules applicable to the new controller, you must move to the **Schedules** tab.

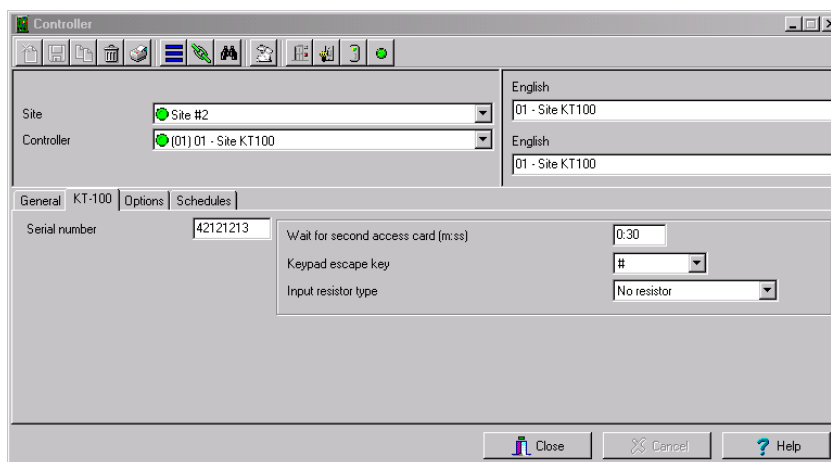


- Select the applicable **Schedules** for the new controller:
 - When a KT-100 or KT-300 is selected: only the **Power supervision schedule** list is displayed.
 - For KT-200, the **Power supervision schedule** and the **Tamper switch supervision schedule** lists are available.
- 6 Click the **Save** icon.

To Configure a KT-100 Controller

Once the general parameters are defined, the **Controller type** tab is displayed.

- 1 Select the **KT-100** tab from the **Controller** window.



- 2 Enter the controller serial number in the **Serial number** field. Usually, the number is found on the controller label. The field is defined to accept only numeric characters, except for the first character which may be an a or A. If a lower case character is entered, the system converts it to a capital letter.
- 3 Enter the **Wait for second access card** delay. The maximum time allowed is 2 minutes 07 seconds. This feature is useful for secured areas where two cards are required to access a secured door. If the value entered is greater than the maximum allowed, the system will use the existing value.
- 4 In the **Keypad escape key** drop-down list, choose a keypad escape key if applicable. This feature is associated with PIN numbers. When a user enters a wrong number, he/she may press the escape key and re-enter the PIN, without incrementing the number of attempts.
- 5 In the **Input resistor type** drop-down list, select the resistor type used with your system. By default, this choice is set to **Single resistor**. This feature is used as a supervision device for all inputs. In fact, if this feature is enabled and if an input is disconnected, an alarm message is generated and sent to the Alarm message desktop (or other desktop configured to receive such events).

To Configure a KT- 200 Controller

Each KT-200 can monitor, in real-time, the state of 16 input points such as magnetic contacts, motion detectors, temperature sensors, etc. The door contact (supervising door state) and the REX (warning the system that a user is exiting) are connected to such inputs.

The KT-200 is equipped with two relays. These relays can be activated according to schedules, reported events or a combination of different logical conditions. The system is expandable to 16 relays using REB-8 relay expansion board modules. REB-8 may be used as relays or as elevator controllers. KT-2252 are only used as elevator controllers.



NOTE: Please note that KT-2252 are no longer available.

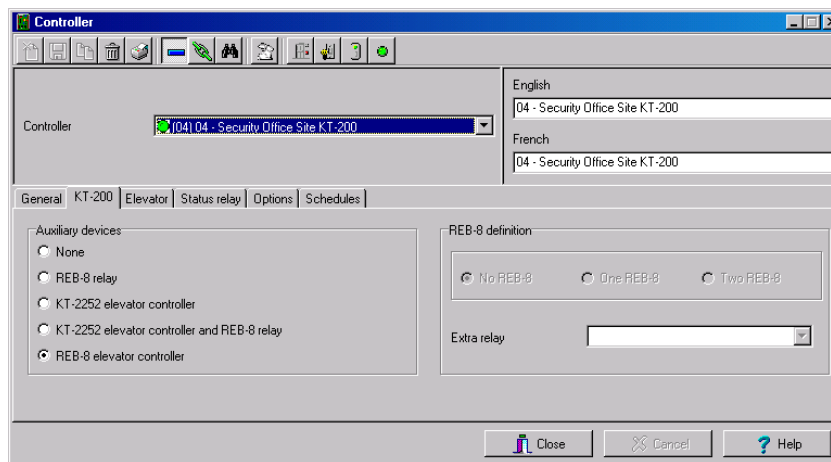


Defining KT-200 Expansion Devices

KT-2252 elevators offer a low voltage interface for up to 32 floors. Up to 4 KT-2252 can be connected to one KT-200 controller for a maximum of 64 floors per cab. One KT-2252 can be shared between 2 cabs, serving a maximum of 16 floors each (one common service switch for both cabs). When users present their cards to the elevator cab reader, the KT-200 verifies which floors can be accessed by this cardholder and sends a list of floors to be enabled to the KT-2252 interface. The KT-2252 closes the electronic interrupters corresponding to the related floors.

Defining KT-200 auxiliary devices

- 1 From the **Controller** definition window, select the **KT-200** tab.



- 2 In the **Auxiliary devices** section, select the type of devices used with KT-200 controller.
 - Check the **REB-8 relay** option if REB-8 expansion boards are used as relays. Only 16 relays can be defined. If two REB-8 are added, the last two relays (the 17th and 18th relays) can be used to perform different actions. You have to specify the additional actions for the two relays in the **Extra relay** drop-down list.
 - Check the **KT-2252 elevator controller and REB-8 relay** option if KT-2252 are used as elevator controllers and REB-8 are used as relays on the same door controller. A maximum of four KT-2252 can be connected to the controller.
 - Check the **REB-8 Elevator Controller** option if REB-8 are used for elevator control. Up to four REB-8 can be used for elevator control.



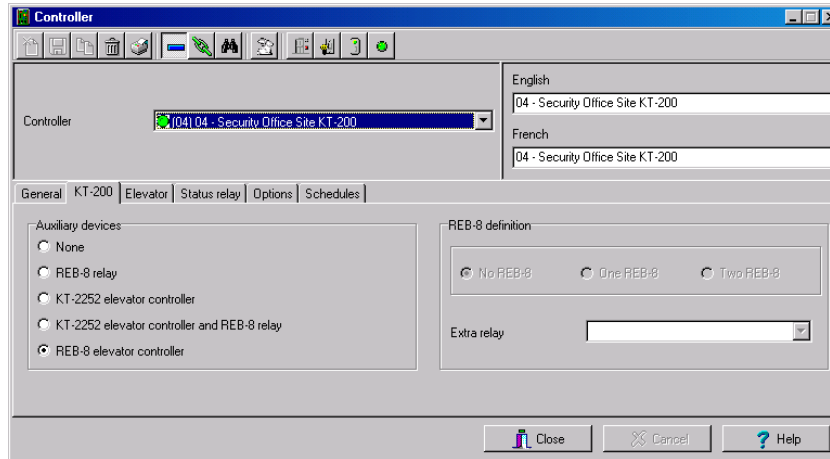
NOTE: When an elevator controller option is checked, an **Elevator** tab appears beside the **KT-200** tab.

The following section explains how to program elevator controls using REB-8 and KT-2252 elevator controllers.

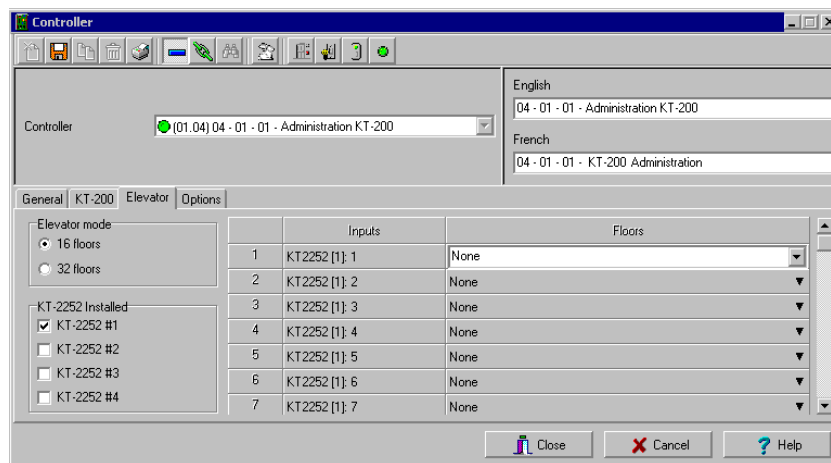
To Program KT-2252 Elevator Controllers

The **Elevator** tab allows you to specify which auxiliary devices are used with the KT-200 for elevator control and how they are used. Depending on the expansion board installed and on the option checked, the Elevator window displays the **REB-8 Installed** or **KT-2252 Installed** section.

- 1 From the **Controller** definition window, select the **KT-200** tab.



- 2 In the **Auxiliary devices** section, select **KT-2252 elevator controller**, or **KT-2252 elevator controller and REB-8 relay**. The **Elevator** tab appears beside the KT-200 tab.
- 3 To configure elevator controllers, select the **Elevator** tab. When KT-2252 elevator controllers are used, the **Elevator mode** section is enabled.



- 4 In the **Elevator mode** section, check the appropriate number of floors. This indicates how the floors are controlled with the KT-2252.
 - Select 16 Floors if there is one KT-2252 for two cabs sharing the same floors.
 - Select 32 Floors if there is one KT-2252 per cab.



NOTE: The **Inputs** column refers to the KT-2252 terminals. When floors have been defined (in the **Floor** menu), the **Floors** column contains the floors that are associated with the inputs.

- 5 In the **KT-2252 installed** section, specify the number of KT-2252 installed. The options are cumulative. If for example the KT-2252 #3 option is checked, KT-2252 #1 & 2 have to be checked as well. The following table summarizes how KT-2252 elevator controllers are used:

Number of Cabs	Number of Floors	Number of KT-2252
1	8	1
1	16	1
1	32	1
1	64	2
2	8	1
2	16	1
2	32	2
2	64	4

- 6 In the **Floors** column, select the floors associated with KT-2252 controller terminals.

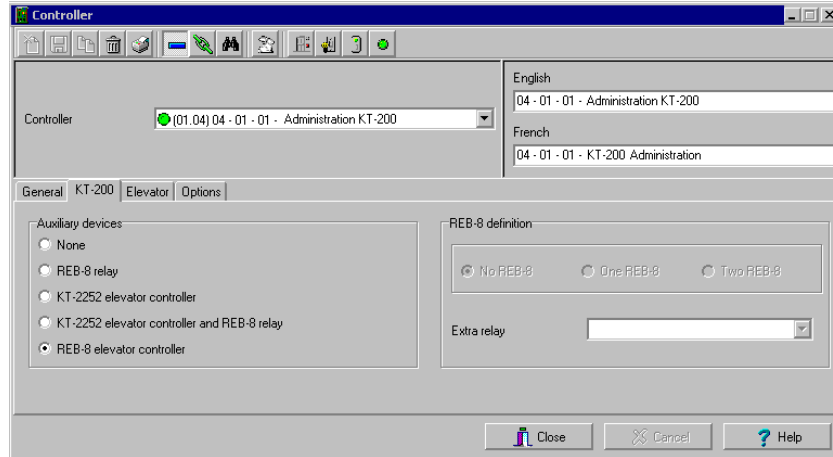


NOTE: The **Inputs** column refers to the KT-2252 terminals. When floors have been defined (in the **Floor** menu), the **Floors** column contains the floors associated with the inputs.

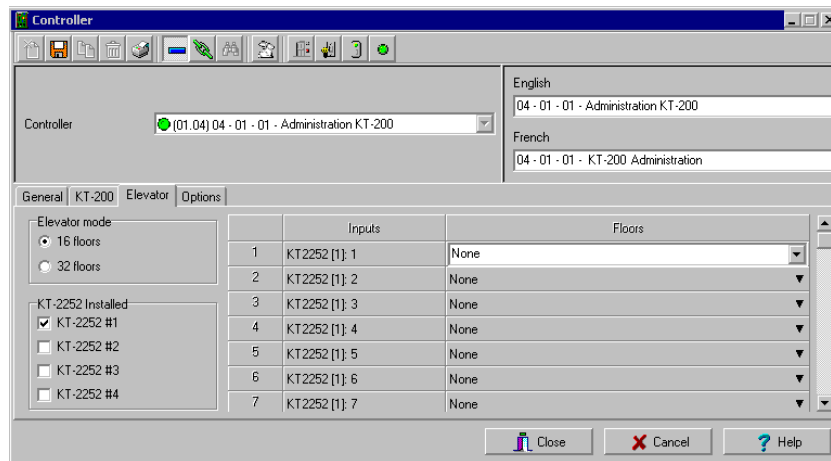
To Program REB-8 Elevator Controllers

REB-8 relay expansion boards may be used as a cost-efficient alternative for elevator control. With a REB-8 expansion board added to a KT-200, the software may control up to two elevator cabs per controller.

- 1 In the **KT-200** definition window, select the **REB-8 elevator controller** option. When the option is selected, an **Elevator** tab appears beside the **KT-200** tab. The REB-8 definition section is only active when REB-8 are used as relays.



- 2 Select the **Elevator** tab to configure the REB-8 elevator controllers. Up to four REB-8 elevator controllers are supported.





- Specify the number of REB-8 that are installed on the controller. The selection is cumulative. For example, if four REB-8 are installed, the first three checkboxes have to be checked also. The following table summarizes how REB-8 are assigned to floors and to elevator cabs.

Number of REB-8	Number of Floors	Number of Cabs
1	1 to 8	Cab 1
2	9 to 16	Cab 1
3	1 to 8	Cab 2
4	9 to 16	Cab 2



NOTE: The **Inputs** column refers to the REB-8 terminals. When floors have been defined (in the **Floor** menu), the **Floors** column contains the floors that are associated with the inputs.

- In the **Floors** column, select the floors associated with REB-8 controller terminals. For details on floor definition and door group definition, see "Doors Configuration" on page 81.

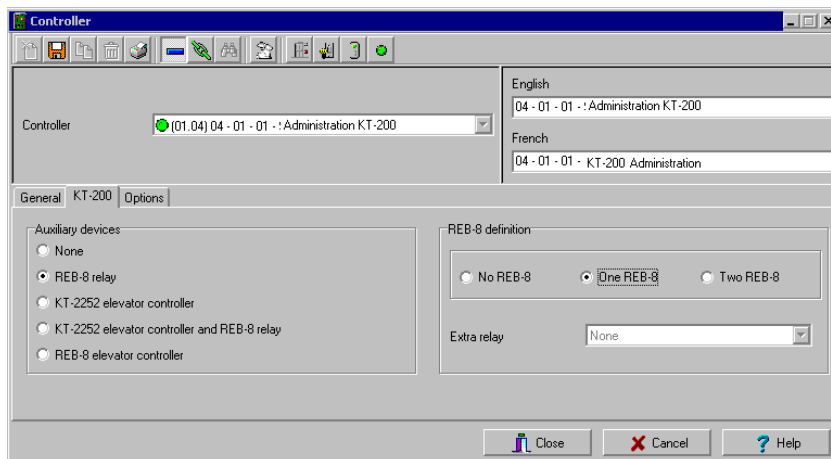


NOTE: There is no floor confirmation when an REB-8 is used as an elevator controller.

Defining REB-8 Relays

When REB-8 are used as relays, you need to specify how many relays are installed on the KT-200. The controller can handle a maximum of 16 accessible relays and already provides 2 on-board relays.

- Under the **KT-200** tab, select the **REB-8 relay** option if REB-8 are used as relays.



- If they are used with the KT-2252 elevator controller, select the **KT-2252 elevator controller and REB8 relay** option. In either case, the REB-8 definition section is enabled.



- 3 In the **REB-8 Definition** section, select the appropriate option: No REB-8, One REB-8 or Two REB-8.
- 4 If two REB-8 are added (for a total of 18 relays), the last two relays can be used to perform different actions: select the use for the extra relays from the **Extra relay** drop-down list.
- 5 Select the **Status relay** tab to program a relay or group of relays that will be activated when an event occurs.

To Configure a KT-300 Controller

The KT-300 constantly supervises battery condition and reports “Low battery / No battery condition” status to the system. It also supervises locking devices for short and open circuits to detect lock failures.

KT-300 controllers support Combus modules. The Combus is a 4-conductor cable bus to which several expansion modules are connected in parallel to add inputs, outputs, relays and an LCD time and date display.

- 1 From the **Site** menu, click the **Controller** icon, then select the **KT-300** tab.

The screenshot shows the 'Controller' configuration window. The 'Site' dropdown is set to 'Administration Floor' and the 'Controller' dropdown is set to '(03) 03 - Administration Floor KT-300'. The language is set to 'English'. The 'Serial number' field contains '00000000'. The 'Wait for second access card (m:ss)' field is set to '0:30'. The 'Keypad escape key' dropdown is set to '#'. The 'Input resistor type' dropdown is set to 'Single resistor'. Below these fields are three rows for 'Local activation relay' and 'Priority call type' configurations:

Event	Local activation relay	Priority call type
Power failure	(01.01) 01 - 01 - Combus Relay	Immediate call
Combus failure	(01.01) 01 - 01 - Combus Relay	Immediate call
Combus - low power	(01.01) 01 - 01 - Combus Relay	Schedule call

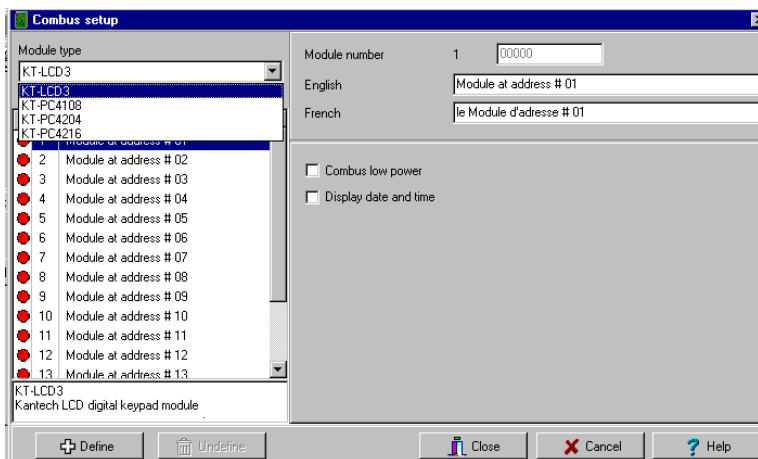
- 2 Enter the controller serial number in the **Serial number** field. Usually, the number is found on the controller label. The field is defined to accept only numeric characters, except for the first character. It may be an a or A. If a lower case character is entered, the system converts it to upper case.
- 3 Enter the **Wait for second access card** delay. The maximum time allowed is two minutes and seven seconds. If the value entered is greater than the maximum allowed, the system will use the existing value. This feature is useful when access to a place is controlled by two cards.
- 4 In the **Keypad escape key** drop down list, choose a keypad escape key if applicable. This feature is associated with PINs. When a user enters a wrong number, he/she may press the escape key and re-enter the PIN, without incrementing the number of attempts.

- 5 In the **Resistor type** drop-down list, select the resistor type. By default, the **Single resistor** option is selected. If you hear a long buzz, verify the number of resistors installed on your system.

To Configure the KT-300 Combus module

Four expansion modules can be connected to KT-300:

- KT-PC4108 (8-zone input expansion module). This module has a tamper contact input.
 - KT-PC4204 (4-relay/power supply expansion module). It has a tamper contact input and also includes a built-in 12VDC, 1A power supply for field devices.
 - KT-PC4216 (16-zone output expansion module). It can be used for elevator control, although additional hardware may be required.
 - KT3-LCD (Kantech 32-character liquid crystal display). The LCD is *green* (normal status), *red* (power failure) and *yellow* (trouble).
- 1 If a Combus module is installed to the KT-300 controller, click the **Combus module configuration** button. Undefined Combus terminals are identified by red flags/bullets. Once a module has been defined, it is identified by a green flag.



- 2 To define a module, select one, then click the **Define** button (lower part of the window). The **Enter Combus module serial number** message box appears.
- 3 Enter the module's serial number, then click **OK**.



NOTE: To obtain this number, you have to activate the Tamper switch or to press any key on the keyboard. The Combus serial number is displayed in the Desktop Message.

- 4 Assign names to the modules in the language fields.

- 5 Check the options related to the module you want to configure (if these are displayed in the window).

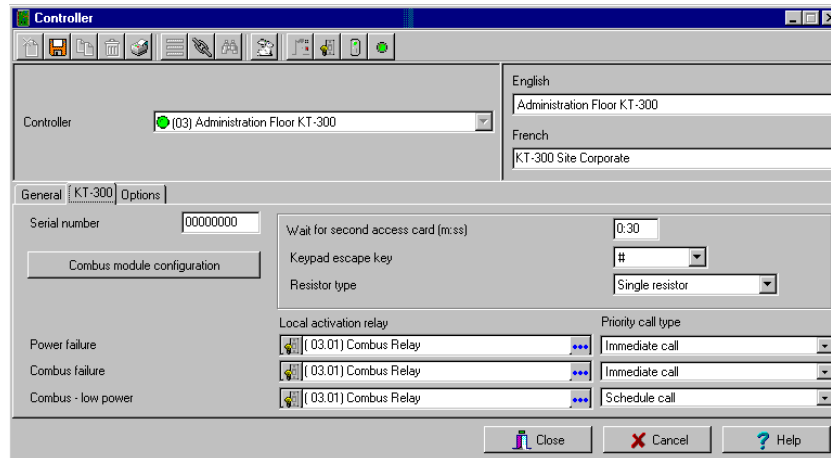


NOTE: Usage options of a module vary according to the selected Combus module. For example, installing the KT3-LCD and checking the options **Combus low power** and **Display date and time** will allow the KT-300 to report Combus low power conditions and to display the date and time.

The following table summarizes the options associated with each module:

Combus type	Options	Additional options
KT3-LCD	Combus low power, display date and time	No additional options
KT-PC4108	Tamper alarm, Combus low power	8 input module May be used as inputs
KT-PC4204	Tamper alarm, Combus low power, Low battery, Power failure, lower auxiliary power	Used as relays (1-4)
KT-PC4216	Tamper alarm, Combus low power	Used as outputs

- 6 Check the **Combus low power** option so that the KT-300 will report any Combus low power condition
- 7 Check **Display date and time** option so that LCD can display the date and time; then click the **Close** button to go back to the KT-300 configuration window.
- 8 When you have finished configuring the Combus module, click the **Close** button to go back to the KT-300 configuration window.



- 9 Associate a **Local activation relay** for **Power failure**, **Combustion failure** and **Combustion low power**. If you want to assign a specific relay, you may click the three-dot button and select a specific relay or group of relays.



NOTE: To configure local activation relay, you must configure relays (**Devices > Relays**), and then select specific relays for local activation.

- 10 Under **Priority call type**, assign the call type option that best suits failure event reporting. To access the **Priority call type** feature, the site connection type must be set to Modem.

To Define Controller Options for

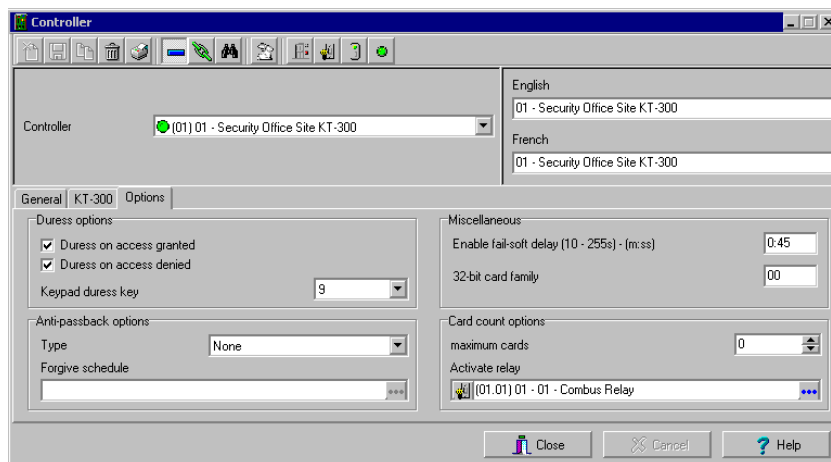
The **Options** tab enables operators to configure such features as:

- Anti-passback (for synchronizing entry/exit readers)
- Duress function (for defining a panic button)
- Card count options (for specifying cards in an area), etc.



NOTE: The anti-passback option works with entry/exit readers. It allows security administrators to keep track of the number of monitored cardholders in an area. It is local to each controller defined by corresponding entry/exit readers. A relay can be activated when the counter reaches the number of cards defined to be inside the area; the relay is disabled when the number of cards in the area goes below the specified number.

- 1 In the **Controller** window, click the **Options** tab to define anti-passback options, duress options and card count options.



- 2 Determine the **Duress** options. When a duress option is selected, you have to assign a duress key, that is a silent panic key.
 - **Duress on access granted:** this option enables the duress key when access is granted.
 - **Duress on access denied:** this option enables the duress key, even when access is denied.

- 3 Select a duress key from the **Keypad duress key** drop-down list.



NOTE: For added security, you may select the two options.

- 4 From the Anti-passback options section, select anti-passback option from the **Type** drop-down list: when an anti-passback option is enabled, a card cannot be used on an exit door unless it has been used on a corresponding entry door.
 - **None:** the anti-passback option is disabled.
 - **Soft passback:** this option allows a cardholder to use an entry (or exit) reader more than once without using the corresponding exit (or entry) reader. Only an “Invalid passback” event is sent to the Message desktop.
 - **Hard passback:** a card used at an entry reader will not be able to access the same entry reader again until it has used the corresponding exit reader.
- 5 In the **Forgive schedule** section, click the three-dot button to set a schedule for resetting the anti-passback option on all other cards.
- 6 In the **Miscellaneous** section, indicate options for **Fail-soft delays** (10-255 second). During a fail-soft mode, the controller operates in stand-alone mode, following a communication failure.
- 7 Enter the **32-bit card family** code. You can locate this hexadecimal code on the access card.
- 8 In the **Card count** option, use the up or down controls to set the maximum card count. The maximum allowed is 65,535. The system keeps track of the number of monitored cards that are in the monitored area and activates a relay when the count is reached. When users exit the area, the counter decrements and the relay will eventually reset when the count is smaller than the value defined.
- 9 You may configure the system to **Activate a relay** when the maximum count is reached. Click the three-dot button to select the relay or relay group that will be activated when the number is reached.

Controller Event Buffer Overflow Message

When a controller is disconnected from the server, the controller buffer starts collecting the controller's events. When the buffer is full, it transfers the oldest events in a secondary buffer (50 to 100 bytes) that can contain approximately 5 to 10 events. When this secondary buffer is full, the system then starts sending messages to the Desktop Message List (shown below) to indicate that the buffer is full and that events are being deleted from the buffer.

Date and time	Event message	Details
12/13/2005 3:55:40 PM	Loop communication trouble	NCC Site #3 VC KT-200 Jigs
12/13/2005 3:55:41 PM	Controller communication restored	VC KT-200 #1 Manual Operation
12/13/2005 3:55:42 PM	Controller successfully reloaded	VC KT-200 #1 Manual Operation
12/13/2005 2:19:16 PM	Fail-soft mode on	VC KT-200 #1 Manual Operation
12/13/2005 2:19:16 PM	Door unlocked by a schedule	NCC Site #3 - VC KT-200 #1 entry, Always valid **
12/13/2005 2:19:16 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:00119,
12/13/2005 2:19:20 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:00120,
12/13/2005 2:19:20 PM	Event buffer overflow	VC KT-200 #1 Manual Operation
12/13/2005 3:19:30 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03674,
12/13/2005 3:19:28 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03675,
12/13/2005 3:19:28 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03676,
12/13/2005 3:19:28 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03677,
12/13/2005 3:19:32 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03678,
12/13/2005 3:19:32 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03679,
12/13/2005 3:19:32 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03680,
12/13/2005 3:19:32 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03681,
12/13/2005 3:19:36 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03682,
12/13/2005 3:19:36 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03683,
12/13/2005 3:19:36 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03684,
12/13/2005 3:19:36 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03685,
12/13/2005 3:19:40 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03686,
12/13/2005 3:19:40 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03687,
12/13/2005 3:19:40 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03688,
12/13/2005 3:19:40 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03689,
12/13/2005 3:19:44 PM	Access denied - card unknown	NCC Site #3 - VC KT-200 #1 exit, 00:03690,

- The controller will delete messages in FIFO order (First In, First Out). The oldest message will therefore be deleted first.
- When the controller is reconnected to the server, the controller events will be sent to the Message list all at once, in the following order: events in the controller's secondary event buffer; events displayed in the controller Event Buffer Overflow, followed by the list of events generated while the controller was disconnected from the server.
- In the Message List above, the highlighted error message "Event buffer overflow" is the first controller event sent to the Message List.

Doors Configuration

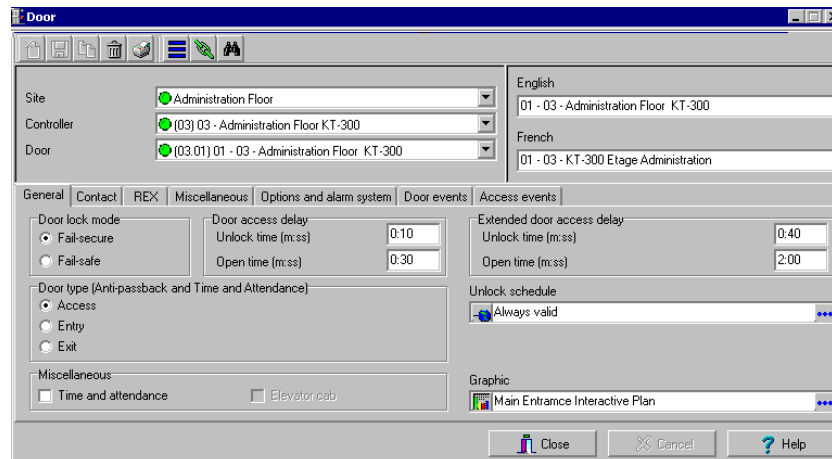
This menu is used to define the door parameters on which readers and/or keypads are installed. A door can be considered as an elevator door, a Time & Attendance door, an entry door for anti-passback, an exit door for anti-passback or an access door. All this depends on how the settings are programmed.

The controlled door may be secured at all times or only during defined schedules. The common locking devices used are electric door strikes and electromagnetic locks.

A door may be equipped with one or two readers, with one reader at each side. For doors equipped with two readers, the outer reader has to be defined as an entry reader and the inner reader as an exit reader.

To Define General Parameters for a Door

- 1 In the Devices toolbar, select the **Doors** icon.



- 2 In the **Doors** window, select a site (from the **Site** drop-down list) and the controller associated with the door you want to define.
- 3 From the **Doors** drop-down list, select the door you want to modify or to define. New items are identified with a red button. The button turns green once the item has been defined and saved.
- 4 Specify the **Door lock mode**: Depending on the lock device used, the locked state will be energized or de-energized to lock.
 - **Fail-secure**: The strike is locked when power is removed (door locks, door strikes).
 - **Fail-safe**: The lock output is energized to lock the door (electro magnetic locks).
- 5 Specify the **Door type**:
 - **Access**: The reader is considered as an access reader. **Time and Attendance** or **Anti-Passback** options are not used with access doors. An access reader generates only "Access granted/Access denied" events.



- **Entry:** An entry door is an entry point for time and attendance or anti-passback. In order for the system to record an entry, the door must be opened after a valid access (if a door contact is installed).
 - **Exit:** An exit door is an exit point for time and attendance or anti-passback. In order for the system to record an exit, the door must be opened after a valid access (if a door contact is installed).
- 6 Specify the **Door access delay**:
- **Unlock time:** The time during which the door is unlocked on a valid card read or a valid request to exit event (when the REX is defined to unlock the door). If this is an elevator door and a push button (input) is used to enable floor selection, this is the time during which a floor selection will be allowed. Usually, a longer period should be defined to allow the user to select floors. For more information, see *"To Define an Input for an Elevator Door"* on page 92.
 - **Open time:** The time during which a door can remain opened following a permitted access or a valid request to exit request. This applies only to a door defined with a door contact input. This time can be from 1 to 255 seconds (4 minutes 15 seconds). After this delay has expired, the system will generate the event "door open too long" and the door piezo will sound to warn the cardholder. You can use the Pre-alarm on door open too long (**Doors** window, **Contact** tab) to sound the door piezo when half of this delay has expired. It will continue to sound until the door is closed.
- 7 In the **Miscellaneous** section:
- If the door is to be used for time and attendance purposes check the **Time and attendance** option. With this option the door must be set as either an entry or an exit door.
 - Check the **Elevator cab** option if the door is to be used for elevator control. When this option is checked, the **Elevator** tab is displayed to define the unlocking schedules.
- 8 If you are using the **Extended door access delay** feature, specify these delays in the **Unlock time** and **Open time** fields. This feature may be useful for cardholders with disabilities.
- 9 When applicable, select an **Unlock Schedule**.
- 10 Select a **Graphic** to which the gateway is assigned, if applicable.

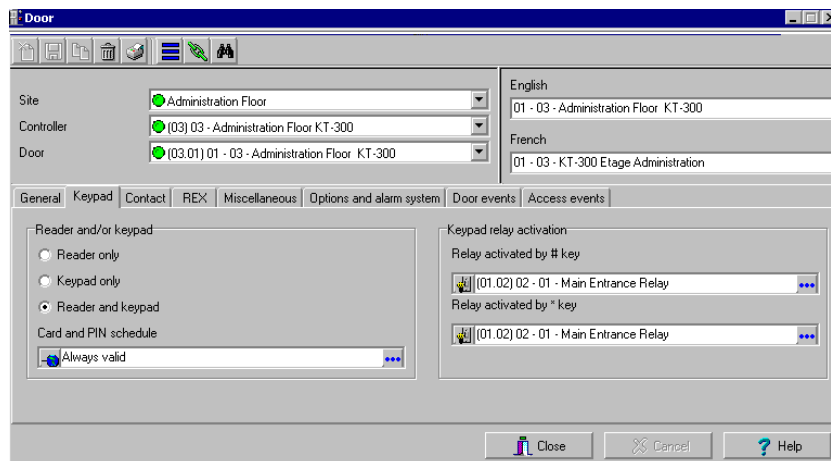
To Define Door Keypad Options

Doors can be defined with relay activation when the * or # keys are pressed on the keypad. This option is available only for KT-100 (with firmware version 1.04 and up) and KT-300 (with firmware version 1.16 and up) controllers.



NOTE: The **Keypad** tab is enabled only if you have selected a keypad type while defining the controller associated with the door being defined.

- 1 From the Door window, select the **Keypad** tab.



- 2 Specify how access to the door is controlled:
 - **Reader only:** Select this option if access is granted using a reader. A reader only installation is the most common application.
 - **Keypad only:** Select this option if access is granted using a keypad only. This option can also be enabled on a reader with an integrated keypad. A keypad only installation is generally considered less secure than a reader only installation, because users may “lend” their codes to another person but cannot prevent further use (in comparison to getting a card back).



NOTE: This option can be enabled on a reader with an integrated keypad if you want, for instance, to use the keypad only.

- **Reader and keypad:** Select this option if both a reader and a keypad are used to permit access to this door. The keypad will only be used when the “keypad schedule” is valid. Adding a keypad to a reader significantly increases the level of security. PIN code requirement can be limited by a schedule for use only outside business hours, for example, rather than during high traffic hours.
- 3 From the **Card and PIN schedule** menu, select a schedule during which cardholders will have to enter their PIN after a valid card read. The time allowed between a valid card read and entering the PIN at the keypad is set in the Gateway definition menu (**Time-out on keypad** option).
 - 4 For doors defined with keypad or reader and keypad, you can program the star key (*) or pound key (#) to activate a relay. When this feature is enabled, users can activate a relay simply by pressing the appropriate key. (This function is only available for KT-100 and KT-300.)

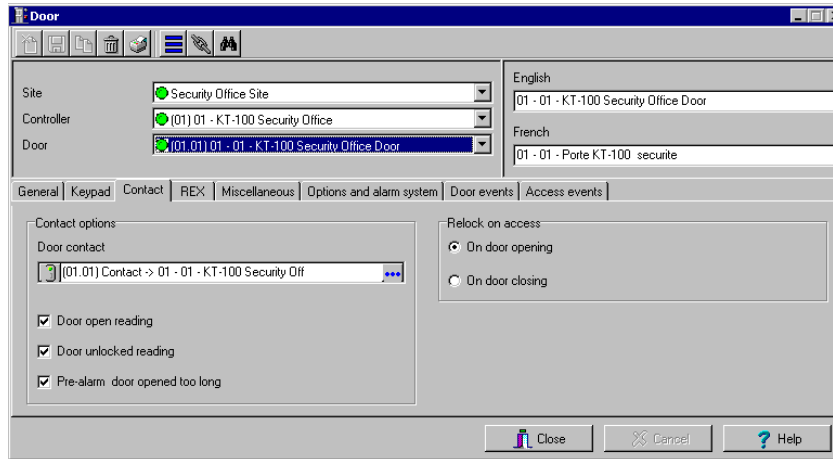
To Define Contact Options

In most applications, the low cost door contact is the only supervisory element that protects the investment made to control access to the door. The door lock and card reader (or keypad) provide



security and prevent unauthorized entry only when the door is closed and locked. A simple door contact allows the ability to monitor several door conditions such as: door forced open, door open too long, interlocks options, etc.

- 1 In the **Doors** window, select the **Contact** tab.



- 2 Select the door contact from the **Door contact** list.



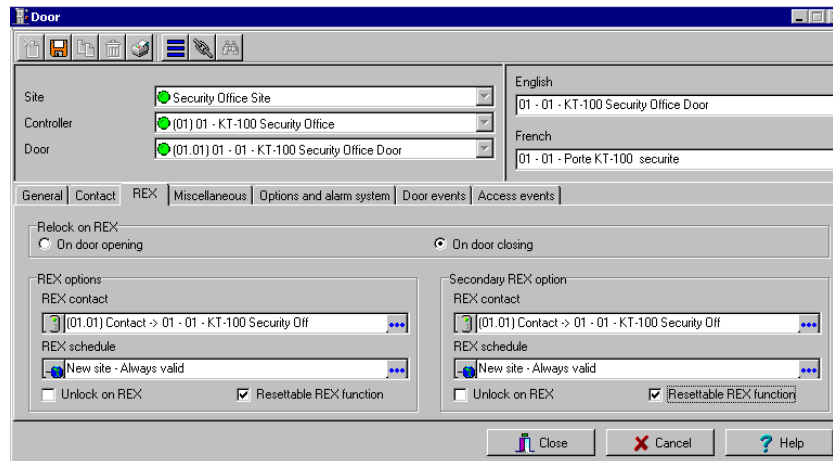
NOTE: For KT-200 Controllers, Input 1 (door contact) and 2 (request to exit device) are ideally reserved for Door 1 of the controller whereas Input 9 (door contact) and 10 (request to exit device) are ideally reserved for Door 2 of the same controller. The input that is used for the door contact or REX contact SHOULD NOT have a “monitoring” schedule defined in the “Input Definition” menu.

- 3 Check the door reading options:
 - **Door open reading**—If selected, this option allows the system to read cards while the door is open. However the system will not unlock the door if it was locked. If selected, the event “Access granted” is generated. Otherwise, the event “Access granted - Door open” is generated.
 - **Door unlocked reading**—If selected, this option allows the system to read cards while the door is unlocked manually by the operator or by a valid unlock schedule. If selected, the event “Access granted - Door unlocked” will be generated on access. To ignore all access events while the door is unlocked, leave this option unselected.
 - **Pre-alarm door opened too long**—If selected, this option allows the system to generate the event “pre-alarm door open too long” and sound the door piezo when half of the delay defined in the **Open time** field is expired. It will continue to sound until the door is closed.
- 4 Select the appropriate **Relock on access** option. You may choose to relock an access **On door opening** or **On door closing**.

To Define REX (Request to Exit) Options

A signal from the REX indicates that someone wants to exit through a controlled door. Devices such as motion detectors, push buttons can provide the REX signal. Entrapass enables users to configure doors with unlock time reset each time the primary or secondary REX is triggered. This option is available only for KT-100 (with firmware version 1.04) and KT-300 (with firmware version 1.16) controllers.

- From the door window, select the **REX** tab, then check the appropriate **Relock on Rex** options:
 - Relock on door opening**, if you want the door device to re-lock following a valid access
 - Relock on door closing**, if you want the door device to re-lock when it closes.



- For the **primary** and **Secondary Rex options**, make the appropriate choices:
 - Assign the **REX contact**: the input to which a “request to exit” detector can be connected. This input must be local; it has to be one of the inputs on the controller operating the door.
 - Select a **Rex schedule**: when this schedule becomes valid, the controller will detect request to exit signals originating for the exit contact. This option applies only to a door defined with a REX contact.
 - Unlock on REX**: the door will be unlocked if a valid request to exit is permitted by the controller. This option may be useful on exit doors such as interior doors, shipping doors or other push doors through which people carrying packages may pass. The system will permit the exit and generates the “request to exit granted” event rather than “door forced open” event.
 - Resetable REX function**: the unlock time is restarted on a valid request to exit. Open and unlock times are defined in the door definition (**Devices > Doors > General**). Select this option for high traffic area doors such as manufacturing doors where many users may need

to exit at short intervals (for example after a work shift) to prevent unwanted door open too long or door forced open events.

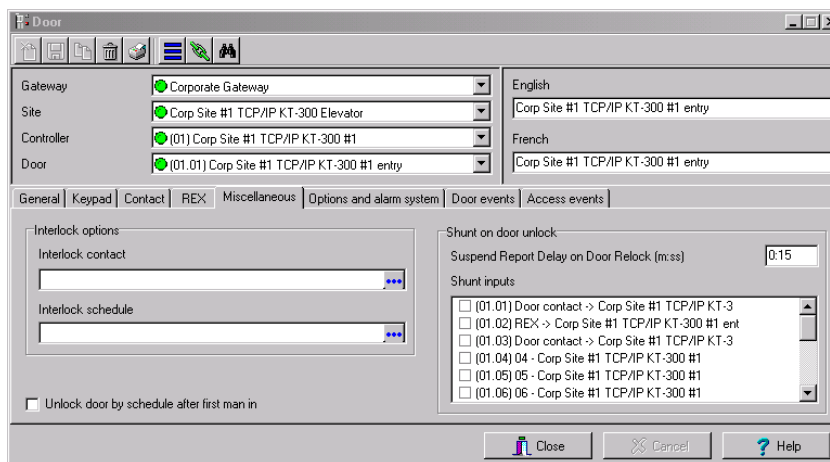


NOTE: It is recommended to choose either **Unlock on REX** or **Resettable Rex function**, not the two options at the same time. If you choose these two options, the door may remain unlocked for long periods of time. Moreover, these features should not be used if a door contact has not been defined.

To Define Miscellaneous Options

You may define interlock options between two doors to synchronize the time when these two doors are open/closed. The interlock option is also called the mantrap option. This ensures that once the cardholder has accessed the first door, that door is closed and locked before the cardholder is granted access to the second door. The two doors have to be controlled by the same controller.

- 1 In the **Doors** window, select the **Miscellaneous** tab.



- 2 From the **Doors** drop-down list, select the first door for which you want to define interlock options.
- 3 From the **Interlock contact** list, select the first input for the interlock feature. The selected input has to be the *door contact of the second door*.
- 4 Return to the **Doors** drop-down list to select the second door for which the interlock options are being defined; then select the interlock input for this second door. It has to be the door contact of the first door.
- 5 Select the **Interlock schedule**: the two doors must have the same interlock schedule. This is the schedule according to which the interlock is checked by the controller before access is granted to users.



NOTE: The interlock feature is not available on doors controlled by a KT-100.

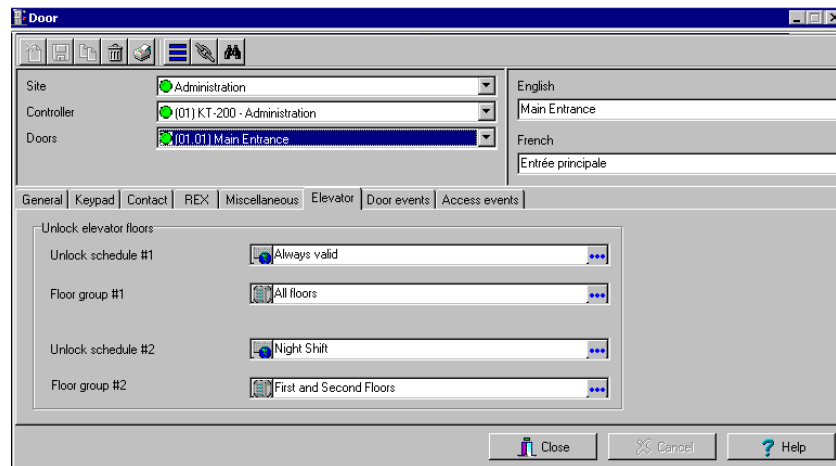
- 6 Check the **No lock by input when lock by alarm system armed option** when applicable.

- 7 Check the **Unlock door by schedule after first man in** option to unlock the door automatically when a first card is read.
- 8 In the **Shunt on door unlock** section, set the time during which selected inputs will not be monitored when the door unlocks. The **Shunt delay** indicates the time during which the selected inputs will not be monitored when the door unlocks. It is not possible to shunt a door contact since the system will automatically shunt it.
- 9 In the **Shunt inputs** scrolling pane, select inputs that will not be monitored when the door unlocks. Selected inputs will remain unmonitored for the delay defined in the **Shunt delay** field.

To Define Elevator Doors

During a door definition, it is possible to specify whether it is a “regular door” or an Elevator cab (**Door** window, **General** tab, **Miscellaneous** section). When a door is defined as an Elevator cab, an **Elevator** tab is displayed in the **Doors** definition window. This tab is used to define the automatic unlock schedules for specific floor groups.

- 1 From the **Doors** definition window, select the **Elevator** tab.



- 2 From the **Unlock schedule #1** list, select the applicable unlock schedule. By default, you may select the Always valid schedule. You may also create a new schedule (**Definition** menu, **Schedules**).
- 3 From the **Floor group #1** list, select the appropriate floor group associated with the Unlock schedule #1. Only floors that have a valid schedule in the **Floor group** definition will be unlocked or available for selection when the Unlock schedule #1 becomes valid.
- 4 From the **Unlock schedule #2** list, select the schedule applicable to the second group of floors.
- 5 From the **Floor group #2** list, select the appropriate floor group. Only floors that have a valid schedule in the **Floor group** definition will be “unlocked” or available for selection when the Unlock schedule #2 becomes valid.

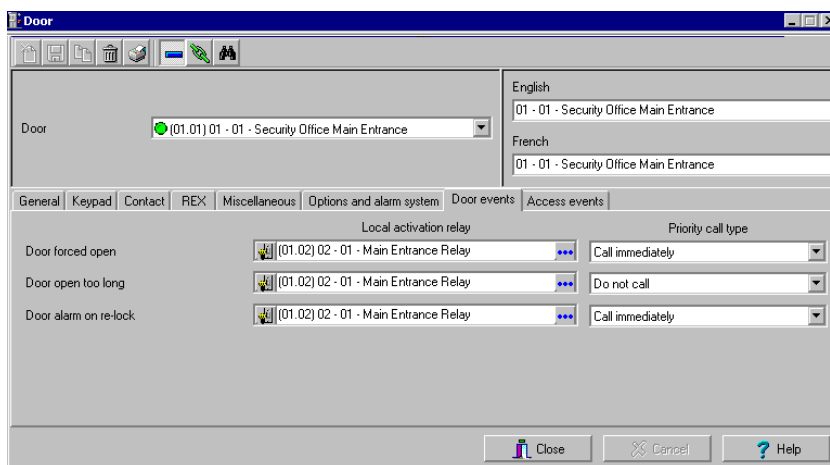
Important Notes:

- The **Unlock schedule** defined during a door definition (**Door** menu, **General** tab) will **OVERRIDE** these schedules even if they are valid.
- Only one **Unlock schedule** can be valid at a time. For example if the first schedule (Unlock schedule #1) is valid from 6h00 to 9h00 and the second schedule (Unlock Schedule #2) is valid from 7h00 to 9h00, then Unlock schedule #2 will **NEVER** be valid since Unlock schedule #1 is already valid.
- Do not overlap schedules. For example, if the first schedule is valid from 8h00 am to 17h00 and the second schedule is valid from 16h00 to 21h00, the gap (between 16h00 and 17h00) can result in erratic operation of the elevator control system.
- Only floors that have a valid schedule in the Floor Group definition will be “unlocked” or available for selection when the unlock schedules become valid.



NOTE: For more information on how to program elevator control using REB-8 relays, see "Defining KT-200 Expansion Devices" on page 70.

- 1 **To Configure Door Events In** the **Doors** window, select the **Door events** tab. This is to define the relays (or relay groups) that are to be activated on specified events.



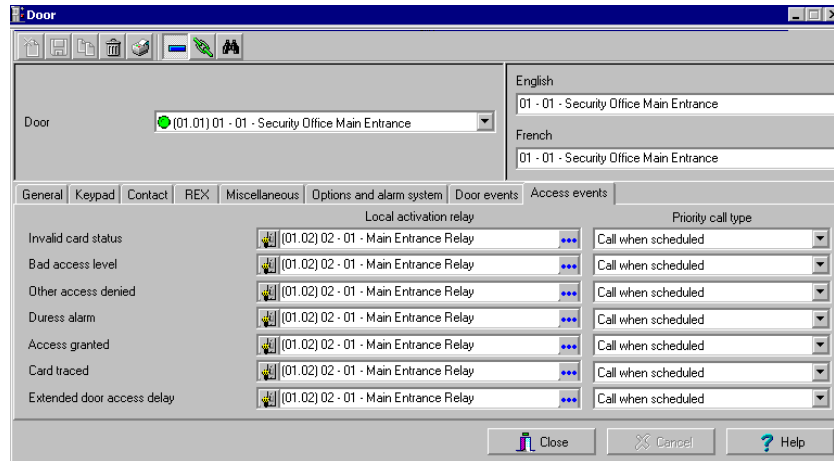
- 2 Select the relay that will be activated locally, on such events as: **Door forced open**, **Door open too long** or **Door alarm on relock**.



NOTE: To access the Priority call type feature, the site connection type must be set to **Modem**.



- Once all door event features have been set, select the **Access events** tab to define relays (or relay groups) that are to be activated on miscellaneous events.



NOTE: *Entrapass offers you the ability to define a relay that will be activated if the **Extended delay** feature is used. The card used must be defined with this feature. Only **KT-100** and **KT-300** can be configured with the **Extended door access delay** feature.*

- Select the relay that will be activated locally, on such events as: **Invalid card status**, **Bad access level**, **Other access denied**, **Duress alarm**, **Access granted** and **Card traced**.
- Under **Priority call type**, assign the call type option that best suits event reporting.



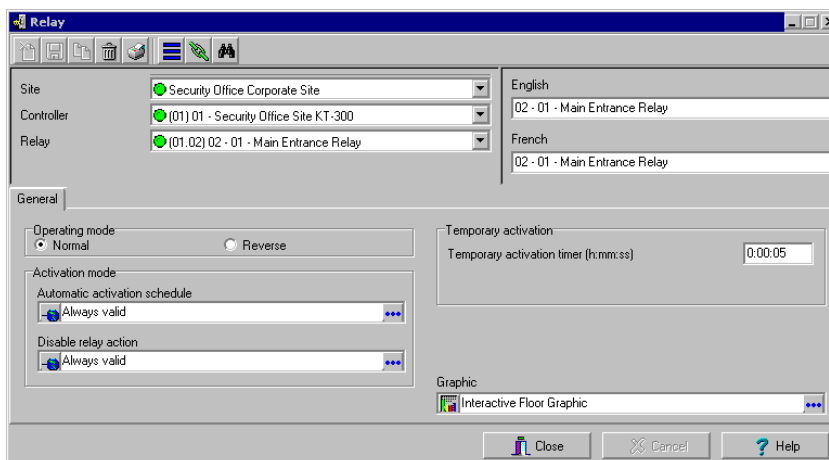
NOTE: *To access the **Priority call type** feature, the site connection type must be set to **Modem**.*

Relays Configuration

The output control relays provided on each KT-100, KT-200 and KT-300 can be used to activate alarms or other devices such as lighting control, ventilation, and air conditioning. These relays can be activated according to schedules, events reported by the system. They can also be activated to indicate the status of an alarm system or a combination of different logic conditions.

To Define Relays

- 1 From the **Devices** definition tab, select the **Relay** icon.



- 2 Select the **Site** and the **Controller** from the displayed drop-down lists, then select the relay for which you want to define settings.
- 3 Specify the **Operating mode** for the relay:
 - **Normal:** the relay is normally de-energized (deactivated) until it is energized (activated) by an operator, an event or any other system schedule.
 - **Reverse:** the relay is normally energized (activated or resting) until it is de-energized (deactivated) by an operator, an event or any other system function.
- 4 Specify the **Automatic activation schedule:** when this schedule is valid, the relay will be triggered (activated or deactivated) according to the specified activation mode.
- 5 Specify the **Disable relay action:** when this schedule is valid, the relay will be deactivated (or activated) according to the predefined operating mode.
- 6 Set the **Temporary activation timer** to indicate the delay during which the relay will be temporarily triggered following a temporary activation.



NOTE: When the timer is set to zero, the default activation delay is set to five seconds. Maximum time allowed: 255 seconds (4 minutes 15 seconds).

- 7 Select a graphic associated with the relay, if applicable.

Inputs Configuration

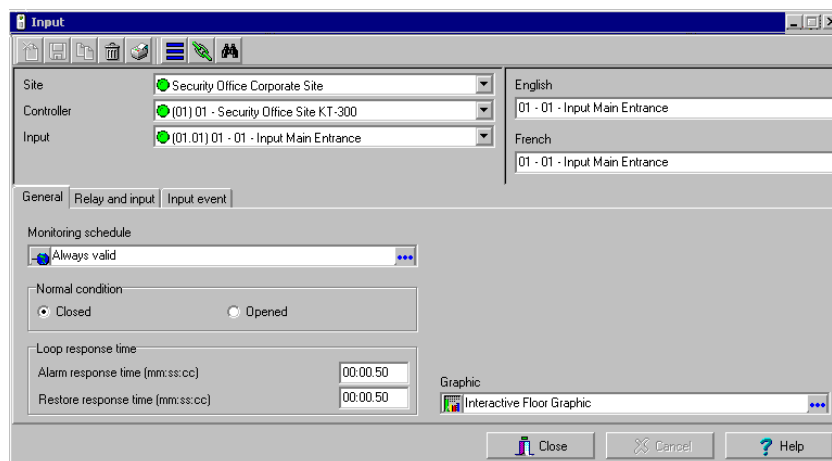
Door controllers can monitor the state of input points such as: door contacts, interlocks, alarm points, motion detectors, temperature sensors, any REX and other devices with dry contacts. KT-100 monitors the state of 4 input points, KT-200 monitors the state of 16 input points, and KT-300 monitors the state of 8 on-board input points, with a maximum capacity of 16.

- **For KT-200 only.** Inputs are normally closed or normally open dry contacts connected in series with one resistor. If the dry contact is connected in series with the green resistor, the input number will be odd. If the dry contact is connected in series with the red resistor, the input number will be even.
- **Input 1 (door contact) and 2 (request to exit device)** are ideally reserved for Door 1 of the controller whereas Input 9 (door contact) and 10 (request to exit device) are ideally reserved for Door 2 of the same controller. The input that is used for the door contact or REX contact SHOULD NOT have a “monitoring” schedule defined in the “Input Definition” menu.
- **For KT-100 Controllers.** Input 1 is reserved for door contact while input 2 is reserved for a request to exit device.
- **For KT-300 Controllers.** Input 1 should be reserved for contact on door 1 while input 2 should be used for request to exit device for door 1 of the controller. Input 3 should be reserved for contact on door 2 while input 4 should be used for request to exit device for door 2 of the controller.

To Define Inputs

You may define Input devices from the **Controller** definition menu or from the **Devices** definition window.

- 1 From the **Devices** definition tab, select the **Input** icon.



- 2 Select a specific gateway (from the **Gateway** drop-down list), a site (from the **Site** drop-down list), a controller (from the **Controller** drop-down list).
- 3 From the **Input** drop-down list, select the input you want to define.



- 4 Assign a **Monitoring schedule** to the selected input: this is the schedule during which the system will supervise the condition of the input. When the schedule is valid, a change in input condition generates either an “Input in alarm” or “Input restore” event.



NOTE: *The input that is used for the door contact, REX contact or interlock contact SHOULD NOT have a monitoring schedule.*

- 5 Specify the **Normal condition** for the input: it may be **Closed** or **Open**.
- 6 Specify the **Loop response time**. This delay is expressed in minutes (mm:ss:cc). The maximum time is 10:55:35 for both the alarm response and alarm restore times.
 - **Response time**—The delay before the system generates the input and alarm event.
 - **Restore site response**—The delay before the system generates the input restore events



NOTE: *Specifying the site response time reduces bouncing when the contact changes state, and helps to generate only one event for each transition if this time is longer than the bouncing time. For example, a 01:00:00 delay requires that a condition remains stable for at least one minute before it is reported.*

To Define Relays and Inputs

- 1 Select the **Relay and input** tab to define which relay(s) or input(s) will be activated or shunted when this input is enabled.



NOTE: *For the system to process properly the reset delay on a temporary shunt, the **Temporary Shunt Timer** option must be set in the definition of the input that will reset the delay. For example, if Input 1 will temporary shunt Input 2, the **Temporary Shunt Timer** must be specified also in the definition of Input 2.*

- 2 From the **Activate relay** list, select a relay or a relay group that will be triggered when this input is enabled.



NOTE: *Setting the timer to 0:00:00 will instruct the relay to follow the input's state.*

- 3 From the **Shunt input** list, select the input that will not be monitored when the input being defined is enabled.



NOTE: *When the input is restored or returns to normal condition, the shunted input will also return to normal condition. The event “Input shunted by input” will be generated by the system. When the input returns to normal condition, the event “Input unshunted by input” will be generated.*

- 4 In the **Temporary Shunt Timer (h:mm:ss)** field, specify the period during which an input is not monitored. Setting the timer to 0:00:00 will instruct the relay to follow the input state. The maximum value for the Shunt delay (h:mm:ss) is 9:06:07.

To Define an Input for an Elevator Door

When the input being defined or edited is used for elevator control, an **Elevator** tab is displayed in the Input definition window.



You may associate an input to a push button. It can then be used by a guard or by a receptionist to temporarily enable the floors defined in the Floor group activation section.

- 1 In the Input definition window, select the **Elevator** tab.

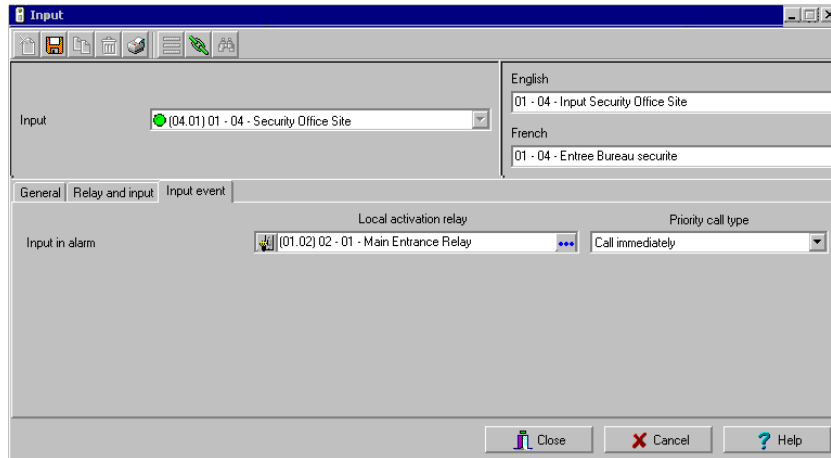


NOTE: Only the floors marked with an “X” in the **State** column in the Floor group menu will be available for selection. The system will temporarily enable floor selection according to the delay defined in the *Unlock time of the Doors* menu. A valid schedule has to be selected (*Enable schedule list*) for this feature to be activated. It may be necessary to define a door as an elevator cab to access this tab.

- 2 In the **Select cab for floor group activation** section, select the cab associated with the input.
- 3 Select the **Floor group** associated with the selected cab, that will be enabled when the input is triggered.
- 4 Select a schedule according to which the defined input will carry out this command.

To Enable Remote Event Reporting

- 1 Select the **Input** event tab.



- 2 From the **Local activation relay** list, select a relay or a relay group that will be triggered when this input is in alarm (activated).
- 3 Under **Priority call type**, assign the call type option that best suits the reporting of the event which triggered the input.



NOTE: To access the **Priority call type** feature, the site connection type must be set to **Modem**.

Output Devices Configuration

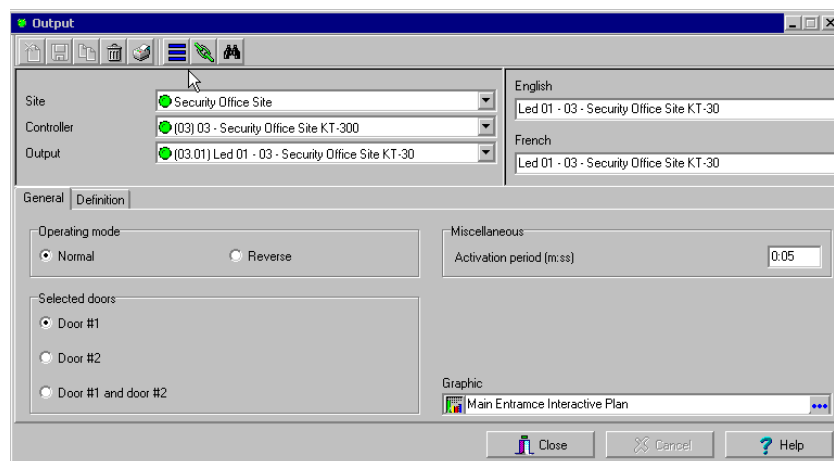
Outputs usually control the reader LED and buzzer. There are four outputs available per KT-200 and KT-300 controllers (2 per door). A KT-100 supervises the state of two outputs.

Electrical outputs are configured as open-collector. They provide an open circuit when deactivated (not connected to ground) and are switched to ground when activated.

You may configure Output devices from a controller definition menu or from a gateway window.

To Define General Options for an Output

- 1 From the **Devices** configuration window, select the **Output** icon.



- 2 Select the physical components related to the output: gateway, site, controller for the output.
- 3 From the **Output** drop-down list, select the output you are modifying.
- 4 Specify the **Operating mode** for the output device:
 - **Normal**—The output is switched to ground when it is activated.
 - **Inverse**—The output is an open circuit (not grounded) when it is activated.
- 5 In the **Selected doors** section, select which door will affect the output you are configuring:
 - **Door #1**—Only the first reader port will follow the state programmed for these events.
 - **Door #2**—Only the second reader port will follow the state programmed for these events.
 - **Door #1 and Door #2**—Both reader ports will follow the state programmed for these events.



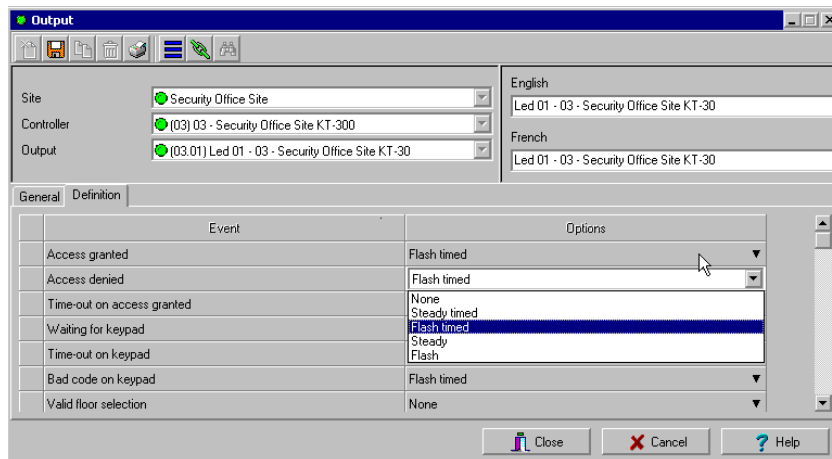
NOTE: This option is not available with KT-100.

- 6 Set the **Activation period (m:ss) delay**. It defines the activation time in seconds during which the output remains active when it is programmed for a temporary activation. An e will leave the output activated indefinitely, regardless of the activation type.

To Associate Events with Auxiliary Outputs

System events can trigger auxiliary outputs. You can define how each event will trigger the output.

- 1 Select the **Definition** tab to associate a door event with an auxiliary output.



- 2 In the **Options** column, associate an event with an output state.
 - **Steady timed**—The output given this option will not flash, it will remain activated for the specified activation period and will return to normal state when the activation period is over.
 - **Flash timed**—The output will flash and remain activated for the specified activation period and will return to its normal state when the activation period is over.
 - **Steady**—The output given this option will not flash, it will remain activated until it returns to normal condition.
 - **Flash**—The output will flash and remain activated until its condition returns to normal.

Chapter 5 • Definitions

Use the **Definition** toolbar to define the system logical components such as:

- Schedules
- Floors
- Graphics
- Holidays

Schedules Definition

A schedule indicates when the system will execute certain operations such as automatically unlocking doors, permitting access to employees, running automatic reports, monitoring inputs, etc. It also determines when events are to be acknowledged or when to activate relays controlling different functions (lighting, heat, etc.).

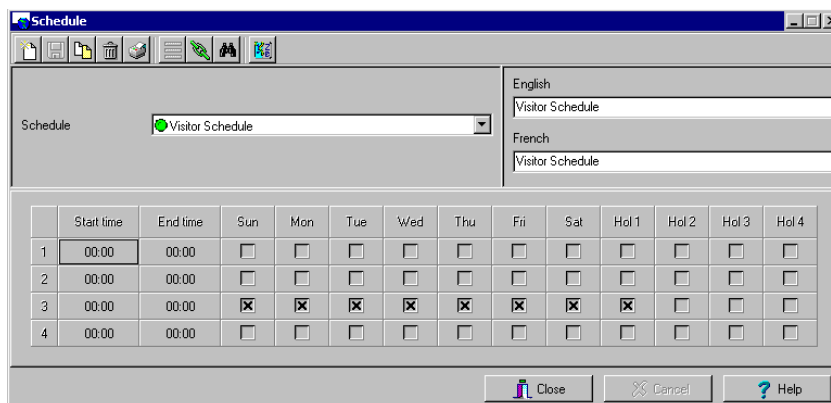
You can use the same schedule in different menus, but it is recommended to create a different schedule for each application, because it is much easier to modify a particular schedule without affecting other applications.

Each schedule is composed of four intervals. Each interval has a starting and ending time. Each of these intervals can be individually selected for the seven days of the week, and for holidays.

You can program up to 100 schedules in the system.

To Define a Schedule

- 1 From the EntraPass main window, click the **Definition** tab. Then click the **Schedules** icon from the **Definition** toolbar.



- 2 From the **Schedule** drop down list, select the schedule you want to modify or click the **New** icon to create a new one.
- 3 Assign a name (or modify an existing one) to the schedule. It is recommended to choose a meaningful name.
- 4 You can click the **Holiday** icon in the toolbar to view the list of holiday that are defined in the system.



NOTE: *EntraPass supports four types of holidays.*

- 5 Specify the **Start time**: this is the scheduled time when the interval becomes valid. It will become invalid when the end time has been reached.
- 6 Specify the **End time**: this is the scheduled time when the interval is no longer valid.



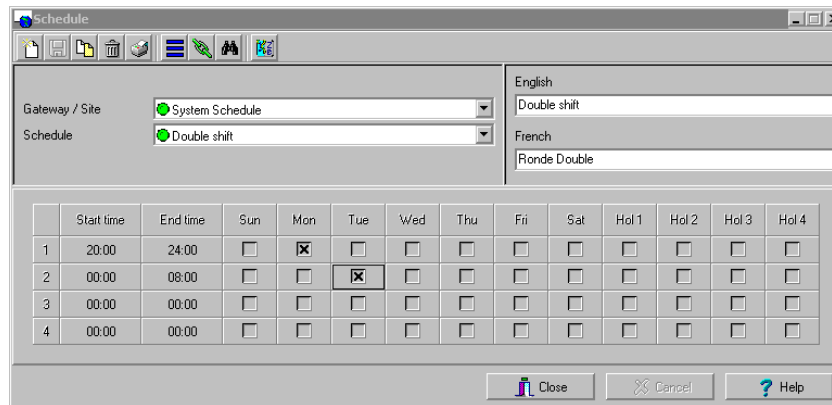
NOTE: *Start and end times are in 24-hour time format; this gives a range from 00:00 to 24:00. For any interval, the end time must be greater than the start time.*

- 7 Check the Days of the week during which this schedule interval will be valid. To do this, click in the check box below each day.
- 8 Check the holiday type (**Hol1**, **Hol2**, etc.) column checkbox if you have defined four holidays in the Holiday definition menu and you want this interval to be valid during a holiday.

Creating a 2-day Continuous Interval

To create an interval from Monday 20:00 (8:00 PM) to Tuesday 08:00 AM, the schedule must be divided into two intervals:

- 1 First define an interval for Monday from 20:00 to 24:00;



	Start time	End time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Hol 1	Hol 2	Hol 3	Hol 4
1	20:00	24:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	00:00	08:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	00:00	00:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	00:00	00:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

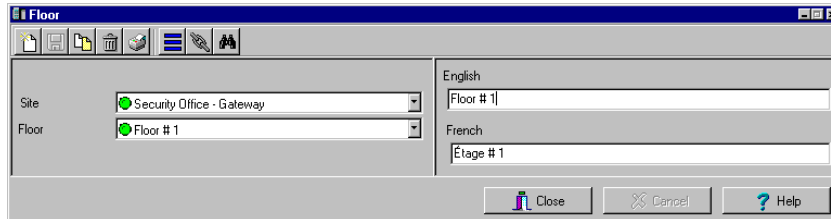
- 2 Define a second interval for Tuesday from 00:00 to 08:00. The system considers these two intervals as one continuous interval.



Floors Definition

The Floor dialog is used to create or edit elevator floors. Once the floors are created, they are grouped and associated with a schedule that will define when access is permitted.

- 1 In the **Definition** toolbar, click the **Floor** icon.



- 2 In the **Site** drop-down list, select the site for which you are defining floors. This allows you to minimize the list of components defined in the system.
- 3 Select a floor or click the **New** icon to create a new floor group.
- 4 Assign a meaningful name to the floor, then click the **Close** button. The system prompts you to save.

Graphics Definition

A graphic corresponds to the secured area of the system where components (Entrapass applications, controllers, inputs, relays, etc.) are located on a site.

With graphics, operators can easily view the exact location of a component installed on a site, or the status of components and devices such as doors, contacts, motion detectors, controllers, assigned to the graphic. Operators can perform manual operations directly from the displayed component (for example, locking/unlocking a door).

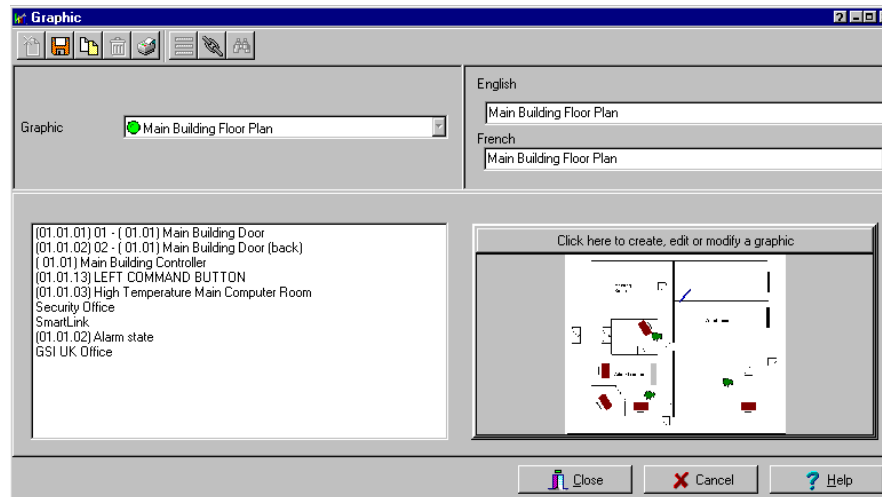
You can create as many graphics as you need. Each graphic can display up to 250 components. You may also import graphics or maps from other programs in the following formats (BMP, EMF, WMF, JPEG, GIF, PCX, PNG, TIF or PCD).



NOTE: Entrapass offers users four sample floor plans. You can customize them to suit your system needs. The sample floor plans are located at: C:\Program Files\Kantech\Server-SE\Generaldata\Demobmp folder.

To Define Components of a Graphic

- 1 In the Definition toolbar, click the **Graphics** icon.



- 2 From the **Graphic** drop-down list, select the graphic you want to modify, or click the **New** icon to create a new one.
- 3 Assign a name to the graphic (or modify the existing name).



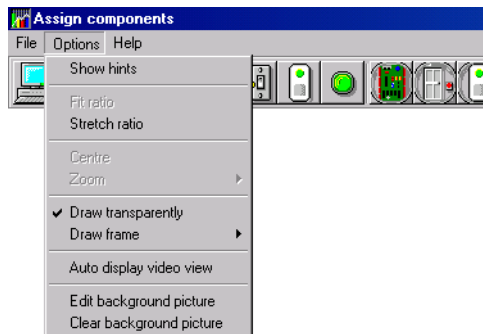
NOTE: When you select an existing graphic, or when you create a new one, all the components that are assigned in your graphic are displayed in the left-hand pane. The right-hand part of the window displays the graphic itself.



- 4 From the **Graphic Definition** window, [Click here to create, edit or modify a graphic](#) to bring up the **Assign Components** window.



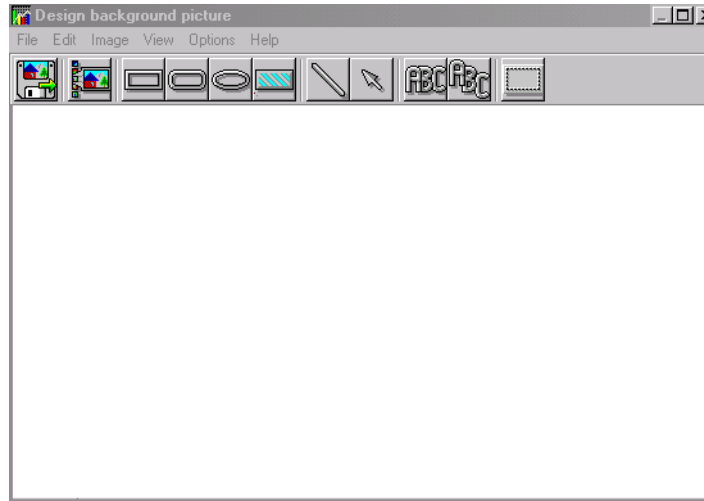
- 5 Click on the **Options** menu to display a pull down menu of drawing options. A check mark appears next to an option that is activated



- **Show hints** provides the component's name (component's address and name) when you point your mouse cursor over that graphic.
- **Draw transparently** will place a transparent icon on top of a background picture for a blended effect.
- **Draw frame** draws a frame around the component. **Frame color** indicates the current frame color and allows you to change the color.
- Select **Edit background picture** to edit the background of the selected graphic. From this window you can modify the graphic's frame and background color and add annotations.
- Select **Clear background picture** for the to clear the background picture of the graphic only leaving the assigned components. You can use this option when you want to insert a new graphic and leave the same components.

To Design the Background for the Graphic Window

- 1 Double-click anywhere in the background of the Assign components window to bring up the **Design background picture** dialog.



- 2 Use this window to import a graphic that was created with another application or create your own background using the drawing toolbar buttons.

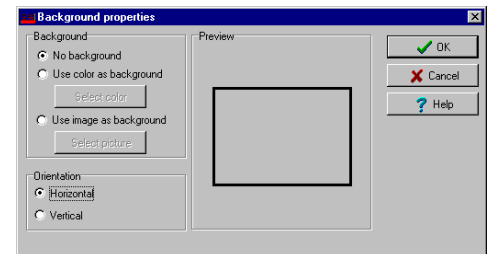


• To import an existing graphic, click the diskette icon, then drag and drop the diskette in the work area. Once you have positioned the component, and released the mouse button, the Image properties dialog will pop up on the screen. The system displays the **Open** window. Locate the graphic you want to import and click **Open**. The graphic will be placed in the graphic area of the dialog.



• To import a custom icon into the background graphic, click the **Custom images** button in the toolbar. The Select an image window pops up on the screen. Select an icon, then click **OK** to close the window and import the image in your design.

- To insert shapes and text in the background image, select a rectangle, a circle, an ellipse, etc. in the toolbar, and drag and drop it in your background.
- To modify a shape you've just placed in the burgeoned window, right-click it to open the Properties dialog. and make the appropriate modifications (color, position, etc.).
- You can setup the system to display the Properties dialog as you drop the shape into the design window. To do so, select the **Show properties on Drop** from the **Options** menu.



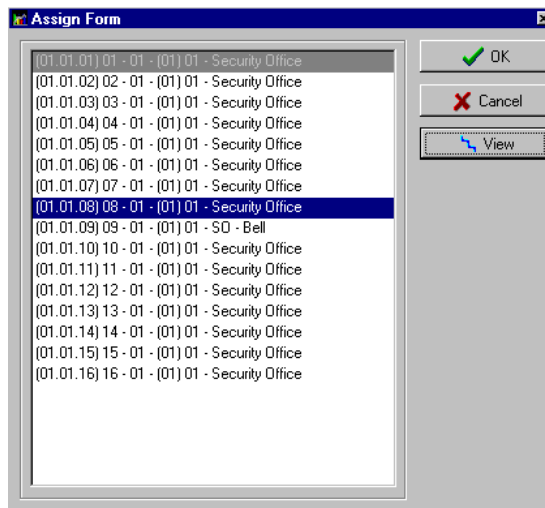
- To retrieve shapes that were previously saved to a disk, select the **Load annotations** option in the **Image** menu. When you add shapes to a graphic, you have the option of saving them as annotation on a separate file in order to retrieve them later.
- To save annotations on a separate file from your graphic, select the **Save annotations** option in the **Image** menu. You will be able to retrieve them for later use.
- To clear the shapes, select **Clear annotation** in the **Image** menu. If you save the graphic with the shapes, the shape become permanent.
- Use the **View** menu to define how the graphic will be displayed.



NOTE: Sizing handles (square handles that are displayed along the sides of the object that surrounds the selected object) indicate the object is selected.

To Assign System Components to Graphic Icons

- 1 From the **Assign Components** window toolbar, click and drag the selected component to the desired position. To drag an object across a window, select the object with your mouse and drag, while keeping the button pressed down, to the desired location in the graphic.



- 2 Once you have positioned the component, and released the mouse button, the Assign Form dialog will pop up on the screen
- 3 Select the system component you want to assign to the icon on the screen.
- 4 Click **OK** to go back to the previous window.



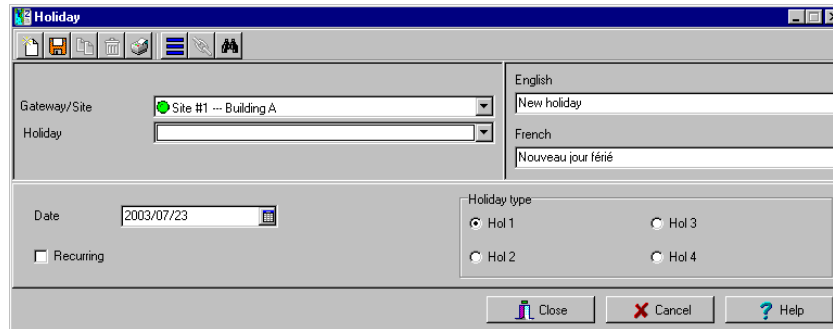
NOTE: If you do not assign the icon to a component, the icon will not be saved in the graphic. Only components that were not selected in the graphic will be available for selection.

Holidays Definition

A holiday is treated differently than other days. It is recommended to program holidays at the beginning of the year; this helps to modify floating holidays for the current year (Easter, Thanksgiving, etc.).

A holiday may be identified by a specific type (Hol 1, 2, 3, 4). The same day may be defined as a holiday at one site, but as a regular day in another site.

- 1 From the Definition window, select the **Holiday** icon. The Holiday window appears.



- 2 To create a new holiday, select the **New** icon.
- 3 To create a global holiday, proceed with the holiday definition. If you want to define a holiday for a specific gateway/site, select the gateway/site from the drop-down list.
- 4 Assign a name to the holiday.
- 5 From the **Date** pull-down menu, select a the holiday date from the calendar.
- 6 Check the **Recurring** option if this is the case for the holiday you are defining.



NOTE: If the holiday is not a recurring holiday, you will have to reprogram it for the following year. You can program holidays years in advance; but it is recommended to review holidays on a yearly basis.

- 7 In the Holiday type section, select the type of the holiday you are defining. This gives you flexibility when defining a holiday. For example, you may decide that a given day is a holiday for a certain group of users, but it is a regular day for another group.

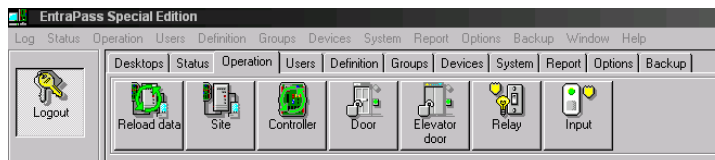


Chapter 6 • Operations

Under the **Operations** tab, operators will be able to perform manual operations on various system components (gateway, site, controller, etc.). Manual operations are used to override schedules or process special requests, when necessary. When you launch a manual operation on a component, it is possible to view the status of the selected components in real-time. You can also edit components by accessing the component directly from the operation window.

The Operations Toolbar

The Operations toolbar, located at the top of the Workstation window will allow you to access all operation dialogs (gateway, site, controller, etc.), where you will be able to perform manual operations such as manually resetting or monitoring devices, disabling readers, etc.



The Operation Dialogs Toolbar

All operation windows have a series of icons in the toolbar. Series of icons will only appear in specific operation windows. The five buttons described below appear in all operation windows.

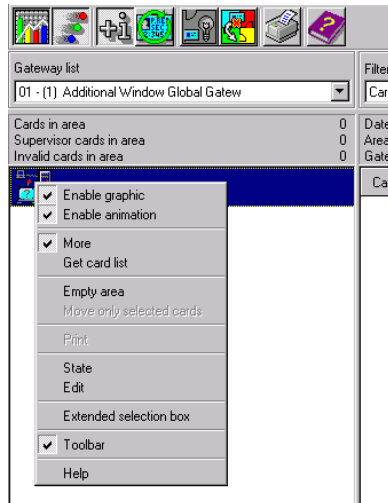
Icon	Description
	Select All is used to select all the items or components displayed in the list.
	Unselect All is used to unselect all the items or components that were previously selected in the list.
	Enable Graphic displays the image related to the selected component (i.e.: door) and will also display the associated components (i.e.: reader). To display in real-time, this button must be used with the Enable animation button.
	Enable Animation will automatically enable the Enable graphic button. This will activate the current component (i.e.: door) and will display its status in real-time.
	Help will open the On line help corresponding to the window you are currently navigating.



NOTE: A hint is displayed when you move your cursor over a button. It gives details about the operation to be performed.

The Operations Contextual Menu

You will be able to access a contextual menu by right clicking within the list in any operation window.



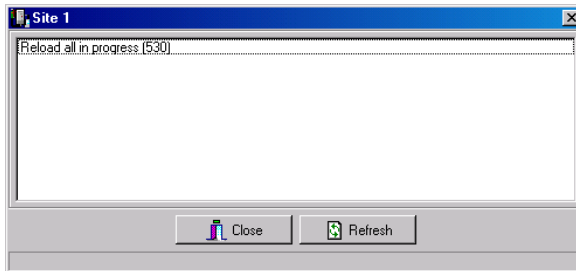
The items in the popup menu correspond to the icons in the operation window toolbar. Three options have been added to the popup menu, when you access it from the Gateway, the Site, the Guard Tour State or the area operation window.

- **State:** Opens a status window that contains the current information corresponding to the component you selected in the list. For more details, see *"The Component Status Window"* on page 110.
- **Edit:** Opens the window corresponding to the selected component to allow editing.
- **Extended selection box:** Opens the Extended selection box dialog that allows you to search for a specific component.



The Component Status Window

A message window that contains the site messages can be accessed by right-clicking within the corresponding operations window under the **Operation** tab, and selecting **Status** in the contextual menu.



In the example above, the information is listed for a Site status in Special Edition. We have listed some of the information that can appear in that window.

Parameter	Description
Number of sites	Indicates the number of sites for this gateway.
Number of cards	Indicates the number of cards processed by this controller
Number of processes	Indicates the number of processes
Version	Indicates the software and hardware version number.
Local Time	Indicates the controller's current local time.
Last startup	Date the last system startup was performed.




NOTE: The information displayed in the status window corresponds to your configuration and will be different whether you access it from a gateway, a site, a guard tour or an area operations window.

Manual Data Reload

The **Reload data** command allows operators to refresh system parameters with new data from the system database. After a reload operation, the database reorganizes the data received and communicates the new data to all the sites and controllers. Communication with controllers will be suspended during a reload operation.

When to reload the data?

- After major changes in the system database such as new cards, new devices, modification of component definition, definition of new schedules;
- When one or more controller(s) is malfunctioning (when it does not receive data for instance).

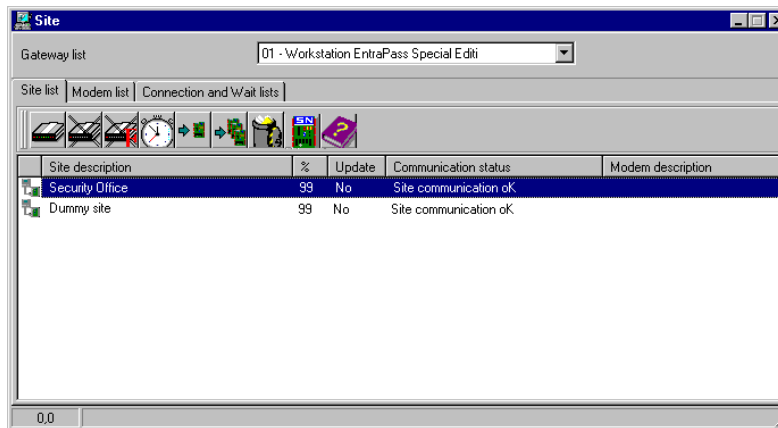
Button	Definition
	Reload data: to refresh system parameter with new data from the system database.

Manual Operations on Sites

The manual operations on site feature is used to poll unassigned controllers. For example, when a controller has been added in the system without a serial number, you can use this command to get the controller serial number.

To Perform Manual Operations on a Site

- 1 From the **Operation** window, click on the **Site** icon to open the Site window, then select the gateway to which the site is connected.










- 2 To poll a controller that is not assigned, click the **Controller** icon. A message is sent to an unassigned controller, asking it to identify itself. When the controller receives the call from the site, it sends an acknowledgement message in the Message desktop.
- 3 You may select the Message desktop to view the controller serial number.



NOTE: The % column shows the communication performance of a selected site. If the percentage is too low (below 75% for instance), it may indicate that the site is not communicating efficiently. Communication problems may stem from various reasons such as interferences, damaged cables, etc.

Communication Options Available from the Toolbar

Icons	Description
	Connect to remote site: Click to connect to a remote site using a pre-configured dial-up connection.
	Disconnect remote site: Click to close the connection between this EntraPass workstation and the remote site.
	Force disconnect site: Force disconnect remote site immediately, even when the system is reloading.
	Disable remaining time: Click to stay connected until clicked again. This action disables preset connection remaining time. This action bypasses any idle time.
	Update remote site: After selecting site, click to connect and update parameters.
	Update all remote sites: Click to connect and update parameters on all sites starting with the first site on the list.
	Remove site from connect and wait list: Select a site then click to suspend connection after all sites had been set for update.








NOTE: A hint is displayed when you move your cursor over a button. It gives details about the operation to be performed.



Manual Operations on Controllers

This dialog is used to reset or reload a controller: soft reset, hard reset, reload and reload controller firmware.

Button	Definition
	Soft reset: will not affect the controller database. This command sends new information to a controller to update its physical components (relays, inputs, doors and outputs)
	Hard reset: will erase the existing controller database and reload it with new information in the controller database Reset commands should be executed with caution. Before you carry out a controller reset operation, we recommend you contact our Technical Support. For more information, see "Technical Support" on page 4.
	Reload: will reload the controller database; if for example a controller database is not reloaded correctly due to an erratic operation
	Forgive: will reset to zero the cards-in and cards-out counters
	Cards-in: displays the number of cards in per controllers

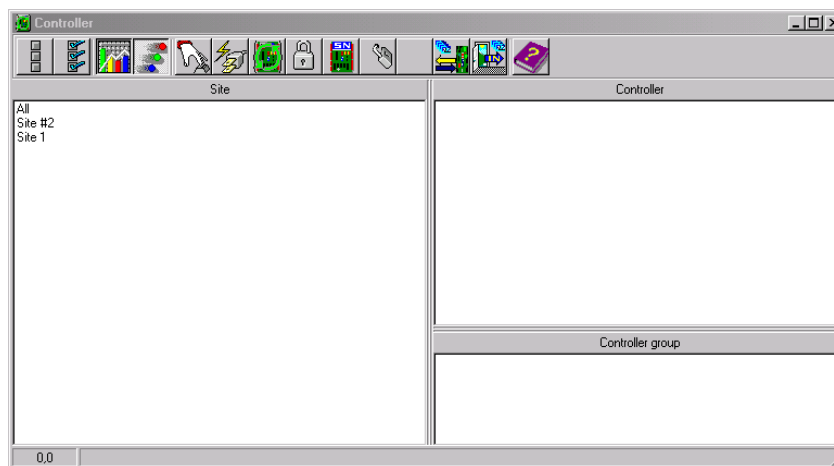


NOTE: A hint is displayed when you move your cursor over a button. It gives details about the operation to be performed.



To Select a Controller

- 1 From the Operations window, select the **Controller** icon to open the Controller window where you will be able to reset the controller.



- 2 From the Site pane, select a site. Controllers attached to this site appear in the right-hand pane.
- 3 From the **Controller** list, select the controller where the operations will take place. It has to be highlighted. To perform the operation on a group of controllers, select **Controller Group** (lower right-hand pane).



NOTE: If only one Site is defined in the system, the Site Controller list pane will not appear on the Controller window.

To Perform a Controller Soft Reset

A soft reset will refresh the data in the controller.

- 1 In the Controller dialog, select desired controller or controller group.
- 2 Click the **Soft reset** icon in the toolbar. This command will send new information to the controller to update its physical components (relays, inputs, doors and outputs, etc.)

To Perform a Controller Hard Reset

A hard reset will delete the existing controller database and reload it with new information in the controller database.



NOTE: Reset commands should be executed with caution. Before you carry out a controller reset operation, we recommend you contact our Technical Support. For more information, see "Technical Support" on page 4.



- 1 In the Controller dialog, select desired controller or controller group.
- 2 Click the **Hard reset** icon in the toolbar. This command will send new information to the controller to update its physical components (relays, inputs, doors and outputs, etc.)

To Manually Reload a Controller

Entrapass allows you to reload a controller database when, for example, a controller database is not reloaded correctly due to an erratic operation.

- 1 In the Controller dialog, select desired controller or controller group.
- 2 Click the **Reload** icon in the toolbar. The controller's database will be reloaded.

To Calculate the Number of Cards In

If you have one or more controllers configured with anti-passback, this function allows you to view a list of cards that are considered inside (**Cards in**) an area. To do so, the passback option (either soft or hard synchronization) has to be enabled on the reader and the door has to be defined as an entry door.

- 1 In the Controller dialog, select desired controller or controller group.
- 2 Click the **Cards in** icon in the toolbar. The system will display the number of cards in for the selected controller or controller group.

***NOTE:** This operation is performed only on one controller at a time as it may be a lengthy operation. The option is only available on a Corporate Gateway.*







To Reset the Cards In Counters

This option allows to reset to zero for the cards in counter.

- 1 In the Controller dialog, select desired controller or controller group.
- 2 Click the **Forgive** icon in the toolbar. Card holders will not be considered inside or outside until the next use of their card at an entry or exit reader.

Manual Operations on Doors

This dialog allows an authorized operator to manually modify the state of a door or group of doors. Operators can manually lock/unlock a door, temporary lock/unlock a door or group of doors, and enable/disable readers on selected doors.

Button	Definition
	Lock door or group of doors: will manually lock the selected door or group of doors.
	Unlock door or group of doors: The selected door or group of doors will be manually unlocked and will remain unlock until the next valid change of the unlocking schedule or an operator manually locks the door or group of doors
	Temporarily lock/unlock door or group of doors: Temporarily unlocks a door or group of doors for a preset delay. Once the delay expires, the door or group of doors re-lock automatically.
	Return to schedule: Will re-apply a schedule after a manual operation was performed on a component.
	Enable card reader: will enable a previously disabled door reader.
	Disable card reader: will disable a door reader and user will not be able to access that door, even if they have access rights.



NOTE: A hint is displayed when you move your cursor over a button. It gives details about the operation to be performed.

There are various reasons why you would want to perform one of these operations; for example you may need to “disable a reader” for a short period in order to deny access to the door, etc.

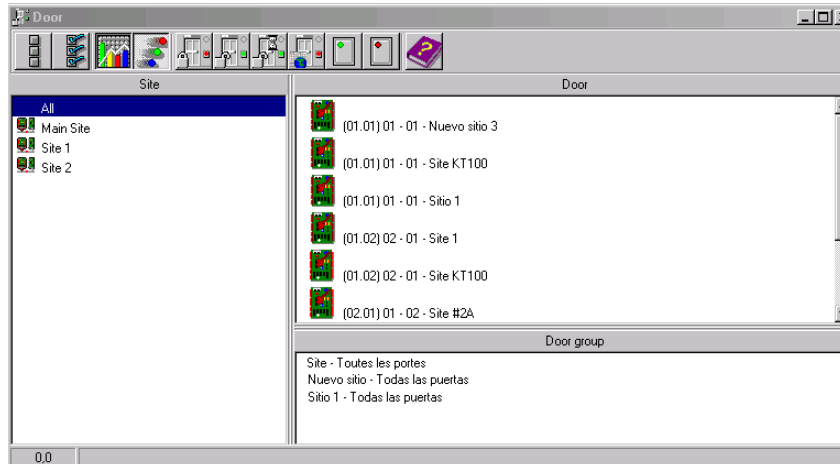
This operation allows an operator to lock a door that was previously unlocked by an operator or a schedule. When a door is manually locked through the Operation menu, it remains locked until:

- The presentation of a valid card (will re-lock after access), or
- The next valid change of the automatic unlocking schedule (for a door defined with an unlocking schedule), or
- An operator manually unlocks the door.



To Select a Door or a Door Group

- 1 From the Operations window, select the **Door** icon. The Door window appears.



- 2 Click the **Enable animation** icon to view a real-time display of the door status.
 - The left-hand pane displays the list of all **Site**. You may select all or select one site.
 - The individual doors associated with the site selected on the left are displayed in the top right side of the pane. If you select **All** on the left, all doors in the system will be listed on the right. You can select one, several or all doors.



NOTE: *If only one site is defined in the system, the site or gateway list window will not appear on the Controller window.*

- **Door groups** associated to the site selected on the left are displayed at the bottom right side of the pane. If you select **All** on the left, all door groups in the system will be listed at the bottom right. You can select one or several or all groups.

To Lock a Door Manually

- 1 In the Door dialog, select desired door(s) or door group.
- 2 Click the **Lock-door** icon in the toolbar.

To Unlock a Door Manually

- 1 In the Door dialog, select desired door(s) or door group.
- 2 Click the **Unlock-door** icon in the tool bar. The selected door(s) will be manually unlocked. The system will prompt for operator confirmation. A door defined with an automatic unlocking schedule will remain unlocked until:
 - The next valid change of the unlocking schedule, or
 - An operator manually locks the door.

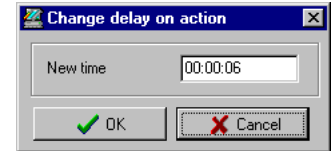
To Unlock a Door Temporarily

Entrapass allows you to temporarily unlock a door for a preset delay. Once the delay expires, the door re-locks automatically. You can use this option in cases where you need to grant access to a user who does not have a card or has forgotten his/her card.



NOTE: *The maximum unlock time: 4:15 (255 seconds).*

- 1 Click the **Temporarily unlock** icon. The Change delay on action dialog will popup.
- 2 Enter the **New time** delay (m:ss) and click **OK**. The selected door will be temporarily unlocked by an operator.



NOTE: *If a door contact is installed, the door will re-lock as soon the system sees a "door open-door closed" transition. There is no "Animation" for this type of operation.*

To Reset a Door Schedule

Entrapass allows you to reset a door schedule after a manual operation has been performed on a component.

- 1 In the Door dialog, select desired door(s) or door group.
- 2 Click the **Return to Schedule** button. This option will reset the schedule for the selected components.

To Enable a Door Reader

- 1 In the Door dialog, select desired door(s) or door group.
- 2 Click the **Reader-enable** button. This option enables a previously disabled door reader.

To Disable a Door Reader









- 1 In the Door dialog, select desired door(s) or door group.
- 2 Click the **Reader-disabled** button. This option disables a previously enabled reader. Disabling a reader prohibits users from accessing the door, even if access rights have been granted.

Manual Operation on Elevator Doors

This dialog allows an authorized operator to manually lock, unlock or temporarily unlock elevator floors. The window will also display, in real-time, the status of the selected elevator door(s).

How Elevator Access Is authorized

- The cardholder pushes an “up/down” button, the elevator door opens,
- The cardholder presents its card at the reader (usually inside the cab),
- The system checks if the schedule assigned to this door is valid. If yes, the system checks which floor group is associated to this door,
- Then the system verifies each floor of the floor group (in the floor group menu) and checks if the schedule associated to each floor of the group is valid or not valid.
- Only floors that have a valid schedule will be available for selection by the user (the elevator panel will enable the buttons corresponding to the floors).

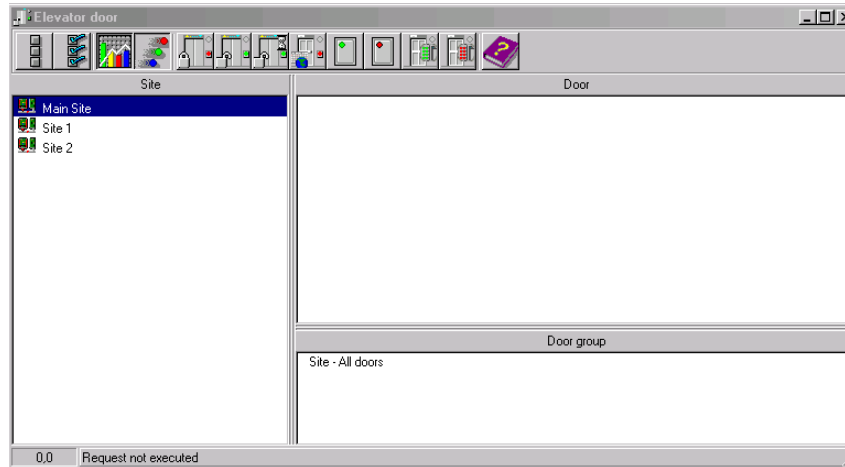
Button	Definition
	Lock elevator floor or group of elevator floors: will manually lock the selected elevator floor or group of elevator floors.
	Unlock elevator floor or group of elevator floors: The selected elevator floor or group of elevator floors will be manually unlocked and will remain unlock until the next valid change of the unlocking schedule or an operator manually locks the elevator floor or group of elevator floors.
	Temporarily lock/unlock elevator floor or group of elevator floors: Temporarily unlocks an elevator floor or group of elevator floors for a preset delay. Once the delay expires, the elevator floor or group of elevator floors re-lock automatically.
	Return to schedule: Will re-apply a schedule after a manual operation was performed on a component.
	Enable card reader: will enable a previously disabled reader.
	Disable card reader: will disable a reader and users will not be able to access any elevator floor, even if they have access rights.
	Enable elevator floor: will enable a previously disabled elevator floor or floor group.
	Disable elevator floor: will disable an elevator floor or floor group and users will not be able to access that elevator floor or floor group, even if they have access rights.



NOTE: A hint is displayed when you move your cursor over a button. It gives details about the operation to be performed.

To Select an Elevator Door

- 1 From the **Operations** menu, select the **Elevator door** icon.



- 2 Click the **Enable animation** icon to view a real-time display of the elevator door status.
 - The left-hand pane displays the list of all **Site**. You may select all or select one site.
 - The individual elevator doors associated with the site selected on the left are displayed in the top right side of the pane. If you select **All** on the left, all elevator doors in the system will be listed on the right. You can select one, several or all elevator doors.
 - **Elevator door groups** associated to the site selected on the left are displayed at the bottom right of the pane. If you select **All** on the left, all elevator door groups in the system will be listed at the bottom right. You can select one or several or all elevator door groups.

To Lock Floors from Elevator Doors

- 1 Select an elevator door or a group of elevator doors.
- 2 Click the **Lock** icon in the toolbar. This command will manually lock the floor group that was previously unlocked by an operator or a schedule.



NOTE: A door defined without an unlocking schedule will only be locked by a manual command. To lock all floors that were previously unlocked, use the **Unlock** option in the **Manual operation on doors** menu.

To Unlock Floors from Elevator Doors

- 1 Select an elevator door or a group of elevator doors.
- 2 Click the **Unlock elevator floors** icon in the toolbar to unlock a previously locked floor. This command will only enable the elevator floors that are defined with an “X” in the “State” column of the Floor group Definition menu. If you do this, the system will prompt the you to select a

floor group that should be unlocked (available). Once the group is selected, the system will prompt the operator to confirm the operation.



NOTE: For a door defined with an “automatic unlocking schedule”, floors will remain available until:

- The next valid change of the unlocking schedule, or
- An operator manually locks the door.



NOTE: A door defined without an unlocking schedule will only be locked by a manual command. To lock all floors that were previously unlocked, use the **Unlock** option in the **Manual operation on doors** menu.

NOTE: When a manual unlocking operation is completed, only floors that are defined with an “X” in the “state” field of the **Floor Group Definition** menu will be available for selection. Also, when communication is lost and the controllers are working in stand-alone mode, only the floors marked with an “X” will be available for selection and the access schedule will be ignored.

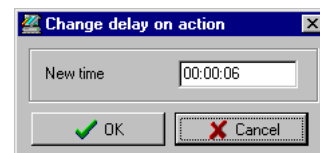
To Temporarily Unlock Floors from Elevator Doors

EntraPass allows you to temporarily unlock a floor from an elevator door for a preset delay. Once the delay expires, the elevator door re-locks automatically.



NOTE: The maximum unlock time: 4:15 (255 seconds).

- 1 Click the **Temporarily unlock** icon. The **Change delay on action** dialog will popup.
- 2 Enter the **New time** delay (m:ss) and click **OK**. The selected elevator floor will be temporarily unlocked by an operator.



NOTE: This command will only temporarily enable the elevator floors that are defined with an “X” in the “State” column of the “Floor group Definition menu” (available for selection).

NOTE: There is no “Animation” for this type of operation. To temporarily unlock all floors, use the “temporarily unlock door” option in the “manual operation on doors” menu.

To Reset an Elevator Door Schedule

EntraPass allows you to reset an elevator door schedule after a manual operation has been performed on a component.

- 1 In the **Elevator door** dialog, select desired elevator door(s) or door group.
- 2 Click the **Return to Schedule** button. This option will reset the schedule for the selected components.

To Enable an Elevator Floor

- 1 In the **Elevator floor** dialog, select desired floor(s) or floor group.
- 2 Click the **Enable elevator floor** button. This option enables previously disabled elevator floors or floor group.





To Disable an Elevator Floor

- 1 In the Elevator door dialog, select desired floor(s) or floor group.
- 2 Click the **Disabled elevator floor** button. This option disables a previously enabled elevator floor. Disabling a floor prohibits users from accessing the floor, even if access rights have been granted.

Manual Operations on Relays

Use this menu to manually change the state of a relay or group of relays. You can activate/deactivate and temporarily activate relays or group of relays manually. The window will also display, in real-time, the status of the selected relay(s).

This feature allows to manually turn off a relay; for example, when an input programmed to activate a relay goes in alarm in unknown conditions.

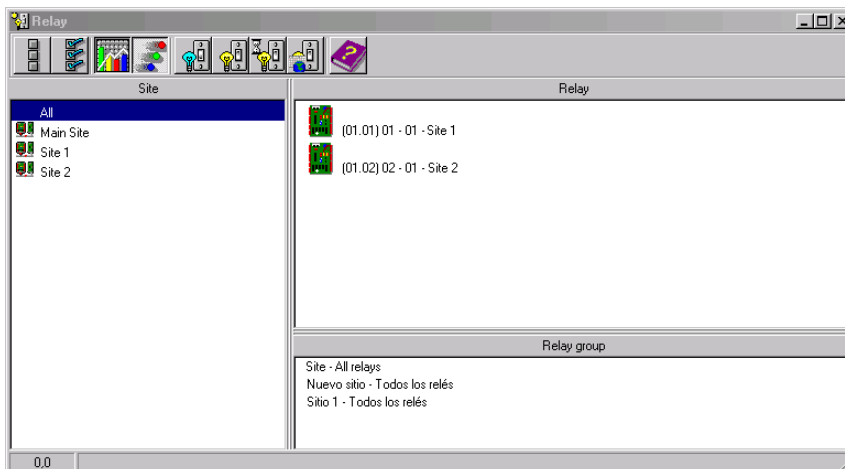
Button	Definition
	Deactivate relay: allows an operator to deactivate a relay which was previously activated by an operator, event, schedule or input in alarm.
	Activate relay: activate a relay which was previously deactivated by an operator, event, schedule or input in alarm.
	Temporarily activated relay: Temporarily activate a relay or group of relays for a preset delay.
	Return to schedule: Will re-apply a schedule after a manual operation was performed on a component.



NOTE: A hint is displayed when you move your cursor over a button. It gives details about the operation to be performed.

To Select Relays

- 1 From the Operation window, select the **Relay** icon.



- 2 Click the **Enable animation** icon to view a real-time display of the relay status.



- The left-hand pane displays the list of all **Site**. You may select All or select one site/gateway.
- The individual relays associated with the site selected on the left are displayed in the top right side of the pane. If you select **All** on the left, all relays in the system will be listed on the right. You can select one, several or all relays.
- **Relay groups** associated to the site selected on the left are displayed at the bottom right side of the pane. If you select **All** on the left, all relay groups in the system will be listed at the bottom right. You can select one or several or all groups.

To Manually Deactivate a Relay

- 1 Select a relay or a group of relays.
- 2 Click the **Deactivate Relay** icon.



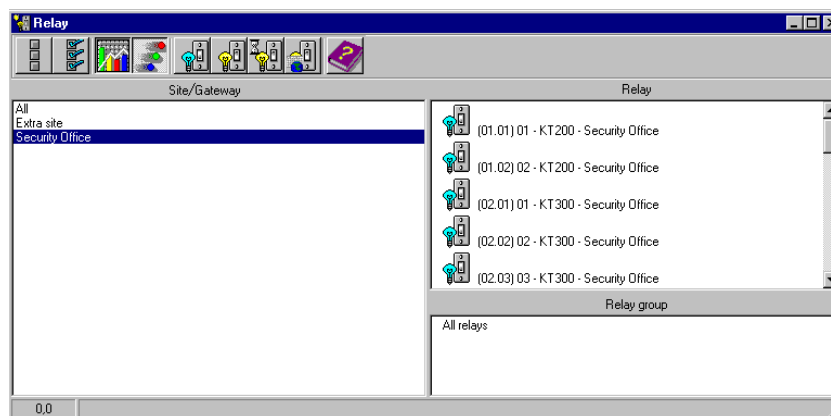
NOTE: If you manually deactivate a relay that is usually activated according to a schedule, it will remain deactivated until its reactivation schedule becomes valid. This means that if a relay needs to be activated according to a schedule and you deactivate it, remember to reactivate it again for the remaining scheduled time, because one relay can be defined for various components of the system; its activation or deactivation will relate to its configuration within these components.

To Manually Activate a Relay

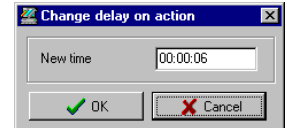
- 1 Select a relay or a group of relays.
- 2 Click the **Activate Relay** icon. The selected relay(s) will be activated. This operation allows an operator to activate a relay which was previously deactivated by an operator, event, schedule or input in alarm.

To Activate a Relay Temporarily

- 1 From the Operation window, select the **Relay** icon.



- 2 In the left-hand pane, you may select a site or gateway, or you may select **All Relays** to display all the relays.
- 3 In the right-hand pane, you may select a relay in the upper part of the window, **All Relays** in the lower part of the window.
- 4 Click the **Activate relay temporarily** icon. The Change delay on action window will popup on screen.
- 5 Enter the **New time** delay (m:ss) and click **OK**. The selected relay will be temporarily activated by an operator.



NOTE: The selected relay(s) will be temporarily activated. This is useful for an operator who would like to activate temporarily a relay which was previously deactivated by an operator, event, schedule or input in alarm. The system displays a message box requesting that a temporary activation delay, is entered. When this delay is over, the relay will be deactivated automatically.




To Reset a Relay Schedule

EntraPass allows you to reset a relay schedule after a manual operation has been performed on a component.

- 1 In the Relay door dialog, select desired relay(s) or relay group.
- 2 Click the **Return to Schedule** button. This option will reset the schedule for the selected components.

Manual Operations on Inputs

This dialog allows you to bring an input back to its normal state, or to stop monitoring an input, or monitor a specific input at all times, or to perform a temporary shunt on a selected input, if it had been previously modified from its original state as setup in the Device menu.

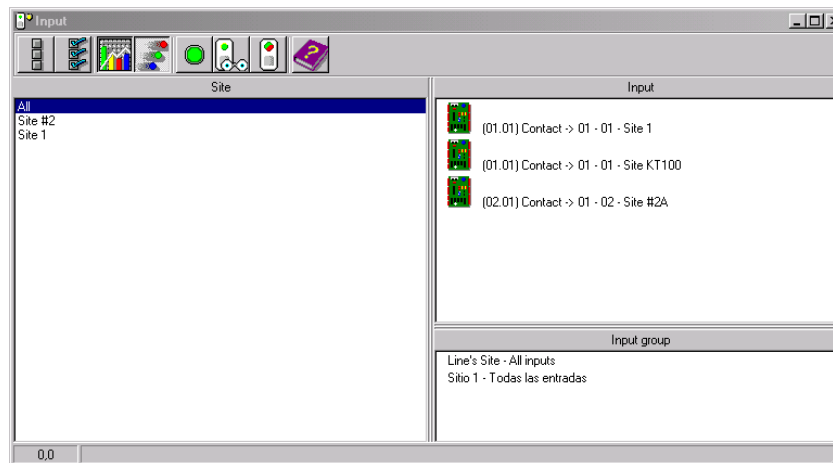
Button	Definition
	Input normal: returns an input to its normal state as setup in the Device menu.
	Input continuous supervision: will monitor the selected input at all times.
	Input with no supervision will terminate the input monitoring, regardless of its schedule, and will start monitoring with the next pre-defined schedule.



NOTE: A hint is displayed when you move your cursor over a button. It gives details about the operation to be performed.

To Perform Manual Operations on Inputs

- 1 From the Operation window, select the **Input** icon.



- 2 Click the **Enable animation** icon to view a real-time display of the relay status.
 - The left-hand pane displays the list of all **Site**. You may select **All** or select one site.
 - The individual input associated with the site selected on the left are displayed in the top right side of the pane. If you select All on the left, all inputs in the system will be listed on the right. You can select one, several or all inputs.

- **Input groups** associated to the site selected on the left are displayed at the bottom right side of the pane. If you select **All** on the left, all input groups in the system will be listed at the bottom right. You can select one or several or all input groups.

To Manually Return an Input to its Normal State

This option is used in cases where an input status has been modified by an operator and you want to return the input to its normal state. For example, if an input is assigned a monitoring schedule in its definition and an operator has reversed the state of the input making it “not supervised”, it can be returned to its normal state using this button.

- 1 Select an input or a group of inputs.
- 2 Click the **Input normal icon**. The selected input returns to its normal state as defined in the **Device** menu.

To Stop Monitoring an Input

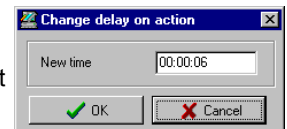
You will use this option to terminate the input supervision, regardless of its schedule (if defined).

- 1 Select an input or a group of inputs.
- 2 Click the **Input no supervision**. The selected input will not be monitored.

To Temporarily Stop Input Supervision (Shunt)

You will use this option when you want the system to bypass a specific input, for a specific period of time.

- 1 To temporarily shunt an input, select the input, then click the **Temporarily shunt** icon. The input will not be monitored temporarily.
- 2 Click the **Input no supervision temporarily**. The Change delay on action dialog will popup.
- 3 Enter the **New time** delay (m:ss) and click **OK**. An icon next to the input will indicate that it is temporarily shunt. If an alarm occurs, or if the input is disconnected, no message will be sent to the desktop Message list.



Chapter 7 • Users

The **Users** menu allows you to easily manage the EntraPass cardholder database.

The **Users** toolbar icons start the following tasks:

- Define and issue cards as well as to perform card-related tasks (find, modify or delete existing cards),
- Design and print badges,
- Define and manage card access groups,
- Define access levels,
- Import or export CSV files.

The Integrated Badging feature was added to EntraPass to allow users to design and print badges. Pictures and signatures can be imported or, with the necessary devices, captured and incorporated into cards for printing badges.

Cards Definition

Cards are defined by the following properties: card number, cardholder name, access level and status (valid, invalid, pending, lost/stolen). Cards records can be searched, sorted and deleted.

The Users menu is used to:

- Create and issue new cards
- Modify or delete existing cards
- Define multiple cards (by creating a group of cards)
- Assign access levels and pictures, etc.

To Issue a New Card

- 1 From the Users menu, select the **Card** icon. The displayed Card window is used to enter/verify general information on the cardholder.

- 2 Click the **New** icon (first icon) in the toolbar. The Card number field is enabled.
- 3 Enter the number printed on the card (**Card number** field), then press **Enter**. If it is a new card, the **Card user name** field is initialized with “New user”. If the card already exists, the system displays information about the card.
- 4 Enter the cardholder’s name in the **Card user name** field. You can enter up to 50 characters.

NOTE: The system automatically displays the Creation date, the Modification date and the Modification count information.

- 5 Fill out the **Information #1 to #10** fields. These are user definable fields. They are used to store additional information regarding the cardholder. For example, you could use Information #1 to store the employee number; Information #2, department; Information #3, the address, etc. Later, card information fields are used to index reports, customize the cardholder lists, etc.



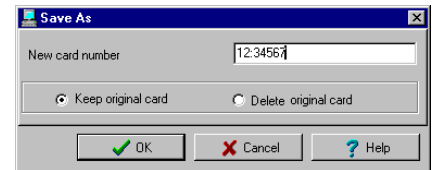
NOTE: These information fields are editable labels. To rename an information field label, double-click it, then enter the appropriate name in the displayed fields. You can enter up to 50 characters.

- 6 Click the **Save** icon.

To Create New Cards Using the “Save as” Feature

The **Save as** feature allows you to create a new card based on an existing card, only making changes to specific information. For example: changing only the user name and keeping all other card information.

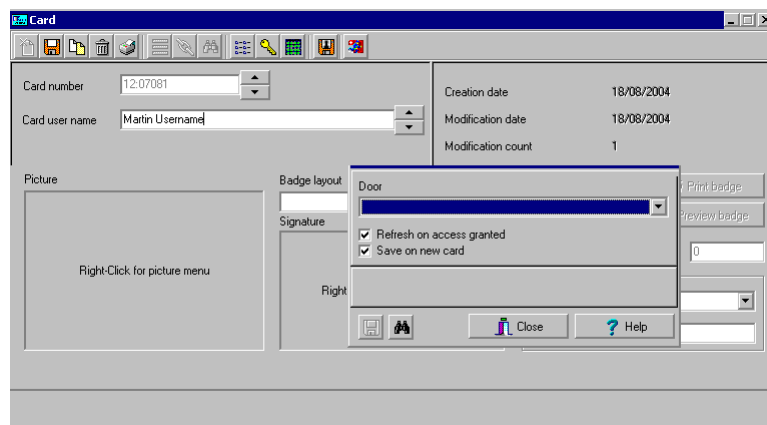
- 1 Type required changes into specific fields in the Card window and click the **Save as** icon. This feature allows you to create a new card under a new card number.
- 2 Enter the new card number in the **New card number** field.
- 3 Select the **Keep/Delete original card** options to specify if the original card should be kept or deleted (usually kept), then click **OK** to save the new information. The Card window is displayed.



To Issue Cards Using the Batch Load Feature

The Batch Load feature allows operators to issue cards by presenting cards to a door reader. The card number is displayed on an “unknown card” or “access denied” event messages. During a Batch Load operation, the operator can create new cards or modify existing ones.

- 1 From the Card window, click the **Batch Load** button.



- 2 From the **Door** drop-down list, select the Door that will be used to read the cards.
- 3 Check the following options:
 - **Refresh an access granted:** if this option is checked, each time an access is granted the information displayed will be refreshed with data relative to the card.

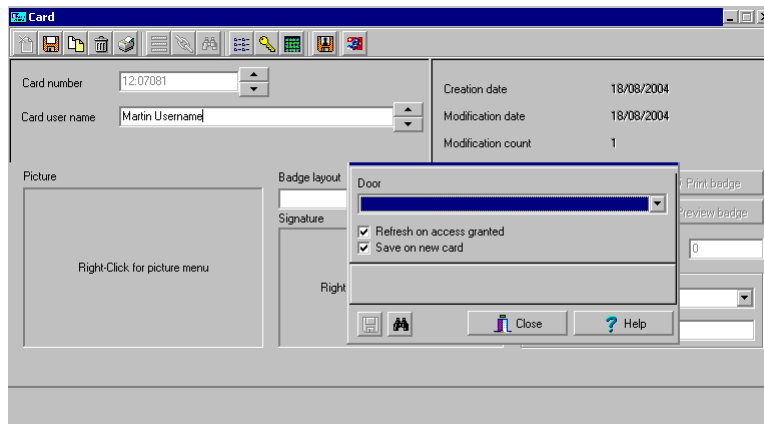
- **Save on new card:** if this option is checked, new cards will be saved in the card database on an “unknown card” event message. If this box is not checked, the operator will have to save the card manually each time a card is read.



NOTE: The **Find** button allows operators to search for an existing card in order to create a new card based on the existing card data.

NOTE: If an operator clicks the **Close** button without saving (when the **Save** button is still enabled), a system prompt will ask to save the last information.

- 4 Right click the **Door** drop-down list to expand your search.

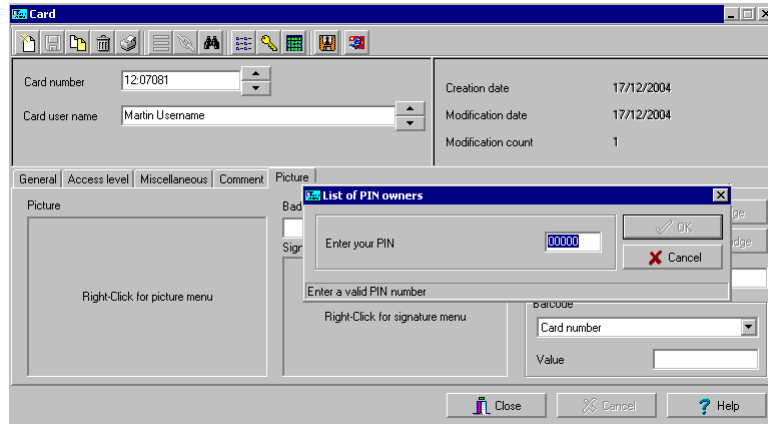


To View and Verify PINs

Entrapass enables you to view and verify cardholders' PINs in the Card and windows.

To View Cards Assigned the Same PIN

- 1 From the **Card** window, click the **List of PIN owners** button.



- 2 Enter the PIN number in the Enter your PIN field.



NOTE: If the system is set to PIN duplication (**Options > Server Parameters**), and if the PIN is used by more than one cardholders, the system displays a list of cardholders who are using the PIN. This feature is useful when for example you want to display the list of cardholders who are using a given PIN or if you are issuing new cards and you want to verify which PINs are already being used.

Cards Handling

To Edit a Card

- Enter the card number in the **Card number** field and press **Enter**. The system displays the card; you may then modify the card as required.
- Browse the **Card number** field using the **Up/down** arrows and then select the card to be modified.
- Browse the **Card user name** field, using the **Up/down** arrows.

To Find a Card

You can perform two types of card searches:



Per card information



Per card user name.



NOTE: For more information on how to search information in EntraPass, see "To Find a Card" on page 39

To Delete a Card

The **Delete** feature allows an operator to remove a card from the cardholder database. A card that has been deleted from the cardholder database must be re-issued again in order to use it again.

- 1 Locate the card you want to delete: to locate the card, you may enter the card number in the **Card number** field and press the **Enter** key or you may browse the **Card number** or **Card user name** fields using the up/down arrows.
- 2 Click the **Delete** icon, then click **Yes** in the **Warning message** box.

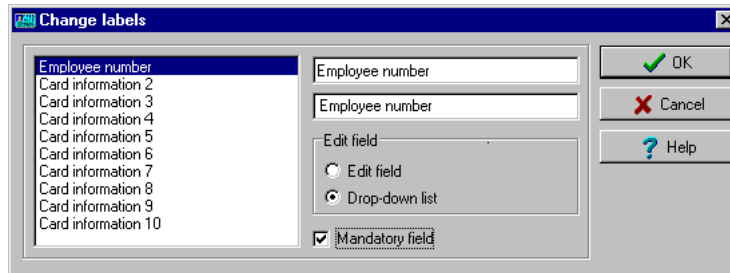


NOTE: Although a deleted card is removed from the card database, it remains in the card history; all events involving that card remain in the event messages database. An event report locating past events that involved any deleted card can be performed.

To Customize Card Information Fields

You may rename Card information fields according to your organization requirements. These fields can contain any information. They can be used as edit boxes or drop-down lists.

- 1 In the Card definition menu, select any card, then double-click the **Card information** field. The system displays the **Change labels** window:



- 2 Select the field you want to modify and enter the name in the language section. For example, if you want to rename *Card Information #1* to *Employee number*, double-click the **Card Information #1** label; it appears in the language section, then enter the new name in the language section.
- 3 Select the **Edit field** option if the information appears as an **Edit field** (one-line information) or **Drop-down list** (as applicable); then click **OK** to save your modifications.
- 4 You need to repeat these steps for all the fields you want to modify.



NOTE: Check **Mandatory field** to ensure a field is not left empty.

NOTE: The changes you make are not immediately effective. They will take effect only when you exit and then re-enter the Card menu.

NOTE: An operator must have full access privileges to edit card information fields. An operator with read only access may only view information in these fields.

Cardholder Access Levels Assignment

An access level must be assigned to each card. Access levels determine where and when the card will be valid. The access level allows the cardholder entry to selected locations during specified schedules.

For information on defining access levels, see "Access Levels Definition" on page 181.



NOTE: When you modify the access level assigned to a card, you also modify the user's access permission to the doors and schedules associated to that access level.

In order to assign an access level to a card, you have to:

- Create schedules that will correspond to the time the user has access to the desired doors,
- Assign the created schedule to the desired doors (in the Access level definition menu),
- Assign the access level to cards.

To Assign an Access Level to a Cardholder

- 1 From the Card definition window, select the **Access level** tab. The Access level window appears, it displays the **Site** column and **Access level** drop down list.

Site	Access level
Administration Floor	None

- 2 Click the **Card access group** button (displayed on the left of the Site or Gateway list). It is used to copy information from a Card access group to a card. The **Site** column displays the sites and gateways to which an access level will be associated.
- 3 From the **Access level** drop-down list, select the access level that will determine the cardholder's access to the doors of the selected site. If you do not want this cardholder to have access to the door of this site, leave this field to **None**.

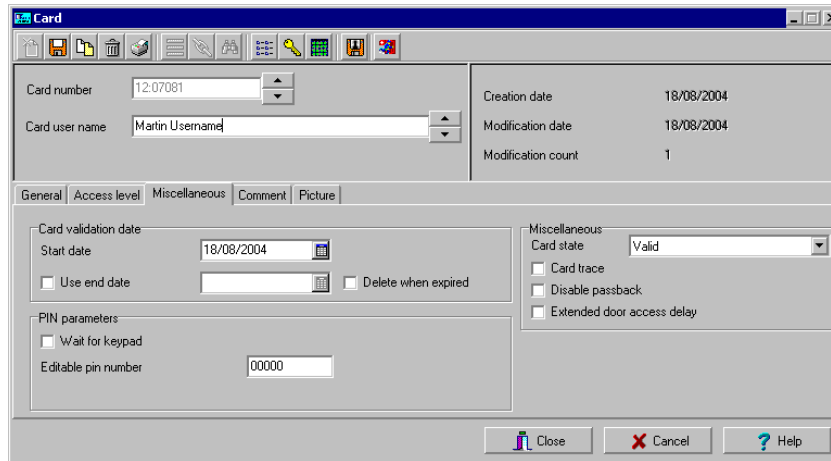


NOTE: You have to create Access levels (**Users > Access Level**) to have them displayed in the **Access Level** drop-down list.

Card Use Options Definition

Use the **Miscellaneous** tab to specify and view card additional information.

- 1 Select a card number using the **Up/down** arrows. The **Start date** field indicates the card creation date. You can change this information by selecting another date in the displayed calendar. The start date must be the same day or earlier than the current date; else, the **Card state** field (Miscellaneous section) will be set to "Pending".



- 2 Check the **Use end date** box if applicable. When this box is checked, the system displays a calendar allowing you to select the end date. When the end date is reached, the **Card state** field is set to "Expired".
- 3 Check the **Delete when expired** option (if applicable). This option can only be used with the **Use end date** option. When selected, the card information will automatically be deleted on the expiry date (using the end date specified), otherwise the **Card state** field will be modified to "Expired".



NOTE: A deleted card is a card that is not active in the system database. Even if a card was deleted, previous events generated by this card are still stored in the archive file.

- 4 Check the **Wait for keypad** option to force users to enter a PIN on keypad to access all doors, then in the **Editable PIN** field enter the PIN that users will be required to enter.



NOTE: Selecting the **Wait for keypad** will delay access to a door for this card until the correct PIN has been entered on a keypad. This only affects doors defined with both reader and keypad in the Door Definition menu (**Devices > Doors**). The keypad schedule must also be valid for this door. For more information on defining a door, see "Doors Configuration" on page 81.

- 5 From the **Card state** drop-down list, assign a state to the selected card. By default, a card is valid. The following states are available:
 - **Valid:** the card is functional,



- **Invalid:** the card is NOT functional,
- **Lost/Stolen:** the card is NOT functional,
- **Expired:** the card has reached its expiry date,
- **Pending:** the card is not yet functional.



NOTE: You cannot force a card state to **Pending** by selecting this state from the **Card state** drop-down list. To do so, you have to change the **Start date**.

- 6 Check the **Card trace** option if you want to monitor the use of a particular card. Selecting this option will cause the “Card traced” event to be generated each time this card is presented to a card reader. For example, you can request and generate a report containing the “card traced” event in order to verify user actions.
- 7 Check the **Disable passback** option if you want the card to override the passback option when defined.



NOTE: If you are issuing a card for a cardholder with disabilities, check the **Extended door access delay** option. To enable this option in the system, you have to define appropriate delays in the **Door** definition.

To Add Comments to a Card

- 1 From the Card window, select the **Comment** tab.

Card number	12:07081	Creation date	17/12/2004
Card user name	Martin Username	Modification date	17/12/2004
		Modification count	1

General | Access level | Miscellaneous | **Comment** | Picture

Night shift

Close Cancel Help

- 2 Enter a comment (if necessary) relative to this cardholder. The displayed field can be used to store additional information in the database. Maximum allowed: up to 241 characters.
- 3 Click the **Save** button, then the **Close** button to exit.

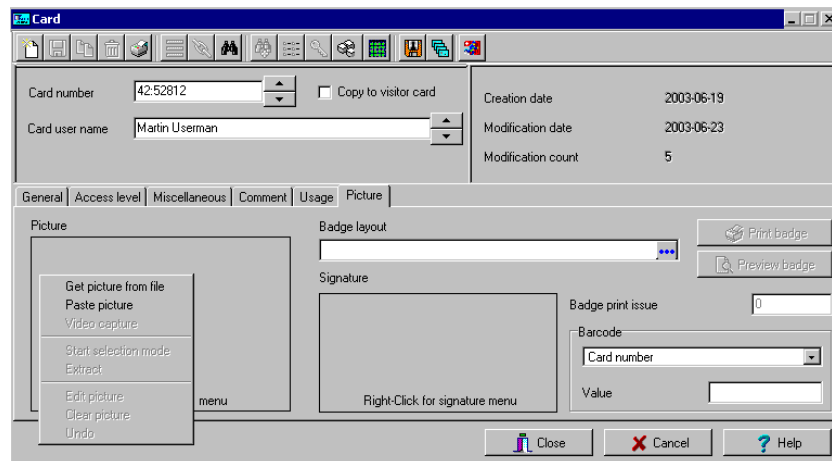
To Assign Pictures and Signatures

Entrapass offers the ability to associate photos and signatures with cardholders and to associate badge templates with cards as well as to print badges.

Photos and signatures can be retrieved from files, pasted from the clipboard, or captured using an appropriate device. To capture video images, use any MCI and TWAIN compliant device. For capturing signatures, signature pads such as Topaz, Penware TTI500 and Penware TT3100 are recommended.

Assigning a Picture from a File

- 1 From the Card window, select the **Picture** tab.



- 2 Right-click the picture area. A shortcut menu appears; choose the appropriate action:
 - **Get picture from file:** this option allows you to select a previously saved picture.
 - **Paste picture:** this option allows you to paste a picture from the clipboard. To use this option, you have to copy the picture, then paste it into the picture window.



NOTE: The Video capture option is enabled only when a video capturing device is installed.

- 3 From the **Files of type** drop-down list, select the file type you are looking for or leave this field to **All** to display all image files. Make sure that the **Auto displayer** option is selected to enable preview.



NOTE: Files with the following extensions are supported: BMP, EMF, WMF, JPG, GIF, PNG, PCD, and TIF.

- 4 Select the directory where the image is stored. Select the image you are looking for, then click **Open** to import it into the **Card** window.



NOTE: To delete the imported picture, right-click the picture, then choose **Clear picture from the shortcut menu**.

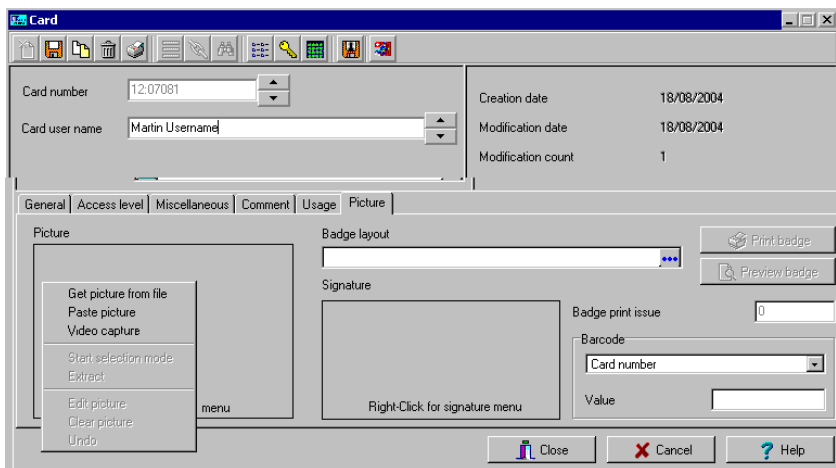
Assigning a Picture Using a Video Camera

The **Video capture** option is enabled only when the option **Enable video capture** is checked: **Options > Multimedia devices > Video** tab.



NOTE: Before you can capture images using a video camera, all equipment needs to be properly configured. For more information, consult your manufacturer's device manual. If you have more than one video driver, you will need to specify the video driver to be used (**Options > Multimedia devices > Video** tab).

- 1 Right-click the picture area.



- 2 From the shortcut menu, select **Video capture**. This option is enabled only when the Video capture capability has been enabled in the Options menu (**Options > Multimedia devices > Video**).



NOTE: Options may vary depending on the video capture program. If you have more than one video driver, you will need to specify the video driver you are using. For more information on configuring your video drivers, see "Multimedia Devices Configuration" on page 304.



- Click the **Freeze** button when you are satisfied with the displayed image, then click the **Capture** button to paste and save the displayed image.

- To associate a badge layout with the defined card, select one from the **Badge layout** list. For information on how to define a badge layout, see *"Badges Designing"* on page 150.

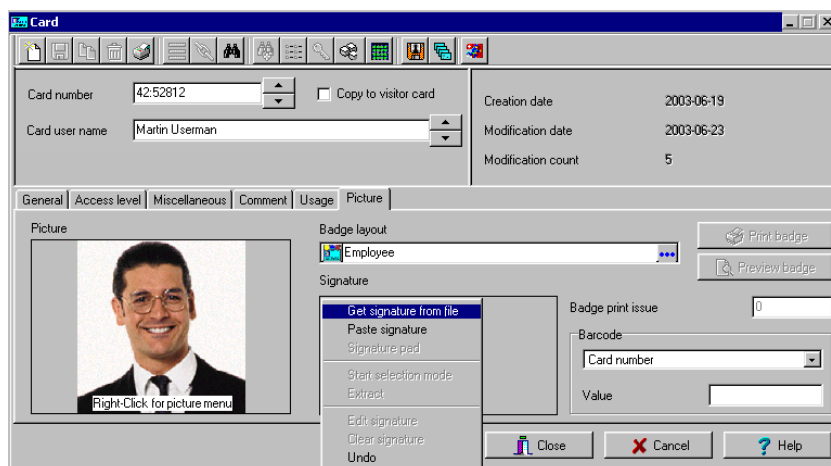


NOTE: The **Print badge** and **Preview badge** buttons are enabled only when a badge printer and badge layout has been selected and the option **Use badge printer** checked: **Options > Printer > Badge printer**. If these buttons are enabled, you can preview and print the cardholder's badge.

To Import a Signature from a File

You can import a signature, just as you import other images such as logos or pictures into the card.

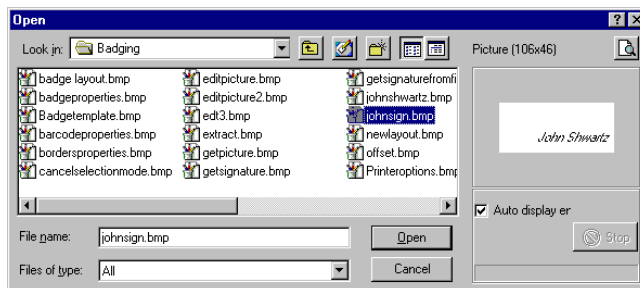
- 1 From the Card window, right-click the signature area. A shortcut menu appears.



- 2 From the shortcut menu, make the appropriate choice:
 - **Get signature from file:** allows you to select a previously saved signature,
 - **Paste signature:** allows you to paste a signature that was previously copied to the clipboard. The option is enabled when there is content in the clipboard.



NOTE: The *Signature pad* option is enabled only when the appropriate device is enabled in the Options menu (**Options > Multimedia devices > Signature**).

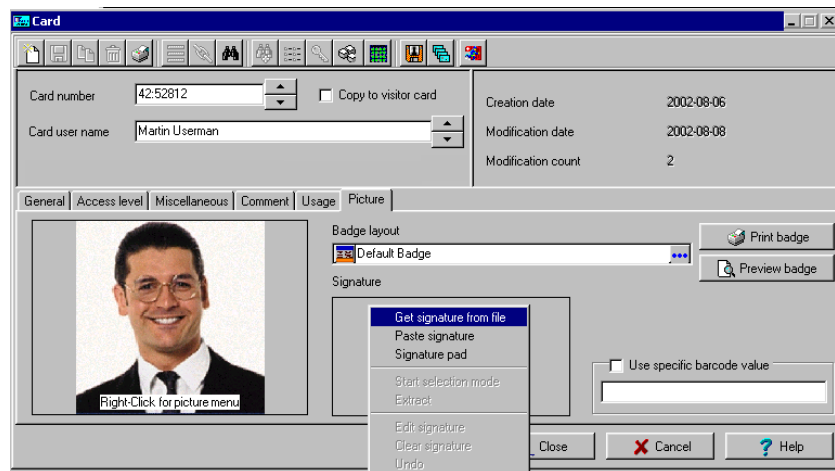


- 3 Select the signature file, then click **Open**.

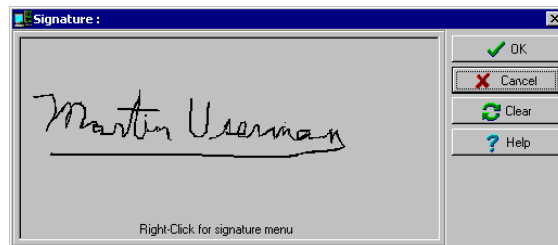
To Add a Signature from a Signature Capture Device

Use this option if a Signature Capture Device is installed and configured. The Signature pad option is enabled only when the appropriate device is enabled in the Options menu (**Options > Multimedia devices > Signature**).

- 1 From the Card window, right-click the signature area. A shortcut menu appears.



- 2 From the shortcut menu, select **Signature pad**. The Signature window appears, allowing you to preview the signature.
- 3 Click **OK** to paste the signature in the card window.



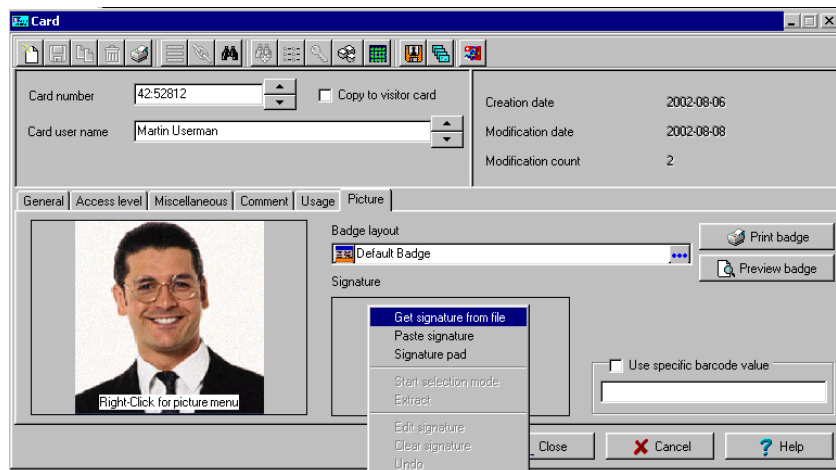
To Work with Photos and Signatures

The Entrapass Integrated Badging feature allows users to extract part of an image or enhance images that are incorporated into cards.

Extracting Part of an Image

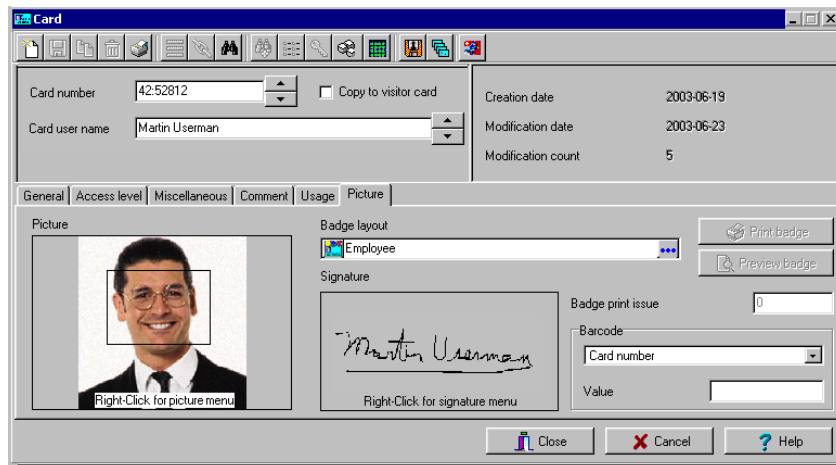
If you have incorporated a large image but you need only part of it, you can select and extract the part that you want to assign to the card (picture, signature).

- 1 Right-click the image you have just imported.



NOTE: The **Extract** option is enabled after you have started the selection mode. Similarly, the **Undo** option is enabled only when an image has been pasted.

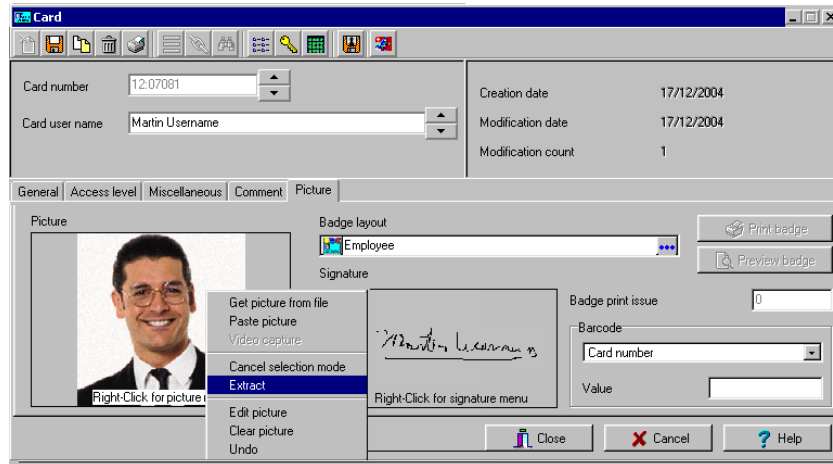
- 2 Select **Start selection mode** from the shortcut menu.



NOTE: You can increase the size of the selection rectangle by dragging its sides and corners to adjust to the part of the image you want to extract. You can also move it by dragging it to the desired area of the image.



- 3 Once you have selected the part you want to incorporate into the card, right-click the image again. A shortcut menu appears.

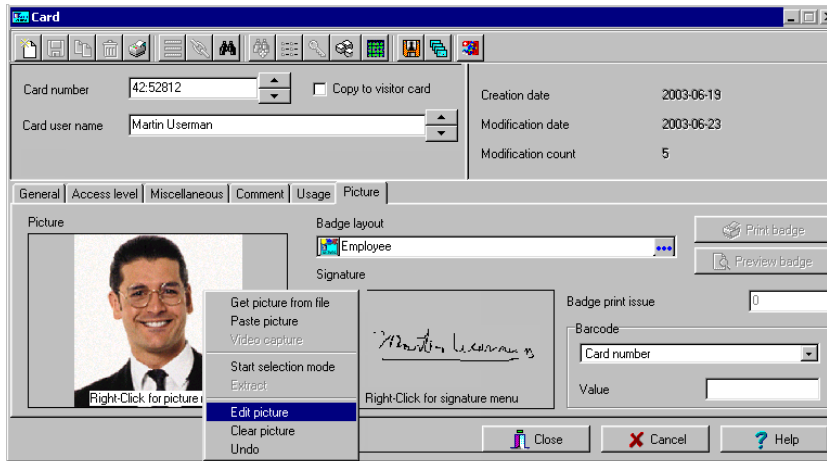


NOTE: To disable the current selection, right-click the picture, then select **Cancel selection mode**. Select **Undo** to discard the changes. The **Undo** option is enabled only when you have pasted an image.

- 4 From the shortcut menu, select **Extract**.

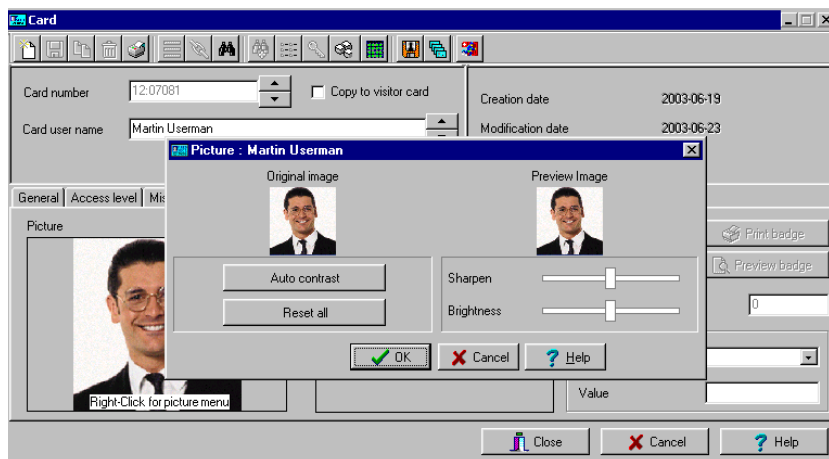
Editing a Picture/Signature

- 1 Right click the image you want to edit.



NOTE: The **Barcode** area allows you to assign a barcode to a badge for identification purposes. Select any item from the drop-down list to be used as the value of the barcode. Select **Custom** to enable the **Value** field and type a specific barcode value. If you do not enter a custom barcode value, the **Card number** is used as the default value.

- 2 From the shortcut menu, select **Edit (picture or signature)**.



- 3 Adjust the features of the image using the displayed options. The **Reset all** option enables you to go back to the original image:

- **Auto contrast:** this feature gives better contrast by intensifying lights and shadows: it makes the darks darker and the lights lighter. In general, this auto contrast feature gives a good result when a simple contrast adjustment is needed to improve an image's contrast.
 - **Sharpen:** this feature provides more definition to blurry images by applying sharpening only when an edge is found.
 - **Brightness:** this feature allows you to add light to the image by sliding towards the positive values.
 - **Reset all:** this feature allows you to undo all the changes and to restore the original image.
- 4 Click **OK** to close the **Picture** editing window.
 - 5 From the Badge layout pull-down menu, select a layout to associate with the card you have defined To define a badge layout, see "*Badges Designing*" on page 150.

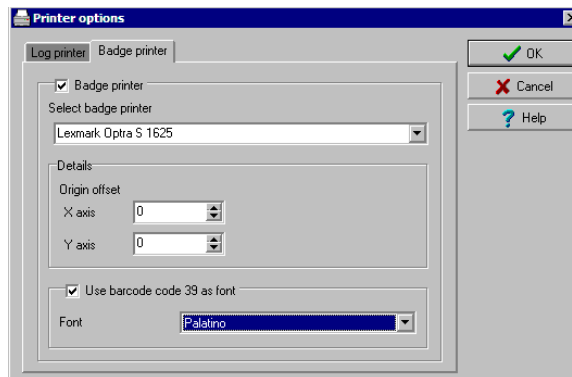
To Print Badges

You may print badges from the **Card** or from all **Badge preview** windows. The software is set up to let you print one single or double-sided badges.

Before you print, you have to select a badge printer. It may be any network printer, or a specific badge printer.

Selecting a Badge Printer

- 1 From the EntraPass Workstation window, select the **Options** tab, then click the **Printer Option** button.
- 2 From the Printer option window, select the **Badge printer** tab.



NOTE: You can print badges to any network printer. However, to print badges on appropriate cards, you have to select a badge printer.

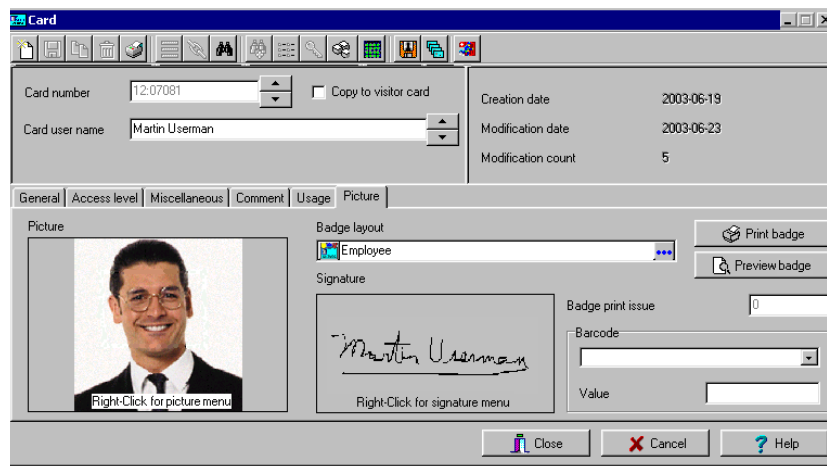
- 3 Check the **Badge printer** option to indicate to the system that a badge printer is selected. If the **Badge printer** option is checked, the Print badge and Preview badge are displayed in windows where you can print badges (Card windows).
- 4 From the **Select badge printer** drop-down list, select the printer dedicated to badging.

- 5 Adjust the margins:
 - Origin offset, X axis: indicates the left margin.
 - Y axis indicates the upper margin.

Previewing and Printing Badges

The **Badge - Preview and Print** window allows you to preview a badge layout with card information (if the badge layout is associated with a card) or with default values (if the template is not yet associated with a particular card). The program permits you to print single or double sided badges.

- 1 From the Card, click the **Preview badge** button.



NOTE: From the Badge design window, the preview option allows you to view a badge with default values since there is no card associated with it (**Badge design > Layout > Preview**).

2 From the Badge - Preview and Printing window, choose a printing option:



- **Print front side:** only the front side (preview in the left-hand pane) is printed.
- **Print back side:** only the back side (preview in the right-hand pane) is printed. This button is enabled only when the badge is defined with two sides.
- **Print both sides:** the front and back side are printed. This button is enabled only when the badge is defined with two sides.



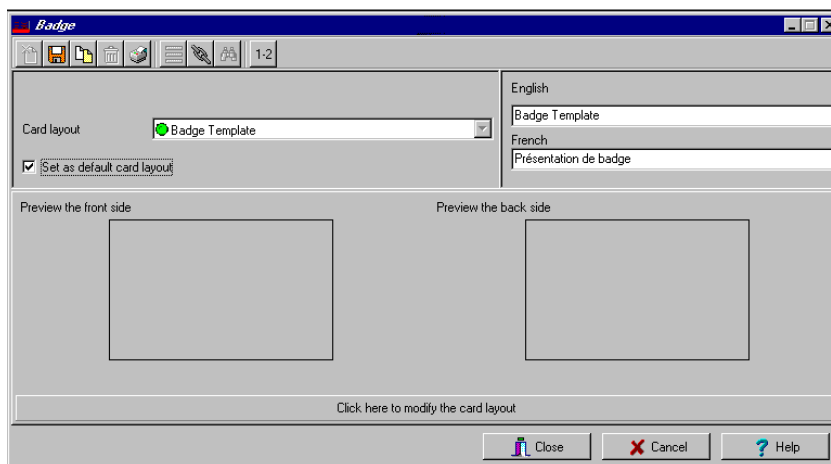
NOTE: Important! In Order to print badges with barcodes, your printer has to be properly set. You have to select the "black resin" option, otherwise, barcode readers may not detect the barcode. If you have problems with barcode printing or reading, refer to your printer manufacturer's manual.

Badges Designing

EntraPass contains a badge layout editor which enables users to create, save, edit or delete badge templates that are later selected and associated with cards for badge printing. You can create and edit badge templates, add colored or graphic backgrounds, logos, text, barcodes, and place photo or signature holders.

To Create a Badge Template

- 1 From the Users menu, select the **Badge** icon. The Badge window appears.

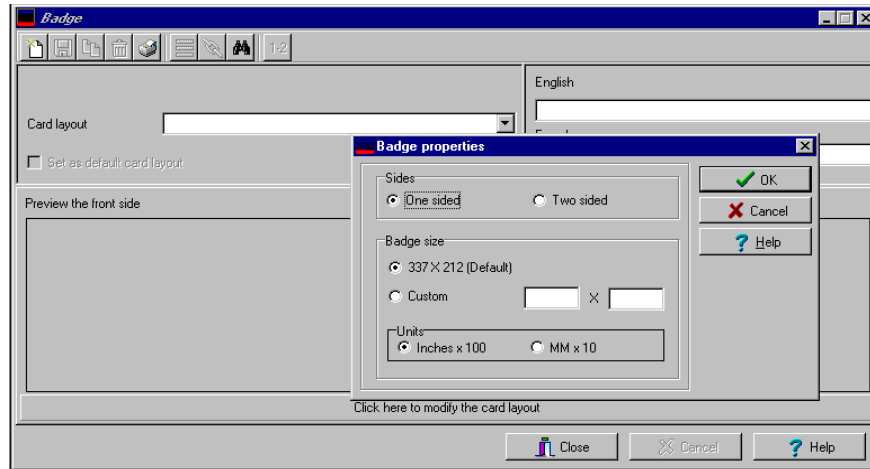


NOTE: The Badge window contains all the tools available in other EntraPass windows: new, save, copy, delete, print, links, search (the Hierarchy button is disabled). However, it contains an additional 1-2 button which allows to modify the number of sides assigned to a badge layout.

- 2 Click the **New** icon in the toolbar. The Badge properties window appears.

Specifying Properties for a Badge Layout

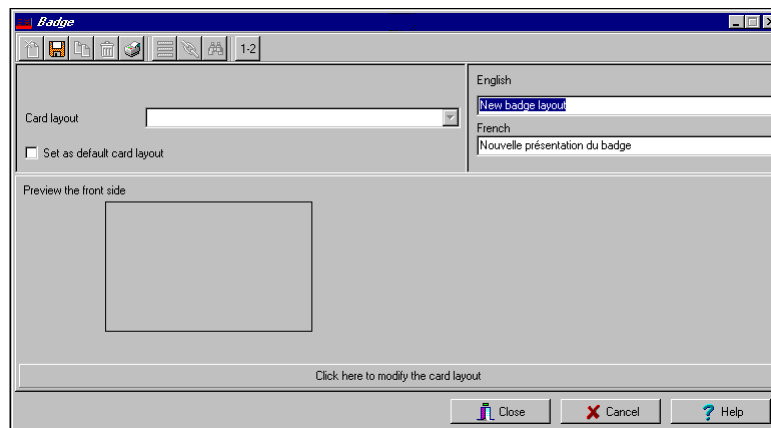
- 1 In the Badge properties window, indicate the number of sides for the badge, then select the desired size for the badge layout, then click **OK**.



- 2 Indicate the number of sides for the badge, then select the desired size for the badge layout, then click **OK**.



NOTE: Measures are expressed either in inches or millimeters (a hundredth of an inch or a tenth of a millimeter). To change the unit of measure, check the appropriate radio button in the Units section.



- 3 Enter the name for the badge template in the language fields. You can enter up to 40 characters.



- 4 You may check **Set as default card layout** if you want this new design to be automatically used for all new badges.



NOTE: Only one default layout is available. When you select one layout and check the option **Select as default card layout**, the current default layout is replaced.

- 5 Click the **Save** icon to save the badge template.

Editing a Badge Layout

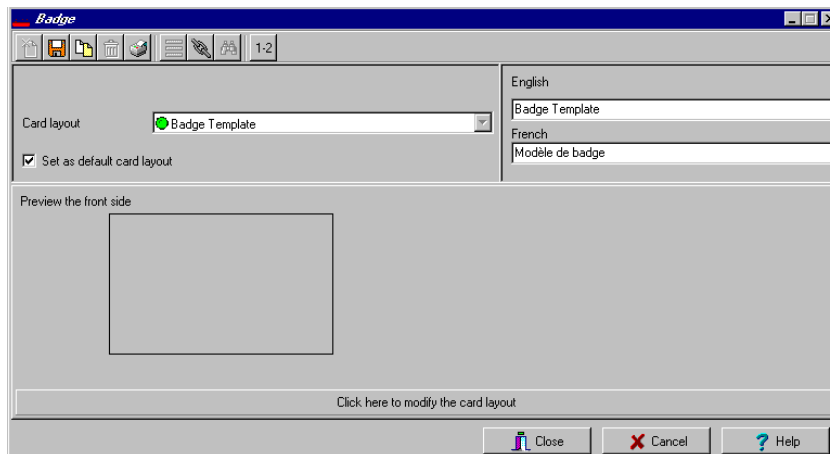
The Badge design utility allows users to edit the badge layout, to add background color or graphics, to modify the font, etc.



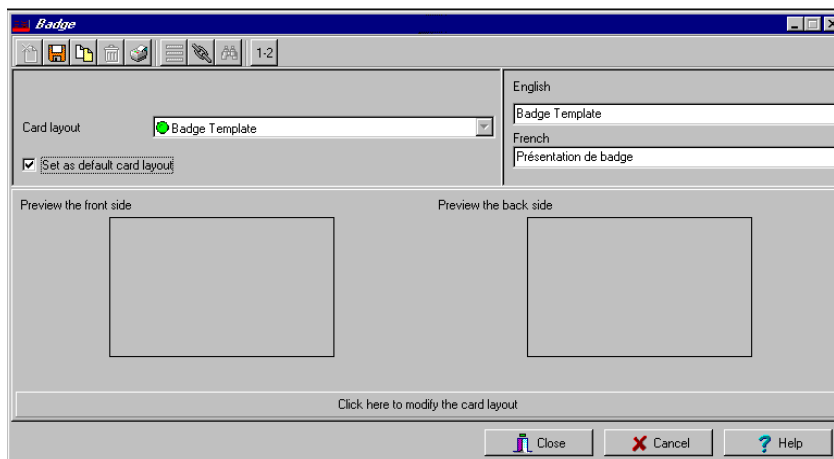
NOTE: Once a card layout is created, you cannot modify its size; you have to create a new layout. However, you can modify the number of sides by clicking on the **Sides** icon in the Badge window toolbar.

Modifying the Number of Sides

- 1 From the badge window, select the badge you want to edit.



- From the Badge window toolbar, click the 1-2 button.

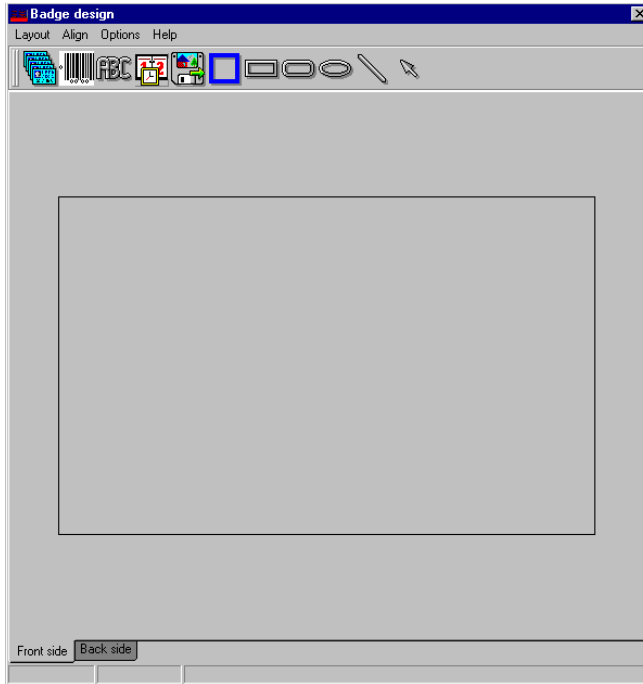


- Click the **Save** icon to save the new badge information.



Modifying the Background Color

- 1 From the Badge window, select the badge you want to modify.
- 2 Click the **Click here to modify the card layout** button (located in the lower part of the window) to open the Badge design window.

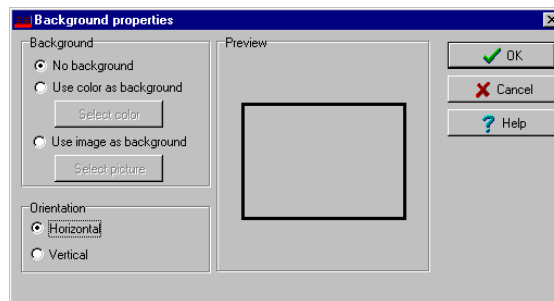


NOTE: When you move the cursor over the Badge design objects, a hint explaining each object appears.

- 3 To modify the template background color, right-click anywhere in the work area. The **Properties** shortcut menu appears.



- 4 Select **Properties**. The Background properties window appears.



- 5 Select the appropriate options for the template:
 - **No background** (default setting)
 - **Use color as background**: this option will allow you to apply a background color to all the designs.
 - **Use image as background**. This option allows you to incorporate an image that will be displayed as a watermark in all the badges.

- **Orientation:** allows you to select a landscape (horizontal) or portrait (vertical) display.

Adding Objects to a Badge Layout

By a simple click and drop feature, the Badging utility permits you to incorporate objects into the badge template:

- Card fields information,
- Barcodes,
- Text boxes,
- Current date,
- Previously saved images and logos (BMP, JPG, GIF, etc.),
- Border,
- Rectangle (including rounded rectangle, ellipse),
- Line, pointer,



NOTE: Objects are incorporated with their default settings. To modify an object's properties, right-click the object, then select appropriate settings from the shortcut menu.

Incorporating Card Information Fields

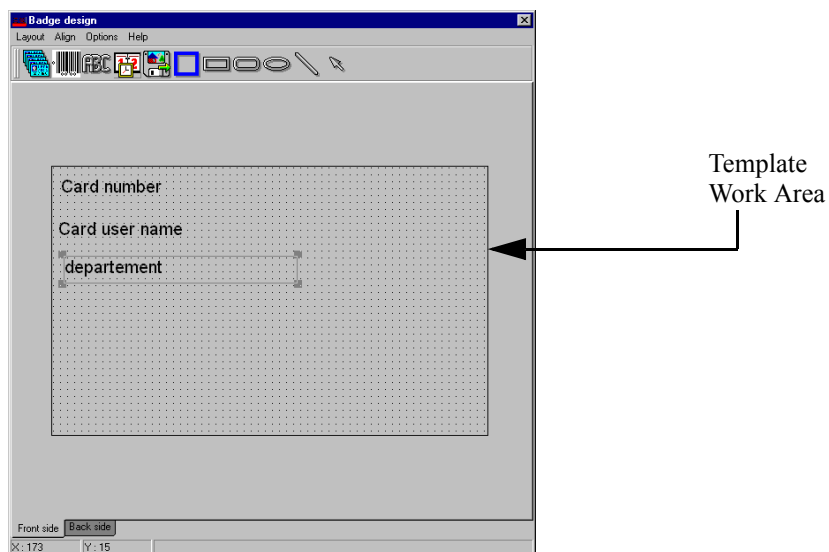
- 1 To add card information fields to the badge template, click the **Card fields** icon. The **Card fields** submenu appears.
- 2 To modify an object property before you drop it, go to **Options** in the Badge design window, then choose **Show properties on drop**. If you do this, the Properties window will open every time you drop an item in the template work area.



NOTE: To enable last and first name selection in the Card fields menu of the Badge design window, go to the **Options menu**, then choose **System options**, select the **User name format** tab, check **Parse user name** checkbox, then select the name (first or last name) that will be used for sorting cardholders' names.

Card number	
Card user name	
Card information 1	
Card information 2	
Card information 3	
Employed number	
Card information 5	
Card information 6	
Card information 7	
Card information 8	
Card information 9	
Card information 10	
Start date	
End date	
Picture	
Signature	
Last name	
First name	

- 3 From the shortcut menu, select the card information field you want to add to the template layout, then click in the template work area to incorporate that field you have selected.

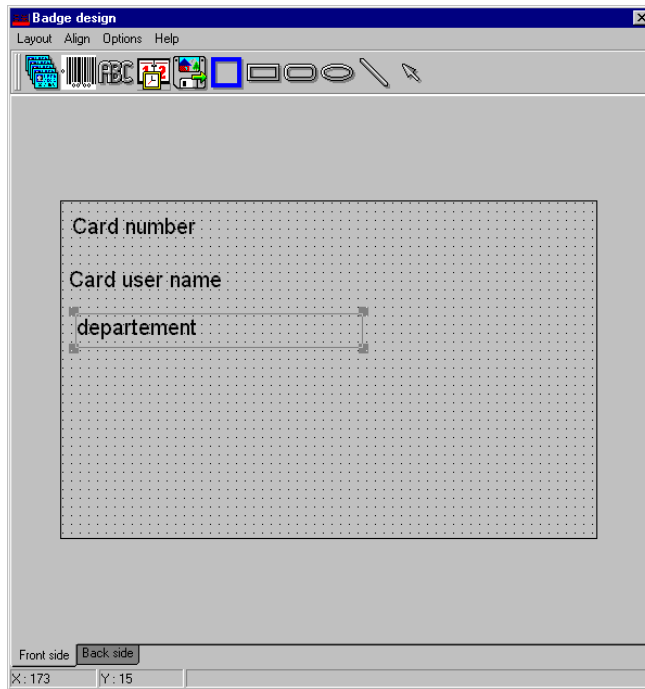


NOTE: When you add a photo to a badge design template, the photo that appears is only a placeholder. It indicates where the cardholder's photo will be displayed. When a badge is assigned to a card, the appropriate cardholder's photo is displayed.



Aligning Objects in the Template Layout

Grids assist you in aligning items in the badge layout template. It can be used as a visual aid to place items on gridlines.



Three options are available to help you align your objects in the badge template:

- **Show gridlines:** displays grid points to aid with object alignment.
- **Align to grid:** must be activated before you start building your template. As you “click and drop” design objects in the template work area, they will be “snapped” to the nearest grid mark.
- **Grid settings:** allows you to specify the horizontal (Height) and vertical (Width) grid spacing (in pixels).

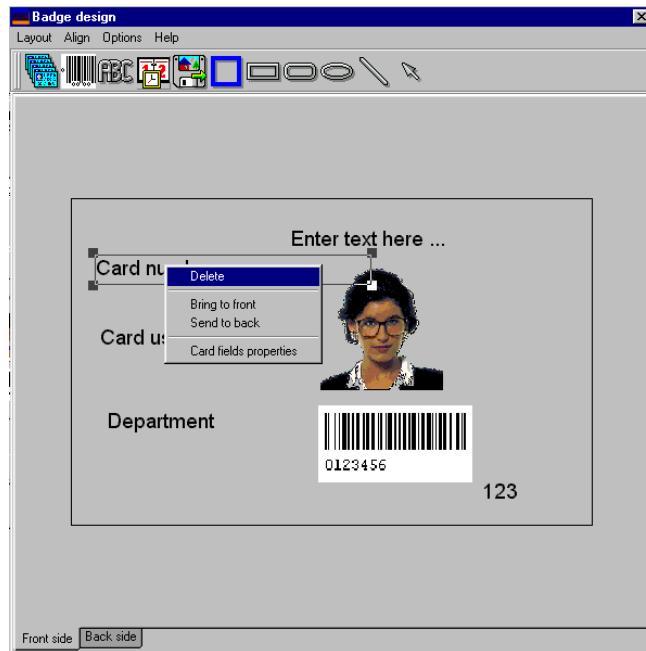


NOTE: To disable the grid unselect **Show gridline** in the **Align** menu.

Modifying Card Fields Properties

Objects are incorporated in the template with their default settings (font, color, etc.). You can modify the settings later. For example, you can modify the appearance of any text object, such as card field, static text, date, etc.

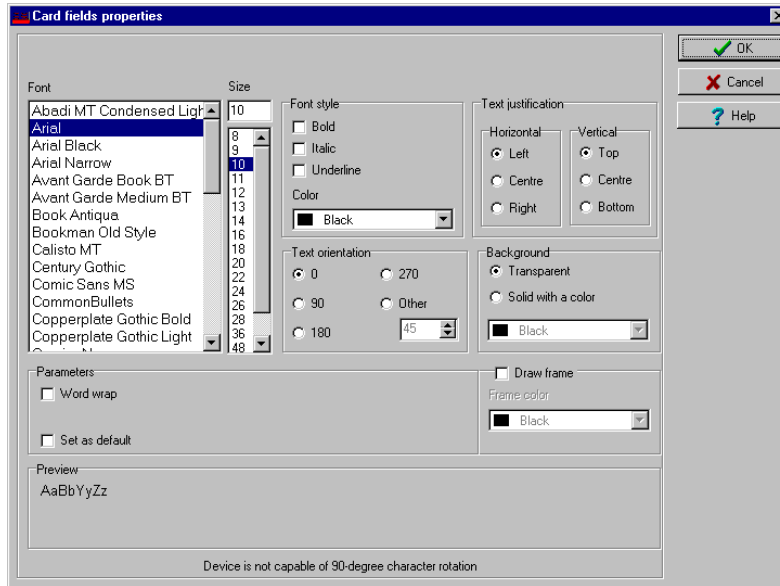
- 1 From the Badge design template, right-click the object you have inserted (in this example, Card information fields).



2 From the shortcut menu, select **Card fields properties**.



NOTE: The Properties menu item depends on the selected item. For example, it will change to Image properties or Current date properties, depending on the selected object.



3 From the Card fields properties window, you can modify all the text properties:

- Font (name, color, style (bold, italic, underline)),
- Background (transparent or solid with a color),
- Justification (horizontal, vertical),
- Orientation,
- Parameters (word wrap, for example).



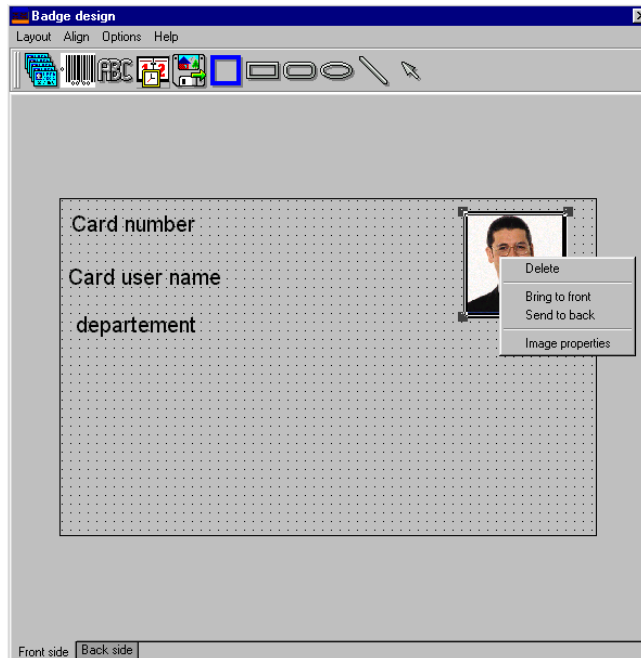
NOTE: The **Set as default** checkbox allows you to apply all the characteristic to all text objects that will be incorporated in the template.

NOTE: When Text Orientation is set to “Other” it is not possible to resize the field.

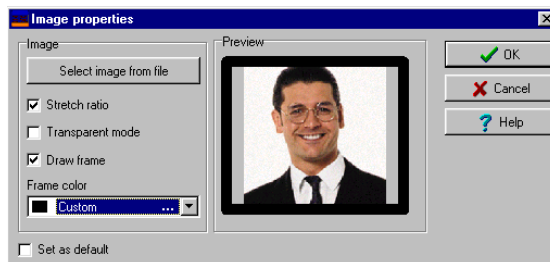
Modifying Picture Properties

This applies to any picture object such as photos, logos, and signatures.

- 1 From the Badge design work area, right-click the image (picture, logo) or signature that you want to modify.



- 2 From the shortcut menu, select **Images properties**.



- 3 You may select another image from file or modify the image properties:
 - **Stretch ratio**: select this option if you want the image to be centered in the image holder space, while keeping the proportion of the original image.
 - **Transparent mode**: if you choose this option, there is no background color,
 - **Draw frame**: select this option if you want a frame around the picture object,
 - **Frame color** (enabled when a Frame option is selected): select this option if you want to apply a specific color to the image frame. The Frame color drop-down list enables you to select a custom color from the frame.



- 4 You may check the **Set as default** option if you want these properties to apply to all image objects you add in the badge template.

Adding Static Text Objects

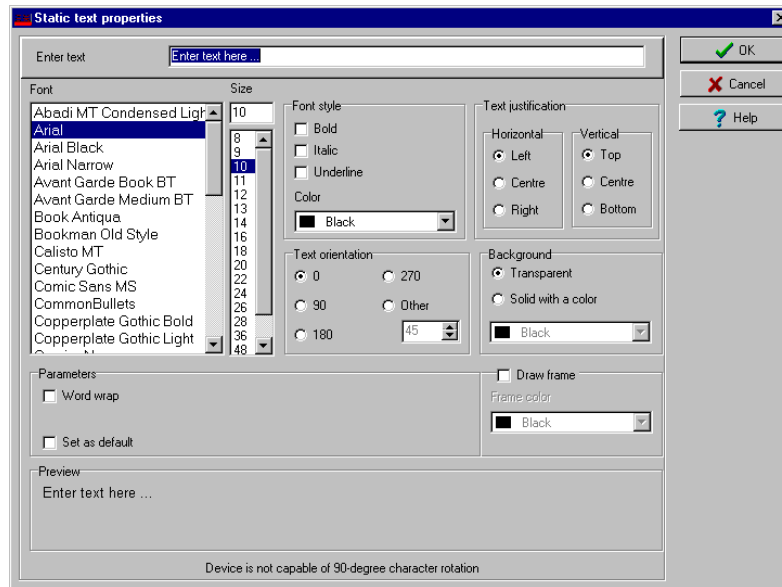
To add text objects to a badge, first click and drop a text box, then enter the text in the Text properties window. It is also in the Text properties window that you modify the text appearance.

- 1 From the Badge design tool bar, click the text icon. To resize the text box, select it and use the two-headed arrow to drag the sizing handles to the desired position. This also allows you to change the height and width of the text box.



- 2 To align the text box, see *"Aligning Objects in the Template Layout"* on page 158.

- To add text to the text box, right-click the text box, then select **Static text properties** from the shortcut menu.



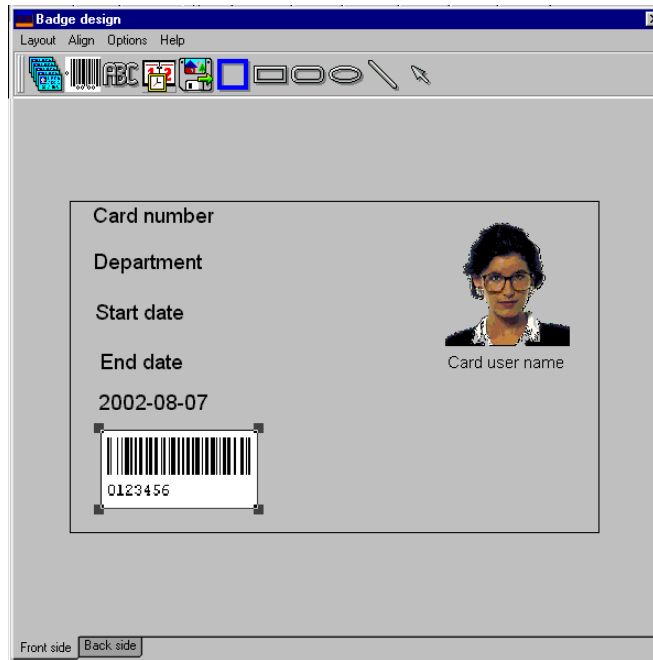
- Enter text in the **Enter text** field; then modify the text properties as desired. The Preview section shows the result of the changes you apply to the text.

Adding Bar Codes

The Badging feature allows users to add bar codes to badges. By default, the barcode value is the card number, if no other value is specified.



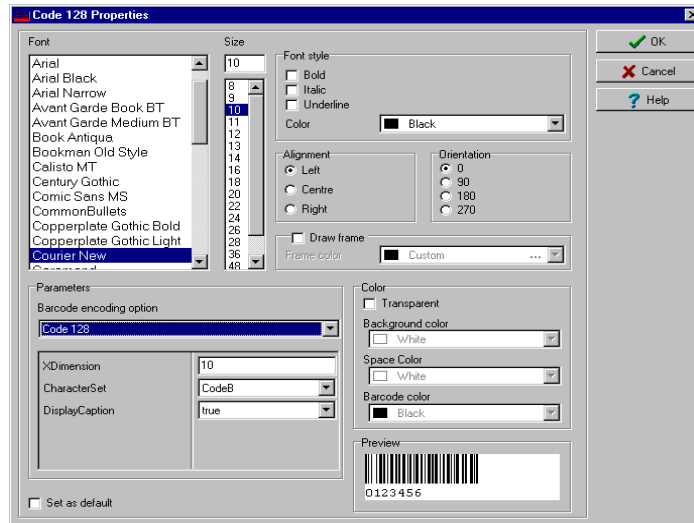
- 1 From the Badge design window, click the **Barcode** icon, then click in the Badge design work area.



- 2 To align the barcode, see *"Aligning Objects in the Template Layout"* on page 158.

Setting Up Barcode Properties

- 1 From the Badge design window, right click the barcode to open the Barcode Properties window.



Supported Encoding Options:
Code 39 or Code 39-Modulo 43
POSTNET
Codabar
EAN 8 & EAN 13
UPC A
UPC E
Code 2 of 5
Interleaved 2 of 5
Code 128

- 2 From the Properties window, you can define settings for the barcode that you want to incorporate in the Badge design.



NOTE: If it is necessary to set **Barcode encoding option** to **Code 39-Modulo 43**, set **Field Checksum** to **true**.

Adding The Current Date

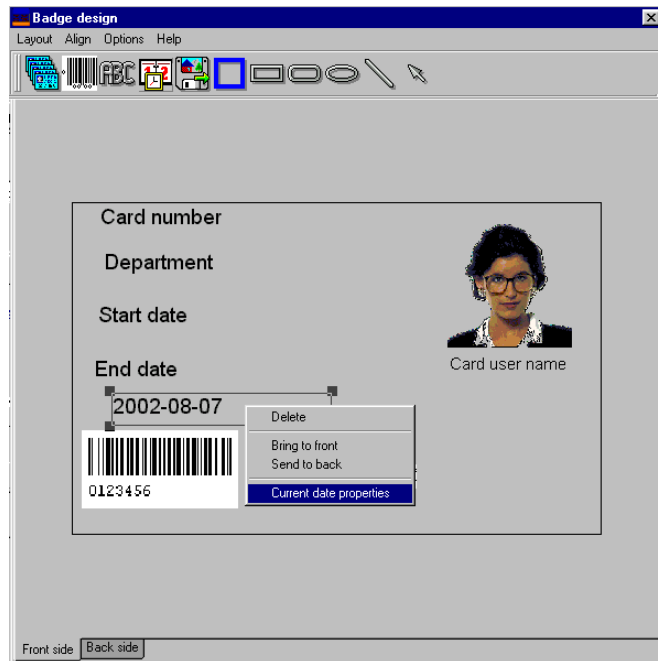
You add the current date just as you add any other design item by selecting the item in the tool bar, then by clicking in the Badge design work area.



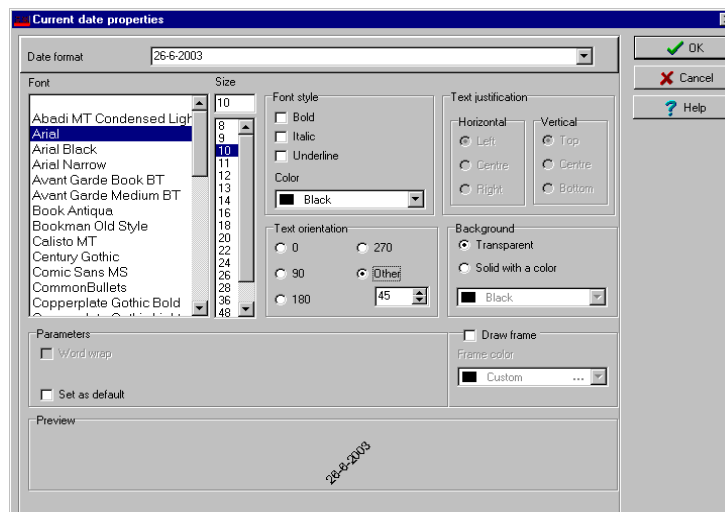
- 1 From the Badge Design template, select the **Current date** icon, then click in the Badge design work area.



- 2 Right-click the current date to display the shortcut menu.



- 3 To align the current date, see *"Aligning Objects in the Template Layout"* on page 158.
- 4 Select **Current date properties** from the shortcut menu.

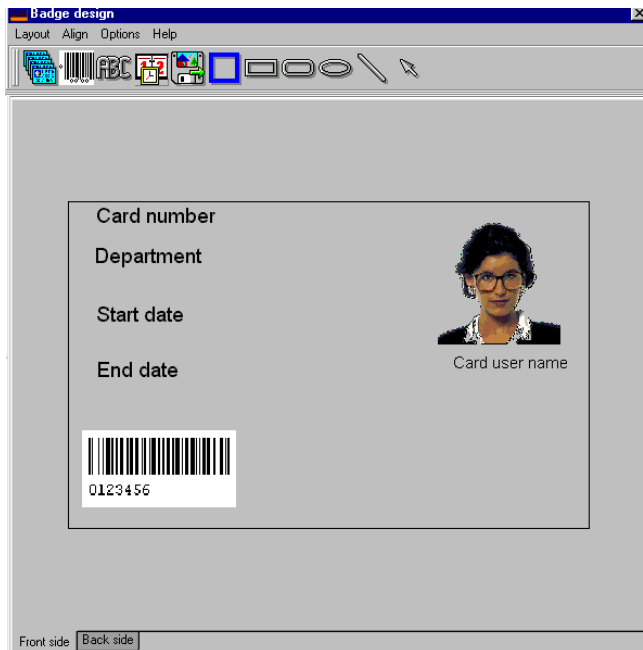


- 5 From the Current date properties window, you can:
 - Select the date format (top of the window)
 - Change the text properties: font, color, justification, orientation etc.

Adding An Image

Background images can be imported from any directory. Scanned images, photos taken with a digital camera and artwork created in any illustration design program can be incorporated into the badge design.

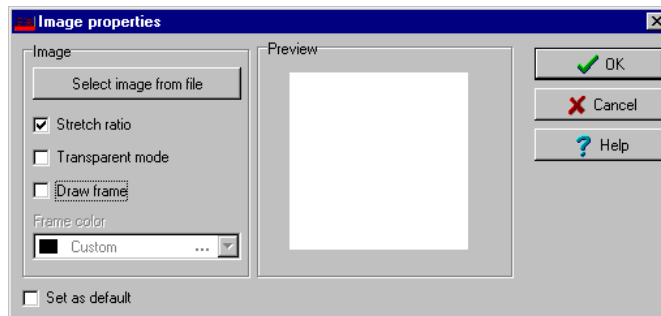
- 1 From the Badge design window, select the **Picture** icon.



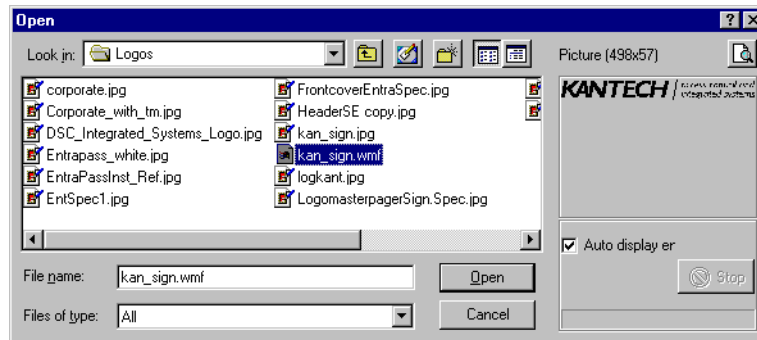
NOTE: The Badging feature supports most available image formats: BMP, JPG, EMF, WMF, GIF, PNG, PCD, and TIF.



- Drop the **Picture** icon in the template work area. The Image properties window appears.



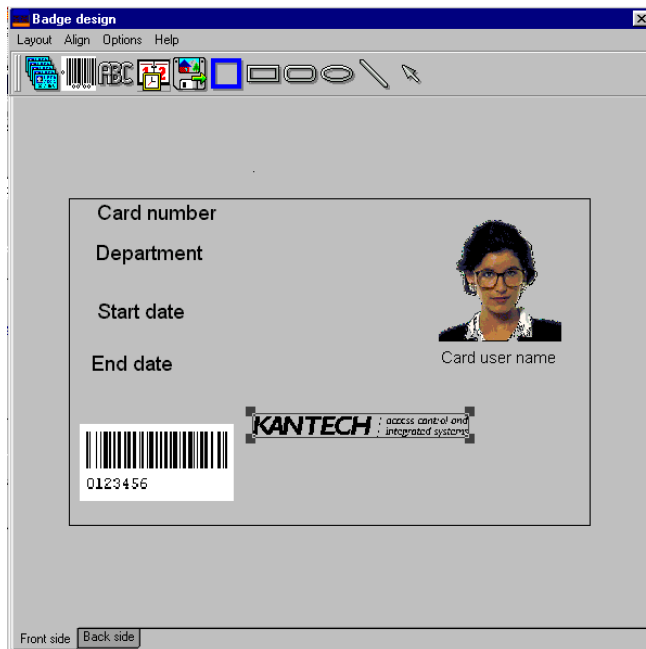
- Click the **Select image from file** button. The Open window appears, allowing you to select an image.



Click the zoom button to increase the size of the image in the preview pane



- 4 Browse to the desired image, then click **Open**. The picture appears in the template area.



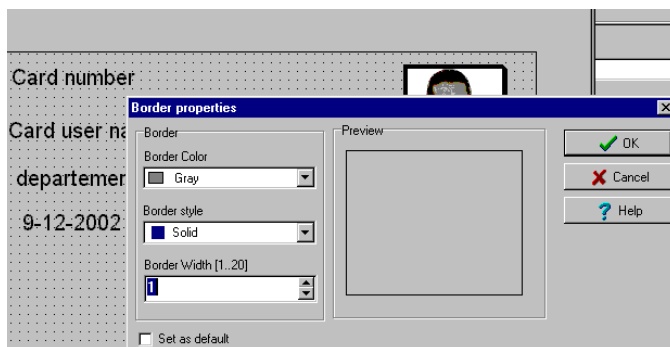
NOTE: When you import an image, you have to resize it to its original size as illustrated on the following image.

- 5 Using the sizing handles, adjust the image to the desired size, then move it to the right-hand position; you can use the grid to align it properly. For more information, see *"Aligning Objects in the Template Layout"* on page 158.
- 6 Right click the image to modify its properties. For details, see *"Modifying Picture Properties"* on page 160.

Placing Other Design Objects

The Badging feature lets you add borders, rectangles (regular, rounded, ellipse), lines and pointers, just as you add any other design object, by a click in the toolbar, then a drop in the design work area.

- 1 From the Badge design window, select the object you want to add (next to the Diskette icon), then click in the Badge design work area. The Border properties window opens.

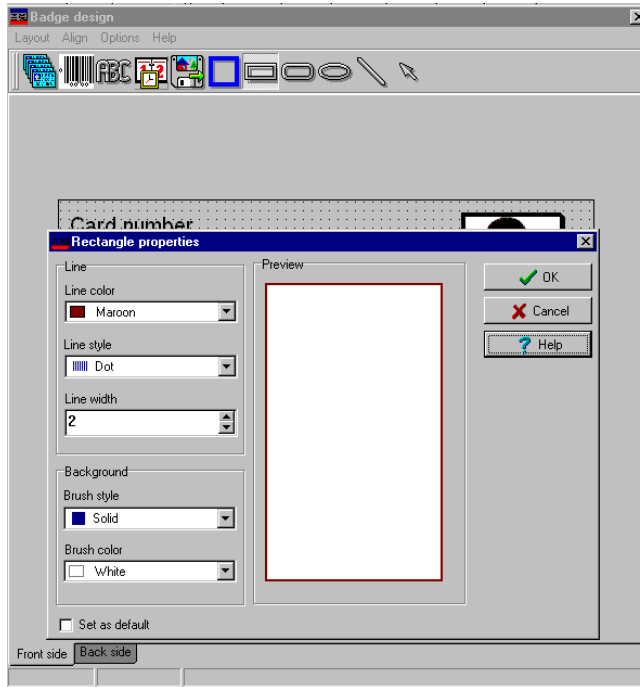


- 2 To modify the border properties, select the border color, the border style, and the border width. You may check the **Set as default** option, then click **OK** to exit.



Placing a Rectangle

- 1 From the Badge design window, select the rectangle tool (next to the Border tool), then click in the work area.



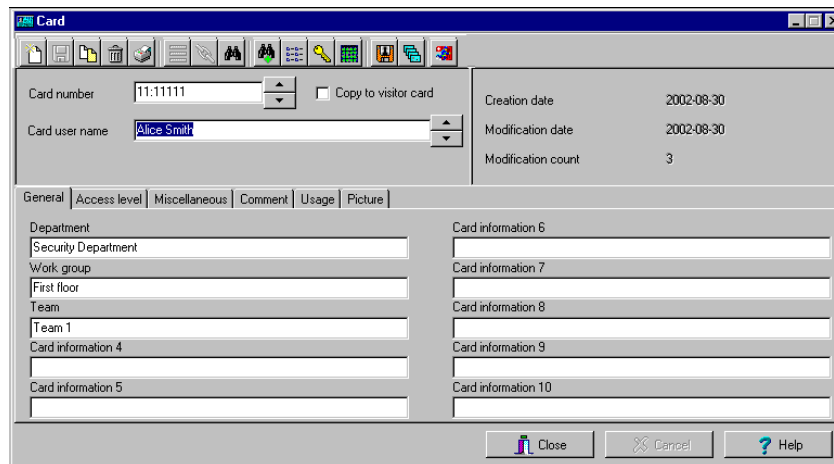
NOTE: This applies also to rectangles, rounded rectangles and ellipses.

- 2 From the Rectangle properties window, you may define the rectangle properties before importing it:
 - Line color,
 - Line style,
 - Background (brush style and brush color).

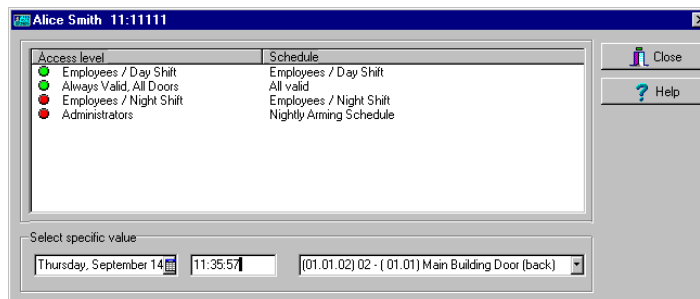
To Validate Card Access

The Validate card access feature lets you view access levels that are assigned to a particular cardholder.

- 1 From the Card window, select a card.



- 2 From the Card window toolbar, click the **View and Validate Access** button (the key icon in the toolbar).



Access level	Schedule
● Employees / Day Shift	Employees / Day Shift
● Always Valid, All Doors	All valid
● Employees / Night Shift	Employees / Night Shift
● Administrators	Nightly Arming Schedule

Select specific value

Thursday, September 14 11:35:57 (01.01.02) 02 - (01.01) Main Building Door (back)

- 3 From the **Select specific value** section, select the date, time and the door on which the validation is required. The system displays the access levels for the selected door as well as the schedules assigned to the displayed access levels. The **Access Level** column displays the access levels associated with the selected door. The **Schedule** column displays the schedule associated with the access level.
 - **Red**—Indicates that access to the selected door on the selected date and time is not allowed (not authorized).
 - **Green**—Indicates that access to the selected door on the selected date and time is allowed (authorized).

Cards Printing

Use the Print feature to print a specific range of all the cards that are stored in the database. You can select various filters to customize the card list.

You can preview your list so that you can modify or verify the settings (fields) before printing.

You can also use the **Font** button to set a different font and font size for your report.



NOTE: Whatever your selections, the card user name and card number will always be displayed. By default, only fields containing information will be printed. If no fields are selected, only cards containing information will be printed. If you want to print empty fields, check the **Print empty fields** option. If you want to simply preview card reports there must be at least one printer installed on the computer.

To Print Cards

- 1 From the Card window, click the **Printer** icon.

The screenshot shows the 'Card' window with the following settings:

- Card index:** Card number
- Specific range**
 - Lower boundary: 00:00000
 - Upper boundary: 00:00000
- Filter**
 - Start date between: 17/12/2004 to 17/12/2004
 - End date between: 17/12/2004 to 17/12/2004
 - Card state: Valid
 - Exist trace
 - Exist comment
 - Exist PIN
 - Exist delete on expired
 - Exist wait for keypad
- Print selected fields**
 - Access level
 - Badge
 - Card information 1
 - Card information 10
 - Card information 2
 - Card information 3
 - Card information 4
- Print empty fields
- Print component reference

Buttons on the right side: Close, Help, Print, Preview, Font.



NOTE: By default, empty fields are not printed. To print empty fields, check the **Print empty fields** option.

- 2 Select a sorting criteria from the **Card Index** drop-down list. These are card information fields.
- 3 If you are printing a specific range, check the **Specific range** option. Select the field that will be used to sort the card list. For example, if you select **Card number**, the cards in the list will be sorted according to the card numbers in ascending order. This field can also be used to target a specific range of cards when using the **Lower/Upper boundaries** fields.

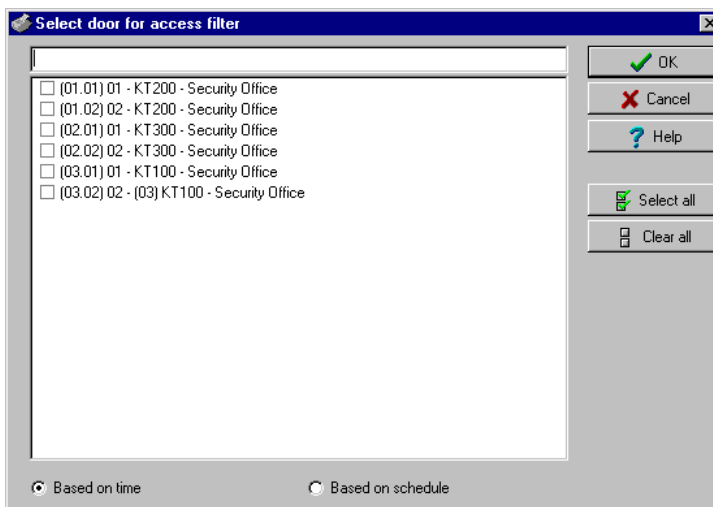
- If you want to print a specific range, you have to specify a starting number in the **Lower boundary** field. It has to be used with the **Upper boundary** field. You must use the “card index field”.
- If you have decided to print a specific range and if you have entered a **Lower boundary** value, enter the last number or letter in the **Upper boundary** field. This field is used with the Lower boundary and the Card Index field.



NOTE: Only cards that match ALL the selected filters will be printed. For example, if you specify six filters, all the six criteria must be met. Cards that do not match all the six criteria will not be included in the range.

- 4 Select the **Filter** option if you do not want the system to search through all the cards of the system. Filters will restrict the search and facilitate the production of the desired card list.
 - **Start date between**—The system will include cards with a “Start date” field which is within the specified range (Miscellaneous tab).
 - **End date between**—The system will include cards with a “Use end date” field which is within the specified range (Miscellaneous tab).
 - **Card state**—Check the option and then select the desired state. The system will include cards that have this card state selected in the Card window (Miscellaneous tab).
 - Select the **Exist trace** for the system to include cards that have the “Card Trace” option in their definition (Card window, Miscellaneous tab).
 - Select the **Exist comment** option for the system to include cards that have information in the **Comment** field in their definition (Card window, Comment tab).
 - Select **Exist PIN**—The system will include cards that have a PIN.
 - Select **Exist delete when expired**—The system will include cards that have information in the **Delete when expired** field (Card window, Miscellaneous tab).
 - Select **Exist wait for keypad** for the system to include cards that have information in the **Wait for keypad** field (Card window, Miscellaneous tab).
- 5 You may also check the **Print selected fields** to include specific data. If you select this field, no other fields below, the system will print the cards that match the filters you specified above with the card number and user name only.

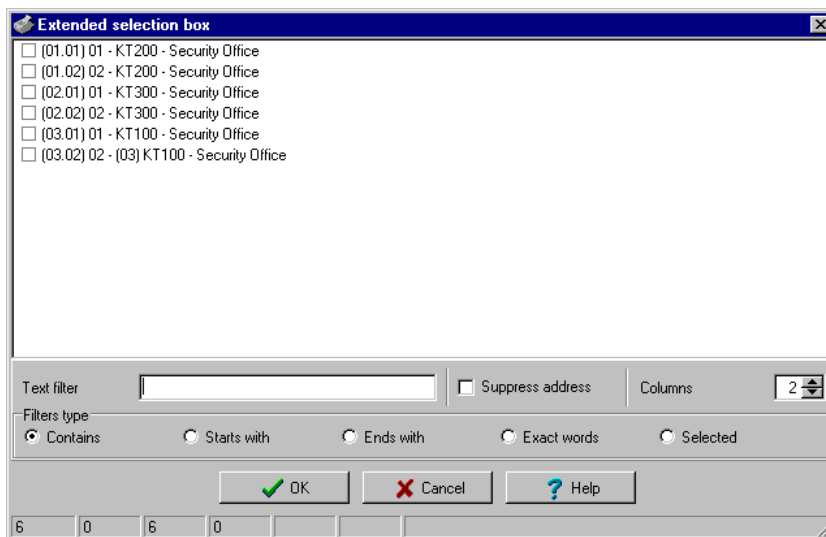
- Click the **Select door access filter** button if you want to include cards associated to a door.



- Select the **Based on time** option if you want to select cards according to the time or select **Based on schedule** if you want to select cards according to a defined schedule.



NOTE: To extend the selection, right click within **Select door for access filter** window.



- Check the appropriate field you want to print. The system will include the field content as it appears in the card definition.

-
- 9 You may save the list as a.QRP file (Quick Report) to view later using the Quick Viewer option.
 - 10 You can also use the “Font” button to use a different font and font size for your list. The changes will appear automatically in the sample box. Use the **Preview** button from the print window to preview your report.

Last Transactions Display

The **View last transactions** feature lets you view the most recent transactions for the selected cardholder. For example, the window will display “Access denied” as the type of event, and will display the date and time as well as the event message that was displayed in the Message desktop. The system displays the 15 most recent transactions for each category:

- Access denied events (bad location, bad access level, bad card status, etc.),
- Access granted events,
- Database events (that have affected the database, such as: card definition modified, relay definition modified, etc.),
- Other/Miscellaneous events (these include events that were generated by cardholders),
- Time and Attendance events (entry, exit).



NOTE: To view more transactions for a specific category, see the “Card use report” option in the menu Historical Report definition menu.

To View the Last Transaction

- 1 From the card definition window, select the **View last transaction** icon.

Type	Date and Time	Event message	Details
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - Administration Works
Access denied	2000-11-02 14:4...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - Administration Works
Access denied	2000-11-14 10:5...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - Administration Works
Access denied	2000-11-14 11:0...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - Administration Works
Database	2000-10-12 17:1...	Card definition modified	Administration Workstation KANTECH
Database	2000-10-12 17:1...	Card definition modified	Administration Workstation KANTECH
Database	2000-10-17 15:0...	Card definition modified	Administration Workstation KANTECH
Database	2000-10-17 15:0...	Card definition modified	Administration Workstation KANTECH
Database	2000-10-24 15:1...	Card position manually modified	Administration Workstation KANTECH

- **Type**—Displays the event category.
- **Date and time**—Displays the date and the time stamp of the event message.
- **Event message**—Displays the event message that was sent when this event occurred. This is the same message as in the Message desktop (Desktop menu).
- **Details**—Displays additional details directly related to the type of transaction. For example, for a “card definition modified” event message, the Details column lists the EntraPass applications from which the card was modified as well as the operator name.

-
- **Refresh**—This button can be used to refresh the window with new transactions as they happen. As cardholders generate events, new information is available.
 - **Parent**—To view the parent component of a selected component. For more information, see *"Basic Functions" on page 37*.
 - **Print**—Use this button to print an exact copy of the window. For more information, see *"Basic Functions" on page 37*.



Card Access Groups Definition

Pre-programmed card access groups allow quick selection of access levels for various sites of the system. This card access group can be recalled during card programming instead of re-entering the access levels for each site.

It is only the card access group information that is associated with the card. Therefore, you can modify the card access group information without modifying the card access information.



NOTE: *When importing cards, the **Card access group** may be used to assign an access level to the cards.*

- 1 From the card definition window, click the access group icon.
- 2 To modify an existing card access group, select it from the **Card access group** drop-down list. To create a new group, click on the **New** button and enter the group name in the language section. The **Site** column displays the site associated with a card access group.
- 3 From the **Access level** drop-down list, select the access level that will determine the access to the doors of the selected site.

Access Levels Definition

Access levels determine where and when the card will be valid. Pre-programmed card access groups allow quick selection of access levels for various gateways. A total of 250 access levels can be programmed per site.

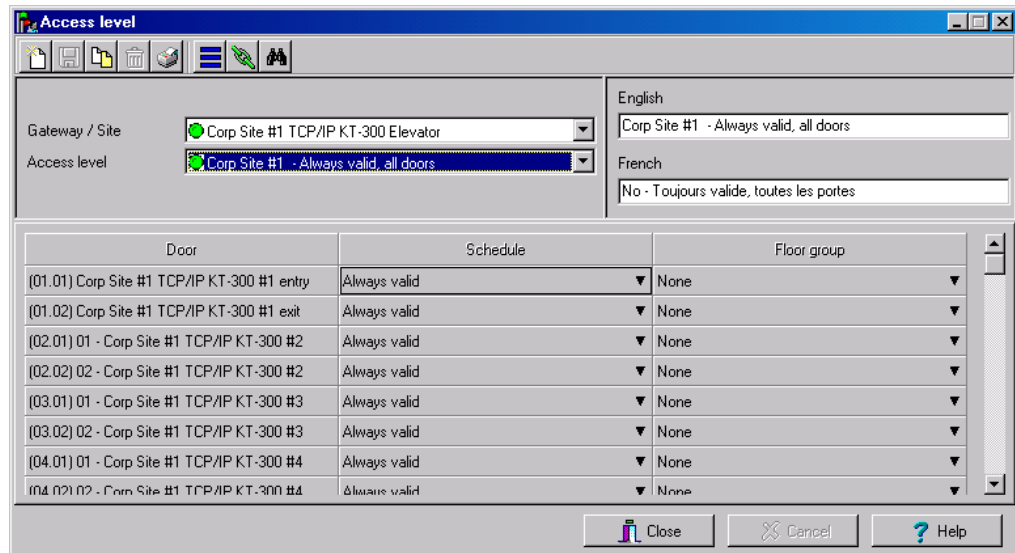
In order to assign an access level to a card, you have to:

- Create schedules that will correspond to the time the user has access to the desired doors
- Assign the created schedule to the desired doors (in the Access level definition menu)
- Assign the access level to a card.



NOTE: The default access level is **Always valid, all doors**: cardholders assigned this default access level have access to all doors at any time. To restrict access to certain doors and at a certain time, you have to create a specific access level.

- 1 From the Users menu, select the **Access level** icon. The Access level window appears.

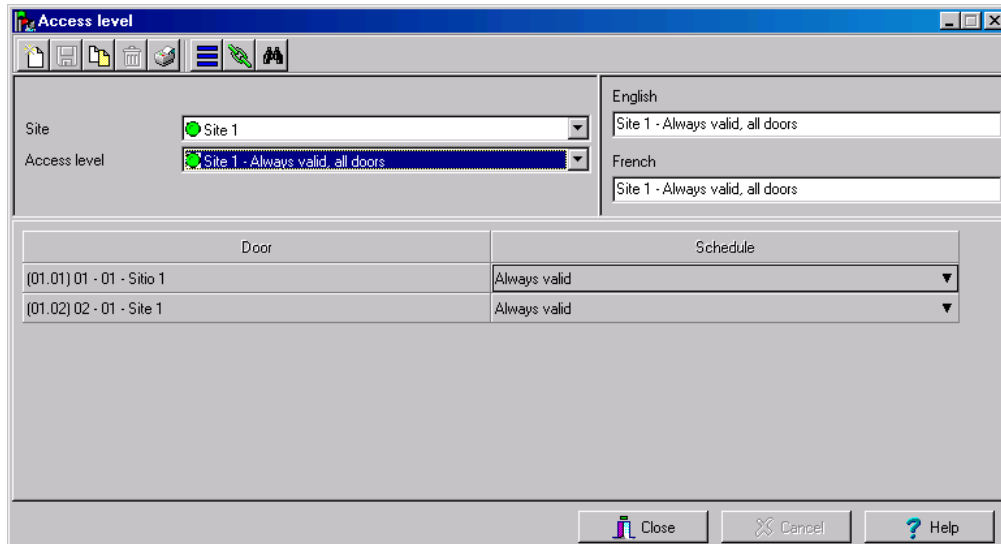


Door	Schedule	Floor group
(01.01) Corp Site #1 TCP/IP KT-300 #1 entry	Always valid	None
(01.02) Corp Site #1 TCP/IP KT-300 #1 exit	Always valid	None
(02.01) 01 - Corp Site #1 TCP/IP KT-300 #2	Always valid	None
(02.02) 02 - Corp Site #1 TCP/IP KT-300 #2	Always valid	None
(03.01) 01 - Corp Site #1 TCP/IP KT-300 #3	Always valid	None
(03.02) 02 - Corp Site #1 TCP/IP KT-300 #3	Always valid	None
(04.01) 01 - Corp Site #1 TCP/IP KT-300 #4	Always valid	None
(04.02) 02 - Corp Site #1 TCP/IP KT-300 #4	Always valid	None



NOTE: You can click the **Hierarchy** button (next to the **Printer** icon) to display the gateway list.

- 2 From the Access level drop-down list, select **New access level**, then assign a meaningful name to the access level you are creating.



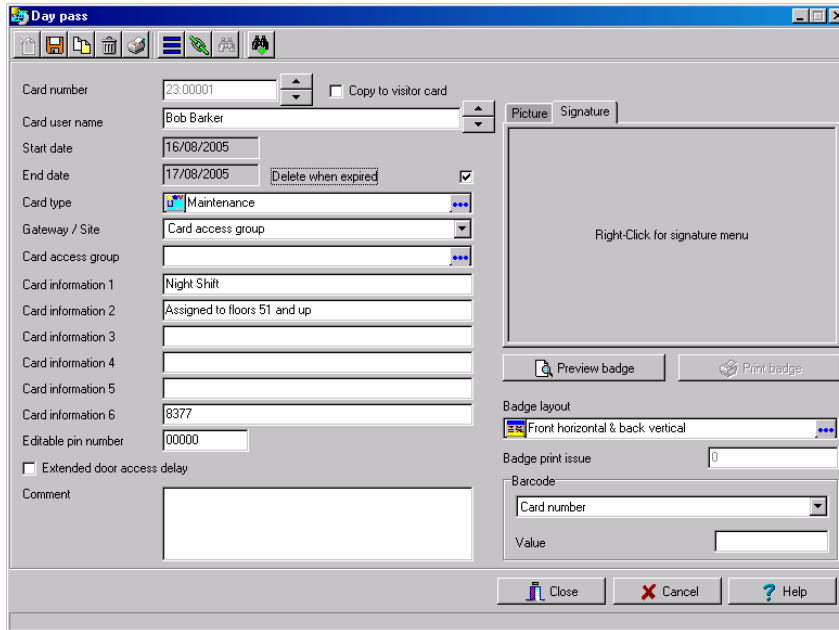
NOTE: Components that are displayed in the Doors, Schedule or Floor group column have to be defined for selection in the Access level definition. To define Doors: **Devices > Sites > Doors**. To define Schedules: **Definition > Schedules**. To define Floors groups: **Groups > Doors**.

- 3 From the Doors list, select the doors to which the cardholder has access.
- 4 From the Schedule column, select the schedule during which the cardholder will have access.
- 5 Select the floor group, if applicable.

To Create a New Day Pass Using the “Save as” Feature

The **Save as** feature allows you to create a new day pass based on an existing one, only making changes to specific information and assigning it new card number. You may, for example, change only the user name and keep all other card information.

- 1 From the **Users** menu, select the **Day pass** icon. The Day Pass window appears.



- 2 To locate an existing card, click the binoculars and select the card you want to duplicate.
- 3 Type required changes into specific fields and click the **Save as** icon.
- 4 You will be prompted for a new card number.

CSV Files Import and Export

The CSV Import/Export feature allows the ability to import or export card files that are saved in a CSV (Comma Separated Value) format. Importing/exporting data between two applications allows the ability to share data.

CSV files can be edited in most applications (Excel, NotePad, etc.).

You will use the CSV Import/Export feature if:

- You are upgrading from EntraPass DOS or WinPass 64 and you want to retrieve the cards created in these previous versions.
- Your company desires to import the card database information into the payroll system. Using the Import/Export feature will save a considerable amount of time in setting up the card holder database.
- Your company has a new database: instead of having to reprogram all the information already available in the card database, the system administrator could export the data contained in the card database (names, departments, card numbers, etc.) into a CSV file that can be imported into the target database.



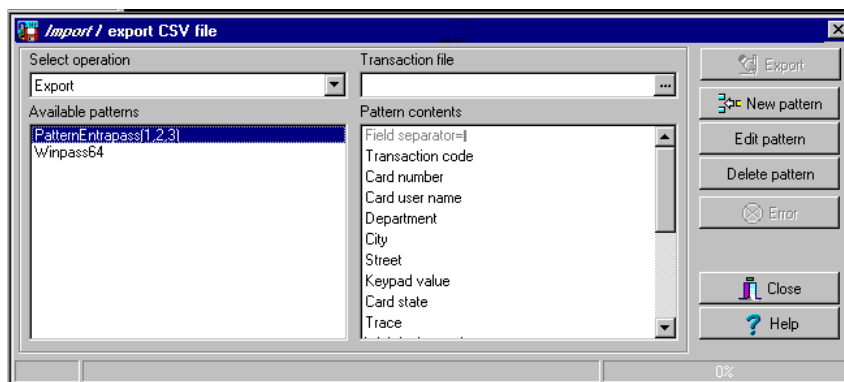
NOTE: The CSV Import/Export feature imposes a number of rules: each field contains a specific value format that has to be respected. For example, the card state field will only accept the following values (0=valid, 1=invalid, 2=stolen/lost).

To Import/Export card information, you may use Kantech pre-defined patterns or you may create your custom patterns. Two patterns are available: the EntraPass (1,2,3) and the WinPass 64 models. You may use the Kantech template “as is” or you may edit it.

To Use a Predefined Pattern

Two patterns are available: the EntraPass (1,2,3) and the WinPass 64 model. You may use the template “as is” or you may edit it.

- 1 From the Users menu, select the **Import/Export CSV** button.



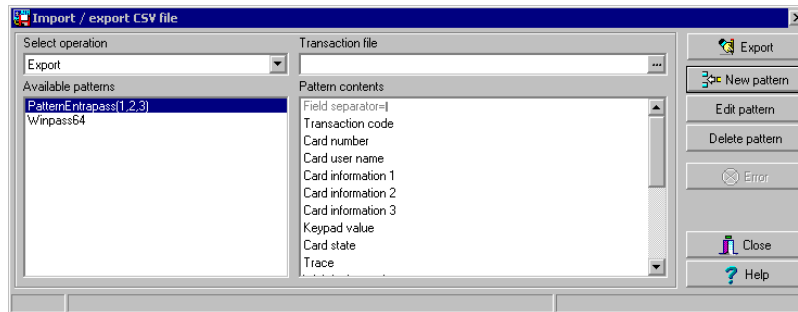
- 2 From the **Select operation** drop-down list, select either **Import** or **Export**.

- 3 In the **Available Patterns** pane, select the pattern you wish to use. This depends on the software you are upgrading from.
- 4 Use the **Edit** button if you want to edit the pattern.

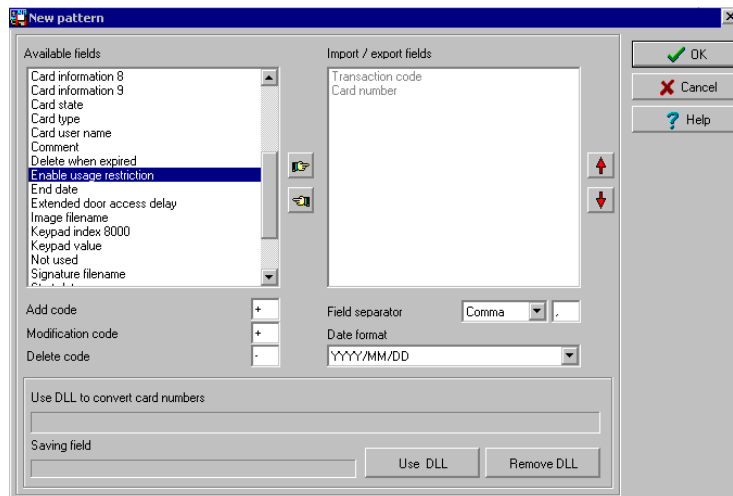
To Create a New Import/Export Pattern

This menu lets you create your own import/export mask that will be used to import or export CSV files.

- 1 From the **Users** menu, select **Import/Export CSV File** icon. The system displays the Import / Export CSV file window.



- 2 From the Import/Export CSV file window, click **New Pattern**. The New pattern window displays a list of all the fields that are available in the EntraPass card databases. They contain specific value formats that have to be respected. For example, the card state field will only accept the following values (0=valid, 1=invalid, 2=stolen/lost).





- 3 Using the **Hand** buttons, select the fields you wish to include in your pattern. The **Transaction code** and the **Card number** fields are displayed by default. Once the fields are selected, you can use the red **Up/down** red arrows to organize information (this will indicate how information will be arranged in the CSV file).
- 4 Specify the **Add code** and **Modification code**. These codes are used by the system to identify, when importing a file, which card has to be modified or added to the card database. Default add code is "+" and default modification code is "+".
- 5 Select the **Delete code**. This code is used by the system to identify, when importing a file, which card has to be removed from the card database. Default delete code is "-".
- 6 Select the **Field separator**. This code will be used to separate the selected fields when importing or exporting data. Usually a comma (,) is selected. Keep this in mind when adding users' last names and first names separated by a commas.
- 7 Select the **Date format**. The date will be exported or imported according to the specified format. The most commonly used format is YYYY/MM/DD.



NOTE: The **Use DLL** feature allows you to enable a program that will convert specific card numbers. You may use the **Remove DLL** when you do not wish to enable the program that converts card numbers.

- 8 Click **OK** to exist the pattern window and to specify the new pattern name.

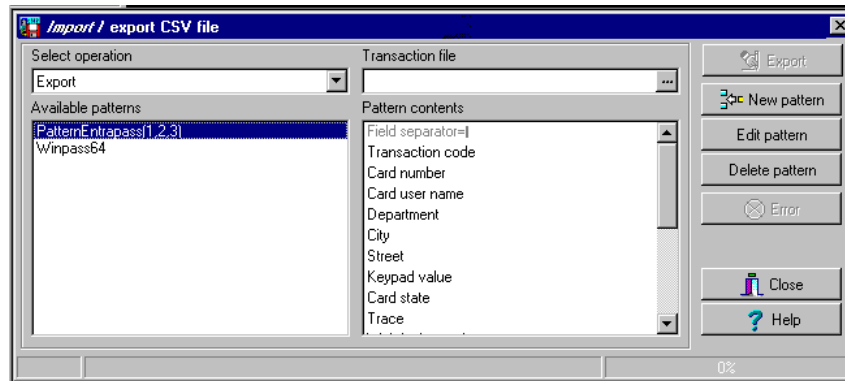
- 9 Enter the pattern name, then click **OK**. The system automatically returns to the Export/Import CSV file window. The pattern you have just created is displayed in the **Available patterns** list.
- 10 If you want to add or remove fields from your pattern, double-click the new pattern to edit and make the necessary modifications. Now you can import or export your information using the new pattern you have just created.

To Export Cards

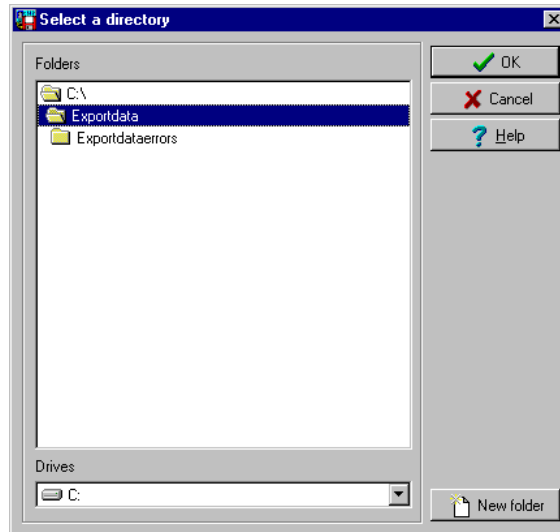
Your organization may need to export the card database data into another application. You may use a predefined template or create a custom template.



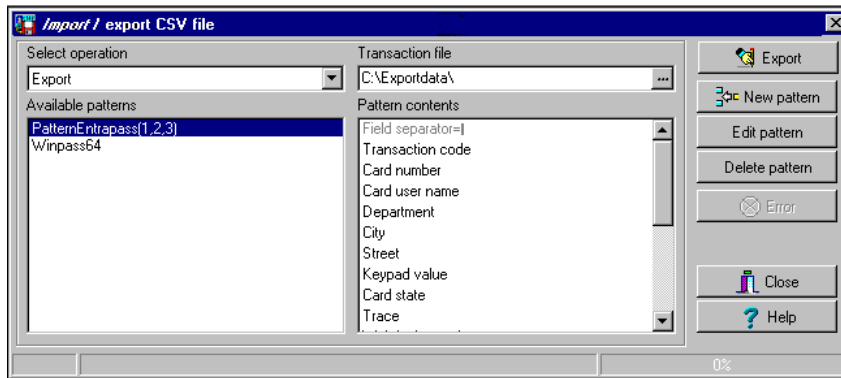
- 1 From the Users menu, select the **Import/Export CSV File** button. The system displays the Import / Export CSV file window.



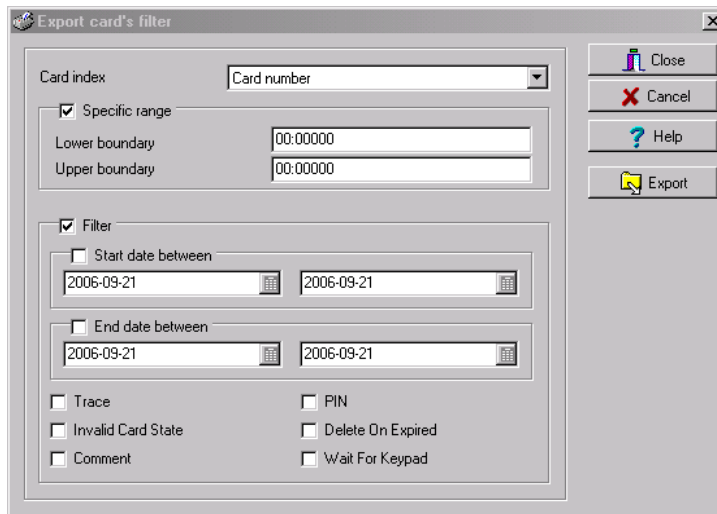
- 2 From the **Select operation** drop-down list, select **Export**.
- 3 From the **Available patterns** list (left-hand pane), select the pattern you want to use when exporting cards. If necessary, you may edit the pattern so that it matches the target application pattern, else, you may create a new one. (For more information on how to create a pattern, see *"To Create a New Import/Export Pattern"* on page 185).
- 4 From the **Transaction file**, select the folder in which EntraPass will save the card database content. You can open the CSV file in Excel, Notepad, etc.



- Once you have selected/created an export folder, click OK to return back to the Import / Export CSV file window.



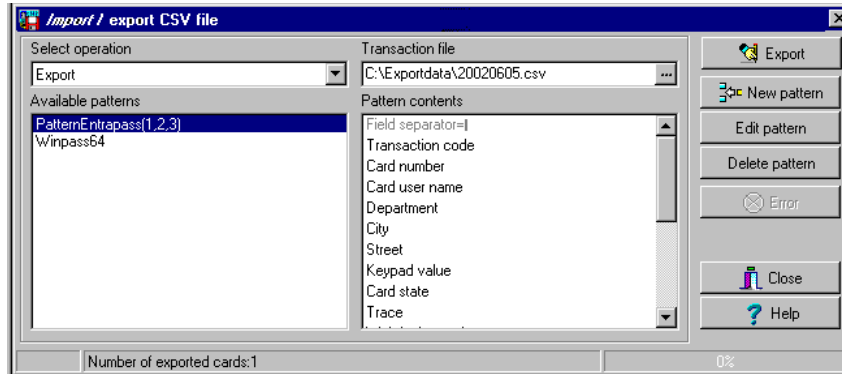
- Click the **Export** button; it is enabled once the transaction file is selected. The system displays a window allowing you to filter the cards you want to export.



NOTE: For cards to be included in your file, they must match all the selected filters, if one or more filters are not matched, the card will not be included.



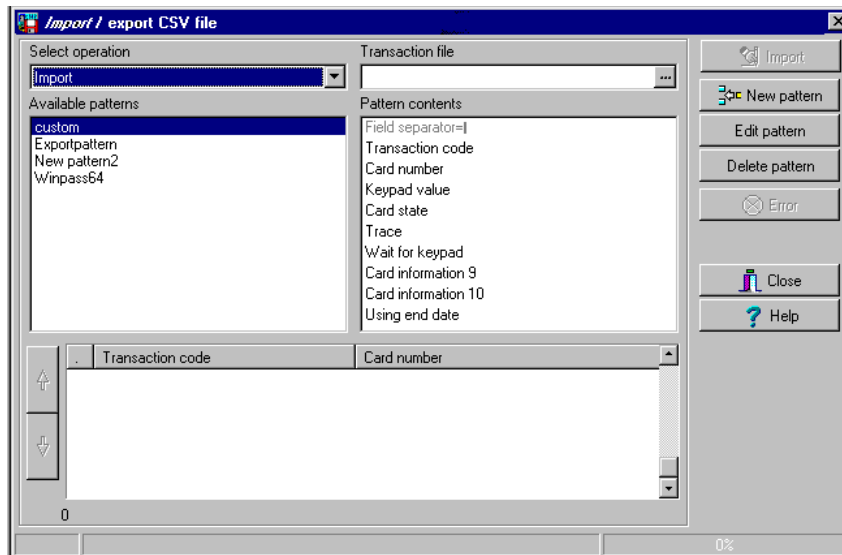
- In the Export Card's filter window, specify the cards you want to export. Once you have made all your selections, click the **Export** button. The Import / Export CSV file window appears.



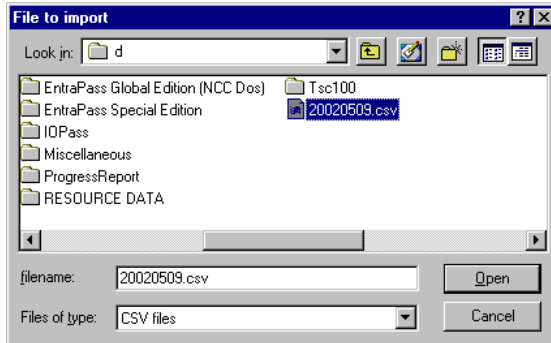
NOTE: The **Transaction file** field shows the target file name and location. By default, the export file is saved in the specified folder (Exportdata, in this example). The status bar (lower part of the window), shows the number of imported cards (1, in this example). The default name is YYYYMMDD.csv. You can open the target file with Notepad for instance.

To Import Cards

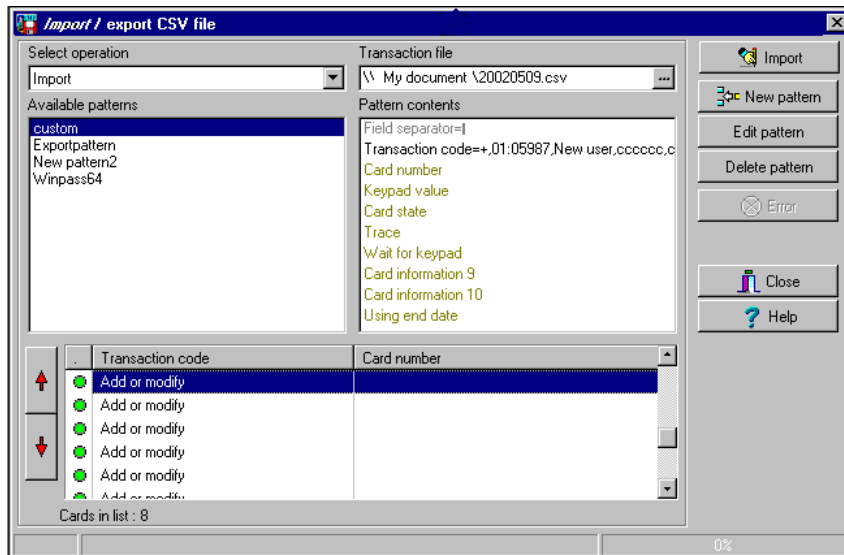
- From the **Users** menu, select the **Import/Export CSV File** icon. Then select **Import** from the **Select operation** drop-down list.



- 2 From the **Available patterns** list, select the pattern that will be used to import the cards information (for more information on how to create a pattern, see *"To Create a New Import/Export Pattern"* on page 185).
- 3 From the **Transaction file** pull-down menu, browse your hard drive to the CSV file that contains the data to import into the card database, then click **Open**.



- 4 Select the **CSV file to import**, then click **Open**. The Import / export CSV file window appears.



NOTE: The system scans the file to be imported; then it displays the results using a color code. Each entry is identified by a color flag. A yellow or red flag identifies an entry in error. Errors are frequently caused by the patterns. You have to select another pattern or edit the pattern you are using so that the pattern entries have to match the source file entries. There may be errors also even if the transaction code is identified by a green flag.



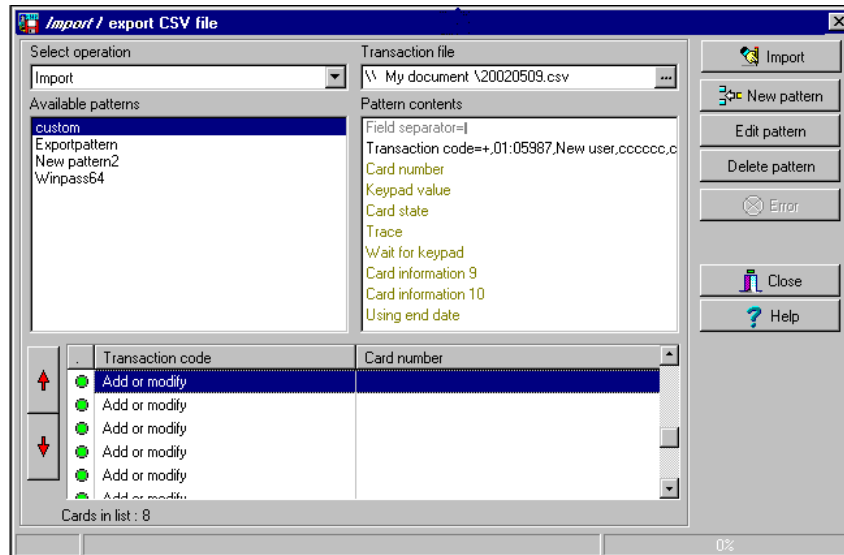
- 5 If no errors are present (or once you have corrected errors), click **Import** to complete the operation.

To Correct Import/Export Errors

The CSV Import/Export feature imposes a number of rules: each field contains a specific value format that has to be respected. For example, the card state field will only accept the following values (0=valid, 1=invalid, 2=stolen/lost). The pattern used has to match the pattern used by the source file.

The present section will assist you in correcting import/export errors.

- 1 Click the **Import or Export** button to start the transaction (the following example illustrates a case of importing CSV data). The lower part of the window displays the number of cards in the list.



NOTE: Although entries in the **Transaction code** column are identified with a green flag, the **Card number** column is empty. This indicates problems in the pattern conversion.

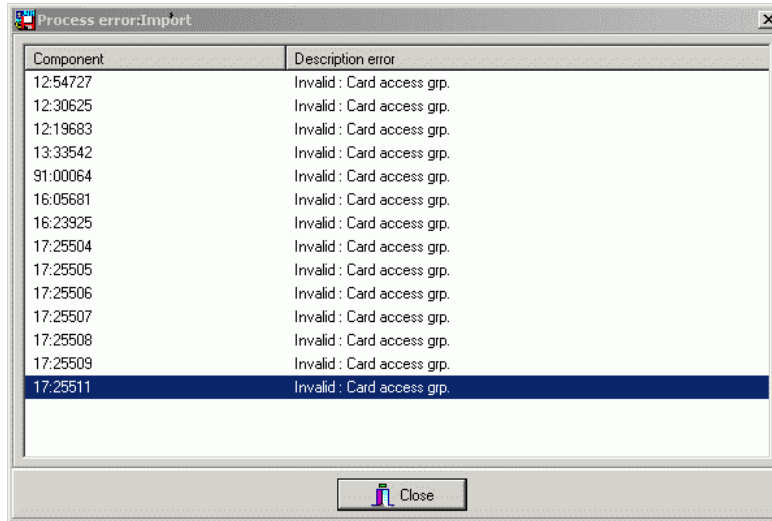
- 2 Click the **Import** button.



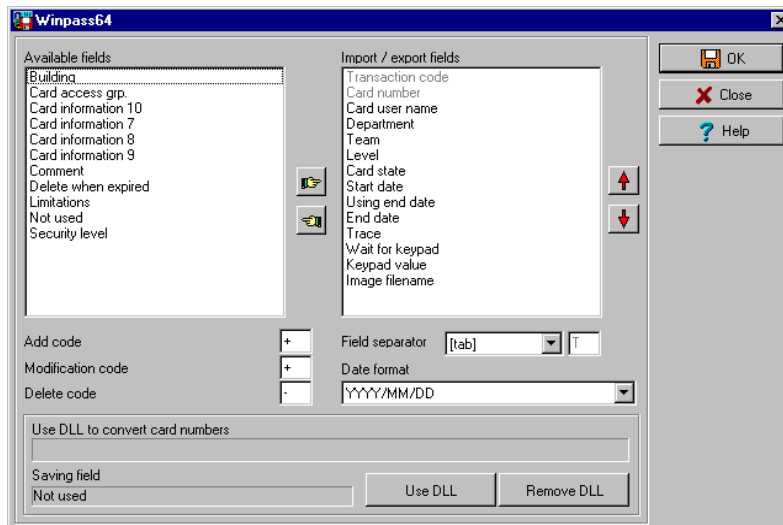
NOTE: The **Error** button is enabled because the system encountered problems during the import transaction.



- You may click the **Error** button to display information about the error. The Process error window shows that the pattern used is invalid.

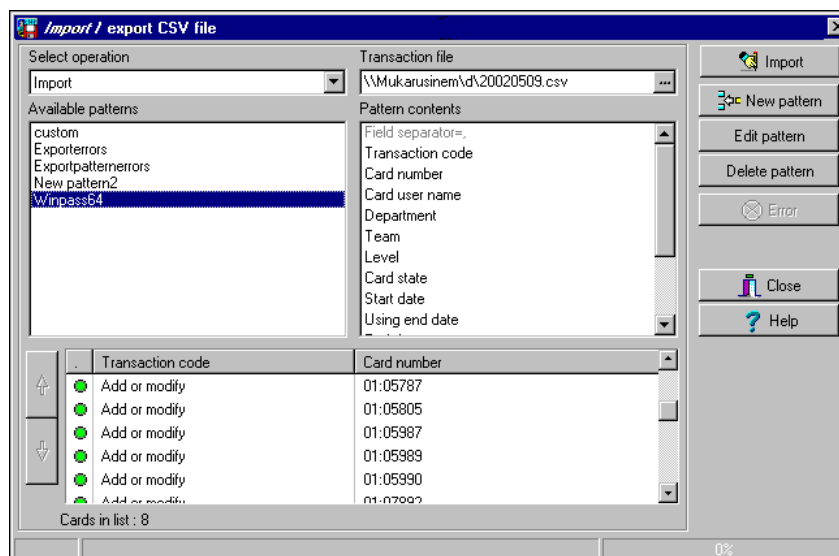


- Click the **Close** button to go back to the Import Export window.
- In the Import/Export CSV window, double-click the pattern you have used for the Import transaction (Custom, in this example).





- 6 From the **Field separator** drop-down list, select **Comma** as the field separator, then click **OK**. The Card number field contains data. This indicates that the import transaction will be successful.





Chapter 8 • Groups

It is useful to create groups so that operators can perform modifications on a group of components or other system functions.



NOTE: *Each system component has to be defined before it can be included in a group.*

You can create:

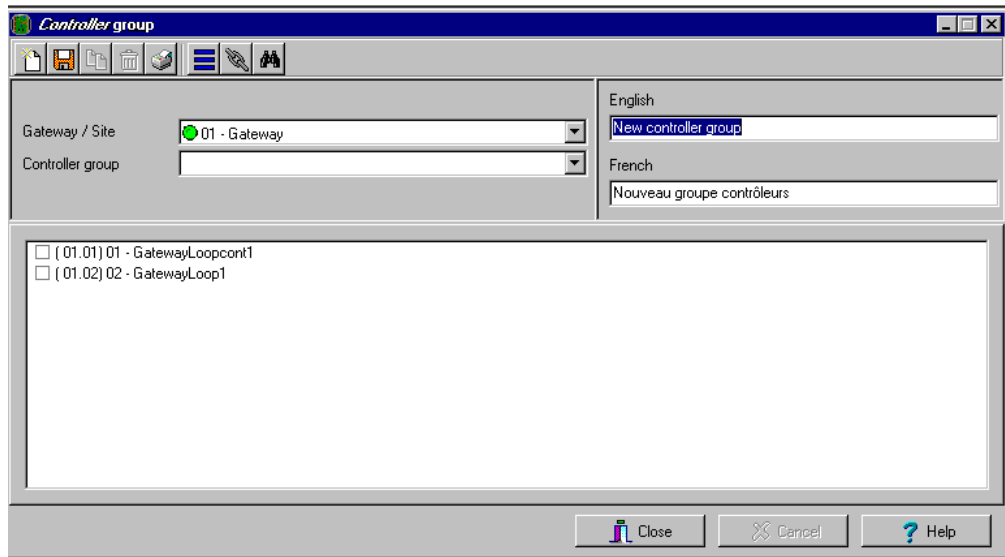
- Controller groups
- Door groups
- Relay groups
- Input groups,
- Access level groups
- Floor groups



Controller Group Creation

The Controller group menu is used to group a number of controllers of the same site. The controller group can later be used to perform manual operations on controllers, for instance (i.e.: reload).

- 1 From the Groups window, select the **Controller** icon.



- 2 Select the **View hierarchy** button to display all the sites defined in the system.
- 3 From the **Gateway/Site** drop-down list, select the site or gateway from which you want to group controllers.
- 4 To create a new group of controllers, click the **New** icon. To modify an existing group, select one from the **Controller group** drop-down list, then enter the necessary information in the language section.
- 5 From the list of controllers connected to the selected site, check the controllers that are to be assigned to the group.

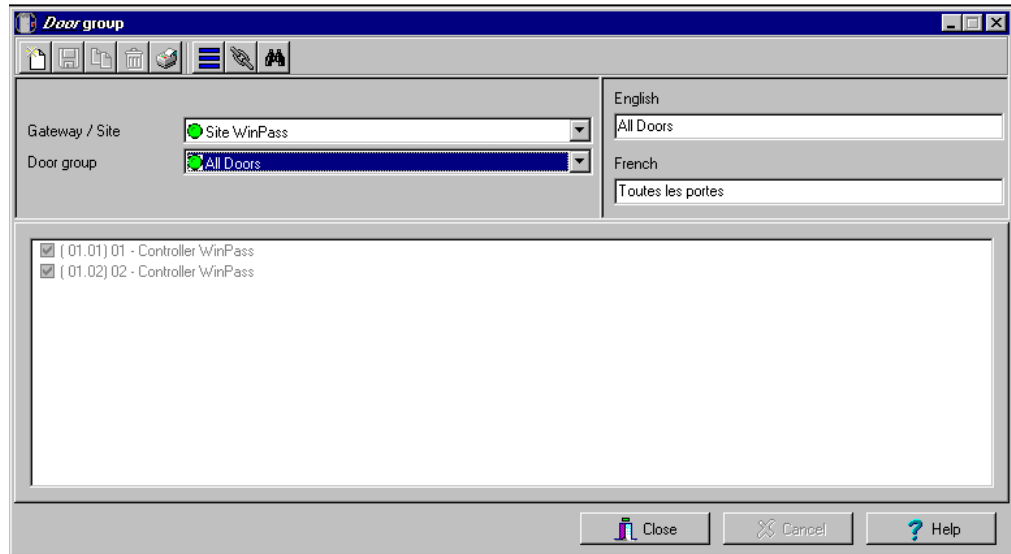


NOTE: For more information on controllers, see "Controllers Configuration" on page 66

Door Group Creation

The Door group menu is used to group doors of a specific site. The door group can later be used to carry out manual operations such as unlocking a group of doors.

- 1 From the Groups window, select the **Door** icon.



- 2 Select the **View hierarchy** button to display all the sites defined in the system.
- 3 From the **Gateway/Site** drop-down list, select the site or gateway from which you want to group doors.
- 4 From the **Door Group** drop-down list, select a door group you want to modify or click the **New** icon to create a new group, then enter the necessary information.
- 5 From the **Door list**, select the doors that must be assigned to the group.



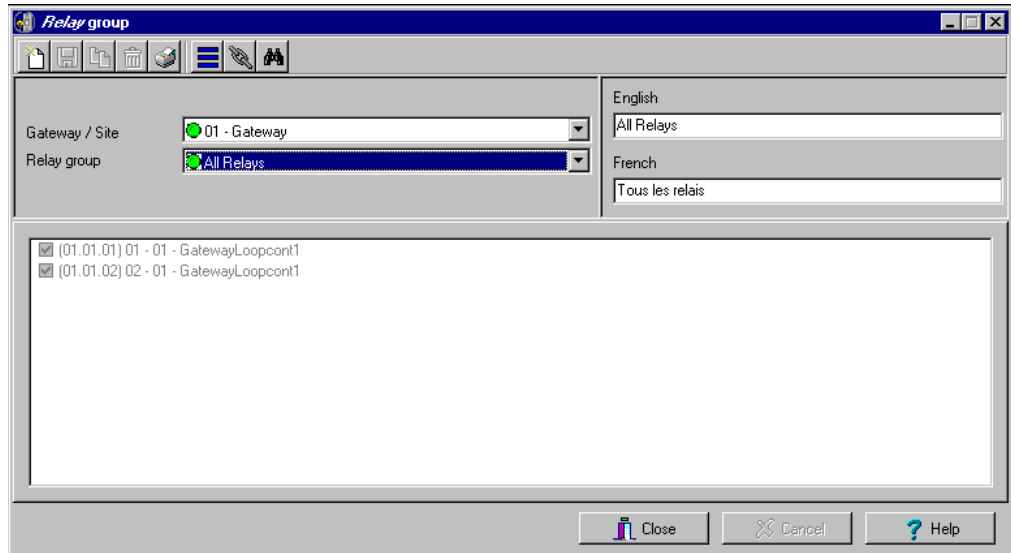
NOTE: For more information on doors, see "Doors Configuration" on page 81.



Relay Group Creation

The Relay group menu is used to group relays of a specific site. This relay group can later be used to carry out manual operations such as temporarily activating relays.

- 1 From the Groups window, select the **Relay** icon.



- 2 Select the **View hierarchy** button to display all the sites defined in the system.
- 3 From the **Gateway/Site** drop-down list, select the site or gateway from which you want to group relays.
- 4 From the **Relay** group drop-down list, select a relay group or click the **New** icon to create a new group; then enter the necessary information in the language section.
- 5 From the **Relay** list, select the relays that must be assigned to the group.



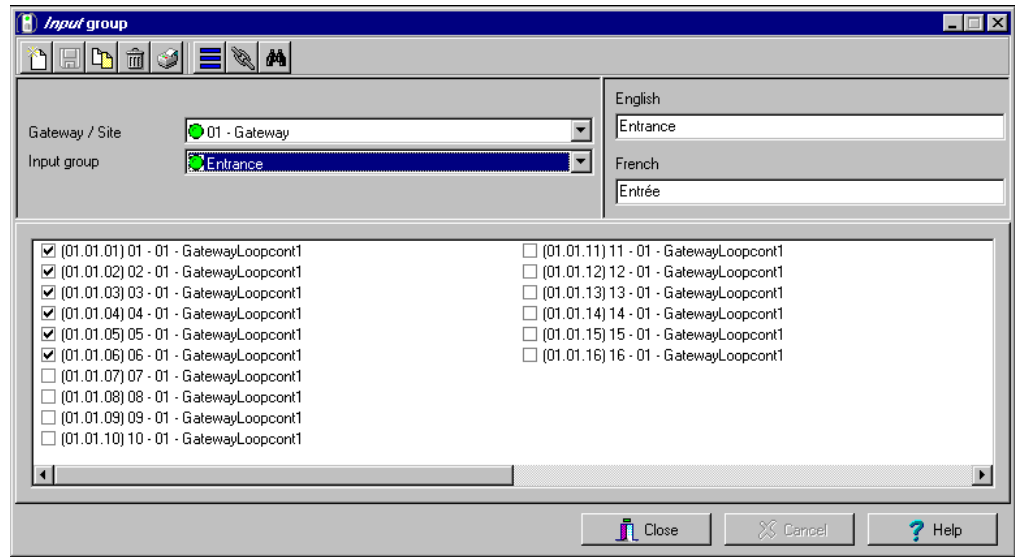
NOTE: For more information on relays, see "Relays Configuration" on page 90.

Input Group Creation

The Input group menu is used to group inputs of a controller site.

This input group can later be used to carry out manual operations such as shunt on inputs.

- 1 From the Groups window, select the Input icon.



- 2 Select the **View hierarchy** button to display all the sites defined in the system.
- 3 From the **Gateway/Site** drop-down list, select the site for which you want to group inputs.
- 4 From the **Inputs** group drop-down list, select an existing group to modify it, or click the **New** icon to create a new group; then enter the necessary information in the language section.
- 5 From the **Inputs** list, select the inputs that must be assigned to the group.



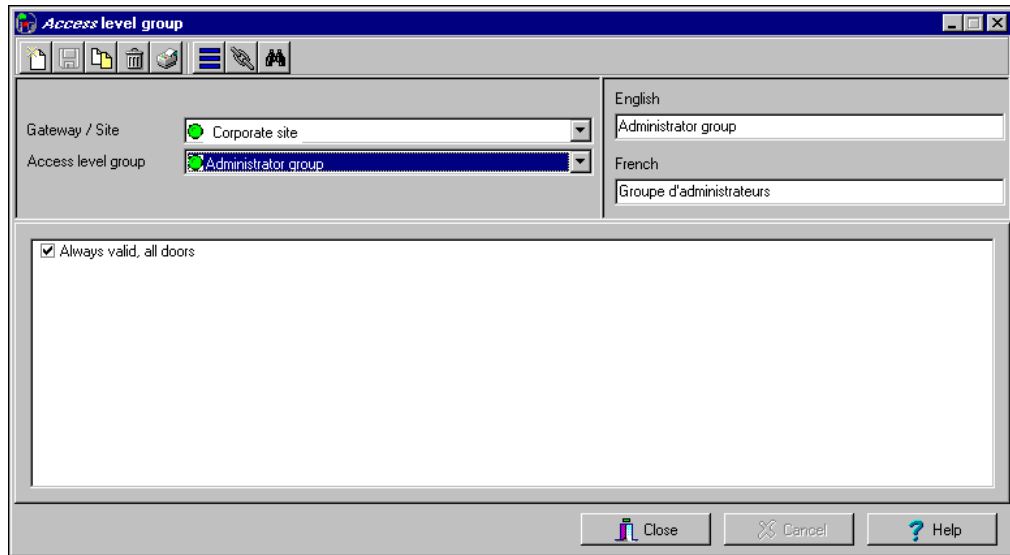
NOTE: For more information on inputs, see "Inputs Configuration" on page 91.



Access Level Groups Grouping

The Access level group dialog is used to group access levels of the same site.

- 1 From the Group window, select the **Access level group** icon.




- 2 Select the **View hierarchy** button to display all the sites defined in the system.
- 3 From the **Gateway/Site** drop-down list, select the site or gateway from which you want to group access levels.
- 4 Click the **New** button to create a new group access level, and assign a name in the **English** field.
- 5 Check the boxes that correspond to the access level group.

Floor Group Creation

This menu is used to group the floors that were created in the floor definition menu. Floor groups are also used for various operations in the system such as: manual operations (unlocking schedules), access levels, etc.

- 1 From the Groups window, select the **Floor/Elevator door** icon.

Floor	State	Schedule
Floor #01	<input checked="" type="checkbox"/>	24/7
Floor #02	<input type="checkbox"/>	None
Floor #03	<input checked="" type="checkbox"/>	24/7
Floor #04	<input type="checkbox"/>	None
Floor #05	<input checked="" type="checkbox"/>	24/7
Floor #06	<input type="checkbox"/>	None
Floor #07	<input checked="" type="checkbox"/>	24/7
Floor #08	<input type="checkbox"/>	None

- 2 Select the **View hierarchy** button to display all the sites defined in the system; then from the **Gateway/Site** drop-down list, select the site or gateway from which you want to group the floors.
- 3 From the **Floor group** drop-down list, select an existing group if you want to modify it; or click the **New** icon  to create a new group. Then enter the name of the group in the language section.
- 4 From the list of defined floors that is displayed by the system, check the **State** column for the Floors you want to include in the group. Only floors that have the **State** field selected will be enabled when:
 - A manual unlock operation is done, or
 - An “input” is programmed, for example, as a push button to enable floors for visitors (**Devices > Input** definition menu > **Elevator** tab),
 - Cardholders present their card to the card reader to enable floor selection when the controller is operating in stand-alone mode (due to communication failure). Only the floors marked with an “X” are available for selection.
- 5 Only floors that have **State** selected will be enabled when:
 - A manual unlocking operation is done, or
 - An “input” is programmed, for example as a push button to enable floors for visitors (input definition menu - elevator tab),



-
- Cardholders present their card at the card reader to enable floor selection and the controller is operating in “stand-alone” (due to communication failure). Only the floors marked with an “X” will be available for selection

Chapter 9 • System Status

The **Status** menu allows system operators to view the status of various devices and components of the access system:

- The **Text** button allows operators to view, in text, the status of EntraPass applications, sites, controllers (KT-100, KT-200, or KT-300), doors, relays, inputs. The status displayed depends on the controller installed.
- The **Numerical** button allows operators to view the statistical status of all components, by gateway. For example, you can view the number of inputs in an alarm.
- The **Graphic** button allows operators to display the graphic status of a controller.
- The **Database** button provides information on the database structure. In addition, an operator can perform configuration operations or manual commands from the database window.

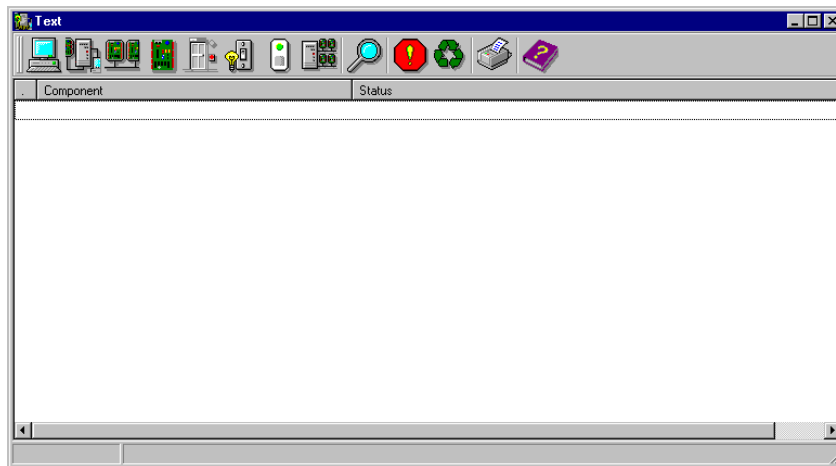
Text Status

The **Text status** allows an operator to display the status of a selected component (and sub-components) as well as all the characteristics associated with this component in a text form. This menu option applies to all the system devices: applications, gateways, sites, controllers, doors, relays and inputs. The text window contains additional buttons/icons that assist operators in their tasks:

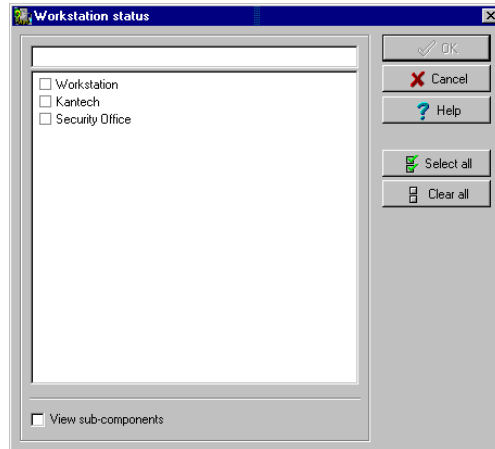
- The first eight buttons represent system devices (Workstation, Gateway, Site, Controller, Door, Input, Output and).
- **Summary / Detailed list**—The magnifying glass icon is used to display components that are not in normal condition. It displays a summary list or a detailed list.
 - Summary: shows the components that are not in normal condition
 - Detail: shows all the components in any condition.
- **Stop display**—This button is used to stop the display when the information is taking too much time. It cancels or interrupts the process.
- **Refresh**—Refreshes the status of the selected components.
- **Print**—Use this button to print the displayed status. You can preview your report before printing it.

To Display a Component Status

- 1 From the Status window, select the **Text Status** button. The **Text status** window appears.



- In the Text window, select the icon of the component for which you want to view the status. If you select the **Workstation** icon, the system displays the list of the EntraPass Applications defined in the system.



- You can check the EntraPass application you want to display the status or enter a few characters of the component name (field at the top) for the system to searched in the database. For example, you can enter “Sec” for Security Office. The system will highlight the first name containing the entered characters. You may also click the **Select all** button to select all the EntraPass applications; or select specific components by clicking in the checkboxes next to each component name. The **Clear all** button removes the check marks from the selected components. Click **Cancel** to return to the previous window without any selections or changes.
- You may check the **View sub-components** box (lower part of the window) to display detailed information on the sub-components linked to the selected component. For example, if you selected a controller, all its components (doors, relays, inputs) with appropriate status will be displayed on the window if this option was checked. For more focus in one window, filter doors, relays or inputs by site.
- Click **OK** to return to the previous window and apply your selections.



NOTE: The **Magnifying glass** button is used to display components that are not in normal condition. When it is in a “summary” position, only components that are not in normal condition will be displayed; the “detailed” position, displays a full status of all components.



Numerical Status

This menu allows an operator to view the number of components in a “not normal” state for a selected gateway.

To View the Numeric Status of a Specific Gateway

- 1 In the Status window, select the **Numerical status** button. The **Numerical** window appears.

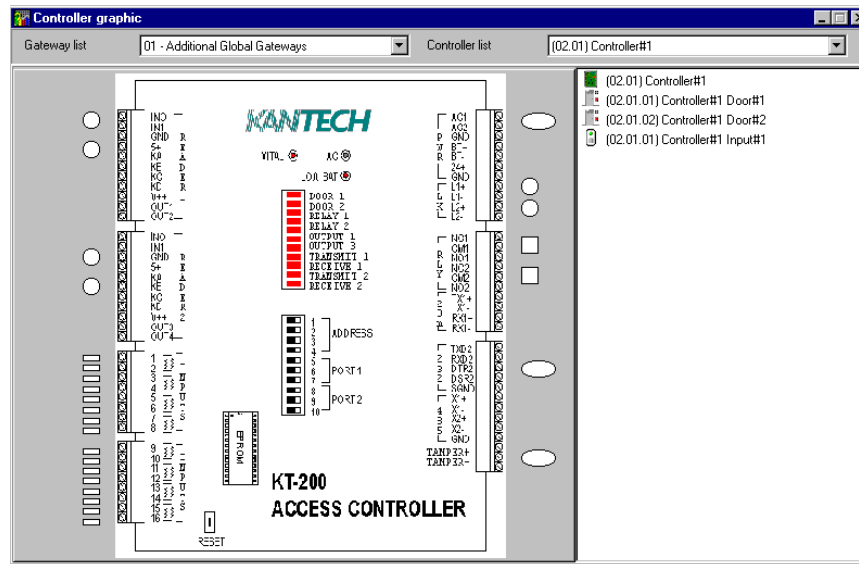
Graphic Status

This feature is used to display a graphical status of a door controller, including the status of all its components (outputs, inputs, power supply status, communication status, etc.) represented by colored shapes (circle, square, etc.).

- An ellipse shape represents the controller
- A circle represents a door
- A square represents a relay
- A rectangle represents an input. Rectangles may be horizontal (KT-200 and KT-300) or vertical (KT-100).

To View a Controller Status

- 1 From the **Gateway** drop-down list, select the gateway on which the controller to display is located. You may select “All gateways” to display all the controllers in the list.
- 2 From the **Controller** drop-down list, select the controller for which you want to display the status.



NOTE: The displayed graphic depends on the type of the controller selected.

- 3 To find out which items are represented by a colored shape, move the mouse over a colored shape. The item highlighted on the right-hand (in the list) identifies the component.
- 4 Select a controller from the **Controller list** drop-down list (right side of the window), double-click the item on which status is required.
 - **Red**—The component is “Supervised” and “in a trouble state”.
 - **Green**—The component is “Supervised” and “in normal condition”.



- **Yellow**—The component is “Not Supervised” and “in a trouble state”.
- **Gray**—The component is “Not Supervised” and “in normal condition”.
- **Blue**—The relay is activated (by an event or an operator).



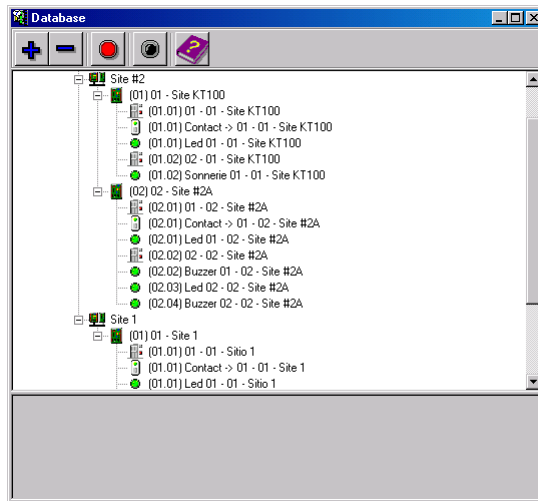
NOTE: *If there's more than one controller site per gateway, the numbers between parentheses (xx) indicates the controller number and the following numbers (xx) indicate the component number.*

Database Status

This window displays the status of the components within the database while browsing the database structure. The system displays all applications (connected or not), the gateway, controller sites, etc. You can also perform manual operations directly from the window and edit components in order to modify their configuration.

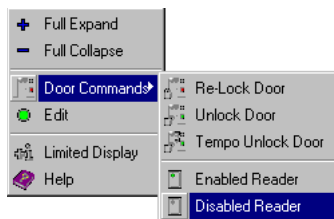
To View Information About the Database

- 1 From the Status window, select the **Database** icon. The Database window appears.



NOTE: The icon identifies the type of component.

- 2 In the Database window, select the application you want to view the database. The lower part of the window displays the actual status of the selected component as well as its full name.
- 3 Select a component to modify its definition directly from the Database window. For example, if you have selected a door, right-click the door to display a shortcut menu.
- 4 Select a command in the cascading sub-menu; select a menu option.



NOTE: The command list varies according to the selected component.



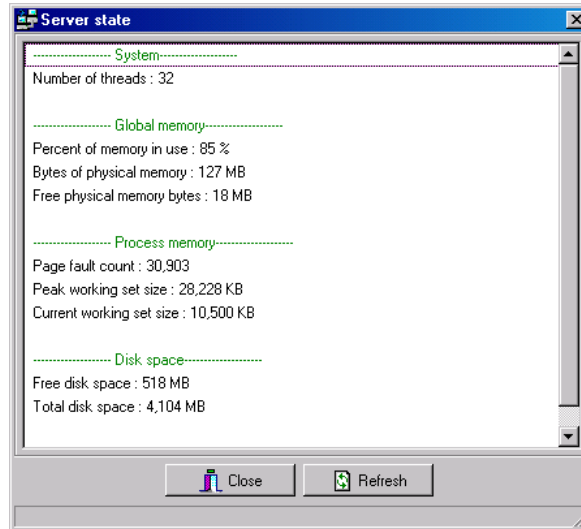
- 5 Make your modifications to return to the Database status window. The **Right-click** shortcut menu offers the following options:
- **Full expand**—This feature allows you to fully expand the tree status and view all components. Only applications that are connected to the server will display a “+” sign.
 - **Full collapse**—This feature allows you to fully collapse the tree status and hide all components of the root component.
 - **Edit**—When you select an assigned component (i.e.: input) and click edit, the system will edit the definition window so you can modify its definition and when finished, return to the window you edited the component from.
 - **Limited display / No limited display**—When you click on a physical component, the bottom part of the window displays its status.
 - By selecting **Limited display**, the system will erase the previous status and display the status of the next selected component.



NOTE: *The icons on the left side components indicate the component type.*

Server State

The Server state dialog allows users to view detailed information on the server such as system information, system global memory, system process memory and system disk space.





Chapter 10 • System

Use the **System** menu to define parameters for systems operators, security levels, event parameters, instructions, and message filters. This menu allows you also to view the EntraPass database structure.

You will define system parameters as follows:

- **Operator:** user name, login name, password settings for EntraPass operators
- **Security level:** use this menu to grant or deny access permission on system logical and physical components
- **Event parameter:** use this menu to define priority, color, schedule (display, printing schedule, acknowledgement) for system events
- **Instruction:** use this menu to create instructions for alarm messages
- **Message filter:** Use this menu to direct event messages from a specific EntraPass application to another EntraPass application and to define sort criteria for messages that are sent to the Filtered Message desktop.
- **Database structure:** Use this menu to display EntraPass physical and logical components and to edit or sort system components.

Operators Definition

Use the **Operator** menu to define system operators and to determine their security level and privileges. An operator is responsible for issuing cards, carrying out manual operations on system components, requesting reports, arming the system, etc.

For security reasons, each person using and accessing the system database should have his/her operator defined to ensure that each action performed in the system will be traceable. You need to create at least one operator account or modify the pre-created accounts in order for the operator to use and operate EntraPass and to receive event messages.

There are three default operators created in the system. These are associated with three levels of access rights:

- Installer (login name and password are kantech): Full access to view, modify, delete, print components.
- Administrator (the login Kantech1 and the password kantech): Medium access with limited access to system menus.
- Guard (login Kantech2 and password are kantech): Limited access to system menus.



NOTE: You can define operators using the default operators or you can create new operators. For details about operators' security levels, see "Security Level Definition" on page 217.

To Create or Edit an Operator

- 1 From the **System** tab, select the **Operator** icon to open the Operator window.



NOTE: The upper right-hand corner shows the last EntraPass workstation where the operator logged on and the last login date for the operator who is logged on.

- 2 Enter the operator name in the **Name** field. The operator name is composed of a maximum of 40 alphanumeric characters (including spaces).



- 3 Enter the operator **Login name**. This is a descriptive name composed of 6 to 20 alphanumeric characters (including spaces).



NOTE: On login, operators must enter their login name followed by their password in order for the system to validate their access. The login name is displayed in the events' details when operator events are generated (i.e. manual operation, login, logout, etc.).

- 4 In the **Password** field, enter the password that will be used to login with the login name. The password is alphanumeric and consists of a maximum of twenty characters (minimum seven characters). The password is not displayed nor printed, the system displays the password as asterisks.



NOTE: The password is **case-sensitive** - make sure that all operators are aware of this.

- 5 In the **Password Confirmation** field, enter the operator password again for confirmation using the proper case. If this password is not identical to the one entered in the password field, an error message will appear.
- 6 In the **Language** section, check the appropriate option for the display language for this operator. If you change the display language, it will be effective only when the operator logs out and logs in again. When an operator logs out and exits an application, the next operator who logs on the application will see the startup window in the language of the last operator.
- 7 In the Privileges section:
 - Select the **Auto acknowledge** option. If this option is selected, the **Manual** button is added to the Alarms desktop (see "Entrapass Desktops" on page 239). The operator can decide to manually or automatically acknowledge events. This is an operator privilege.
- 8 Click on the **Security** tab to set operator access parameters.

- 9 From the **Login Schedule** pull-down menu, select the schedule during which the operator will be allowed to login into the system. You may want to create a specific schedule for an operator (**Definition > Schedule**), and then assign the schedule to the operator.



- 10 From the **Security Level** pull-down menu, select a security level that will determine which components an operator has access to. A security level consists of menus through which an operator can modify the database, create components, view system components and events, etc.



NOTE: *It is possible to define up to 250 custom security levels; the system offers 3 built-in security levels (Installer, Administrator and Guard) on configuration. The default configuration for Installer permits access to all system commands. The Installer must program other security levels to limit operator access to menu commands and/or options.*

- 11 Access the **Security** section to edit the security features of the currently displayed operator profile:
- **Operator disabled:** use this feature if you want to suspend or limit an operator access. If you select an operator and then check this box, the selected operator will not be able to run the application.
 - **Change password at next log on:** use this feature if you want an operator to change his/her password at next log on.
 - **Disable operator on bad password:** use this feature to limit the number of retries on bad password. For example, if you set this number to three (3), the operator will be disabled after three errors when entering his/her password.
 - **Days before password is reset:** this feature allows to manage operators' passwords. At the end of the number of the days specified in this field, the operator will be prompted to change his/her password.
 - **Use expiration date:** this feature allows you also to manage operators' password. When this feature is checked, you have to select an expiration date (Operator expiration date).
 - **Operator expiration date:** used with the **Use expiration date feature**, the **Operator expiration date** allows you to disable an operator's access at a specified date.



NOTE: *Changes to the currently displayed profile will take effect at the next log on attempt.*

Security Level Definition

Security levels refer to the permissions granted to an operator to modify the database, create items, view components, print lists or reports, etc. There are three default operators and security levels. It is possible to customize an operator security level; the system allows you to create up to 250 security levels.



NOTE: *You have to program the appropriate security levels if you want to limit operator access to commands and/or options of the system menu.*

Each default operator has a separate login name, password and a corresponding security level. The password is case-sensitive. These are: Installer, Administrator and Guard.

- **Installer:**
 - **Login name and password:** kantech
 - **Security level:** By default, a user defined as Installer has full access to all the system menus. He/she can read and edit system components and has unrestricted access to the system.
- **Administrator:**
 - **Login name:** kantech1; password: kantech
 - **Security level:** Administrator. By default, a user defined as Administrator has limited access to a number of the system menus.
- **Guard:**
 - **Login name:** kantech2; password: kantech
 - **Security level:** Guard. By default, a user defined as Guard has limited access to the system menu.

To Create/Modify an Operator Security Level

Assigning security levels is critical to the system. In fact, if a Security level is given full access to a system menu, operators who are assigned this security level can modify system parameters. Make sure that each operator is given the security level corresponding to his/her tasks.

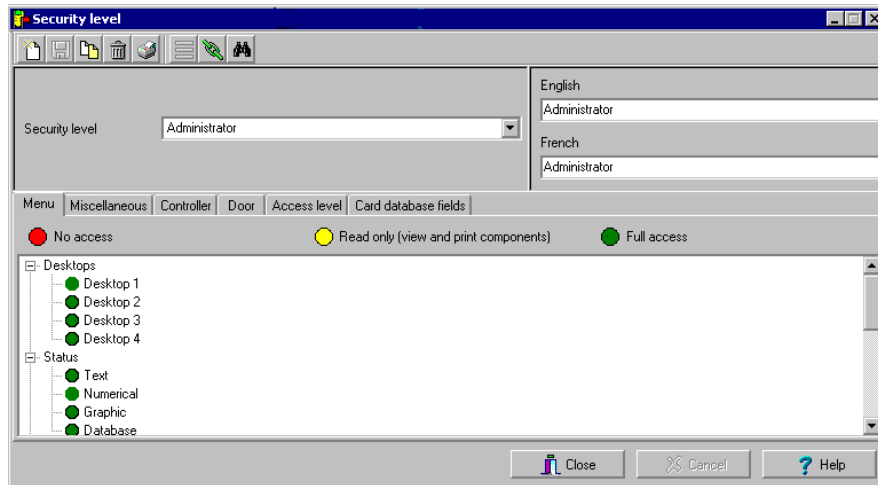
Items in the Security Level window are presented in a root tree with all components available for selection. This structure makes it possible to target specific components when granting security level for manual operations.

Each security level is identified by a color: full access (green), read-only (yellow) and no access (red). The security manager or an operator with appropriate permissions can easily change or assign a component to a lower level security level by double clicking an item until it changes to the desired color code.



NOTE: *Operators will not be able to see items for which they have not been given access.*

- 1 From the **System** main window, select the **Security level** icon. The Security level window appears with the **Menu** tab enabled.



- 2 To modify a security level, select one from the **Security level** drop-down list. To create a new security level, click the **New** button and enter the necessary information in the language section.
- 3 In the **Menu** window, double-click an item to make it **No access** (red), **Read-only** (yellow) or **Full access** (green). You can specific components when granting security level for manual operations

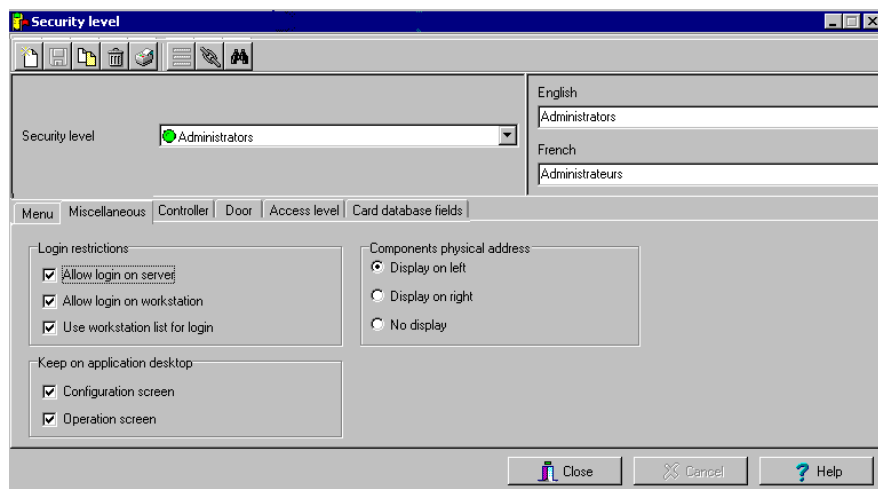
To Define Login Options for an Operator


The **Miscellaneous** tab allows you to define operator login and system display options:

- Operator login options: you can allow or restrict an operator to log on an Entrapass workstation
- Active windows that can be kept on the desktop: Entrapass allows operators to keep two active windows on the desktop
- Component display options: components can be displayed with or without their physical address. The physical address can appear on the left or right of the component name.



- 1 Select the **Miscellaneous** tab to define other parameters for the Security level being defined. These include login restrictions and viewing parameters.



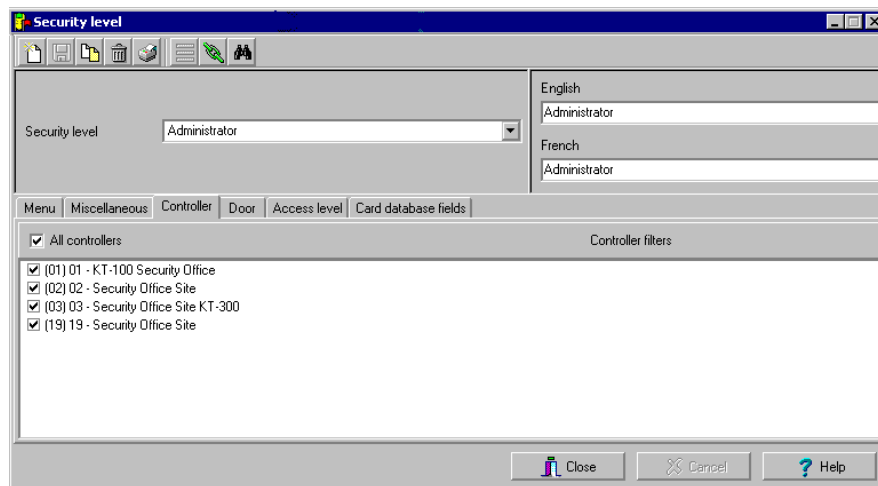
- 2 In the **Login restrictions** section, select the appropriate login options:
 - Select **Allow login on server** to allow the operator to log onto the an Entrapass server
 - Select **Allow login on workstation** to allow the operator to log onto the system. To narrow down the list of authorized applications, use this option with the **Use workstation list for login** feature. This option is checked by default when a new operator is created.
 - Select the **Use workstation list for login** option to restrict the number of authorized applications for an operator. If selected, the operator will only be allowed to log onto the workstations that are selected in the **Entrapass application** tab. The **Allow login on workstation** option must also be selected.
 - 3 The **Keep on application desktop** section allows users to increase the number of active windows on the desktop. In fact, operators can open two windows at the same time. Entrapass windows are classified in two categories:
 - **Configuration screen:** this group includes all the menus that allow an operator to program the system. This group includes such menu items as: User menu (card, Badging, card access group, access level, Definition menu; Group menu; Devices menu; System menu; Historical and Time and attendance reports.
 - **Operation screen:** this group includes all the Operation menu items.
-  **NOTE:** These options allow operators to keep active four operation windows on the desktop. They can bring to front or send to back the window they want to display, simply by pressing ALT-F6.
- 4 In the **Components physical address** section, specify how the component's physical address will be displayed for the security level being defined. This will also affect how components will be sorted.

- **Display on left**—If selected, components will be sorted by their address (i.e. 01.01.01 Controller xyz).
- **Display on right**—If selected, components will be sorted by their component name (i.e. Controller xyz 01.01.01).
- **No display**—If selected, the address will not be displayed (i.e. Controller xyz) and components will be sorted by name.

To Filter Controllers Available to an Operator

EntraPass allows you the ability to assign to a security level Controllers that will be available for view. To do so, you must select the Operator security level, then select the Controllers tab and check controllers that you to be available for the selected security level.

- 1 From the **Security level** drop down list, select the security level you want to define.



- 2 From the Security level window, select the **Controllers** tab to assign controllers to the selected security level. The selected controllers will be available for viewing or editing to the operator who is assigned this security level.

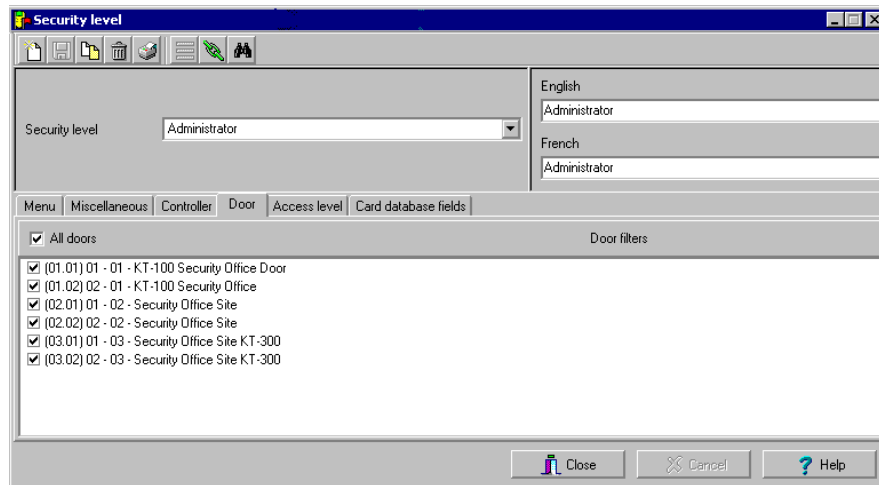


NOTE: When you select a controller, you also select all the components defined “under” or related to the controller (i.e. doors, relays, inputs, outputs).

To Filter Doors Available to an Operator

EntraPass allows you the ability to assign to a security level Doors that will be available for view. To do so, you must select the Operator security level, then select the Controllers tab and check controllers that you to be available for the selected security level.

- 1 From the Security level drop-down list, select the security level you want to define/modify, then select the **Door** tab.



- 2 Select **All doors** if you want all the displayed doors to be available to the operator assigned this security level when modifying doors, relays, inputs, etc. or performing modifications/operations related to controllers. You can also select only the doors you want from the displayed list.



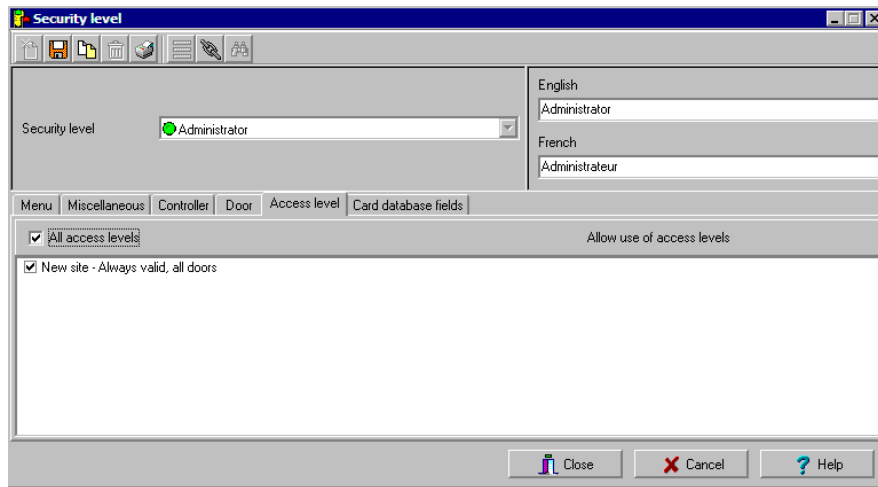
NOTE: Make sure that you have also selected the controller for which the selected door is defined. If the controller is not selected, the door will not be available even if it is selected in the list.

To Filter Access Levels

Associating specific access levels to a security level allows you to control the access levels that an operator can define or modify. For example, a security guard may have the right to issue cards that are valid for a given door or access level only.



- 1 From the Security level drop down list, select the security level you want to define/edit.

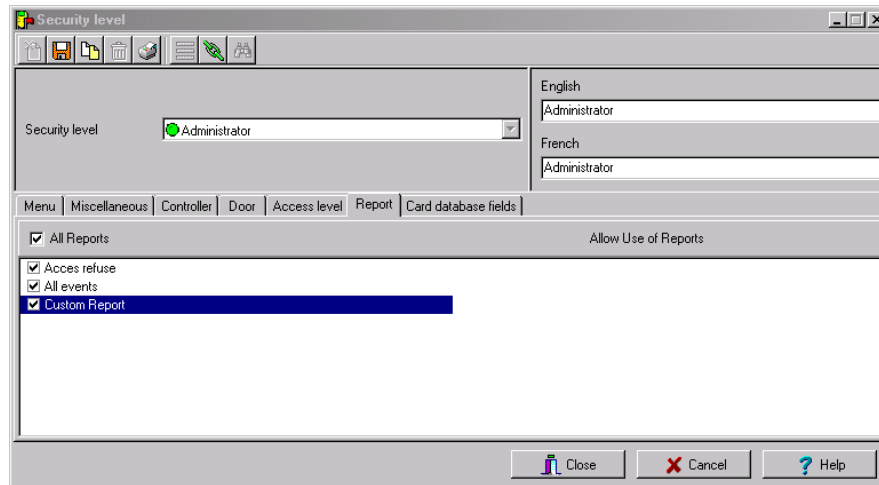


- 2 Select **All access levels** if you want all the displayed access levels to be available to the operator assigned this security level when creating cards or performing modifications related to access levels. You can also select only the access levels you want from the displayed list.

To Filter Reports Available to an Operator

This feature gives operators access to specific reports according to their security level. For example, a System Administrator may have access to all the reports that can be generated whereas the Guards' Supervisor may only have access to all Guard Tour related reports. The reports will be generated from the **Archived Message list** on the workstation desktop. Once the reports have been assigned to security levels, operators will only have access to reports that correspond to their security level.

- 1 From the Security level drop-down list, select the security level you want to define/edit.

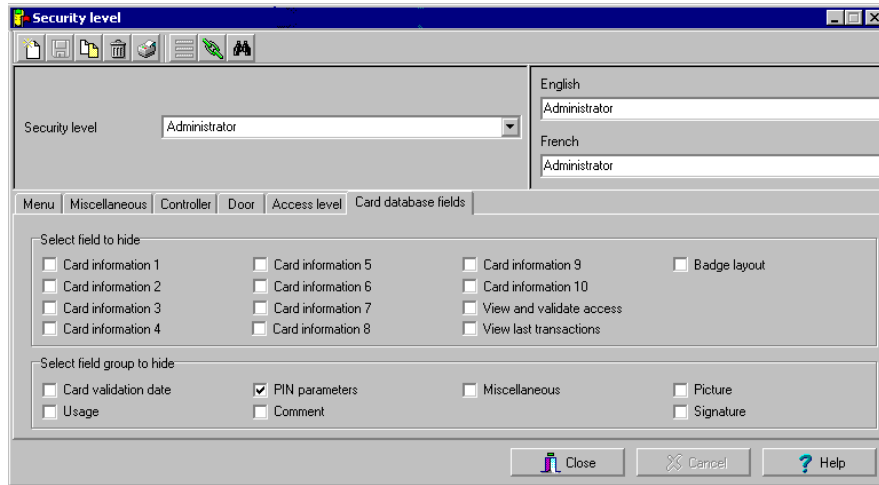


- 2 In the **Report** tab, select the reports you want to assign to the selected security level. Or, check the **All reports check box** if you want to give full access to all reports to the operator assigned this security level.

To Hide Card Information

Entrapass offers you the ability to hide card information fields from view. For example, you can decide that a certain security level (Guard for example) will not modify card information field. To do so, select the security level, then in the Card database fields (Security level), select fields you want to be hidden.

- 1 Select the **Card database fields** tab to limit the number of card fields which are visible to the operator who is assigned this security level.



- 2 Select the fields (either individually or in groups) that will be hidden to the selected security level. In the example above, operators who will be assigned the Guard security level will not see the selected fields.

Event Parameters Definition

Defining event parameters is one of the most powerful features of the system. For each event, you can determine how it will be processed by the system. For example, you can:

- Direct events to output devices (such as Messages desktop and log printer),
- Define schedules that will allow, for example, to send alarms only at night

There are more than 400 system events including:

- Access granted
- Input in alarm
- Card modified by operator, etc.

Events are associated with system components, such as doors, controllers, etc. Every event message is associated with a system component and output devices or group of devices. For example, an *Access granted event* can be defined for each individual door or by default it can be defined for all doors. This flexibility allows for different actions or responses on a door-by-door basis.

To Define Events Parameters

The **Event parameters** dialog allows you to customize your system events. In fact, you can specify events that will be printed automatically or acknowledged during a specific schedule. You can also send instructions to inform an operator of an alarm or through other media (i.e. e-mail, pager, etc.) when alarms are generated.

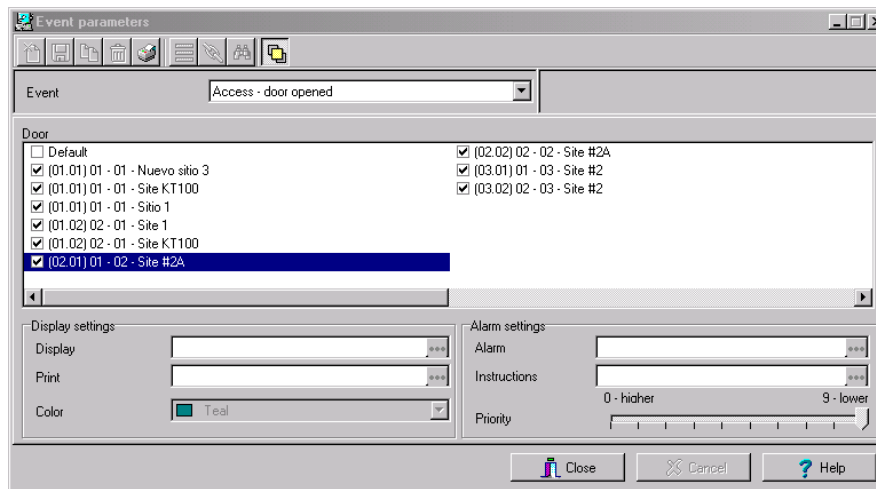
By default, all events are defined to be displayed on all the Message desktops. You can customize your system events by manually associating events and components.



There are two types of associations: manual and default association. For details about associations, see *"To Create and View Associations"* on page 227.



NOTE: *Manual associations take priority over default associations. When you define a manual association between an event message and a component, the default association is ignored. It can be restored by deleting the manual association.*

- 1 From the System main window, select the **Event** parameters icon.



- 2 From the **Event** drop-down list, select an event for which you want to define settings.
 - 3  *By default, all events are defined to be sent to the Messages desktop with an always valid schedule. It is recommended to keep default settings especially when these settings apply to all components/events.* In the **Display settings** section, specify the display options: by default, all events are programmed to be displayed in the Messages desktop window. By default, they are assigned an **Always valid** schedule.
 - 4 From the **Print** pop up-down menu, select a schedule to determine when the event will be printed. When this schedule is valid, the selected event will be printed on the printer to which it is being sent.
-  **NOTE:** *You must also select a printer and specify if the printer should print messages or alarms, or both. For more information, see "Basic Functions" on page 37.*
- 5 From the **Color** drop-down list, select the color that will be used to display the event in the Message desktop. The default colors are set according to the following convention:
 - **Red** for alarm events;
 - **Green** for elements returning to a normal condition;
 - **Yellow** for warnings and errors;
 - **Blue** for other events.
 - 6 In the **Alarm Settings** section, specify:
 - **Alarm (schedule)**—When this schedule is valid, the event will be sent to the Alarms Desktop and will require an acknowledgement from the operator.
 - **Instructions**—Select the instruction that will be sent to the Instruction desktop with the event to be acknowledged. Instructions will only be sent when the alarm schedule is valid.

- 7 Assign the **Priority** level to the event. This determines the sequence in which alarms messages will be displayed to the operator in the alarm queue. The priorities are preset to the most common values (0 = higher, 9 = lower).

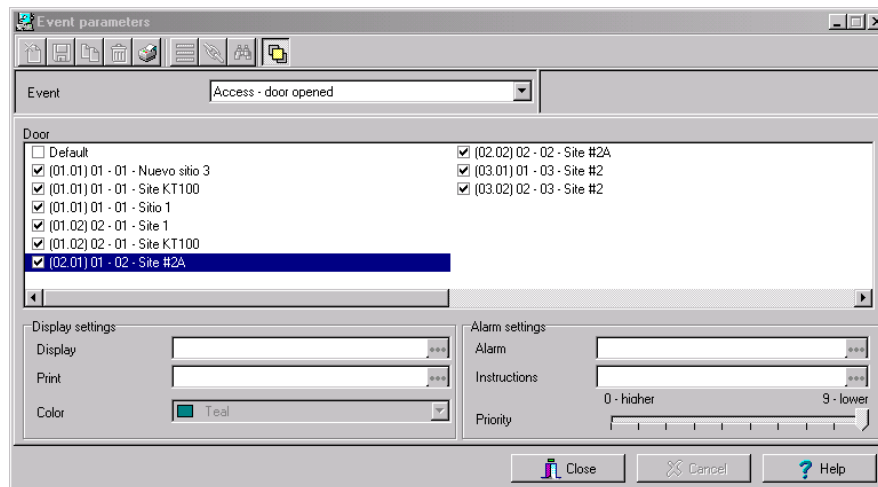
To Create and View Associations

There are two types of associations:

- **Default.** The default associations are preset in the system. By default all events messages occur on all components associated with them. You may keep the default settings. However, EntraPass offers you the ability to create manual associations.

Creating an Association

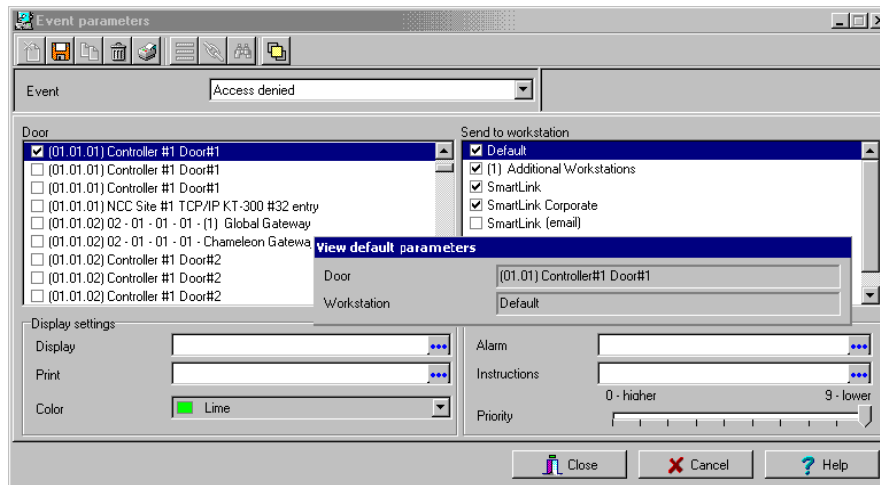
- 1 In the Event parameters window, select an event from the **Event** drop-down list. From the component pane select a component.



- 2 Click the **Save** icon to create the new association. In this case, *All access - Door opened* events that will occur on the selected door will be sent to the message desktop.

Viewing an Association

- 1 In the Event parameters window, select a component from the left-hand pane.



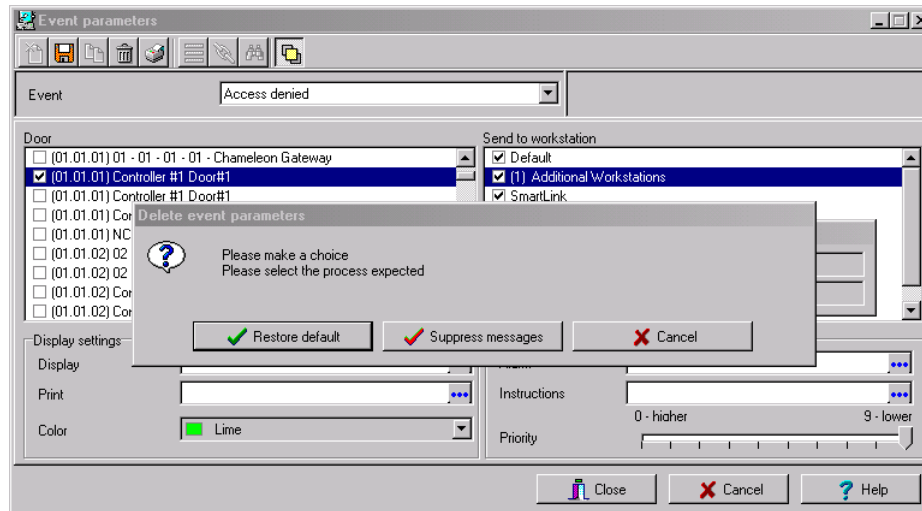
- 2 Click the **View association** icon in the toolbar. The View default parameters message box shows the component and EntraPass application.
- 3 You can click the **Delete** icon in the toolbar if you want to modify the displayed association.

Deleting and Restoring Associations

You may decide that events from Door 1 should no longer be sent to the Message Desktop, but to a specific desktop. To do this, you have to delete the existing association and then create a manual association. It is recommended to use this feature with caution.

- 1 In the Event parameters window, select an event message from the Event drop-down list.
- 2 From a component, then click the association icon. The View default parameters message box appears.

- 3 Click the **Delete** icon in the toolbar.



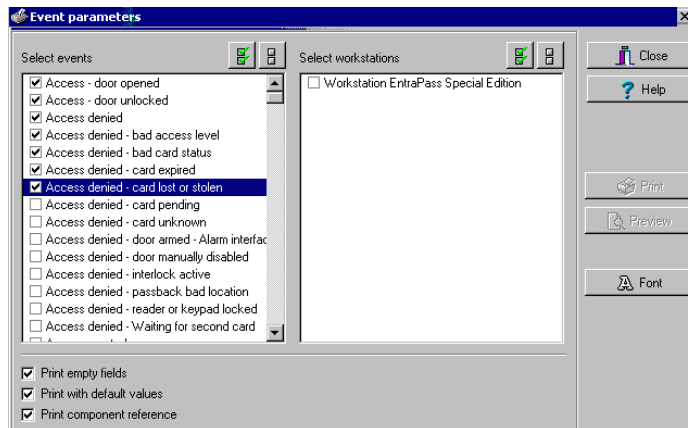
- 4 From the Delete event parameters window, make your choice:
- **Restore default:** this option will apply the default alarm and display settings.
 - **Delete association:** if you select this option, the alarm and display settings fields will be left blank and ready for new information. Once you have deleted the settings, you must re-define them.
 - **Cancel:** select this option if you want to cancel the delete operation.

To Print Event Parameters

Entrapass allows you to print events parameters (alarm and display settings) for the selected events.

You can also use the **Font** button to choose a different font (and font size) for your report.

- 1 From the Event parameters window, select the **Printer** icon.



- 2 In the **Select events** pane, select the events to be included in your printout or click on the **Select all** button to select all the events from the displayed list.
- 3 In the **Select applications** pane select the EntraPass workstation to be included in your printout or click on the **Select all** button to select all the EntraPass workstations from the displayed list.
- 4 You may check the **Print empty fields** option in the bottom of the window. If selected, the system will print the fields that do not contain any information. Only the field title will be printed.
- 5 You may check the **Print with default values** option. If selected, the system will print the default associations as well as manual associations.
- 6 You may check the **Print components reference** option. If selected, the system will print the component physical address next to the component identification.



NOTE: If you **do not** select this field, only manual associations (not involving defaults) will be displayed in the report. If you do not have manual associations (component x with event y), the report will be empty.

- 7 Select the **Preview** button before printing, if desired.

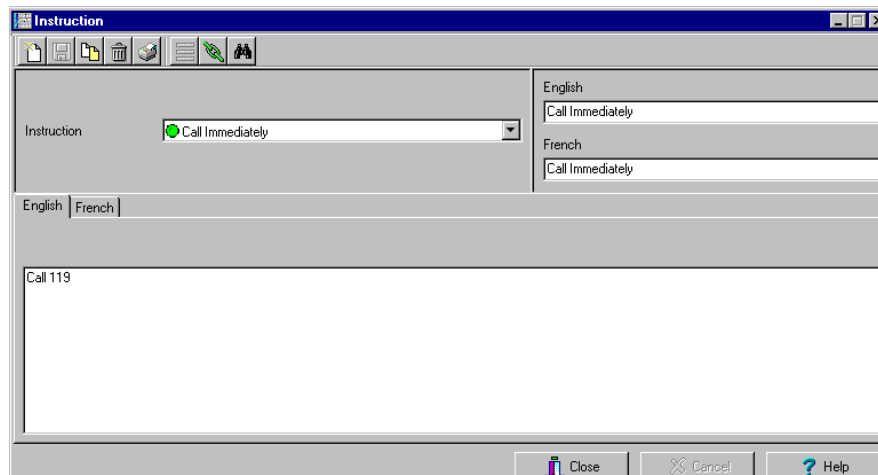
Instructions Definition

This menu is used to define instructions that must be assigned to events. When an alarm is generated, the instruction will display in the Instruction window (Desktop menu) for acknowledgement.

Usually, each line will contain a single directive; the response instructions will be composed of several directives (lines). This allows for greater flexibility when modifications are required.

To Define an Instruction

- 1 From the **System** main window, select the **Instruction** icon.



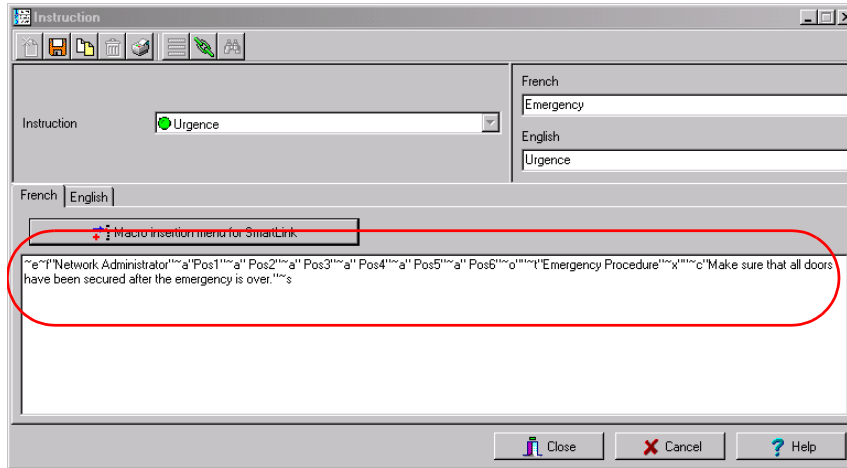
- 2 To create a new instruction, click the **New** icon. To modify an existing instruction, select one from the **Instruction** drop-down list.
- 3 Enter the instruction name/identification in the language section.
- 4 Select an appropriate language tab to enter the instruction. Instructions are entered in one selected language.



NOTE: You may enter up to 511 characters (including spaces) per instruction.



5 To assign instructions to events, see *"Event Parameters Definition"* on page 225.





Message Filters Definition

The Message filter feature allows you to define filters for the Filtered Messages desktop. These filters are used to view a specific selection of events. For example, you may define specific filters for an operator: a Guard may be only interested by “Guard tour events”. You can then create filters so that only guard tour events are sent to the Guard’s Entrapass workstation.

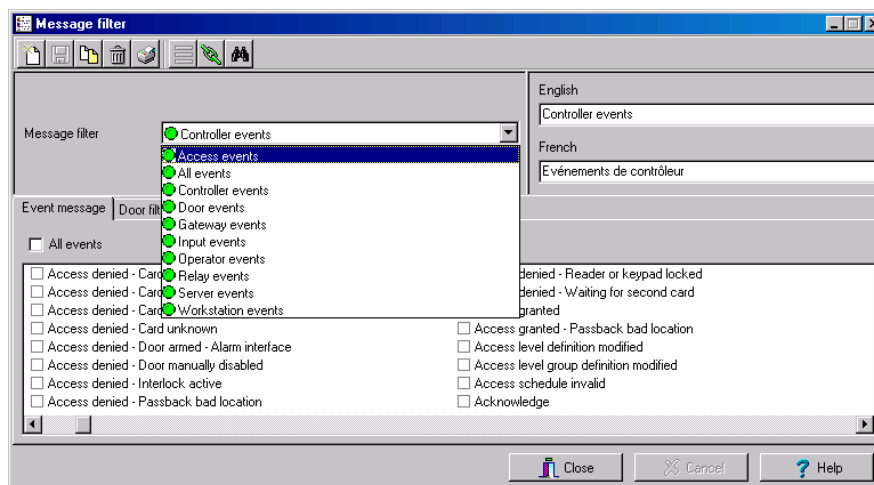
There are many pre-defined filters such as: access events, controller events, etc. These filters can be accessed by all operators. You can select or create filters directly from the “Filtered Messages” desktop or from the Message Filters menu.



NOTE: For more information, see “Filtered Messages Desktop” on page 252.

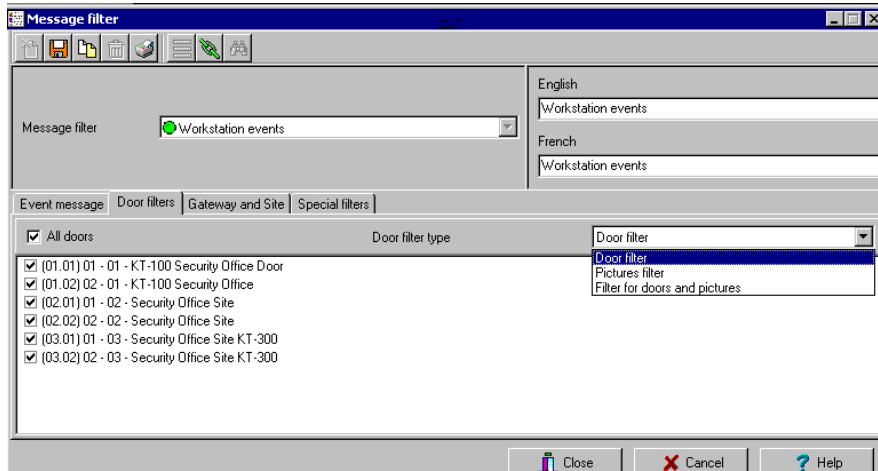
To Define Event for a Message Filter

- 1 In the System main window, select the **Message Filter** icon. The Message filter window appears.

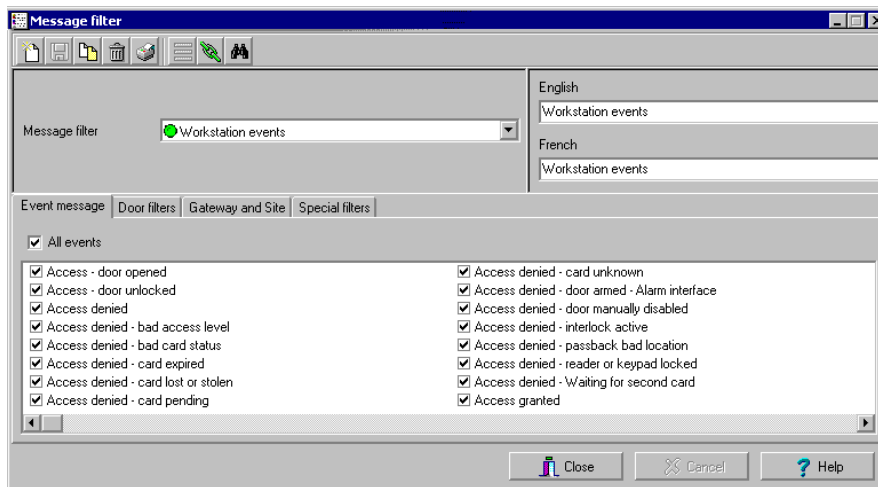


- 2 From the **Message filter** drop-down list, select an event message type (for example: Door events or Relay events) for which you want to define a filter. You may also click the **New** icon to create your own filter.
- 3 From the **Event list**, select the events that must appear in the selected filter. You may check the **Select all events** option, if you do not want to select specific events. For example, for a Door events type filter, you may decide to include all events or select the **Access-denied** events.
- 4 Select the **Door filters** tab to filter doors that will send messages to the Filtered messages desktop. Additionally, when “Access events” are filtered, the cardholder’s picture can be

displayed with the event (if pictures are assigned to cardholders). You can select which doors will display the cardholder picture when the event for this door is generated.



- 5 Check the **All doors** option or choose specific doors for which the cardholders's picture will be displayed an door event.
- 6 From the **Door filter type**, select the filter that will be used for filtering Door events:
- 7 Select the **Gateway and site** tab to filter gateways and sites events sent to the Filtered Messages desktop.

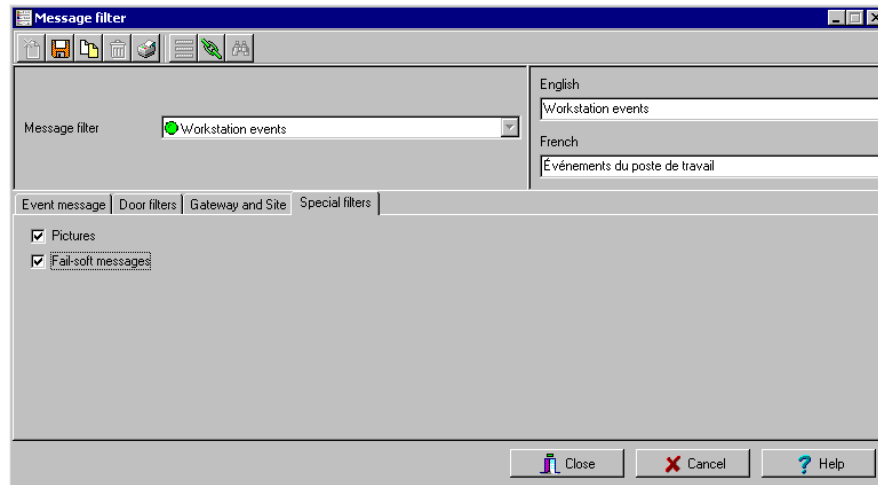


- 8 Check the **All gateways and site** option to receive events originating from the components of the sites. You may select the site that will send events to be displayed.



NOTE: When you use filters, the system retrieves events that are already displayed in your Message desktop and sorts these events according to the settings of the selected filter.

- 9 Select the **Special filter** tab to filter events according to their type.



- **Picture:** all events associated with a cardholder's picture will be displayed in the Filtered Message desktop.
- **Fail-soft:** all events generated by a controller in stand-alone mode following a communication failure will be sent to the Filtered Message desktop. Fail-soft messages are identified with a + sign in the Filtered Message desktop (and Message Desktop) when this option is select when defining the Messages list properties (**Desktop > Message Desktop > right-click an event > Properties**).



NOTE: When you use filters, the system retrieves events that are already displayed in your Message desktop and filters these events according to the settings of the selected filter.

Database Structure Definition

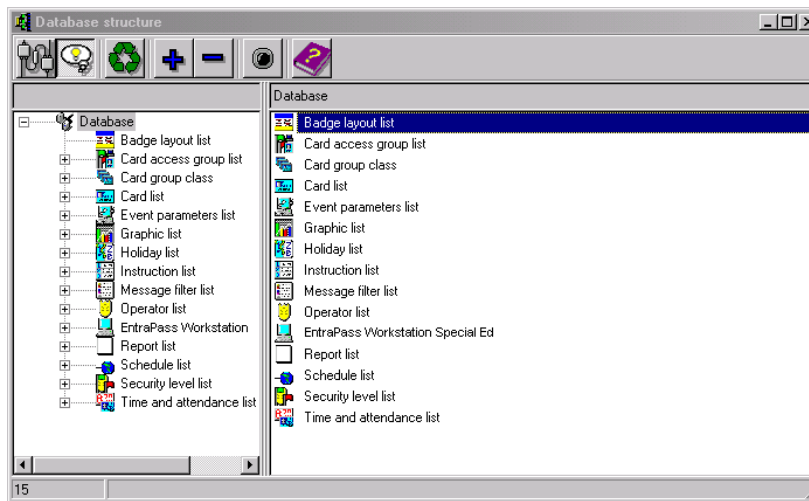
Use the Database structure menu to browse the system database. It will display the entire structure of the database including:

- The system *physical components* (EntraPass applications, sites, controllers, doors, relays, inputs and auxiliary outputs), and
- *Logical components* (cards, schedules, reports, instructions, groups, etc.).

Operators can edit or sort the system components from the Database structure window.

To View the Database Components

- 1 Form the **System** menu, select the **Database structure** icon.



- 2 To display only the **Physical component**, select the physical components icon. When selected, only the physical components of the database will be displayed.



NOTE: By default, *physical components are ALWAYS displayed.*

- 3 To display **Logical components**, select the logical components icon. When selected, logical components of the database will be displayed along with the physical components.
- 4 You may use the **Refresh** button to refresh the display in order to obtain the most recent information saved in the server database.
- 5 You may select the **Full Expand** button to fully expand the tree structure and view all sub-components of a selected component. For example, if you use this button on a controller, the system will display the controller components (doors, inputs, relays) on the right-hand side of the window.
- 6 You may select the **Collapse** button to fully collapse the tree structure and hide all sub-components of a selected component.



- 7 To edit a component, right-click it and select **Edit** from the contextual menu. The system will display the definition window so you can modify the component's parameters.
- 8 To sort the component, right click the component, then select **Sort** from the contextual menu. Sort the components listed in the right-hand pane of the window for an easier find. You can sort by component address or name.



NOTE: *You can define how the component's physical address will be displayed. This will also affect how components will be sorted. For more on this, see "Security Level Definition" on page 217.*



Chapter 11 • EntraPass Desktops

Desktops receive and display system events (current or historical), alarms, cardholders's picture, system graphics, etc. A desktop can also be used to acknowledge alarms, display instructions, etc.

There are four (4) pre-defined desktops. These can be configured as follows:

- Desktop 1: All system events
- Desktop 2: System events and pictures
- Desktop 3: Alarms screen
- Desktop 4: Graphic screen

The following windows can be combined with other desktops:

- Instructions
- Pictures
- Historical Reports

It is possible to display more than one window at a time. Depending on their security level, operators can modify the settings of each of these windows (background color, size, toolbar, etc.). However, an operator whose access level is 'read-only' on a given desktop cannot modify, move, maximize or minimize a desktop.



NOTE: Only operators with the required security level can customize their desktops (**System menu > Access Level**). They also have the ability to allow "Read-only operators" to modify their desktop settings. In this case, the changes apply only to the current session.

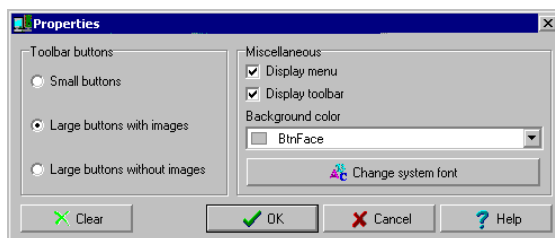
Work Area Customizing

EntraPass enables operators with appropriate permissions to customize their work area and to modify the desktop properties.

To define an operator's security level: **System** menu > **Security Level**.

To Change the Display Properties

- 1 From the Desktop window, right-click anywhere in the window.
- 2 Select **Properties** from the shortcut menu.



- 3 From the Properties window that appears, select the display options: you may change the default size of buttons, the default background color, etc.
 - **Small buttons:** If this option is selected, small components' icons are displayed with no descriptive text. This option can be appropriate for operators who are familiar with EntraPass icons and do not need an additional description.
 - **Large buttons with images:** Icons are displayed with their description.
 - **Large buttons without images:** Large buttons are displayed with no description.
 - **Display menu:** check this option to view the system menu.
 - **Display toolbar:** check this option to view the toolbar for system menus.
 - **Background color:** select a background color for the whole work area.
 - **Change system font:** click this button to change the font for all the user interface.

Specific Desktop Customizing

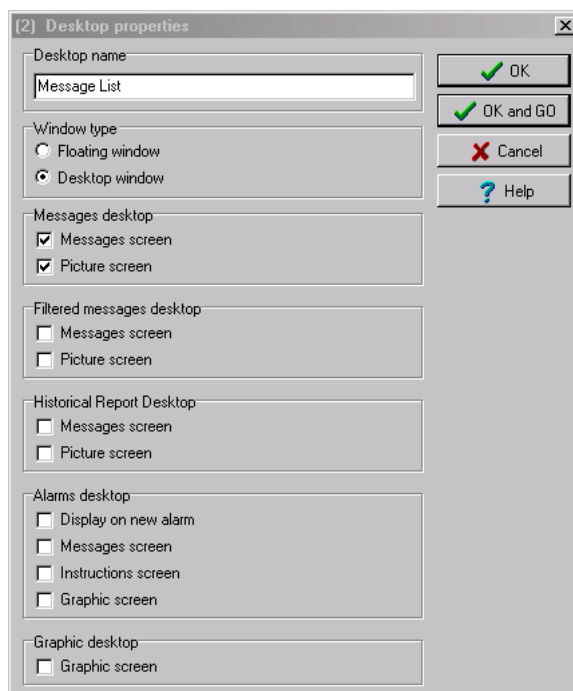
Entrapass enables operators with appropriate permission to customize their desktop. Moreover, operators with full access permissions can permit operators with read-only permission to customize their desktop for a limited time. They can also customize a specific desktop and transfer this customized desktop to other operators using the Assign desktop feature. The following sections explain how to customize a desktop:

- Customizing a desktop by a full access operator
- Customizing a desktop for a read-only operator
- Transferring a customized desktop

To Customize a Desktop (Full Access Operator)

Operators with full access permission have the ability to customize their desktops. To grant full access to an operator: (System > Security Level).

- 1 Select the desktop you want to customize, then right-click to open the Desktop properties window, then select **Properties** from the short-cut menu.



- 2 From the **Desktop name** field, assign a meaningful name to the desktop you are configuring.
- 3 Select the window type:
 - **Floating window**—a floating window can be resized and positioned anywhere in the work area screen. For example, you can choose to send it to the back or to bring it to the front. If

a floating window was sent to the back, you may bring it to the front by right-clicking the desktop button, then selecting the **Bring to front** menu item.

- **Desktop window**—a desktop window is trapped within the work area. It is not possible to send the window in the background. It always remains within the main work area.
- 4 To save your changes:
- Click **OK**—If selected, you just save your the changes, the window is not displayed.
 - Click **OK & GO**—If selected, this function saves your changes and displays the window you have just configured.

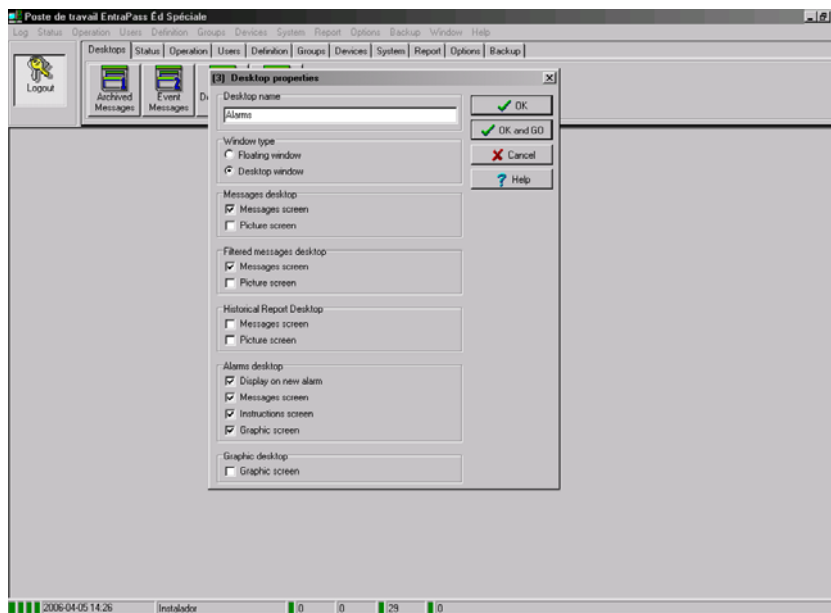


NOTE: When opening a desktop window for the first time, you may need to re-size it in order to view the information correctly. To do so, point to the frame border you want to change; when the pointer turns into a double-headed arrow, drag the border to exact size. You may then position the window in the work area to the desired position.

To Customize a Desktop for a “Read-Only” Operator

The security manager or an operator with the appropriate security level can give permission to operators who do not have the appropriate permission to customize their desktop during a session.

- 1 Log on, using the user name and password of the operator with ‘read-only’ security level. To do this, use Kantech2 as the username and kantech as the password.
- 2 Then, right-click a desktop, then select **Properties**. The desktop properties window appears.



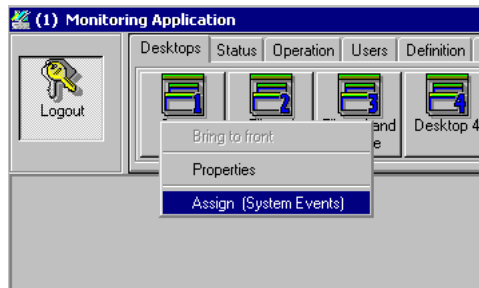
NOTE: The **Permit** button appears when the operator who is logged on has ‘read-only’ access permission. The permission acquired during this session will be valid until the operator logs out.

- 3 Click the **Permit** button. The operator login window appears. Enter your username and password, and click, **OK**. The temporary permission will be granted.

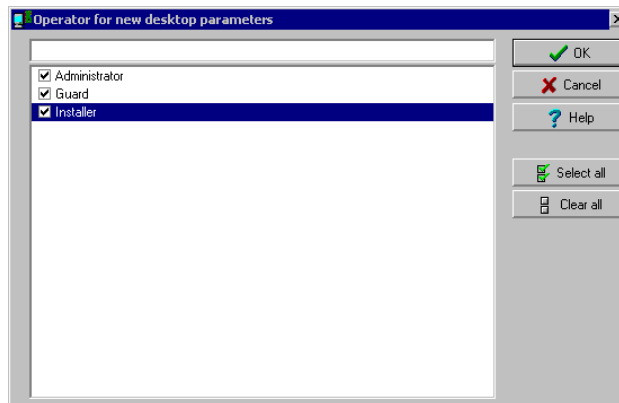
To Transfer a Customized Desktop

Another possibility available to the Security Manager (or to the operator with the appropriate security level) is to customize a desktop, and then to assign the settings to other operators who may not have the appropriate security level to modify their desktop settings.

- 1 Right-click the desktop you want to assign the settings.



- 2 Select the **Assign (desktop)** option from the shortcut menu.



- 3 From the displayed window, select the operators to whom you wish to assign the desktop properties (you must check the appropriate checkbox). You may select operators one by one, or you may use the **Select all** button.

Message List Desktop

By default, the first desktop is defined as the **Messages List Desktop**. It displays all system events. Events are displayed with their icon, date and time, description, system components involved in the event such as controllers, cardholder pictures (if defined), etc. When a new event is displayed, the window scrolls up. The newest events are added at the bottom of the window.

To View and Sort System Events

By default, the first desktop is dedicated to displaying system events. When you select an event from the list, you interrupt the incoming sequence (the green status indicator located at the bottom left part of the desktop turns red when scrolling is interrupted). By default, the scrolling will restart automatically after a pre-set period of time, unless the auto-scroll parameter was disabled. In that case, to restore the normal scrolling, click the **Restart Scroll** button.



NOTE: If you configure a Desktop as a message screen and a picture screen, two windows are displayed simultaneously when you select the desktop.

- 1 Select the first desktop. By default, all system events are displayed in ascending order with an area at the bottom of the screen that displays the selected event in the list.



NOTE: You may change the message color: **System > Events parameters**. You may also change the events display order; see "To Customize Event Display in the Message Desktops" on page 245.

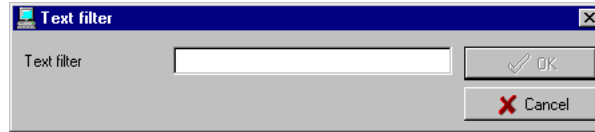
- 2 From the Message list screen, you may change the sorting criterion (**Sorted by** scroll-down list). You may choose to sort by:
 - **Sequence**—Events are sorted according to the normal sequence (default). New events are added at the bottom of the window. (This option is not available for Archived Messages Lists.)
 - **Date and time**—This sort order interrupts the normal scrolling of events. This feature is useful when you want to know when an event was generated. This time may be different from the "normal sequence" for dial-up sites for instance or after a power failure.
 - **Event**—When selected, the system sorts the **Event message** column in alphabetical order, grouping *identical* events. For example, all **Input in alarm** events are grouped together in alphabetical order.
 - **Message type**—When selected, the system sorts the **Event message** column in alphabetical order, grouping *similar* events. For example, all **Site** events are grouped together in alphabetical order.



NOTE: To go back to the default display, Select **Sequence** from the **Sorted by** drop-down list.



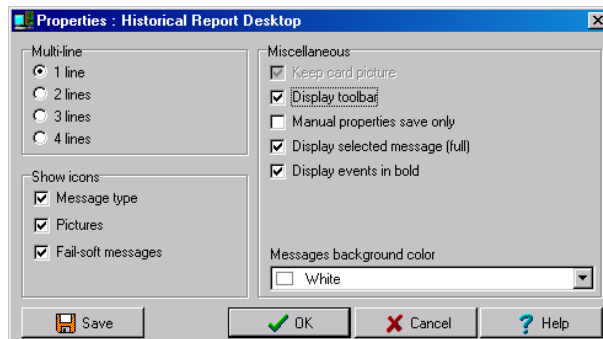
- Click the **Text filter** button (top of the **window**) to display specific events containing a text string. When you do this, the **Find** dialog box appears. Enter the string that will allow you to display specified events, then click the **Find next** button.



- To close the **Find** dialog box, click the **Cancel** button or the Windows closing button (X).
- To return to the normal display in the Messages list screen, click the **Text filter** button.

To Customize Event Display in the Message Desktops

- From the displayed shortcut menu (**Message desktop** > Right-click a message), select **Properties**.



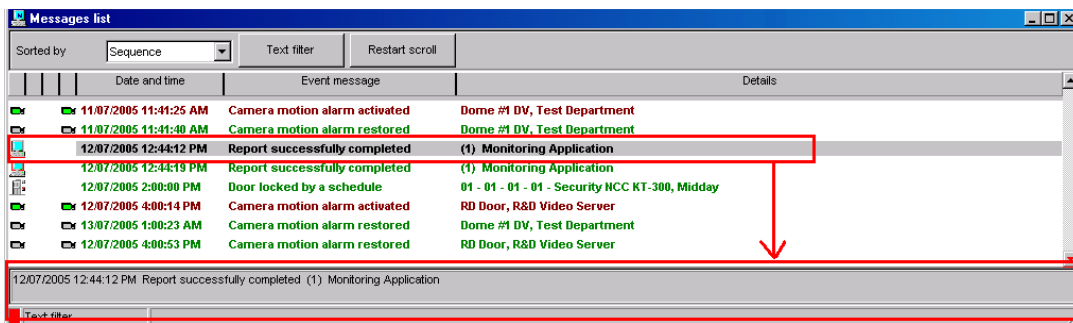
- From the Properties window, select the appropriate display options.
 - Multi-line**—Usually, events are displayed on a single line. You can increase the line spacing between events by checking the appropriate option (1, 2, 3 or 4 lines).
 - Show icons** —You can choose to display different types of icons beside each event.
 - Message type**—When you select this option, the system inserts an icon next to events indicating the type of event. For example, if the event is a “door forced open” an icon representing a door is displayed (a hand represents a manual operation, a diskette represents the operation that modified the database, etc.). Access events are represented by the login/logout icons.
 - Picture**—When you select this option, the system inserts a card icon next to events containing cardholder pictures.
 - Fail-soft messages**—When you select this option, the system displays a plus (+) sign next to the events that occurred when controllers were off-line.
 - The **Miscellaneous** section allows you to enable additional options:



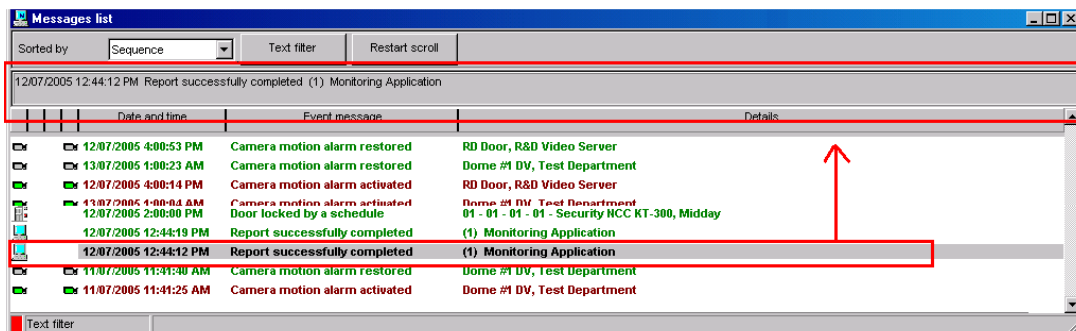
- **Keep card picture**—When selected, the system keeps the latest card picture (if the Picture window option is selected) until another event containing a card occurs.
- **Display toolbar**—Displays/hides the toolbar on the top of the Message Desktop.
- **Manual properties save only**—When you select this option, you have to click the **Save** button (once selected, the button is disabled). The system saves all the settings defined in the **Properties window** as well as the position of the window within the Messages Desktop.
- **Display selected messages (full)**—When you select this option, a smaller window is added at the bottom portion of the **Message window**. It displays the selected event with its full description. This feature is very useful when your Message window is too small to display the entire description of an event.
- **Display events in bold**: select this option to increase the legibility of text event messages displayed in Entrapass desktops (Message list, Filtered messages and Alarm desktops). Moreover, if the color selected for an event message is the same color as the background color, the event message will be displayed in black bold so that it can always stand out. (This option is not available for Archived Messages Lists.)
- **Last Message on Top**: By default, event messages are displayed in ascending order of occurrence, with the area at the bottom of the screen reserved for the highlighted



event. You can select to display the events in descending order, with the highlighted event showing above the list of event messages.



Ascending Order



Descending Order

- **Auto-scroll delay (mm:ss):** Will automatically start scrolling the message list after a preset delay when the operator selects an item in the list. By default, this option is turned on with a preset delay. You can select to turn this option off which means that the operator will have to click the **Restart Scroll** button in the Messages List. (This option is not available for Archived Messages Lists.)
- **Message background color**—Allows the operator to modify the background color of the message window.



NOTE: To change the font color of system messages: **System > Event parameters.**

To Perform Tasks on System Messages

Entrapass enables you to perform various tasks on system events. These include:

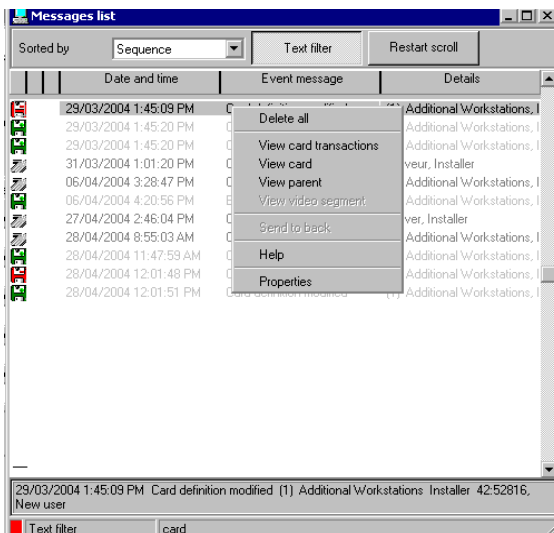
- Deleting messages

- Viewing card information
- Validating card status and card transaction
- Modifying the desktop properties (such as display options), etc.



NOTE: Some tasks are related to the selected desktop. For example, if you right-click an alarm event, the shortcut menu displays tasks that are related to alarm events. For details, see "Alarms Desktop" on page 256.

- 1 From the Message desktop, right-click an event to enable a shortcut menu:



- 2 Do one of the following:
 - **Delete all**—This option allows an operator to delete all the events displayed.
 - **Card**—This menu items offers two choices: **View card transactions** and **Search card**. Select **View card transactions** to display all access information related to the cardholder who has triggered the access event. The **Search card** shortcut allows you to browse the card database and to display information about a card from the View card information window. From this window, operators can perform a variety of tasks including viewing and validating information contained on a card, such as the card number, cardholder name, card state (valid or invalid), etc. They can also select a card and view its transactions or view and validate a card access. For details about validating cardholders' access and last transactions, see "Cards Definition" on page 130.
 - **View parent**—Displays the parent of each component related to the selected event.
 - **Edit**—This feature offers you the ability to edit each component associated with the selected event. If **Edit** is selected, a shortcut menu displays components associated with the selected event. In this example, the *Site definition modified* event involves the EntraPass application, the operator who was on duty when the event was generated and

the site related to the event. It is now possible to edit any of the three components by selecting it from the shortcut menu.



NOTE: *If the selected event is an access event and if the card that triggered the event has already been registered in the system, it will be possible to edit the card. However, if the card is associated with an Access denied - card unknown event, the card will be created and registered in the system.*

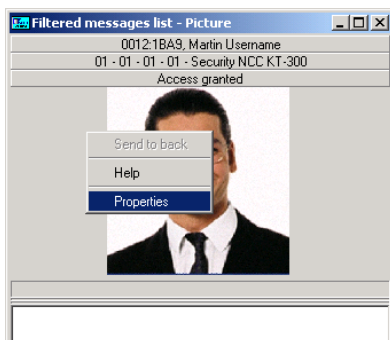
- **Send to back**—This option only works when the window type is set to floating. It sends the active window behind the main application window. To bring back to front, right click the desktop button, then select **Bring to front**.
- **Properties**—This menu item enables users to modify the display properties for the selected desktop.

Picture Desktop

If you selected **Picture screen** when defining the Message desktop, the Message desktop always appears with a Picture window. Access events are displayed with the cardholder's picture if you have set the appropriate display option in the Message filter definition (System > Message filters). For details, see *"Message Filters Definition"* on page 233.

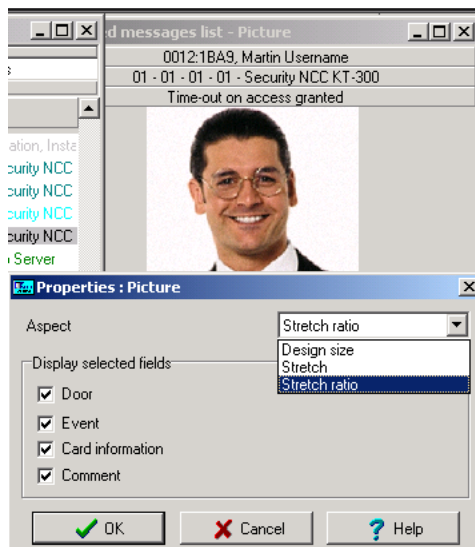
To Modify Pictures Display Options

- 1 From the Filtered Message list and Picture, select an access event, then right-click the cardholder's picture.



Send to back—This option only works when the window type is set to floating. It sends the active window (Picture window) behind the Message desktop main window. To bring it back to front, right click the Message desktop button, then select **Bring to front** from the shortcut menu.

- 2 From the shortcut menu, select **Properties**.



- 3 From the **Aspect** drop-down list, select the display size for the picture:

-
- **Design size:** the cardholder's picture will be displayed with its original size.
 - **Stretch** —This option stretches the picture to the window size without maintaining proportions. The picture may appear distorted.
 - **Stretch ratio**—This option stretches the picture to the window size while maintaining proportions.
- 4 Select the information you want to see displayed with the cardholder's picture:
- **Door:** The door where the card was presented will be displayed above of the cardholder's picture
 - **Event:** The event message will be displayed
 - **Card information:** The card information field will be displayed above the picture.
 - **Comment:** If this option is selected, a comment field appears below the cardholder's picture. The comment entered when defining the card appears in this field.

Filtered Messages Desktop

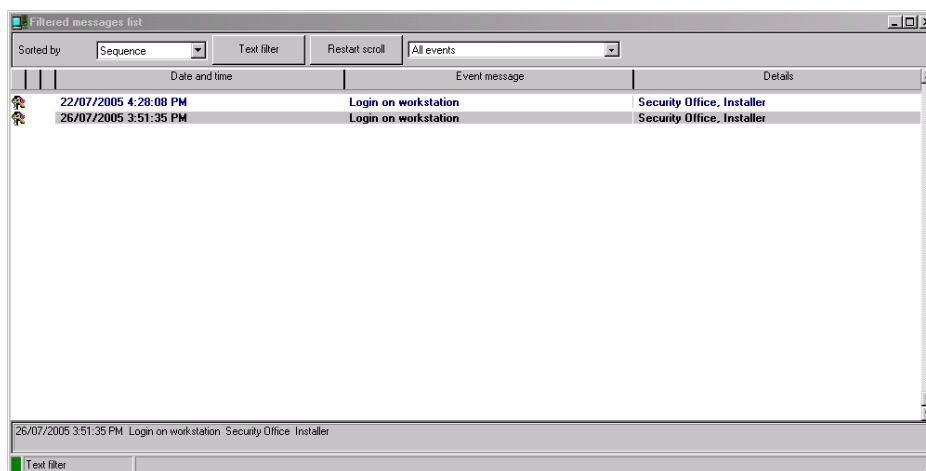
The Filtered Messages desktop allows operators to display specific events. For example, you can create filters to display events that are related to a specific controller and from a particular gateway of the system. If this is the case, those events will be displayed in the Filtered Message desktop. Filtered messages are defined in the Message filters menu: **System > Message filters**.



NOTE: When you use filters, the system retrieves events that are already displayed in the Messages desktop and filters these events according to the selected filters.

To Configure a Filtered Messages Desktop

- 1 From the Desktop main window, select the desktop you want to configure as a **Filtered messages desktop**.
- 2 Assign a meaningful name to the **Filtered message desktop**; then define the desktop type (Message window, Picture window or both).



- 3 You can change the **Text filter**, to display specific events. For details on the Filtered messages desktop, see *"Message List Desktop"* on page 244.



Historical Report Desktop

The **Historical Report** desktop allows operators to display events that come from pre-defined, historical reports, view the report generation state. Security levels will determine which historical reports are available to each operator.

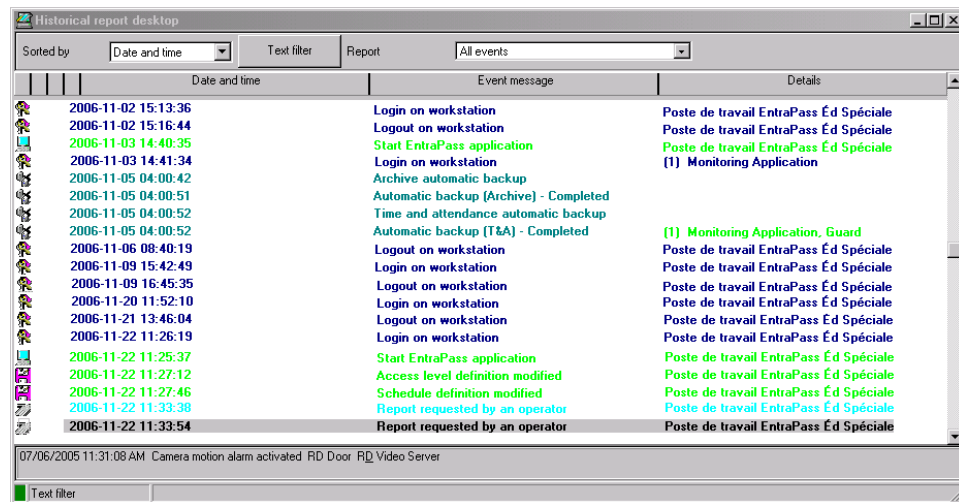
The **Historical Report message list** operates the same way as all message lists in EntraPass except that it has an extra combo box that allows operators to select a pre-defined historical report.

Historical reports are defined under **Report > Historical Report**

Security levels for reports are defined under **System > Security Level >** under the **Report** tab.

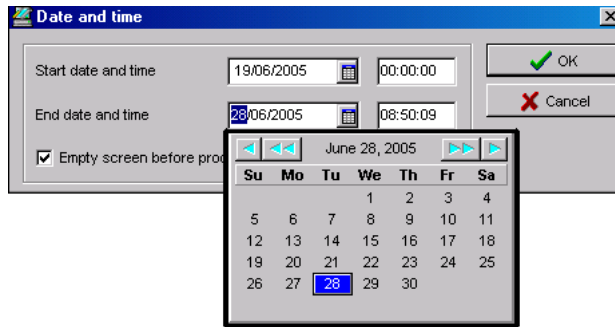
To Configure a Historical Reports Desktop

- 1 From the Desktop main window, click the desktop button you want to configure as a **Historical Reports Desktop**.
- 2 Assign a meaningful name to the Historical Reports Desktop, then define the desktop type (Message window, Picture window or both).



- 3 Select the sort criteria you want to use to display historical data (**Date and Time**, **Event**, or **Message Type**).
- 4 You can enter a text string that will be used for searching specific archived messages (when applicable).
- 5 In the combo-box, select the historical **Report** you want to generate. The list of available reports corresponds to your security level.

- After selecting the report, a **Date and Time** window will popup requesting a reporting date and time period.



- Enter **Start** and **End date and time** or click the calendar icon to open the calendar and select the start and end dates, and then type in the start and end times.
- Check the **Empty screen box process request** box in order to clear the Historical Report message list of the previous search results.
- Click **OK**. The status indicator light located at the bottom left of the screen will change from green to blue to indicate a historical report is being generated. It will turn green again when the data transfer will be completed and the historical data will be displayed according to the criteria you have selected.

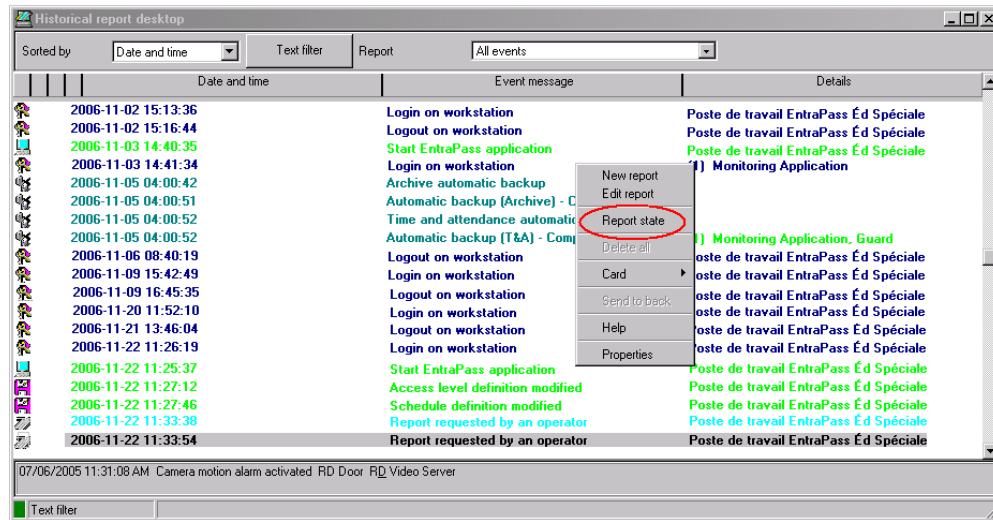
To Create and Edit Historical Reports

- When your security level allows you to create new reports, you can access the Historical Report dialog from the **New Report** command in the Historical Report Desktop pop up menu. For more information on Historical Reports, see *"Historical Reports Definition" on page 271*
- When your security level allows you to edit existing reports, you can access the Historical Report dialog from the **Edit Report** command in the Historical Report Desktop popup menu. For more information on Historical Reports, see *"Historical Reports Definition" on page 271*

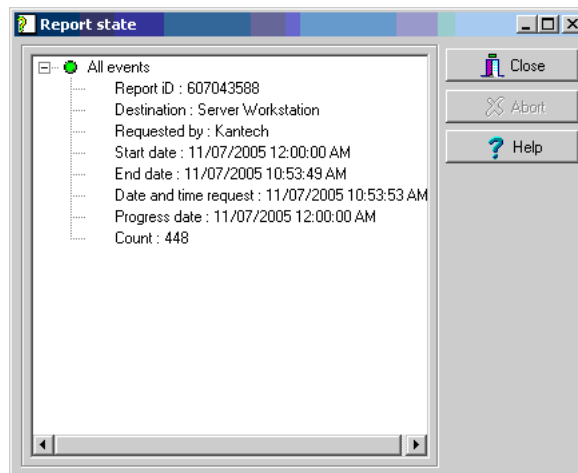
To Display Historical Report State in Real-Time

This feature allows you to view the progress of report generation for a specific report in the Historical Report Desktop List

- 1 Right-click an entry in the Historical Report Desktop window. A contextual menu will pop up.



- 2 Select **Report State**. The Report State dialog will open displaying Report generation information.



- 3 When the report is finally generated in the Desktop window, the information in the Report State dialog will disappear. Click **Close**.

Alarms Desktop

The Alarms desktop is used to view and to acknowledge alarm events. Alarm events are defined in the Event Parameter menu (**System > Event Parameters**). Any event can be defined as an alarm event. Alarm events require operator acknowledgment and are displayed in the Alarms desktop. A schedule must be defined for all alarms (**System > Event parameters, Alarm settings**). When an alarm is generated during a valid schedule, operators have to acknowledge the alarm. Alarms are displayed with date and time, alarm description, details, instructions (if defined) and associated graphic (if defined). New events are added at the bottom of the Alarm desktop unless you have setup the list to display in descending order (in the Alarm Desktop Properties dialog).



NOTE: An Alarm desktop may be defined as a Message window, a graphic window and an Instruction window. These features may apply to a single desktop. When you select a desktop defined with these three features, three windows are displayed simultaneously. For a better display, you may need to resize and to position the windows.

To Define an Alarms Desktop

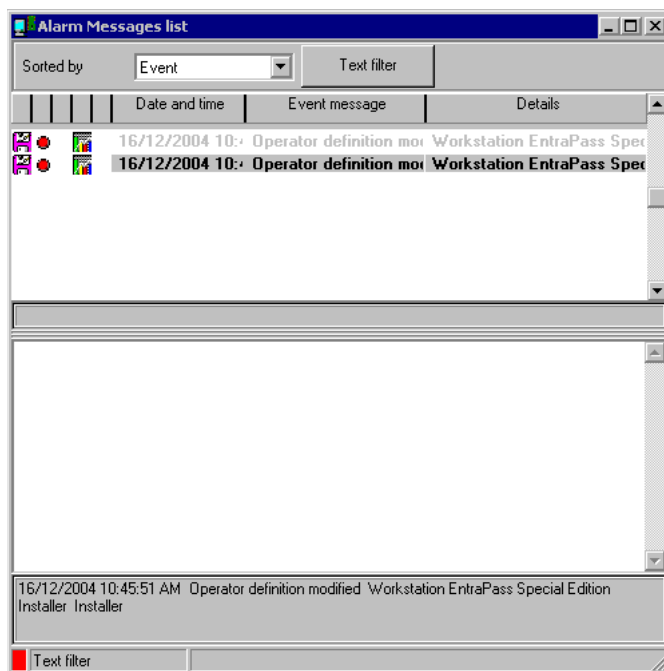
- 1 From the Desktop main window, select the desktop in which you want to display alarm messages, then define the window type: **Floating** or **Desktop type**.

- 2 Specify the secondary windows that will be associated with the Alarms desktop:

- **Display on new alarm**—Will open the Alarms desktop automatically when an alarm occurs.
- **Message screen**—This window allows operators to view and acknowledge alarms that have an “acknowledgement schedule” selected in the **Event Parameters** definition menu (**System > Event Parameters**, Alarm settings).
- **Instructions screen**—This window displays the instruction that is linked to the event to be acknowledged (i.e. call the police, send a message to a client application, etc.). Instructions are defined in the **System > Instructions**. Then after, they may be associated with events.
- **Graphic screen**—This window will display the location of the alarm being reported (if graphics are defined in the system). For more information on assigning graphic, see *“Graphics Definition” on page 101*.

To View System Alarm Messages

- 1 Select the **Alarm** desktop. Alarm events are displayed according to the criteria selected in the **Sorted by** field.



- 2 You can double-click the log area (middle of the window) to add a comment. The Add a comment window opens and enables you to enter text data. Once you have finished and clicked the **OK** button to close the window, the alarm event will be preceded by a + sign, indicating that an annotation has been added to the alarm event.
- 3 You may change/define the sorting order (**Sorted by** drop-down list):

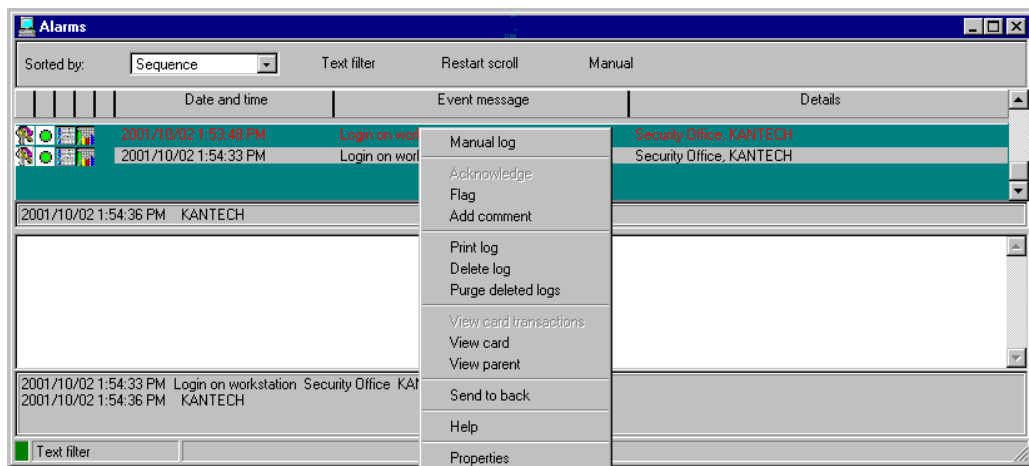


- **Sequence**—alarms are sorted by their order of arrival. This the default sequence. The window scrolls to the end each time a new alarm is displayed.
 - **State**—alarms are sorted according to their status (acknowledged, to be acknowledged or flagged). When you use this option, you interrupt the normal scrolling of events. Select “sequence” to go back to the default display.
 - **Date and time**—alarms are sorted according to the date and time of their arrival.
 - **Event**—The **Event messages** column is sorted in alphabetical order, grouping *identical* events For example, all **Input in alarm** events are grouped.
 - **Priority**—Events are sorted by priority (as defined in **Event parameter**).
- 4 You may right-click anywhere in the window to enable the Properties window from which you can enable alarm status icons:
 - **Red**—To be acknowledged or suspended. If suspended, the suspension delay is displayed. When the delay expires, the operator is required to acknowledge again. If the delay is not expired but the operator wishes to acknowledge a suspended alarm, he/she has to click on the delay. The delay will be reset to zero.
 - **Green**—Acknowledged.
 - **Yellow**—Flagged.
 - **Black**—Deleted. To view alarms that have been manually deleted, select the **View deleted logs** from the **Properties**.
 - **Blue**—Manual log.
 - 5 Select the **Manual / Automatic** buttons to toggle the acknowledgement method (automatic or manual). Only operators who are assigned this feature in the Operator Definition menu can use this option. For more information, see *“Operators Definition” on page 214*.



NOTE: The **Manual / Automatic** acknowledgement option is only available through the Alarms Desktop. When the operator logs out, it will return to “manual” by default.

- 6 Right click an alarm message to perform additional tasks on alarm events:

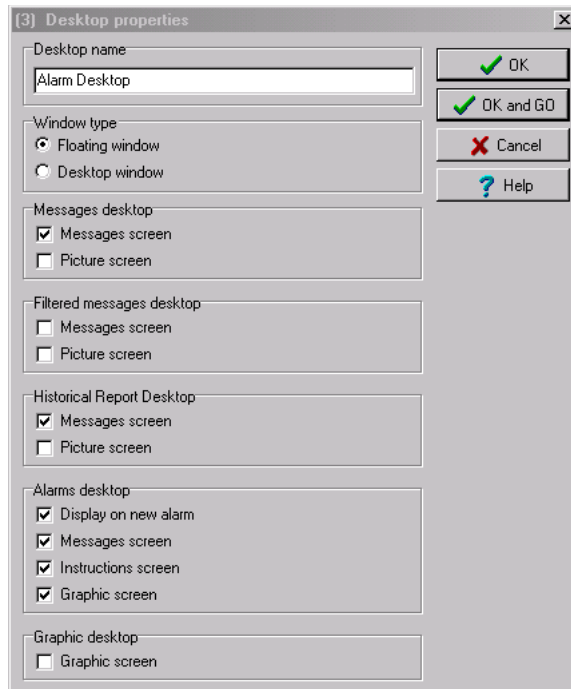


- **Manual log**—When selected, the system displays the Manual log window to allow an operator to add log comments, and hence to generate a customized event (with priority, event details, color etc.). When a manual log is added, a hand and a blue circle are added beside an alarm message. These are visible when icons are enabled (right-click an alarm event > **Properties** > **Show icons**)
- **Acknowledge**—When selected, a green point is inserted beside an alarm message to indicate that the event was acknowledged.
- **Flag**—When selected, the system flags the selected event. A yellow indicator is inserted beside flagged events.
- **Add comment**—Allows operators to enter comments concerning the selected event. The added comments are displayed in the bottom part of the alarm window. A blue + sign beside an alarm message indicates that a comment was added to the alarm message (visible when icons are enabled: right-click an alarm event > **Properties** > **Show icons**)
- **Print log**—When selected, the system prints the alarm message.
- **Delete log**—When selected, the selected alarm message is marked for deletion (the indicator becomes “black” to indicate that the log has been marked for deletion). To view the logs marked for deletion, before you actually purge them, right click anywhere in the window and select **Properties** then select **View deleted logs**.
- **Purge deleted log**—Select this option to permanently remove logs that were marked for deletion.

To Display Alarm Desktops Automatically

EntraPass enables users to display graphics automatically - from any desktop - as soon as an alarm occurs. This feature enables operators on duty to automatically view new alarms without having to open the alarm desktop and secondary windows associated with it. If **Display on new alarm** is checked the alarm desktop (and its secondary windows) will be displayed as soon as an alarm occurs regardless of the active window.

- 1 Define a desktop and customize it as an alarm desktop: for this, you have to check the items of the Alarms desktop section.



- 2 Check the **Display on new alarm** option so that operators can automatically view new alarms without having to open the alarm desktop and secondary windows associated with it.



NOTE: If this option is checked and if an operator calls up the alarm desktop, the desktop icon background color turns blue, indicating that the alarm and its secondary windows are displayed when a new alarm occurs. If however this option is selected when defining a Filtered message desktop for instance and if the desktop icon is selected, the filtered message desktop will be displayed (the background color of its icon turns blue), but the windows below the Display on new alarm section will not be displayed; they are only displayed when a new alarm occurs. If those windows are displayed (on new alarm), clicking the “X” in the top right hand corner of one of them will close all the open windows. If **Display on new alarm** is not checked, the alarm desktop and all its secondary windows will be displayed on call (that is, when the alarm desktop is selected).

- 3 Click **OK and Go** for your configuration to take effect immediately.



NOTE: When you define a desktop as an alarm desktop to be displayed on new alarm, it is recommended to reopen the Automatic Alarm Display desktop, to position its windows the way you want them to appear, then to click **OK and GO** again. This way, it will appear exactly as you have defined it.

To Acknowledge Alarms/Events

Usually, operators have to acknowledge receipt of an alarm condition (event—such as intrusion, input in alarm, etc.) by responding in ways such as depressing an acknowledgment button. In EntraPass, operators acknowledge alarm messages from an alarm warning box or from the Alarms desktop window.



NOTE: A sound can be added to alarm events. For more details about setting options for an alarm sound, see "Multimedia Devices Configuration" on page 304.

Acknowledgement options are setup in the EntraPass application definition (**Devices > EntraPass application > Alarm** tab, Acknowledgement parameters). Events that require operator acknowledgment are defined in the **System > Event Parameters**.

Automatic Acknowledgement

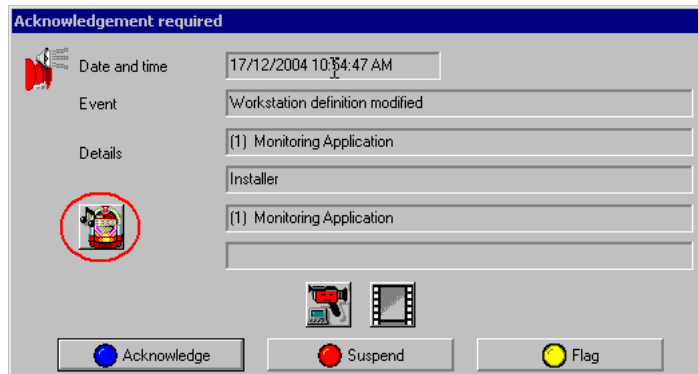
Alarms can be automatically acknowledged without operator intervention. This option is enabled in the Operator definition menu (**System > Operators > Privileges, Auto acknowledge**).



NOTE: Only operators granted the appropriate access privilege should be using this option. If the **Automatic acknowledge** feature is used, the alarm message box is not displayed; therefore, it will not be possible to suspend alarms. If this option is enabled in the Operator definition menu, the **Manual** button is added to the Alarms desktop. This button toggles between **Manual** and **Automatic** acknowledgement.

Acknowledging an Alarm Message

- 1 When the **Acknowledgement required** message box appears, take one of the following actions:



- Click the **Acknowledge** button to acknowledge the displayed alarm event. The red status button turns green once an alarm is acknowledged.
- Click the **Suspend** button to suspend alarms while doing other operations in the system. The alarm will be suspended for the delay time specified in the **EntraPass application** definition menu. Once the suspended alarm delay time expires, the system prompts the operator to acknowledge the alarm.



- Click the **Flag** button if you want to acknowledge an alarm message, and if you want to identify it for future reference. A flagged alarm is identified by a yellow button.
- Click the **Mute** button if you want to stop the alarm sound.



NOTE: The **Acknowledgement required** message box will be presented in a format without the Instructions window if there are no instructions associated with the alarm message.

Acknowledging Alarms from the Alarms Desktop

- 1 Select the alarm event you want to acknowledge (one that has been flagged, for instance), Right-click to enable a shortcut menu.
- 2 Select **Acknowledge** from the sub-menu. The status indicator becomes green.



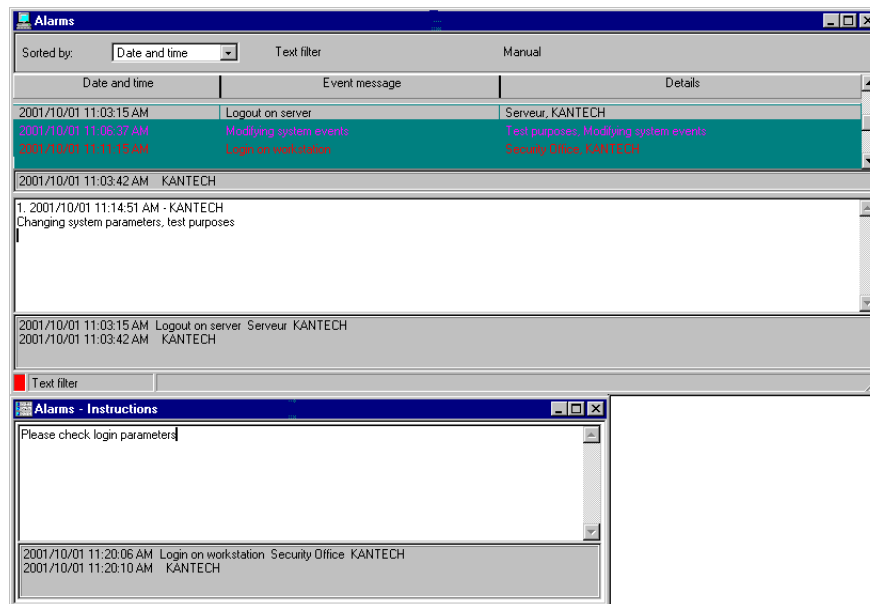
NOTE: To tag an alarm message for specific purposes, select the alarm event you want to identify; right-click and select **Flag** from the sub-menu. You can also click an alarm message until the color of its status indicator changes to the desired color.

Instruction Desktop

The Instruction window displays the instructions to follow when an alarm is reported. Instructions will only be displayed if this option is enabled during the Event Parameters settings (**System > Event parameters, Alarm settings**).

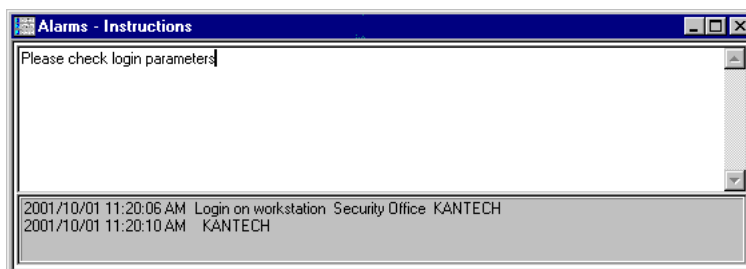
To View an Instruction about an Alarm Message

- 1 You may view instructions about an alarm by selecting the Alarms desktop defined as a message and an instruction window, or defined as an instruction window. When a desktop is defined as being both a message window and an instruction window, the two windows are displayed at the same time:





- 2 You may also view an instruction about an alarm by selecting an alarm message and right-clicking it.



NOTE: This feature is very useful when the Alarms desktop is too small to display the entire description of an event.

Graphic Desktop

The Graphic desktop displays the graphical location of the alarm being reported (if graphics are defined in the system). A graphic corresponds to the secured area of the system where components (Entrapass application, controllers, inputs, relays, etc.) are located on a site.

With graphics, operators can easily view the exact location of a component installed on a site, or the status of components and devices such as doors, contacts, motion detectors, controllers, assigned to the graphic. Operators can perform manual operations directly from the displayed component (for example lock/unlock a door). To define interactive floor plans, see *"Graphics Definition" on page 101*.

To View Graphics in the Graphic Desktop

- 1 Right click the desktop icon you want to assign to graphic, name the desktop (Graphics, for example), then define the window type (**Floating** or **Desktop**).
- 2 Click **OK and Go** to display the Graphics desktop.
- 3 Right click anywhere in the Graphic desktop, then, from the shortcut menu, select the graphic you want to display.

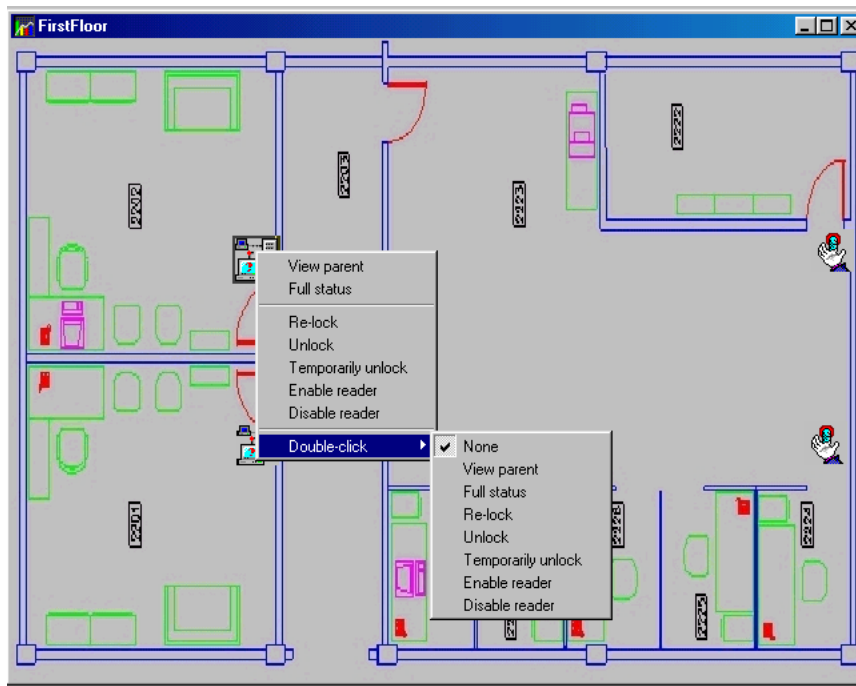


NOTE: *If the window is smaller than the graphic size, you can click-hold-and-drag the graphic to move it around within the Graphic window.*

- 4 You may right click anywhere in the graphic to enable a shortcut menu in order to:
 - Adjust the display size of the selected graphic (**Fit to screen**, **Design size** or **Picture size**).
 - Select **Auto result** for the system to display a message indicating the cause of the communication loss in case of communication failure. If **Auto result** is not selected, operators will have to manually request the results for the component by using the **Show result**.



- 5 Right-click a component in abnormal condition to enable a sub menu:



NOTE: Components in alarms are represented by their animated icons. Selecting an animated icon and viewing its parent components allows operators to learn more about the “alarm condition”.

- 6 Select **Full status** from the shortcut menu to display the error list related to one or all the components in alarm.
- 7 Select the **Double click** menu item to allow operators to modify the status of a component in alarm from the Graphic desktop. For example, if the displayed component is a door and if the **Double click** menu item was set to **Unlock**, an operator can manually open the door from the Graphic desktop.



NOTE: When you modify the Double-click feature via the Graphic desktop, the system does not save the modifications. Modify the default Double-click feature via the **graphic definition** (**Definition > Graphics**, Design window, right click a component > **Default dbclick** menu item). For more information on how to create graphics and on how to assign components to graphics, see “Graphics Definition” on page 101.

Chapter 12 • Reports

Entrapass software allows users to define and generate reports. These reports may be generated automatically or requested manually. Reports can be sent by e-mail.

There are three types of reports:

- **Quick reports:** these are based on selected group of events (i.e.: door, controller, etc.) and event types (normal, abnormal, etc.)
- **Historical reports:** these are historical and card use reports. The historical report type contains archived and filtered events, whereas card use reports contain events related to card use.
- **T & A reports (Time and attendance):** these are defined according to selected doors and cards defined as time and attendance.

From the Report toolbar, Entrapass users may also:

- **View reports**— this feature allows an operator to select pre-defined reports to view on screen or to print.
- **View Report states**—this features allows an operator to view the status of all reports that have been previously generated.
- **Perform Manual operations** on Time and Attendance reports to add, insert, and delete Time and Attendance entries.

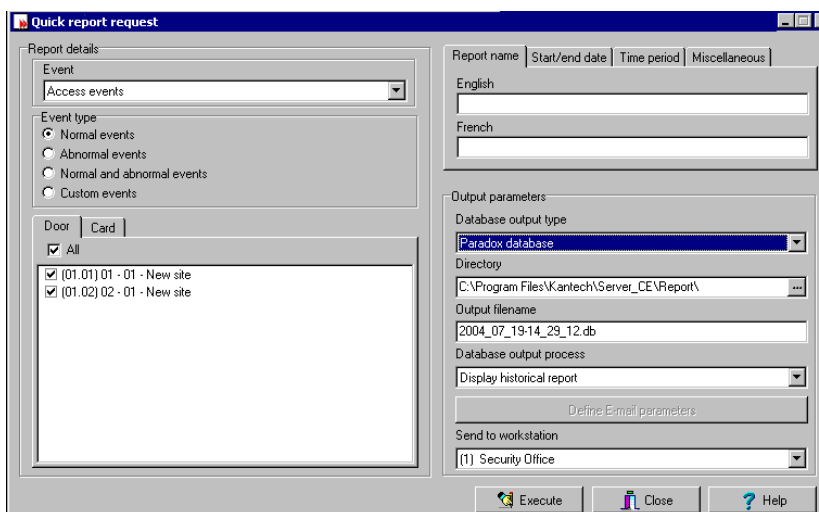
Quick Report Definition

The Quick report feature offers a rapid method of creating reports for certain types of events. For example, it is possible to create a report regarding all abnormal or normal access events in just a few seconds.

Quick report files may be viewed using the EntraPass Quick Viewer, a utility that allows users to display Quick report files and all.QRP files. These include report files that are saved from a report preview. The Quick Viewer is launched from Windows **Start** menu, without the need to launch the software.

To Define a Quick Report

- 1 From the Report toolbar, select the **Quick report request** icon.



- 2 From the **Event** drop-down list, select the event type for the current report (access, controller, door, relay, input, operator, manual operation events, etc.). If you have selected “access events”, the **Card** tab appears in the window.
- 3 Among the **Event type** options, select the event type to be included in the report.
 - **Normal**—Quick report can create reports based on normal events. In an access report, normal events would be such events as “access granted” for instance.
 - **Abnormal**—Such events as access denied (bad access level, supervisor level required), workstation server abnormal disconnection, gateway communication failure, or all events related to a process that is not complete (a controller reload failure, for example), are considered abnormal.
 - **Normal & abnormal**—Select this option to include normal and abnormal events in the report.
 - **Custom events**—Select this option to include your own events. The **Custom** tab appears when the **Custom events** option is selected. This option allows the operator to select the

components that have generated the selected events according to the setting in the “event” field.



NOTE: When you use the **Event** field, you have to specify which component(s) should be used or not used. Once you select an event (i.e. access), the system displays all the doors of the gateway. If you select Controllers, the system displays all the controllers for the gateway. Once you have selected an event (i.e. controller events), select the controllers (i.e. list of controllers) to be included in the report.

- 4 Select the **Card** tab to specify filter details about the report. The **Card** tab appears only if a card-related event is selected.

- 5 In the **Card index** drop-down list, specify the information that will be used as the filter. For example, if you select “card number”, only access events in which the defined card numbers appear will be selected.



NOTE: If you select **Card number**, the **Lower** and **Upper boundary** editable fields display the default numerical values to be replaced by card numbers. If you select **Card user name**, these fields are enabled to receive text data. For example, you can enter **A** in the **Lower boundary** field and **F** in the **Upper boundary** fields for the system to include events in which the selected door is defined and events in which the defined card numbers appear but only for card users whose names begin with A to F. If you select **All**, the editable fields are disabled.

- 6 In the **Report name** tab, enter a name for the report (this name will be displayed on your report).
- 7 In the **Start/end date** tab, enter the date and time on which the system will start to collect the events. For example, if you enter 7:00 and an event occurred at 6:00, this event will not be included. To target events that occurred during a specific time frame, use the **Time period** tab.
- 8 In the **Time period** tab, check the **Specific time frame** option to include events that match the specified time frame. Enter the target time for the report.



- 9 If you want to overwrite the previous file, select the **Miscellaneous** tab then check **Overwrite existing output file**. If you do this, the existing default output file will be replaced by this new one.
- 10 Define the output parameters:
 - **Database output type**: Select the database output format (Paradox, Dbase IV, or CSV).
 - **Directory**—Indicates where the report is saved and stored. The default folder is: C:\ProgramFiles\Kantech\Workstation_SE\Report\your file.xx.
 - **Output filename**—Indicates the output file name. By default, reports are saved on disk in C:\ProgramFiles\Kantech\Workstation_SE \Report\your file.xx. The report filename is composed of the date and time on which the report was created. You can modify the filename if necessary, but do not modify the extension.
 - **Database output process**—Select the appropriate output processes. A report template is associated with each output.
 - Database only (the report will be saved in the system database)
 - Display historical report (the report will appear on-screen)
 - Report printed (sequence, date or events) (the report will be printed according to the specified sort order)
 - **E-mail historical report**: the report will be sent by e-mail to a specified valid e-mail address.
- 11 Click the **Execute** button to launch the report. To view the report, select the **View report** tab.

Historical Reports Definition

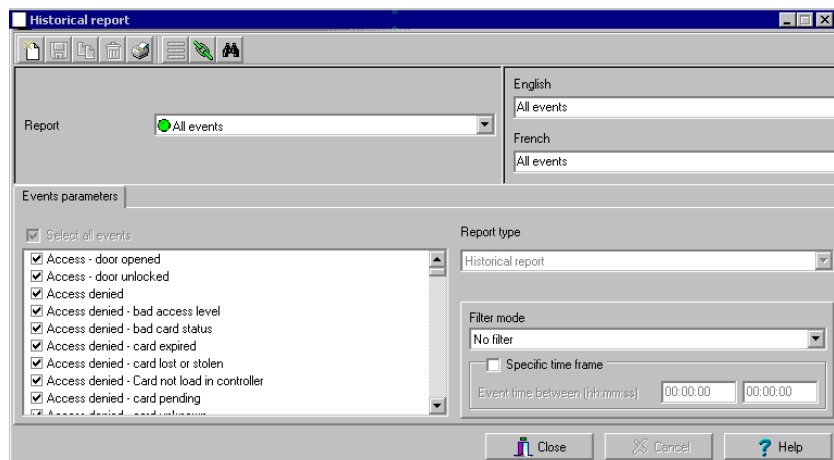
The Historical report definition feature allows users to define customized historical reports and card use reports with their own automatic execution parameters.

Reports that are defined with automatic settings are automatically generated at the specified time. However, they may be requested manually when needed. The “Historical Report Request” menu enables operators to trigger reports by overriding automatic settings. When requested manually, automatic settings are ignored.

To Define a Default “All Events” Report

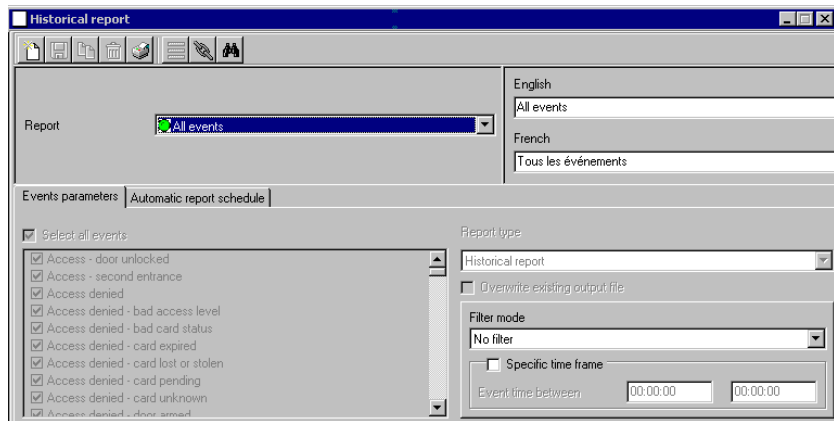
You may generate a default report that will include all events. The default report is an Historical report type. EntraPass enables you to send an automatic report by e-mail.

- 1 Select the **Historical report** icon from the Report toolbar. The Historical report window appears.



To Define a Custom Historical Report

- 1 From the Report window, select the **Historical report** icon. The Historical report window appears.



- 2 To create a new report, click the **New** icon (in the toolbar) and enter the necessary information in the language section. The **Report type** field shows the selected/created report (Historical or Card use report). To modify an existing report, select it from the **Report** drop-down list.
- 3 You may check the **Select all events** option. All the listed events will be checked and included in the report. You may choose to check specific events that you want to include in the report.
- 4 If you are creating a **Historical report type** report: from the **Report type** drop-down list, select **Historical report**. This is the first filter for the report. The selected report will show events such as access granted events (with the time, the door that was accessed, as well as the card number).
- 5 If you selected the **Historical report** type, you have to select components associated with the event. The Components tab appears in the window when the selected report is an **Historical report type**.



NOTE: When you select **Historical report** and when a filter mode is selected (**Filter mode** drop-down list), the system displays additional tabs, the **Components** and **Cards** tabs. The **Card** tab is also displayed when “Access” events are selected.

- 6 Check the **Overwrite existing output file** option if you want the system to replace the existing output file each time the report is automatically generated according to the settings defined in the “Automatic report schedule”.
- 7 *Historical Reports Only.* Select the **Filter mode** if you want a report from specific components. These filters are used to target specific events that were generated from selected components. You can select various filtering methods. When you use this field, you have to specify which component(s) to use.
- 8 *Historical Reports Only.* If you selected **Historical report**, check the **Specific time frame** option. If selected, the time frame specified will be used by the system. Only events (event time) that are



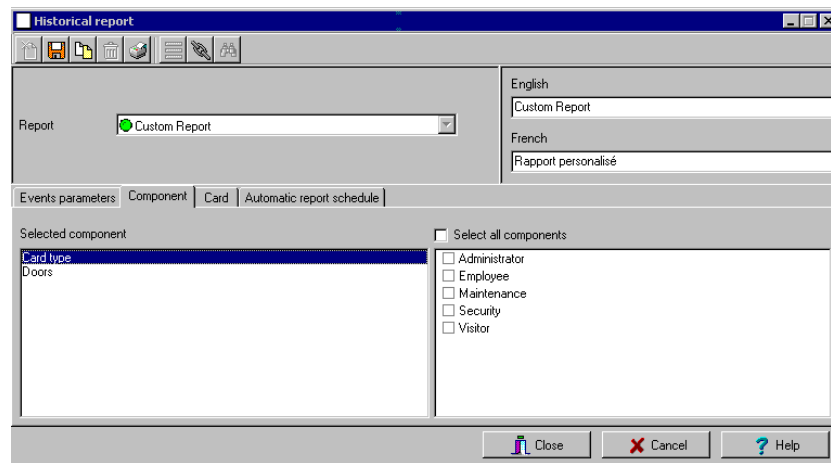
within this specific time frame will be included in your report. For example, if you define 8:00 to 8:30, only events which occurred during this time frame will be included in the report.

- 9 Select the **Automatic report schedule** tab to specify details about the report. For details about defining an automatic report, see *"To Define Automatic Report Schedules"* on page 276.

Defining Components for an Historical Report

If the selected report is a **Historical report** type and if you have selected a **Filter mode**, the **Components** and **Cards** tabs appear next to the Event parameters tab. You have to specify the components and filters that may affect the report.

- 1 From the Historical report window, selected the **Components** tab. The Components window lists all the component types that have a direct link with the selected events.



- 2 Select an event type to display its items in the right-hand pane. If you select Doors, all the access system doors are displayed in the right-hand pane.



NOTE: If an item in the left-hand pane (*Selected components*) is selected, its color changes (turns red). When it is deselected, it resumes to the default color.

Defining Card Options for an Historical Report

- 1 From the Historical report definition window, select the **Card** tab. It is displayed only when access events are selected. It is used to add more filters to your report in order to target specific events.

Filter index	Filter mode	Lower boundary	Upper boundary
Card user name	None		
Card information 1	None		
Card information 2	None		
Card information 3	None		

- 2 Select the **All Cards** option to include all cards.
- 3 Specify the information that will be used as a filter (**Filter index** drop-down list). For example, if you select “Card number”, as the filter index, only access events in which the defined card numbers appear will be selected.
- 4 From the **Filter mode** drop-down list (None, Include, Exclude), specify if the system should exclude or include the value range that you specify in the Upper/Lower boundary fields. When a filter mode is selected (**Exclude** or **Include**), the “Boundary” fields are enabled.
- 5 Enter the value range in the **Upper/Lower boundary** fields according to the selection in the **Filter mode** field. These may be, for example, alphabet letters (if the filter index is by names; or numeric, if the filter index is by card number). You could, for instance, use the card user name and specify A to F in the **Upper/Lower boundary** as the lower and upper boundaries. As a result the system will include events in which the selected door is defined and events in which the defined card numbers appear but only for card holders whose names begin with A to F.



NOTE: Users may select more than one filter for the same report using the filter index. Events will be filtered *n* times depending on how many filter indexes are defined for the report.

To Define a Card Use Report

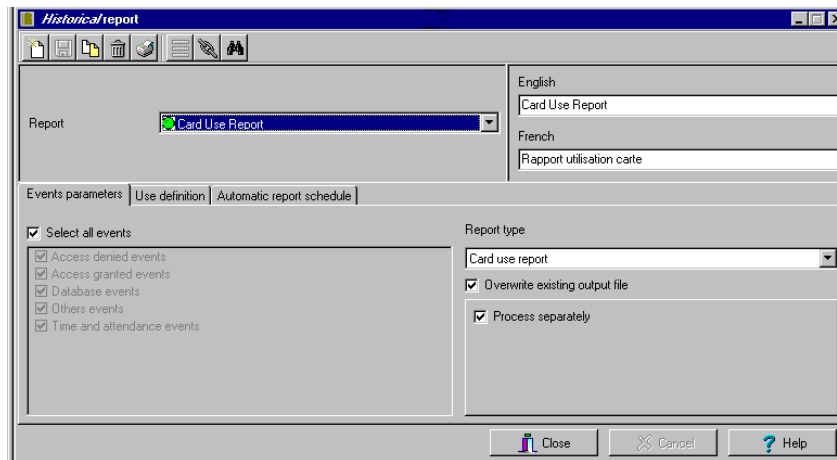
The card use report feature is used to create reports that will list cardholders who did/did not generate events since a specific number of days or a specific date. For example, operators could request a report including “access granted” events that were generated since a specific date.



NOTE: When you select a card use report option, the *Use definition* tab appears in the *Historical report* window. It allows you to define the card use parameters, such as: used since a specific date, not used since 30 days before today, etc.

The system displays five event types:

- Access denied (bad location, bad access level, bad card status, etc.)
 - Access granted
 - Database (events that have affected the database, such as card definition modified)
 - Time and Attendance events (entry, exit).
- 1 From the *Historical report* window, select a report from the **Report** drop-down list. If you are creating a new report, click the *New* icon in the toolbar, then enter the necessary information in the language section.



- 2 You may check the **Select all events** option (when it is checked the display pane is disabled), or you may select only the events you want to include in the report.
- 3 The **Report type** drop-down list, displays **Card use report** if the selected report is a Card use report type. If you are creating a new report, select Card Use report. When the selected report (in the Report drop-down list) is a **Card use report** type, only events related to card use are displayed in the left-hand pane.
- 4 You may check the **Overwrite existing output file** option, to replace the existing card use report every time you generate a new one. You may keep the default target folder.
- 5 You may also check the **Process separately** option if you want the events to be processed individually for each card. For example, if you want a report for “Access denied events” and “Access generated events”, if you do not check the **Process separately** option, the report will

contain all these events. When the **Process separately** option is checked the report will display Access granted event and Access denied events separately.



NOTE: The **Process separately** option appears only when the report type is a **Card use report**.

- 6 Select the **Use definition** tab to specify the card use options (**Not used since** or **Used since**) and target periods.



NOTE: The **Use definition** tab appears only when the selected report type is a **Card use report**.

The screenshot shows the 'Historical report' dialog box. The 'Report' dropdown menu is set to 'Card Use Report'. The 'Use definition' tab is selected, showing the 'Use period' section with 'Not used since' selected and 'Used since' unselected. The 'Defined period' section has 'From' selected with the date '2006-02-20' entered in the text box, and 'Many days back' unselected with '0' in the spinner box. The 'Automatic report schedule' tab is also visible. At the bottom, there are buttons for 'Close', 'Cancel', and 'Help'.

- 7 To define the target period, check the **From** checkbox and enter a date in the **From** field. You may select a date in the calendar when you click the **Calendar** button. Alternatively, you may use the up/down controls or enter the **Number of days back**, starting from today's date.
- 8 When you have finished defining the report, save it. You may request it using the **Report request** button in the Report toolbar.

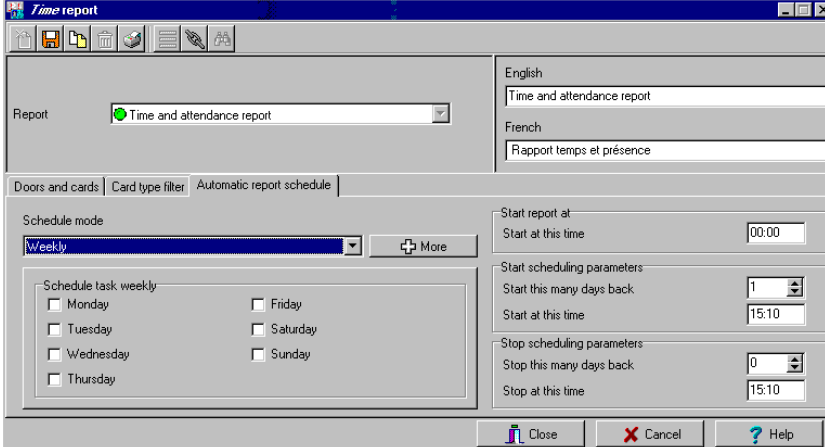
To Define Automatic Report Schedules

For both Historical and Card use reports

Use the **Automatic report schedule** tab to define automatic settings for your reports so they can be automatically generated when needed. These settings indicate:

- The frequency: when the report should be generated (none, weekly, monthly, once)
- The time period covered
- The output process (display, print, etc.)
- The output type (dBase, Paradox, CSV)
- The language and the filename

- 1 From the Historical report window, select the **Automatic report schedule** tab.



- 2 From the **Schedule mode** drop-down list, select the frequency at which the report should be executed:
 - Select **None** if you want the report to be manually requested (see *Historical Report Request*).
 - Select **Weekly** if you want a report every week. You have to check the day on which the report should be executed automatically.
 - Select **Monthly** if the report is needed once a month. You have to specify the day (ex. the second Friday of the month or the 15th day of the month) when the report will be executed automatically.
 - Select **Once** if you want the report to be executed automatically on a specified date.
- 3 In the **Start at this time** field, enter the time at which the system will start executing the report.
- 4 Specify the **Scheduling parameters**.



NOTE: These settings are *ignored* when the report is requested manually by an operator.

- **Start this many days back**—The report will start collecting events according to the number of days specified in this field. It is based on the present date.
- **Start at this time**—Once you specify the amount of days, specify the starting time (i.e.: 7:00am). For example, if you enter 7:00, events that occurred at 6:00 will not be included in the report.
- **Stop this many days back**—The report will include the specified number of days entered in this field. It is based on the present date.
- **Stop at this time**—Once you specify the number of days, specify the ending time (i.e.: 5:00 pm), that is, the day on which the system will stop collecting data; you may also specify the time at which it will stop. For example, if you enter 7:00 and an event occurred at 8:00, then

this event will not be included. To target events that occurred during a specific time frame, you have to use the **Specific time frame** option.



NOTE: The start and end time are only used for the first day and last day, for example if you start collecting events on Monday at 8:00 and end on Friday at 17:00 all events between 8:00 Monday and 17:00 Friday will be included. The system **does not use** the start and end time for each day but for the whole period.

Specifying Additional Options for an Automatic Report

- 1 Select the **More** button to add more settings to the automatic scheduled report. When you click the **More** button, the Automatic report output definition window appears.

- 2 From the **Output type** drop-down list, select the output format of the report. You may choose Paradox, Dbase IV, or CSV formats.



NOTE: From the **Database output process**, you can select **E-mail historical report** if you want this report to be automatically sent to specified recipients. If you choose this option, select the **E-mail** tab to enter the recipients' e-mail address in the **Send E-mail to** field. EntraPass enables you to protect the report by a password before e-mailing it.

- 3 You may check the **Automatic filename (...)** option. The default file name is YYYY_MM_DD-HH_MM_SS.X, indicating the year_month_day-hours, minutes_second.file extension.



NOTE: For details on the output type and the output process, refer to the table below. It gives a comparison of the different report formats.

The following table shows the difference between these database formats and their output file formats:

Database	Description	.db	.rdf	.csv
Paradox	In addition to the traditional.db,.rdf output formats, the Paradox database generates the.px,.xg0,.xg1,.yg0,.yg1 files. These contain the indexes and are useful when using a "Paradox" database. They can also be used by the database administrator.	X	X	X



Database	Description	.db	.rdf	.csv
Dbase IV	A popular database management system format for storing data that is supported by nearly all database management and spreadsheet systems. Even systems that do not use the DBase format internally are able to import and export data in Dbase format.	X	X	-
CSV	Will save the report in a comma separated values format (yourfile.csv). A data format in which each piece of data is separated by a comma. This is a popular format for transferring data from one application to another; because most database systems are able to import and export comma-delimited data.	-		X

- 4 Refer to the following table for information on the editing tools compatible with the output files. Only.db file formats can be edited.

Output file	Paradox	Dbase IV	CSV
.db, Editing tool	dBase IV, dBFast, MultiEdit, DbVista, Paradox, SmartWare and XtreeGold.	dBase III, IV, FoxPro, dBFast, DataBoss and Excel.	-
.csv, Editing tool	-	-	Excel, NotePad, WordPad, etc.
.rdf, Viewing tool	Entrapass tool (Borland Database Engine)	Entrapass tool (Borland Database Engine)	NotePad

- 5 From the **Output process** drop-down list, select the report template. It will be used with the requested report. For details on the output format, see *"To Define a Report Output Format"* on page 279.

To Define a Report Output Format

Historical and Card use reports

- 1 If you select **Database only (CSV, Paradox and Dbase)**: The report will include the following information: event sequence, date and time, event message, description types (displays a specific number that identifies a component in the system), description names (displays the name of the component as defined in the system—name of description type number) as well as the card number (for card-related events).



NOTE: A database only report is saved in the reports folder in the specified format. It will not be printed nor displayed.

- 2 If you select **Display Historical report - Display card last transaction report (Paradox Only)**: The report will automatically be displayed on your desktop when completed. You can customize the report before you print it manually. For more information on how to customize the report, see *"To Preview Historical Reports"* on page 294. The report will include the following information:



event sequence, date and time, event message, card number (for card-related events) and descriptions 1 to 4 which contain details on the event.

- 3 **Report printed by sequence** (*Paradox Only*): This report is sorted by event sequence number (order in which they were generated by the system) and printed automatically at the printer.
- 4 **Report printed by date and time** (*Paradox Only*): This report is sorted by date and time and printed automatically at the printer of the destination workstation.



NOTE: *The printed reports (option three and four) will be saved in the reports folder in the specified format. They will also be printed but not displayed.*

- 5 **Report printed by event** (*Paradox Only*): This report is sorted by event message (alphabetically) and printed automatically at the printer. The report is saved in the reports folder in the specified format, but not displayed.

Time and Attendance Reports

Time and attendance reports will be saved in the reports folder, they are not printed nor displayed. User have to manually retrieve the report to view it, they can also use the “View Report” menu.

- 1 **Single file with all data** (*CSV only*): The report is generated in one file containing the data and the descriptions (date & time, transaction ID, card number, card user name and door description).
- 2 **Database with transactions** (*CSV, Paradox & DBase IV*): The report is generated with all the data and transactions in one single file. It includes the date & time, the transaction ID, the card number and the card user name.
- 3 **Display time and attendance report** (*Paradox only*): The report will automatically be displayed on the desktop when completed. You can customize the report before you print it manually. It contains: the card number, card user name, entry time, exit time, contents of the card information field as selected in report definition and total hours per cardholder. For more information on how to customize the report, see “*To Preview Time and Attendance Reports*” on page 295.
- 4 **Two (2) databases with all data** (*Paradox & DbaseIV*): the report will be generated in two separate files:
 - **One file containing:** date, time, event message (transaction type), pkcard, pkdoor, pkdoorgroup.
 - **One file containing:** pk description (explaining pkcard, pkdoor and pkdoorgroup), card number, object and contents of card information field selected in the report definition menu.



NOTE: *Pk refers to a component unique number within the system*

- 5 **Single database with all data** (*Paradox & DbaseIV*): The report will be generated in one file containing the data and the descriptions (date and time, transaction ID, card number, card user name, door description and sequence).
- 6 **CSV compilation time and attendance** (*CSV Only*): The report will be generated in two files. One file containing a total, of hours for instance, by department, and the other file containing detailed information. Depending on the number of days covered by the report, a “day” column will be reserved for each day.



- **Automatic filename**—Select this feature if you want the system to automatically use the date and time as the filename. You cannot use the “overwrite existing output file” when you use this option.
- **Filename**—If you wish to overwrite the same report (for example—every week), you can enter a filename here and when the report will be executed according to specifications, the new report will replace the oldest report.
- **Destination**: this is where the report should be sent/printed automatically. You can also use the **Overwrite existing output** option to specify a different destination file.
- **Report language**—This field is used to include additional information in your report. Select from the displayed list.

To Request Historical Reports

With this feature operators can request pre-defined **Historical reports** or **Card use** reports that were created using the Historical Report menu. Operators can also e-mail the report to one or multiple recipients.



NOTE: *If your report contain automatic settings, these will be ignored. You must indicate new settings.*

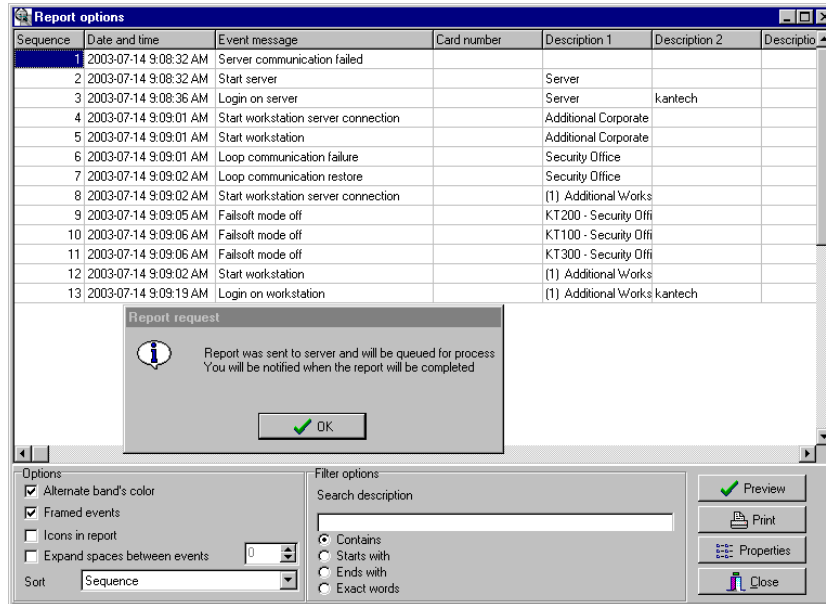
- 1 From the Report toolbar, select the **Report Request** icon. The Report request window appears.

- 2 In the **Report list** display pane, select the report that you want to execute.
- 3 You may define output parameters, including the database output type, the target folder, the output filename, etc. For more information on how to select an output format, see *"To Define a Report Output Format"* on page 279.



NOTE: *If a Card use report is selected, the “Date and time” section is disabled.*

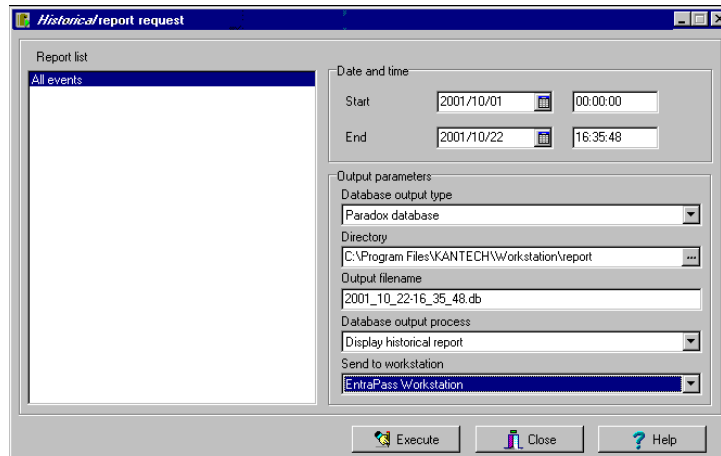
- Click **Execute**. A system message informs you that the report is being processed. The Report options window appears and is then minimized to the task bar.



- Select the **Preview** button to define the report and filter options. This will increase the readability of the report by adding, for instance, alternating band colors, framing events, icons in the reports, etc., or by sorting events in the report (by event ID number, alphabetical order or date and time). (TO check)
- Enter the **description** in the **Search description** field. The report is updated in real-time when you enter a filter option.
- You may use **Preview** to preview the report or the **Properties** button to view details about the report. When you click the **Preview** button, the system will display the result of the report. From that window, you can save the report (in a.QRP format) or print the report.

To Request an Event Report

- 1 Select the **Report request** icon from the Report toolbar. The Historical report request window appears.



- 2 Specify the **Start** and **End** time. By default, the end date and time are set to the system time.
- 3 You may specify the output parameters or leave these to default.



NOTE: It is important to know the differences among the output type and processes. For details, see "To Define a Report Output Format" on page 279.

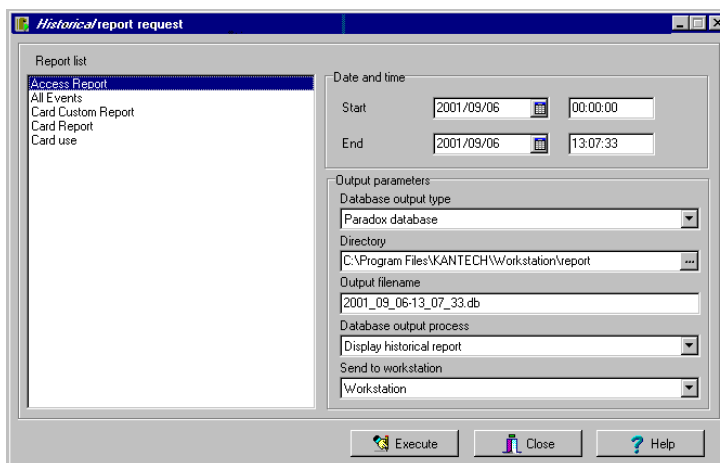
- 4 You may select the **Report state** icon from the toolbar to view the report status.
- 5 Select the **View report** icon from the toolbar to view the report. The default report name is YYYY_MM_DD_-HH_MM_SS.db.

E-mailed Reports

EntraPass allows you to e-mail any report to one or more recipients. The e-mail feature is enabled when defining an EntraPass workstation and when specifying the report database output format. Historical, time and attendance and quick reports can be sent by e-mail to any valid e-mail address.

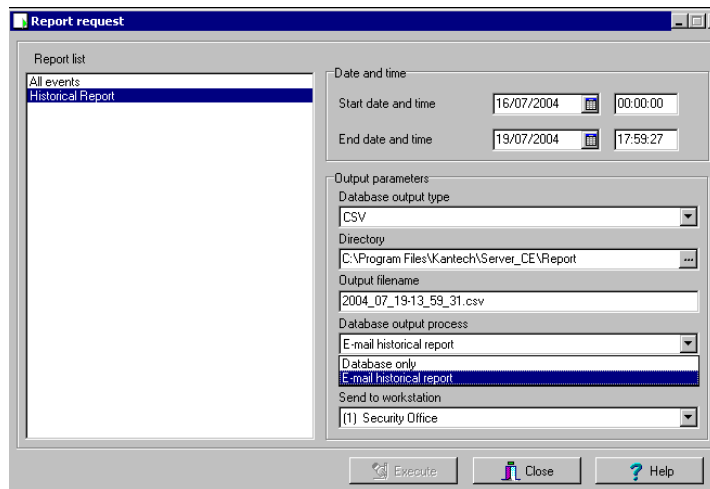
To Define a Report to Send by e-Mail

- 1 From the Report toolbar, define a new report or select an existing one, then select the appropriate **Report Request** button.

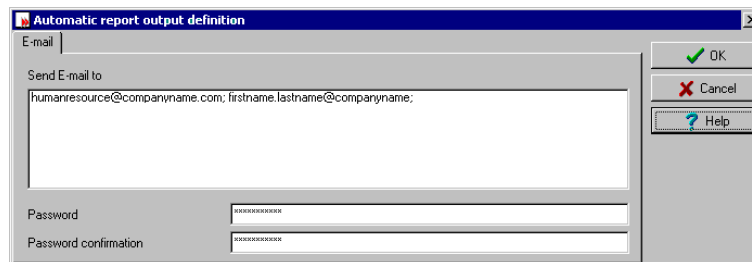


- To send a historical report, click .
- To send a time and attendance report, select **Time Request Report**.

- To send a quick report, select **Quick Report Request**.



- 2 From the Report request window, select **E-mail report** as the Database output process option. When you select this option the **Define E-mail parameters** button is enabled. Click the **Define E-mail parameters** button. The Automatic report output definition window appears.



- 3 In the **Send E-mail to** enter the recipient's e-mail address. For multiple recipients, addresses are separated by a semi-colon.



NOTE: Sending reports does not compromise the security of your data. In fact, Entrapass allows you to protect rpf files with a password. Only recipients with the correct password will be able to access the file. You cannot set a password to CSV files.

- 4 Click the **Execute** button to send the report to the specified recipient. The report will be sent to the workstation selected in the Send to workstation drop-down list and to the specified recipients.

Time and Attendance Reports Definition

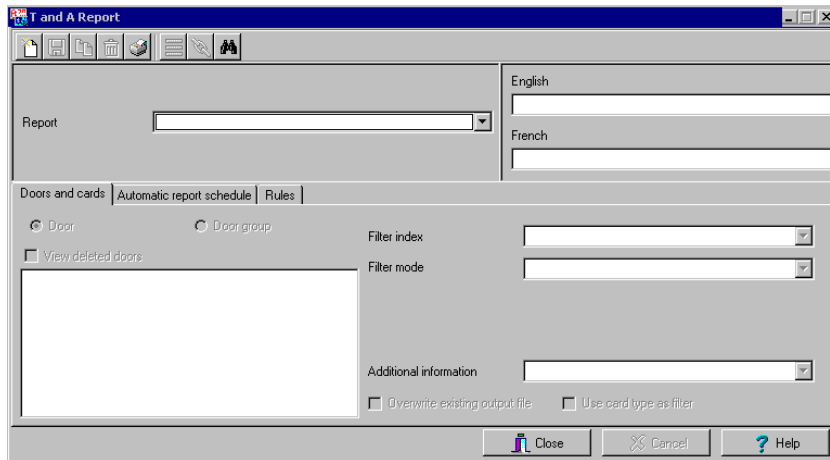
This feature is used to define customized time and attendance reports with automatic execution parameters.



NOTE: Reports can be defined with **automatic settings** so they are generated when you need them or can be requested **manually** using the “Time and attendance report request” icon. When requested manually, automatic settings are **ignored**.

To Define Time and Attendance Reports

- 1 From the Report toolbar, select the **Time and Attendance** icon.



- 2 If you select the **Doors** option, only the doors defined as “Time and attendance” doors (in the Door definition menu) are displayed. Check the **View deleted doors** to add deleted doors to the list. When you select the **Door group** option, the **View deleted doors** option is disabled. The system displays the door groups of your system; then you may select one.
- 3 Check the **Overwrite existing output file** option if you want the system to replace the existing file. If you leave this option unchecked, the system will create another output file.
- 4 Select the **Card** tab to add other filters for the report.
- 5 Select a filter index, then select a filter mode (**None**, **Include**, **Exclude**). If you have selected a filter index, select the filter mode and enter the value range in the **Upper/Lower boundary** fields. To include all the fields, leave the filter mode to **None**. For example, if you select Card number as the Filter index, leave the filter mode to **None** so that all events triggered by cards will appear in the report.



- 6 To add information in the sort criteria, select an item from the **Additional information** drop-down list.



NOTE: Repeat these steps for all the card information fields that are listed in the filter index field. You could use the card user name and specify A to F in the **Upper/Lower boundary** fields for the system to include events in which the defined card numbers appear but only for card users whose names begin with A to F (G and up will not be included even if the card number is included in the range).

- 7 Select the **Automatic report schedule** tab to specify information for automatic reports. For details, see *"To Define Automatic Report Schedules"* on page 276.
- 8 Select the **Rules** tab in the **Time Report** window to define the rules of time and attendance in employee time reports. Rules can be created to define periods of time as specific values. For example, all employee entries between 7:50 AM and 8:15 AM can be defined as the value of 8:00 AM on reports.

Rule type	Lower time	Upper time	Adjust time
1 [dropdown]	00:00	00:00	00:00
2 None	00:00	00:00	00:00
3 None	00:00	00:00	00:00
4 None	00:00	00:00	00:00
5 None	00:00	00:00	00:00

Time and Attendance (T & A) Reports Request

The Request Time and attendance reports feature is used to request the pre-defined Time and Attendance reports that were created using the Time and Attendance Report Definition menu. This feature is useful when you want to override automatic settings.



NOTE: If the report contains automatic settings, these will be ignored.

To Request a T and A Report Manually

- 1 From the Report toolbar, select the **T and A Request** icon. The T and A Request report window appears.

- 2 From the **Report list** display pane, select the Time and Attendance report that you want to execute.
- 3 Specify **Date and time** as well as the **Output parameters**.
- 4 Click **Execute** to trigger the report.



NOTE: The Time and Attendance report is automatically saved in the output folder of the Application selected in the Send to workstation field. For the Paradox output type, the system displays a report preview window. For other output formats, you will have to retrieve the report manually since it is not printed or displayed. To view all the reports that have been generated, use the View report button in the Report toolbar. For details on reports output formats, see "To Define a Report Output Format" on page 279.



Operations On Time and Attendance

Use the Operation on Time and Attendance feature to manually insert, add or delete Time and Attendance transactions in the database. This feature is useful for an organization using the Time and Attendance feature for the payroll system, for instance.

To Add Transaction in the Time and Attendance Database

- 1 From the Report main window, select the **Operation on T and A** icon.

Delete	Date	Time	Transaction	Doors
<input type="checkbox"/>	2001/09/13	12:56	Manual entry	(01.01) 01 - KT200Corporate
<input type="checkbox"/>	2001/09/13	12:56	Manual entry	(01.01) 01 - KT200Corporate

- 2 Enter the **Card number** for which you want to modify the Time and Attendance transactions, then click the **Load** button. If you do not know the number, use the **Find** button.



NOTE: The card number field is mandatory to start loading.

- 3 Select the **View deleted transactions** option if you want to view the transactions that were previously deleted. Deleted transactions are marked with an “X” in the **Delete** column.
- 4 Check the **Find deleted cards** option if you want to find the deleted cards. This does not apply to entries that were added manually.
- 5 Specify the **Start date**, the day on which the system will start to collect the events, by clicking the **Calendar** icon and selecting a specific date. Only events that occurred on this date and after are displayed.



NOTE: The Start date is mandatory to start loading.

- 6 Specify the **End date**, that is the day and time on which the system will stop collecting events. Only events that occurred on the specified date and before are displayed. If you do not specify an end date, the system will include all the data up to the present day time.
- 7 In the **Site** drop-down list, select the appropriate site to view the Time and Attendance doors.



NOTE: The gateway is mandatory to start loading.



- 8 You may check the **All Doors** option, then all the doors displayed under this field will be selected. You may also select specific doors. All the Time and Attendance events that were generated for the selected doors will be displayed.
- 9 Check the View deleted doors option so that even doors that are no longer defined as time and attendance doors (but that have been defined as time and attendance) will be displayed.



NOTE: *Doors are mandatory to start loading.*

- 10 Enter the necessary information in the transaction table. The transaction table displays the transactions for the selected cardholder:
 - The **Delete** column indicates transactions that have been deleted (if the **View deleted transactions** option is checked). These are identified by an X.
 - The **Date** column indicates the date on which the transaction occurred. Use this field to specify the date when you manually insert a new transaction.
 - The **Time** column indicates the time at which the cardholder entered or exited an area. Use this field to specify the time (entry or exit) when manually inserting a new transaction.
 - The **Transaction** column indicates the transaction type. For every entry transaction, there should be an exit transaction.
 - **Entry**—indicates that this is an entry transaction generated when a cardholder presented his/her card at a door defined as entry.
 - **Exit**—Indicates that this is an exit transaction generated when a cardholder presented his/her card at a door defined as “Exit”.
 - **Manual entry**—Indicates that this is an entry transaction that was manually inserted or added in the system. When you manually insert a transaction, you have to specify if this transaction is an “Entry” transaction or an exit transaction. For every entry, there should be an exit.
 - **Manual exit**—Indicates that this is an “exit” transaction that was manually inserted or added in the system. When you manually insert a transaction, you have to specify if this transaction is an entry transaction or an exit transaction. For every entry, there should be an exit.
 - The **Door** column indicates which door was accessed by this user. When you manually insert a transaction, you have to specify the door according to the transaction type (Entry or Exit).



NOTE: *If you are inserting an entry transaction, only doors defined as “Entry doors” will be displayed in the list. If you are inserting an exit transaction, only doors defined as “Exit doors” will be displayed in the list.*

- 11 Click the **Load** button to load the transactions from the server for this cardholder. You have to enter the card number, select the gateway/site, door(s), then click the **Load** button. The button is disabled once you have loaded the transactions.
- 12 Click the **Add** button to add a transaction to the existing transaction list. The new transaction will be added at the end of the list.
- 13 Use the **Insert** button to insert a transaction between existing transactions or above any transaction.

14 Click **Cancel** to cancel any insertion or modification that was made BEFORE saving.

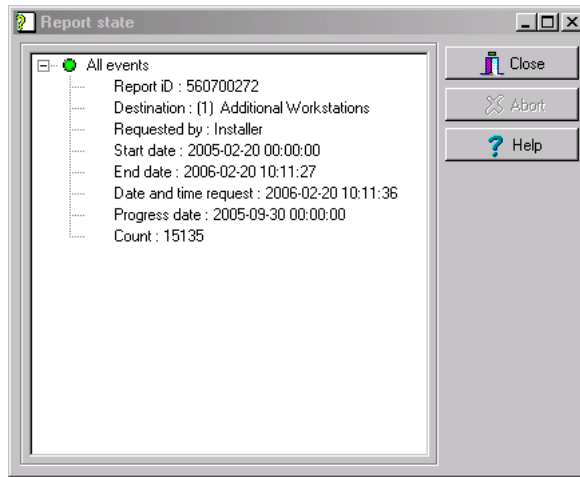


NOTE: *When you delete a transaction that was added manually, it is permanently deleted from the list; as opposed to transactions that were generated by controllers. When they are deleted, they are identified by an X in the Deleted column.*



Report State

Use the **Report state** feature to display a list as well as the status of all requested reports that are still pending.



- 1 To delete/stop a pending report, select it, then click **Abort**.

Reports Viewing

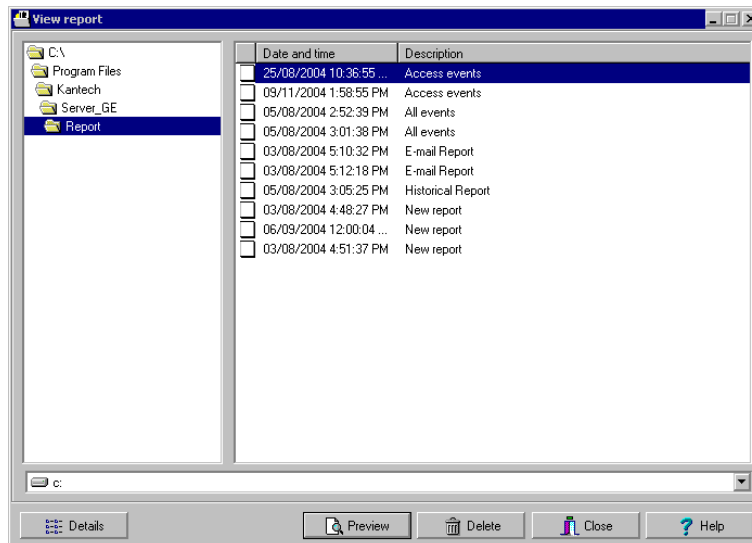
The View Report feature enables users to view the reports that were defined and saved in the system. Operators can use it to view reports in any format, or to customize a report before printing it.



NOTE: When you create a report (csv, db or dbf), the system automatically creates an associated rdf file. This rdf file is the one that is listed in the View report window. When you click “Preview”, the system automatically launches the appropriate program to view the report.

To Display a Report

- 1 From the Report window, select the **View report** icon. The system displays the default destination folder. If the report was saved in a different folder, browse the disk, using the scroll-down arrow (bottom of the window) to the report you want to display.



- 2 Select the report you want to view. If there is a printer installed, the **Preview** button is enabled. It is used to preview the report before printing it.



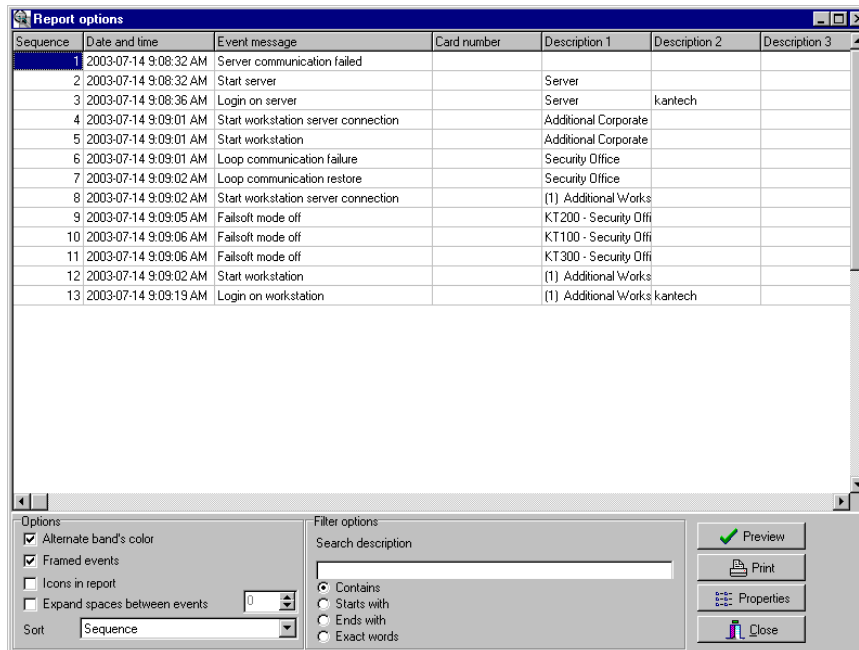
NOTE: You **must** have a printer installed on your computer in order to preview or print reports. To setup a printer, click on **Start > Settings > Printers > Add Printer**. For more information, consult your system administrator.

- 3 Click the **Details** button to display information about the report. If you click the **Details** button, the Report details window appears, displaying information related to the selected report file such as the report filename, title, type, date, etc. To close the Report details window, click the **Details** button again.
- 4 Click the **Preview** button to view the report in the system displays the Report preview window.



To Preview Historical Reports

- 1 From the View report window, select the report you want to view in the right-hand pane. If you select an Historical report, the following window appears. It allows you to customize the report before printing it

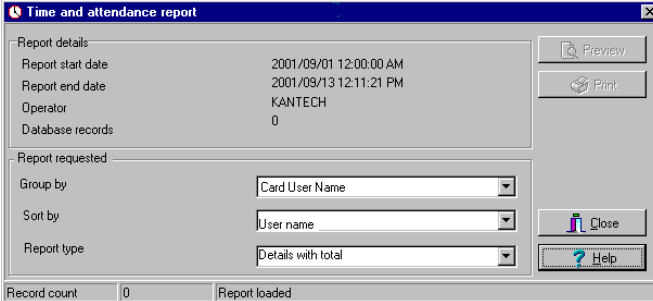


- 2 Select the display options. If one of the following options is selected:
- 3 Define the filter options: enter a text string in the **Search description** field. The report will be sorted leaving only events containing the specified text string. You may refine your filter:
 - **Contains**—All events which contain the specified text will be included in the report.
 - **Starts with**—All events which start with the specified text will be included in the report.
 - **Ends with**—All events which end with the specified text will be included in the report.
 - **Exact words**—All events containing the exact specified text will be included in the report.
- 4 Click **Preview**. The system displays the result of the report. From that window, you can save the report (in a.QRP format) or print the report.
- 5 Use **Properties** to view the settings and details of a pre-defined report. The selected report displays the following information:
 - **Report filename**—Displays the whole path where the report was saved as well as its name.
 - **Report title**—Displays the title of the report.
 - **Start date**—Reports are created for a selected time frame. This option specifies the starting date of this time frame.

- **End date**—Reports are created for a selected time frame. This option specifies the ending date of this time frame as well as the time.
- **Requested**—Displays the date and time at which the report was last requested.
- **Delivered**—Displays the date and time at which the report was produced and printed.
- **Requested by**—Displays the operator name that requested the report.
- **Count**—Displays the number of transactions (lines) in the report.
- **Output process**—Displays a list of the possible templates used for this report.

To Preview Time and Attendance Reports

- 1 From the **View report** window, select the report you want to view. If the selected report was defined as a “Display Time and Attendance Report” and “Paradox Database” as the output format, the following window appears.



- 2 Select the display options:
 - **Group by**— Select this option for easier management. The report data may be grouped by card user names or by card numbers.
 - **Sort by**—You may choose a sort order, by user names, or by card numbers.
 - **Report type**—Select this option for easier management. You may choose to include details with or without total.
- 3 Click **Preview** to display the result of the report. From that window, you can save the report (in.QRP format) or print the report.



Chapter 13 • EntraPass Options

The **Options** toolbar offers users the ability to change a number of system parameters. These include changing the card format, the date and time, or changing server parameters. Some of the system utilities may be accessed from the Server or the Workstation windows.

- Change card format
- Select a language
- Change the system date and time
- Modify the system parameters

The following utilities are available from the **Option** menu only in the EntraPass Workstation application:

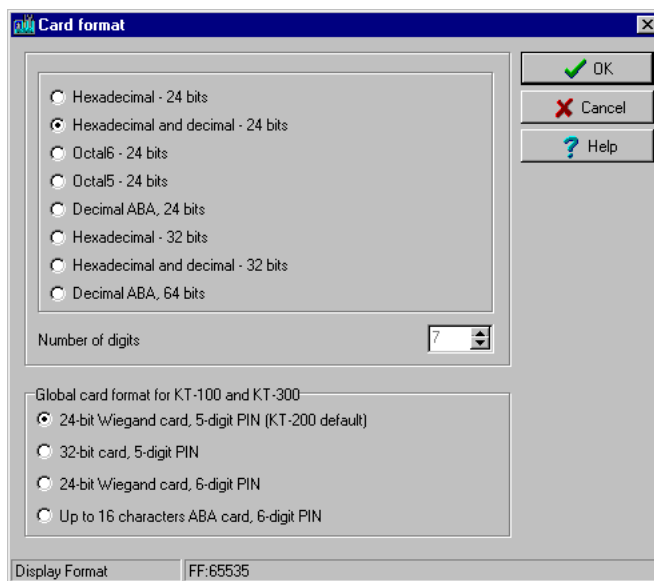
- Printer option (select a log printer and a badge printer)
- Multimedia devices (alarm, video and signature capture settings)
- Verify database integrity
- Custom Messages

Card Format Modification

The system can accommodate various reader types. Depending on the reader type, the card display format may vary. Use this menu to specify how the system will display the card numbers

To Define a Display Format

- 1 From the Options main window, select the **Card format** icon.



- 2 Select a display format—When you select a format, the system displays a preview of the selected format in the bottom part of the window.
 - **Decimal**—Refers to numbers in base 10.
 - **Octal**—Each octal digit represents exactly three binary digits. An octal format refers to the base-8 number system, which uses eight unique symbols (0, 1, 2, 3, 4, 5, 6, and 7). Programs often display data in octal format because this format is relatively easy for humans to read and can easily be translated into a binary format, the format used in computer programming.
 - **Hexadecimal**—Each hexadecimal digit represents four binary digits. An hexadecimal format refers to the base-16 number system, which consists of 16 unique symbols: the numbers 0 to 9 and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (8 bits) as two consecutive hexadecimal digits. It is easier for humans to read hexadecimal numbers than binary numbers.



- 3 Indicate **How many digits** are to be displayed. You may use the up/down controls. When a 64-bit decimal format is chosen, it is possible to specify the number of digits the system must use.



NOTE: *Avoid alternating between different card formats because this may result in lost card information.*

NOTE: *KT100 and KT300 Controllers will do a hard reset on format change.*

System Language Selection

EntraPass allows you to run the software in the language of your choice. The basic languages are English, French, Spanish and German. The Vocabulary Editor utility enable users to add other custom languages.

To Change the System Language

- 1 From the EntraPass main window, select the **Options** tab, then select the **Select language** icon.



NOTE: *Important note: When you modify the primary language, the database operation will be suspended during the operation and the changes will be effective only when you shutdown and then restart the system. The database language will be modified according the ascii values of the characters in the primary language. Accents and special characters of different languages may have an impact on your database.*

- 2 From the **Select primary language** drop-down list, select the language you want to use as a primary language. From the **Select Secondary language** drop-down list, select the language you want to use as a secondary language.
- 3 Restart your computer, and login to EntraPass.

Printers Selection and Configuration

The **Printer option** menu allows users to select a log printer that will be used when printing events and to select a badge printer that will be used to print badges.

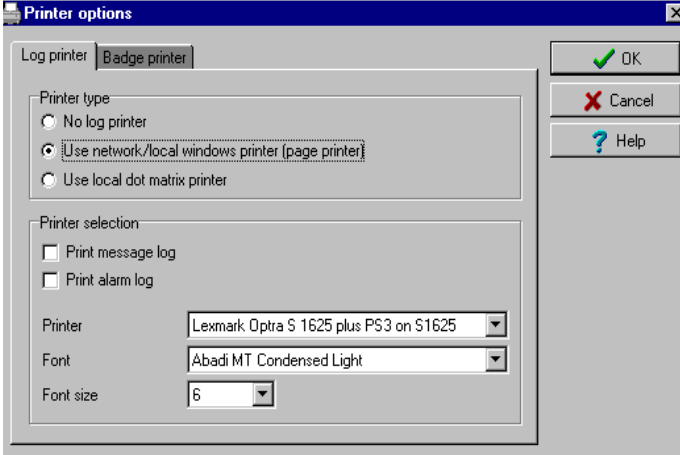
To Select and Set Up a Log Printer

When you define events (in the **Events parameters** definition menu), it is possible to determine how and when events will be printed. For example, you can decide to dispatch events to an EntraPass application, a printer, or to activate a relay. Your decision may be based on, for instance, schedules that will send alarms to a remote terminal at a specific moment.



NOTE: You need to assign a “print” schedule to certain events to print them at a specified time.

- 1 From the Options menu, select the **Printer option** icon.



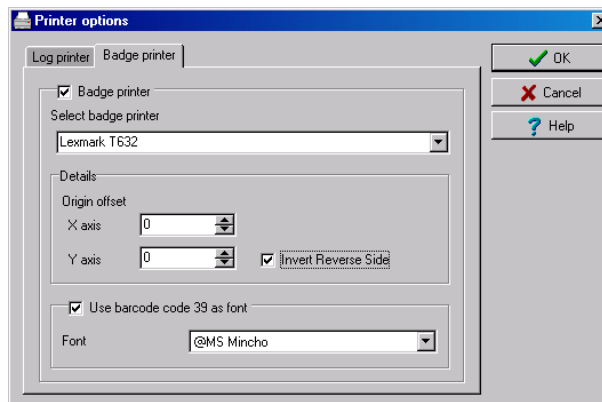
- 2 Select a printing option in the **Log printer** section:
 - **No log printer**—If you select this option, no event will be printed, even if a print schedule is defined for the events.
 - **Use Network/Local Windows printer (page printer)**—If you select this option, all events sent to the printer will be buffered and printed when a full page is ready to be printed. Events will be printed on the network/local printer - not on a specific log printer.
 - **Use local dot matrix printer**—If you select this option, all events sent to the printer will be printed one-by-one and one under the other, or it will print one event per page, depending on your printer type. Select the printer port that will be used in the “printer” field. Specify if messages and alarms will be printed on this printer.
- 3 In the **Printer selection** section, specify whether you want to print message or alarms.
 - **Print messages log**—If you select this option, all events that are assigned a “display” schedule in the events parameters menu will be printed.



- **Print alarms logs**—If you select this option, all events that are assigned an “alarm” schedule (and need to be acknowledged) in the events parameters menu will be printed.
- 4 From the **Printer** drop-down list, select the specific printer that will be used as a log printer.
 - If you have selected a **dot matrix printer**, select the **Port** on which the printer is connected to communicate with the computer. The **Port** field appears when a dot matrix printer is selected.
 - If you are using a **network/local printer**, select the **Font** and the **Font size**. The font and font size influence the number of events that will be printed on one page. Using a smaller font increases the number of events printed on a page.

To Select and Set Up a Badge Printer

- 1 From the Printer option window, select the **Badge printer** tab.



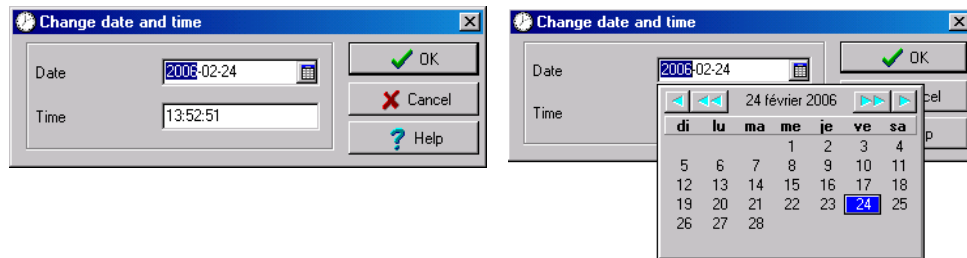
- 2 Check the **Badge printer** option if a badge printer will be used; as a result, the Print badge and Preview badge button will be displayed in the Card.
- 3 From the **Select badge printer** drop-down list, select the appropriate badge printer.
- 4 If you want the picture on the reverse side of the badge to be inverted, click the **Invert Reverse Side** box.



System Date & Time Modification

The **Change system y** option should be used with caution and only when necessary; this functions may affect logical components of the access system (i.e. schedules, etc.).

- 1 From the Option main window, select the **Change System date and time** icon.



- 2 Enter the date in the **Date** field, or select a date from the calendar. Connected components of this application will also receive the date change notification.
- 3 Enter the time in the **Time** field. Connected components of this application will also receive the time change notification.
- 4 Click **OK** to exit.

IMPORTANT NOTE: You should not change the time using Windows settings. It is strongly recommended to change the system time through the server parameter settings.

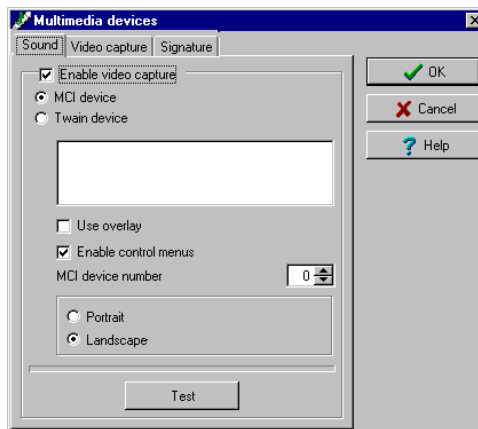
Multimedia Devices Configuration

The Multimedia devices utility allows you to set up your system multimedia objects:

- Alarm sound
- Video capture devices
- Signature capture devices

To Select an Alarm Sound

- 1 From the Options main window, select the **Multimedia devices** icon.



- 2 Check the **Enable alarm sound** option if you want an alarm sound notification.
- 3 Select a sound from the displayed list.
- 4 Select a **Priority** level for the selected sound so that it is played when an alarm defined with this priority is sounded.



NOTE: The **Priority** level refers to the order in which alarm messages are displayed in the Alarm desktop. In *EntraPass*, 0 is associated with the highest priority, and 9 to the lowest. For more information, see "Event Parameters Definition" on page 225.

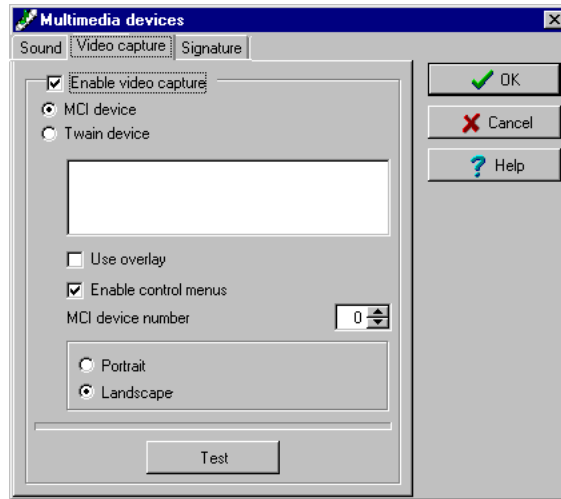
- 5 Click the **Play** button to listen to the selected sound. The system will play the selected sound.
- 6 Click the **Add** button to add a new sound from your personal files. Clicking on this button displays a new window allowing you to add new alarm sounds.



NOTE: The **Current selection** section displays the sound currently selected (in use). You can adjust the delay of the alarm sound in the **Delay** field.

To Define Video Options

- 1 From the Multimedia devices window, select the **Video capture** tab.

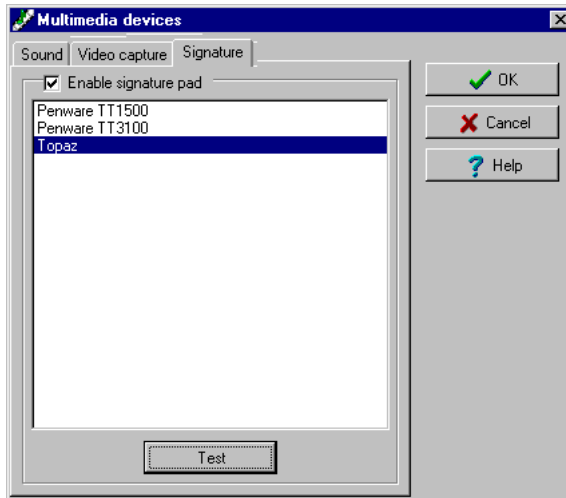


- 2 Check the **Enable video capture** box to enable the video capture options in your system.
 - **MCI device**: Standard Windows capture drivers.
 - **Twain device**: Twain capture drivers. (Recommended).
 - **Use overlay**: Option activated for image capture devices.
 - **Enable controls menu**: Activates options (such as zoom, pan and tilt) on image capture devices, if applicable.
 - **MCI device number**: Select identification number of MCI device.
 - **Portrait**: Enables portrait orientation of captured images.
 - **Landscape**: Enables landscape orientation of captured images. (Default value).
- 3 Click the **Test** button to verify if the video camera is functional.



To Set Up the Signature Capture Device

- 1 From the Multimedia devices window, select the **Signature** tab.



- 2 Check the **Enable Signature pad** option to enable the use of a signature pad device.
- 3 From the displayed list of supported Signature pad devices, select the driver for the signature pad you want to use.



NOTE: The **Test** button allows you to check if the driver selected is functional. When you click the **Test** button, the Signature Pad Test window appears. This window appears whenever you choose the **Signature pad** option (Card definition windows).

System Options

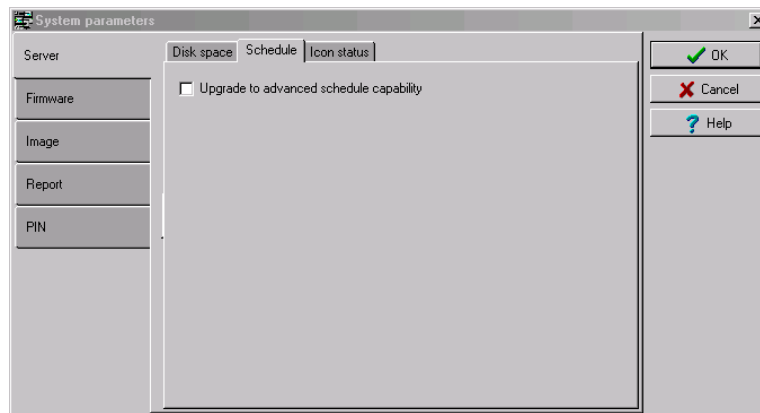
Server Parameters

Under the **Server** tab, you will define disk space threshold and icon status

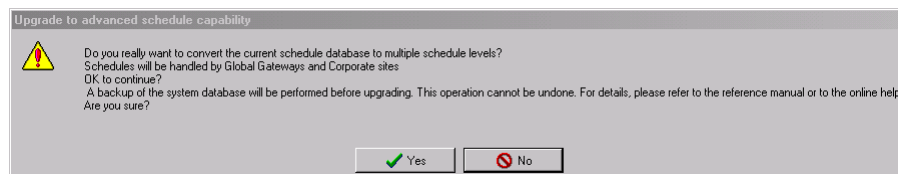
Schedule

The **Schedule** tab is where you will be able to upgrade to advanced schedule capability. In fact, EntraPass offers users more flexibility and ease of use by grouping schedules per site or system logical components. This option is not automatically enabled upon installation of this new version. Schedules are grouped as follows:

- **System schedules:** System schedules are applicable to system logical components such as: event parameters, operators login schedules, video triggers, etc. System schedules are not loaded in a particular controller; they are applicable to all the system. You can program an unlimited number of system schedules.



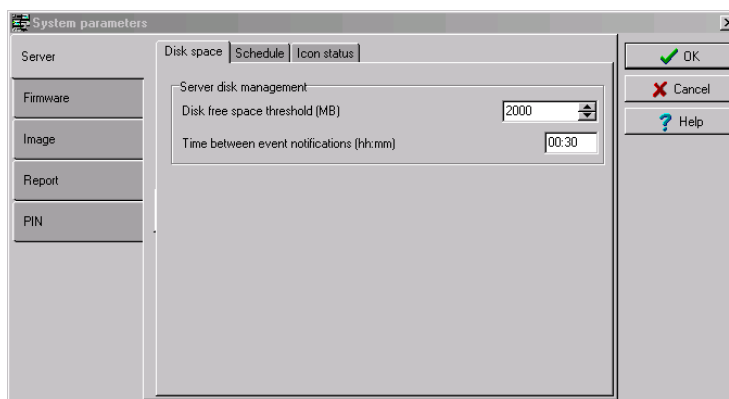
- After checking the box and clicking **OK**, a warning will popup on screen indicating that the action is irreversible before it performs a backup of your data.



Disk Space

The Disk Space feature has been developed as a protection against system failures that may be caused by the lack of disk space. This feature allows you to monitor the amount of free disk space

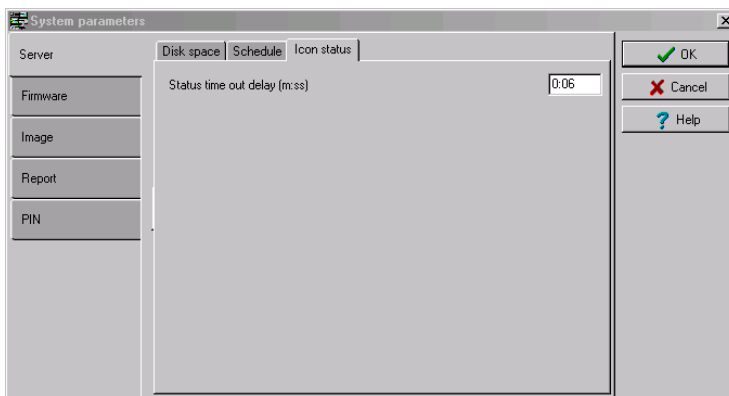
for optimal system operation or for generating reports. In fact, EntraPass offers the ability to have the system abort the execution of a report if the free disk space has reached a specified threshold.



- **Disk free space threshold (MB)** scroll-down list: specify a disk space threshold that indicates when you want the system to send a warning when the amount of free space falls below the value indicated. This value is in mega bytes.
- **Time between notifications (hh:mm)** field: enter the amount of time between notifications when the disk free space has reached the quota specified in the **Disk space threshold** field. For example, if you enter 00:30 in the field, a system warning will be displayed every half an hour.

Icon Status

The Status time out delay (mm:ss) parameter allows you to define a period of time before the server queries workstations for the latest icon statuses. The higher the delay, the lower the icon refresh rate will be therefore creating less traffic on the network.

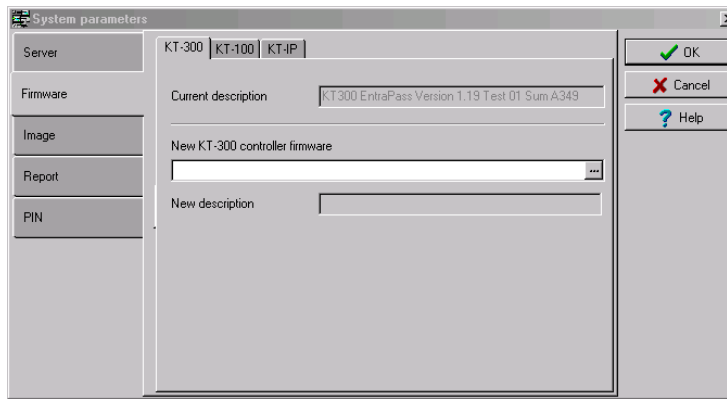


Firmware Parameters

This section contains all the information pertaining to your controllers, as well as the section to update your firmware.

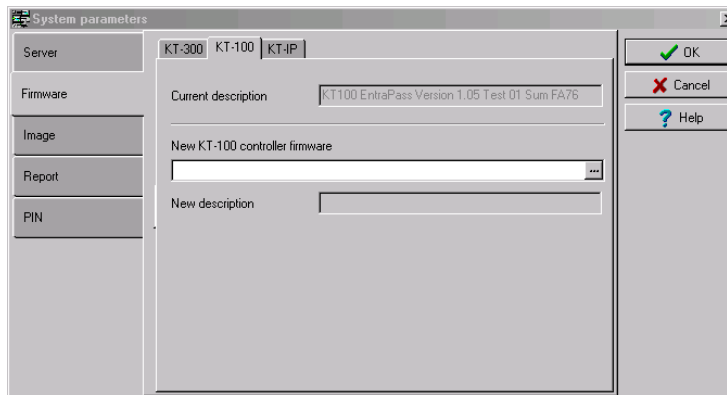
KT-300

The **KT-300** tab specifies the location of the folder containing the firmware for KT-300 controllers. The system will use this data to update the installed controllers.



KT-100

The **KT-100** tab specifies the location of the folder containing the firmware for KT-100 controllers. The system will use this data to update the installed controllers.



KT-IP

The **KT-IP** tab specifies the location of the folder containing the firmware for Kantech IP Link module. The system will use this data to update the installed controllers.

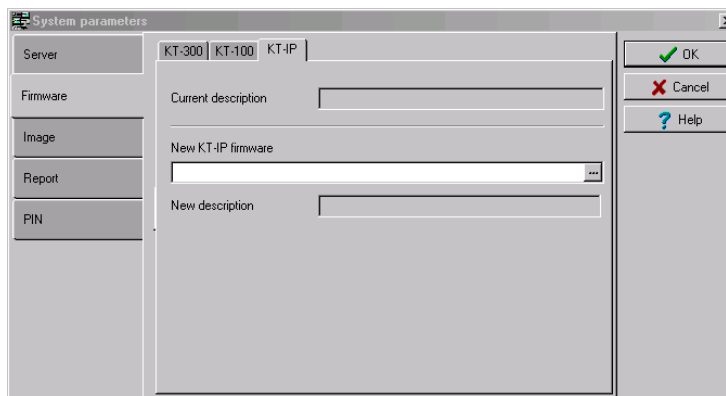


Image Parameters

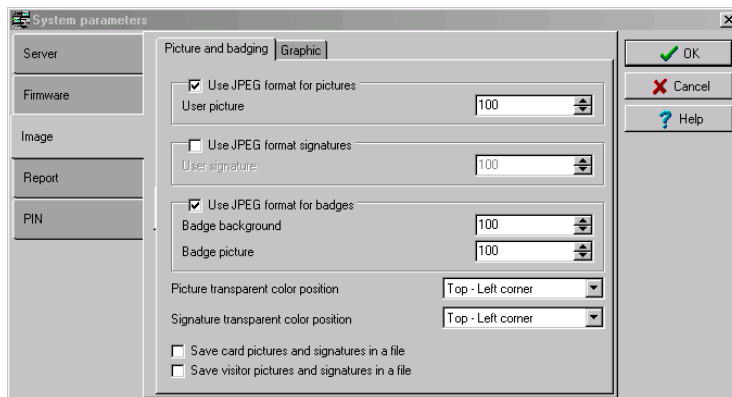
the Image directory is where you will define parameters for the badging features. You will define image quality for picture, signature and background images.

If you are using the badging feature, it is recommended to leave the jpeg quality to default. If you are not using the badging feature, you may reduce the jpeg quality of your images so that they will not occupy a large space in the database. You must take in consideration, however, that reducing the quality of the saved images may affect the quality of the photos imported into badges.

A parameter allows you to save cards and visitor card pictures, signatures and background graphics to a file instead of directly to the database. We are offering this option for sites that have large banks of pictures and graphics. The picture, signature and graphic database can currently contain up to 2 Gb of data each. The parameter will be used in instances where a site may need more space to save pictures, signatures and graphics.

Picture and Badging

The picture and badging feature allows you to adjust the image and signature quality for use with the Badging feature.



- Unchecking **Use JPEG format for pictures, signatures and badges** tells the system to save pictures (or signatures) in a tiff format.



NOTE: Remember that this may affect the image quality. If you are not an advanced user, leave these values to default.

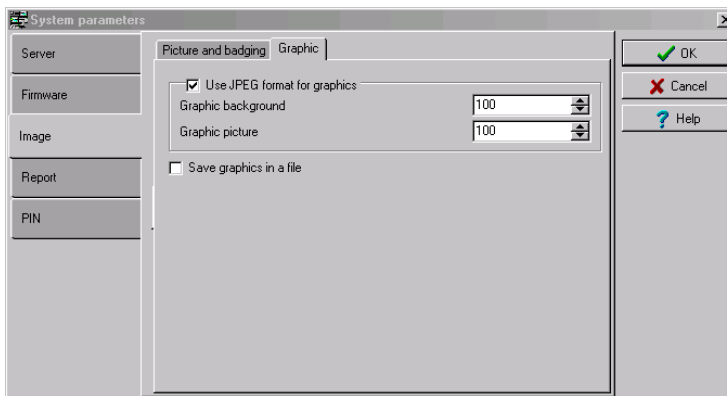
- The **User picture, Signature, Badge background** and **Badge picture** indicate the quality of the image that will be saved. If you choose 0, the saved image quality will be poor; 100 indicates an excellent quality.
- Select the location of the **Picture (Signature) transparent color position** for pictures and signature. Four choices are available (top-right, top-left, bottom-right and bottom-left). By default, the system chooses the bottom left-hand corner for the transparent background color. EntraPass allows operators to choose a more suitable color.
- When checking the **Save pictures (signatures) in a file** box, the system will create **Picture** and **Signature** directories under **C:\Program Files\Kantech\Server_SE\Data** where all pictures and signatures will be saved instead of directly in the database.
- When checking the **Save visitor pictures (signatures) in a file** box, the system will create **Picture** and **Signature** directories under **C:\Program Files\Kantech\Server_SE\Data** where all visitor pictures and signatures will be saved instead of directly in the database.



NOTE: When modifying an existing picture or signature, EntraPass will save it to the appropriate file and delete the corresponding entry in the database.

Graphic

The graphic feature allows you to adjust the graphic quality for use with the EntraPass software.



- Unchecking **Use JPEG format for pictures (signatures)** tells the system to save pictures (or signatures) in a tiff format.

NOTE: Remember that this may affect the image quality. If you are not an advanced user, leave these values to default.

- The Jpeg quality value for **Graphic background (picture)** indicates the quality of the image that will be saved. If you choose 0, the saved image quality will be poor; 100 indicates an excellent quality.
- When checking the **Save graphics in a file** box, the system will create a **Graphic** directory under **C:\Program Files\Kantech\Server_SE\Data** where all graphics will be saved instead of directly in the database.



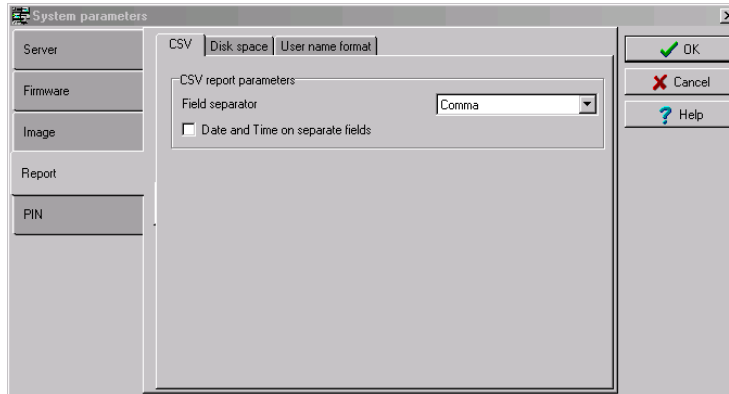
NOTE: When modifying an existing graphics, EntraPass will save it to the appropriate file and delete the corresponding entry in the database.

Report Parameters

The **Report** tab enable users to define the field separator for reports, disk space threshold and user name format.

CSV

Under the **CSV** tab, you can define the field separator for your reports.



- By default, the system uses a comma (,) as the **Field separator**. You can modify the comma for another character. Other options are: Period, Equal, Semicolon, Colon, Space and tab.
- It is recommended to check the **Date and time on separate fields** option. When selected, CSV (comma separated values) as the output process for your reports, by default, the system includes the date and the time in a single field. When you select this option, the system will separate the date and the time fields.

Disk Space

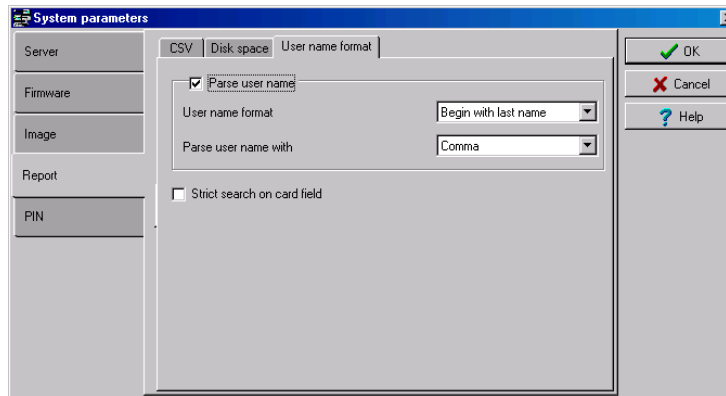
This feature is a protection when for instance a huge report has been requested. In this case, the system will abort the execution of the report and displays an alert message indicating the reason of the abortion.



- **Abort report if free space lower than (MB)** scroll-down list allows you to specify the minimum amount of free disk space required for the execution of reports.

User Name Format

Specifying the user name format will tell the system how cardholder's names will be sorted by the system.



- **Parse user name** should be checked if you want to select a method of parsing the user's name in the system.
- **User name format** lets you select the parsing method. Options are: Begin with last name, Begin with first name.
- **Parse user name with** lets you select the character that will be used to parse the user name fields. Options are: Comma, Period, Equal, Semicolon, Colon, Space.
- **Strict search on card field** should be left empty unless you wish to keep the previous method (EntraPass Version 3.17 and lower) of strict searching a card field for reports.

NOTE: Prior to version 3.18 of EntraPass, the system used a strict search method that required Administrators to enter specific upper and lower boundaries to attain specific results. For example, for generating a report that included all users whose last name started with A, the lower boundary had to be A and the upper boundary had to be AZZZZZ. Now, the system will display all user names that start with an A just by entering A as a lower and upper boundary.

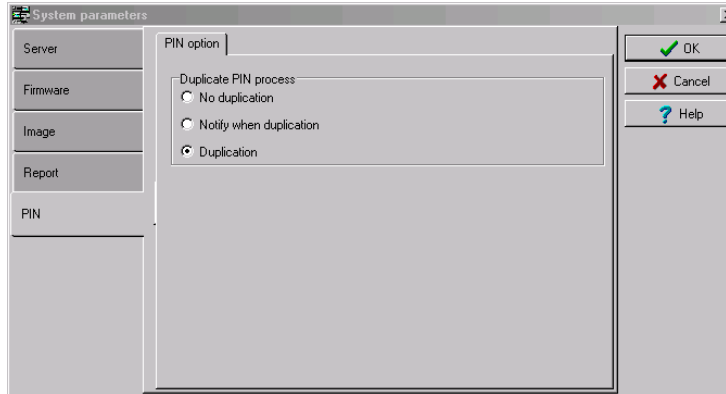
PIN Parameters

EntraPass has the ability to prevent or allow PIN duplication. The system can also be configured to send a notification if a PIN is duplicated. Each time a card is issued, the system checks the PIN settings.

This feature can be used for example while loading cards in a batch. An operator may decide to set the PIN option to allow duplication. Later, if desired, the duplicate PINs can be changed to prevent confusion.



NOTE: *Optionally, the operator can display the list of PIN owners. For details, see "To View and Verify PINs" on page 132.*



In the **Duplicate PIN process** section:

- **No duplication:** a warning appears on the workstation, the PIN field will be reset to the value you are attempting to duplicate and will be enabled, inviting you to enter a valid PIN. Only PIN 00000 will be duplicated regardless of the PIN setting option.
- **Notify when duplication:** the server verifies if this PIN already exists. If the PIN exists, a message box appears, indicating that the PIN exists. A **Details** button will allow operators to view a list of cardholders who were issued this PIN.
- **Duplication:** no test will be processed, the PIN will be accepted even if it is a duplicate.



NOTE: *By default, the system will automatically backup your files every Sunday at 4:00 AM for all new installations. Setting this feature at 4:00AM has an added benefit of not interfering with the system processing time or other tasks scheduled around midnight.*



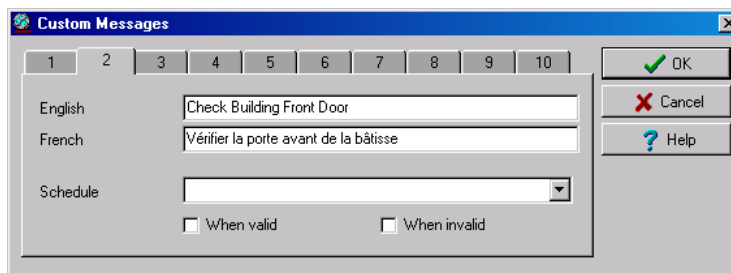
Custom Messages

The Custom Messages option allows operators with proper security rights to define custom messages that can generate an event based on a schedule. Up to 10 custom messages can be programmed to trigger an event at a preset time. And each custom message can be triggered when the schedule becomes valid, invalid, or both. In other words, you can trigger up to 20 custom events if you take into account the start and/or end of a schedule interval.

Each custom events will be displayed in the Messages List on the Desktops.

To Set Up Custom Messages

- 1 From the Options Main window, click **Custom Messages**.



- 2 In the first tab, enter the first custom message you want to see display in the Messages List. Two fields are available for primary and secondary languages.
- 3 Select a preset schedule that will determine when the custom event will be triggered.
- 4 Select if you want the custom event to be triggered when the schedule becomes **Valid** or **Invalid**, or both.
- 5 Move to the second tab to enter a second custom message, and so on.

Database Integrity Verification

The database utility program allows to verify and to repair the system databases. When the **Database Utility** is launched, the system scans all the tables for any possible errors and repairs them automatically.

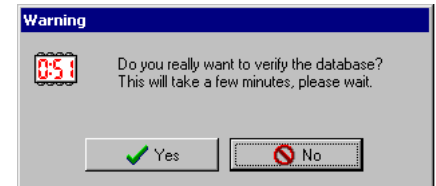
Note that when you launch the **Verify Database** Integrity utility from the EntraPass application menu, this is a surface operation. If your system is experiencing problems, when your system experiences problems, you have to run the Database Utility program from Windows Start menu

To Perform a Quick Verification of the Database Integrity

- 1 From the Option toolbar, click the Database Integrity icon. The system displays a warning.
- 2 Select **Yes** to continue.



NOTE: When you launch the **Verify Database Integrity** utility from the *EntraPass* application menu, this is a surface operation. If your system is experiencing problems, you must run the Database Utility program from Windows Start menu.





Chapter 14 • The Server Module

The EntraPass Server manages the access control system database. It receives and dispatches information received from the gateways and the workstation receiving information from connected controller sites.

The server module is used for:

- Creating and restoring backups (Data, Archives, Time and Attendance databases)
- Restoring data (Data, Archive, Time and Attendance databases)
- Verifying database integrity



Backups

A backup is a copy of your system database which serves as a substitute or alternative in case the computer fails. Backing up your files safeguards them against accidental loss when for example the hard disk fails or when you accidentally overwrite or delete data.

If your system computer fails, you may restore a backup copy onto another computer (on which the EntraPass software has been installed). The EntraPass **Backup** tab allows operators to perform manual backups of the system data, archive and time and attendance databases. It is also used to restore backup data.

Safeguard tips:

- Back up your files regularly, at least once a week or more if many modifications were made to the database.
- We recommend that you make two backups of all your database files. To be safe, keep them in different locations.
- To backup your files, you can use:
 - The menu of the EntraPass Backup utility, or
 - Other third party software and hardware.



NOTE: By default when you backup or restore files, the EntraPass databases will temporarily be disabled. The second colored square of the database status turns red when the database is unavailable. The Workstations will not be able to modify the databases.

All the system data can be found under the following path: C:\Program Files\Kantech\Server\XXXX. If you are using a third party program to perform backups, it is recommended to backup the whole Kantech directory and sub-directories.

Each time a backup is done (even if it is done automatically), a new sub-folder containing the data or the self-extracting file is created. If you are using the “incremental” backup type and you want to restore information, you will have to restore all the sub-folders one-by-one (starting with the oldest).

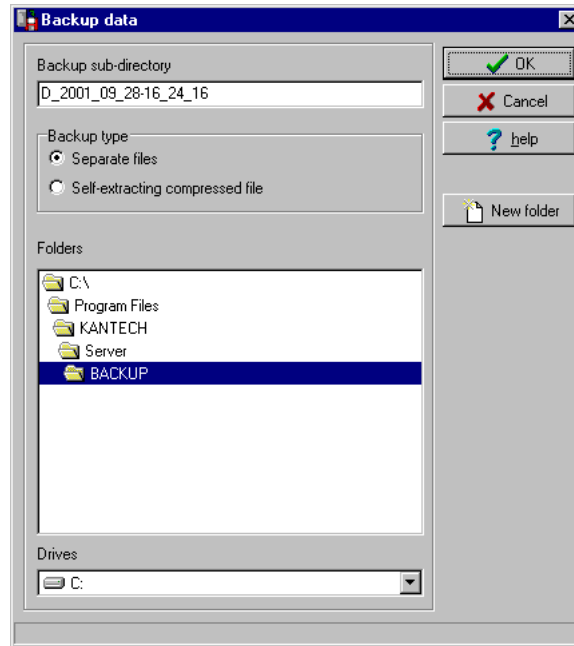
To Create Backups of Type D, A, and T

By default, the name of the sub-directory in which the data/archive/time and attendance databases will be saved is generated automatically according to the following convention: X_YYYY_MM_DD-h_mm_ss, where X is the data type (D for Data, A for archive and T for Time and Attendance).

The following steps explain how to backup data. The same steps apply also when you backup archives or time and attendance data.



- 1 Select the item you want to backup: data, archive, time and attendance databases. The system displays the backup sub-directory in which the information will be saved. You may keep the default folder, or you may browse your disk to specify a new destination folder for the backup.



NOTE: By default, the system/workstation will backup all the information originating from the following directory: C:\Program Files\Kantech\Server_SE \Data or Archive or Time and attendance to C:\Program Files\Kantech\Server\Backup\X_YYYY_MM_DD-h_mm_ss, where X is the data type. The data type is followed by the year, month and day information as well as the time of the backup.

- 2 Select the Backup type:
 - **Separate file:** the system will back up the databases one by one (standard). This backup type includes the *Regdata.ini* file containing the following identification data: software used to create the backup, backup type (data, archive, time and attendance), operator who requested the backup, date and time of the backup as well as the software version.
 - **Self-extracting compressed file:** the system will create an executable file (.exe) that will compress the information so as to reduce the amount of disk space taken by the backup. The system displays information identifying the backup: software used to create the backup, backup type (data, archive, time and attendance), operator who requested the backup, date and time of the backup as well as the software version.
- 3 From the **Drives** drop-down list, select the drive on which the backup will be performed. A list of choices is available according to your computer settings. To save as default, leave as is.
- 4 You may click the **New folder** button if you want to specify a new destination folder.



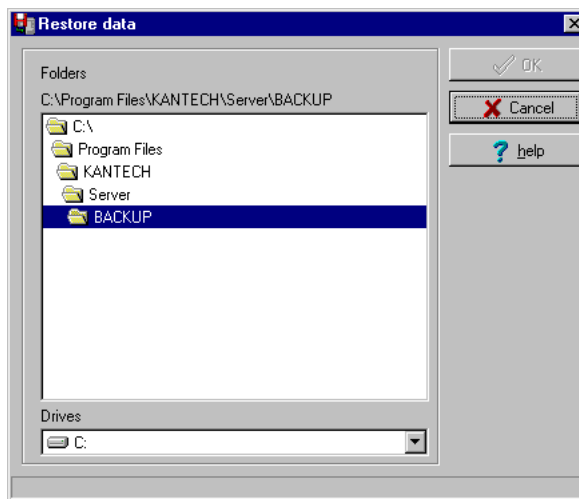
- 5 Click **OK** to launch the backup procedure. The backup process can be viewed on the bottom part of the window.

To Restore Data (D, A and T)

If you are restoring data, it is strongly recommended to perform a backup before.

If you are using a third party program to restore the data, it is recommend to restore the whole Kantech directory and sub-directories.

- 1 From the Server window, select the desired **Restore** button (**Data, Archive, Time and attendance**). The system displays the Restore data window. It displays the path of the backup folder.



NOTE: By default, the system restores all the information originating from the following directory: *C:\ProgramFiles\Kantech\ Server_SE\Backup\ X_YYYY_MM_DD-h_mm_ss* to *C:\Program Files\Kantech\ Server_SE\Data* or *Archive* or *Time and Attendance*.

- 2 To change the destination folder, browse the **Drives** drop-down list. Click **OK** to launch the restore process.



NOTE: It is recommended to reload the Gateway after restoring the data (**Operation > Reload data**).

Chapter 15 • System Utilities

This section groups the utility programs of the EntraPass Software. These programs are accessible from the Windows **Start** menu.

- **Database Utility** —Program intended to re-index archived files, update database fields, verify archived files, verify the database integrity, verify the database index, verify the database links and to verify the database hierarchy while the server is shutdown.
- **Express Setup** —Program used to configure all the components related to a gateway including the type of readers used, type of connection, number of controller sites, number of controllers in a site, etc.
- **Quick Report Viewer** —Program used by the operator to view reports without having to start EntraPass.
- **System Report Viewer**—Program used by the operator to view reports without having to start EntraPass. This utility is installed from the Setup window.
- **Vocabulary Editor**—Program used to translate, in the language of your choice, the display text of the software.

Database Utility

Since the information from the system databases is sent back and forth between components, some data might end up in the wrong table.

Some of these verifications such as re-indexing the archive files, updating database fields, verifying archive files, or swapping database descriptions require that the Server be shutdown.

When an operation that requires the server to be shutdown is launched, the operator is warned that the databases will be suspended during the operation.

From EntraPass, the Database utility program verifies the integrity of the tables that are used to store events, alarms, network alarms, and graphic. Basically, the system scans all the system tables and correct errors (if they are found).

You may want to start this utility when your systems hangs up frequently.

To Verify the Database Integrity

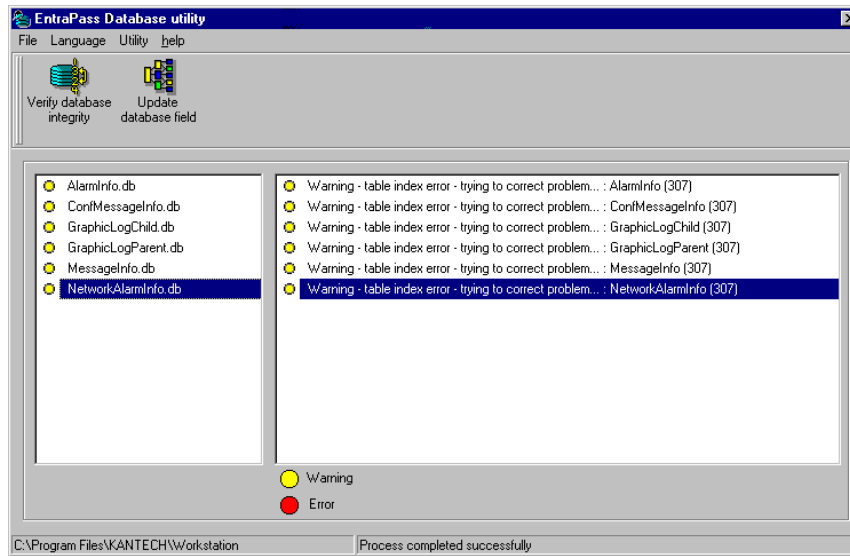
The database utility program allows to verify and to repair the system databases. When the **Database Utility** is launched, the system scans all the tables for any possible errors and repairs them automatically.

- 1 You can use the icons under the Utility tab in the EntraPass server application, or launch the Database Utility from the Windows® **Start > Programs > EntraPass Global > Workstation > Database Utility** menu.
- 2 To verify the database integrity, click the **Verify database integrity** icon in the toolbar. You have the choice to perform a **quick** or **complete** check.

NOTE: *When you launch the Verify database integrity utility from the Options menu, this is only a surface operation. When your system hangs frequently, you have to run the Database Utility program.*

- 3 Select the type of verification you want to perform. If you select a quick check, the system scan through the tables, but does not display a detailed report after.

- 4 If you select a **Complete check of the database**, a detailed report is displayed.

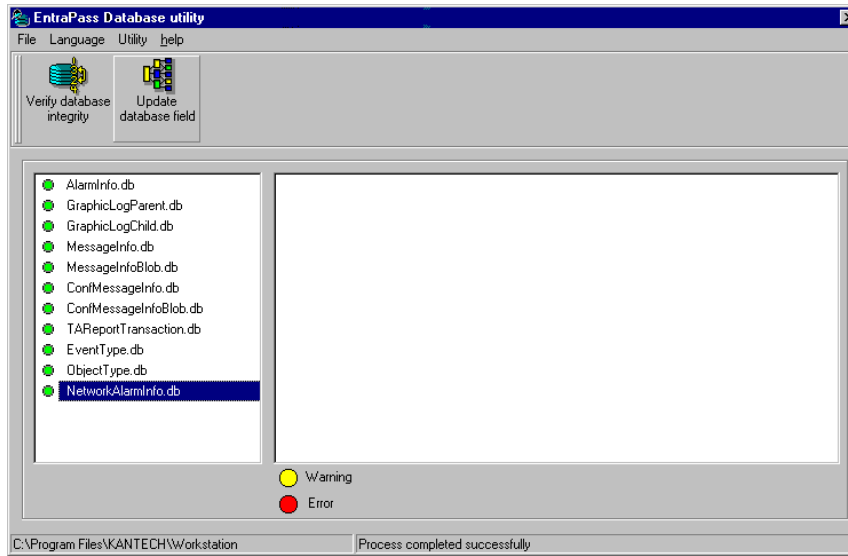


To Update Database Fields

This function is automatically executed when the software is updated.

If an operator performs a database restore (**Server, Options** tab, **Restore**), the database fields are automatically updated when the information is restored. Even when an operator performs a database restore outside the Server (copies the databases from a third party backup program), this function is automatically carried out when the Server is started up again.

- 1 From the EntraPass Database utility window, select the **Update database field** icon.



NOTE: When the system does not start, this may imply that there are problems in the database; that the source and the structure do not match, for instance.

Vocabulary Editor

The Vocabulary Editor allows users to translate the display text of the software in the language of their choice.

Entrapass offers you the possibility of adding up to 99 languages for the purpose of changing the text language in the graphic user interface. However, you can only run the software in two languages at a time, a primary and a secondary language.

If you want to use the software in a language other than English, French, German or Spanish, you can have the database dictionary translated in the language of your choice. You will then have to integrate the translated dictionary in the software. The creation of a new display language is carried out in three stages:

- Translating the source text,
- Integrating the newly created language to the Entrapass dictionary in the Server,
- Distributing the new custom language to all Entrapass application.



NOTE: *In order to be able to run a new language, your operating system (Windows) must support the desired language. For example, your keyboard (characters) and window (display) must support the specific characters of the desired language. The computers where Entrapass applications are running must also support the language. For more information on language support, refer to your system administrator.*

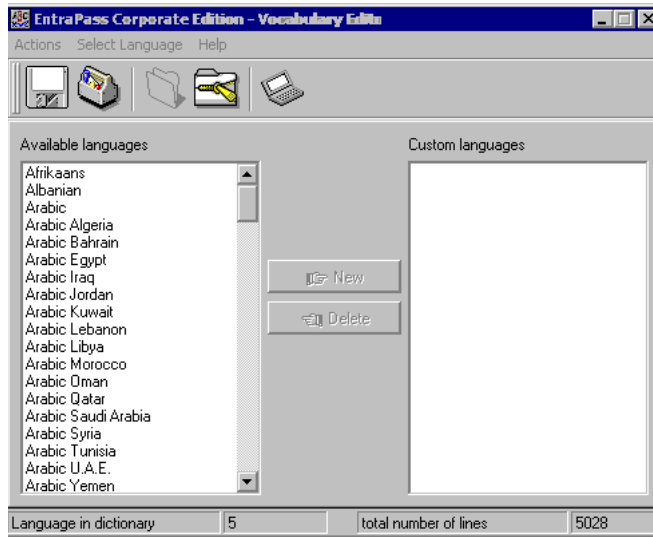
To Install the Vocabulary Editor


Entrapass Vocabulary Editor is a stand-alone program. You can install it and run it independently. If you want to translate the system language, you just have to install the Vocabulary editor and then to translate the vocabulary database.

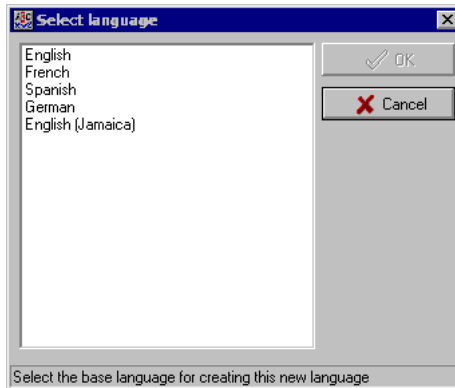
To Translate the System Language


Entrapass Vocabulary Editor is a stand-alone program. You can run it independently, you do not need to launch Entrapass software to run the Vocabulary editor. The Vocabulary Editor program will assist you if you want to translate the software in a language, other than English, French, Spanish or German.

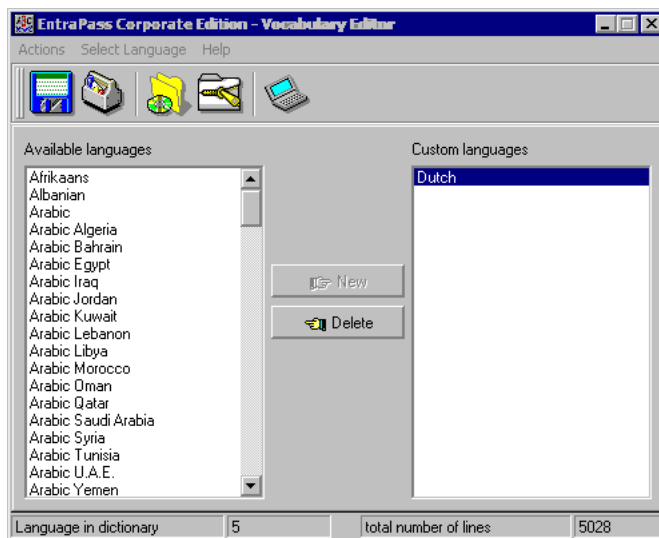
- 1 Start the Vocabulary editor from the Windows **Start** menu: click **Start > Programs > EntraPass Special Edition > Vocabulary Editor > Vocabulary Editor**.



- 2 From the available **Language list**, select the new language, then click **New** . The system displays again the **Select language** window. Select the source language for the translation, then click **OK**. The newly selected language is transferred to the right in the **Custom Languages** display list. The **Edit** and **Delete** buttons are enabled.

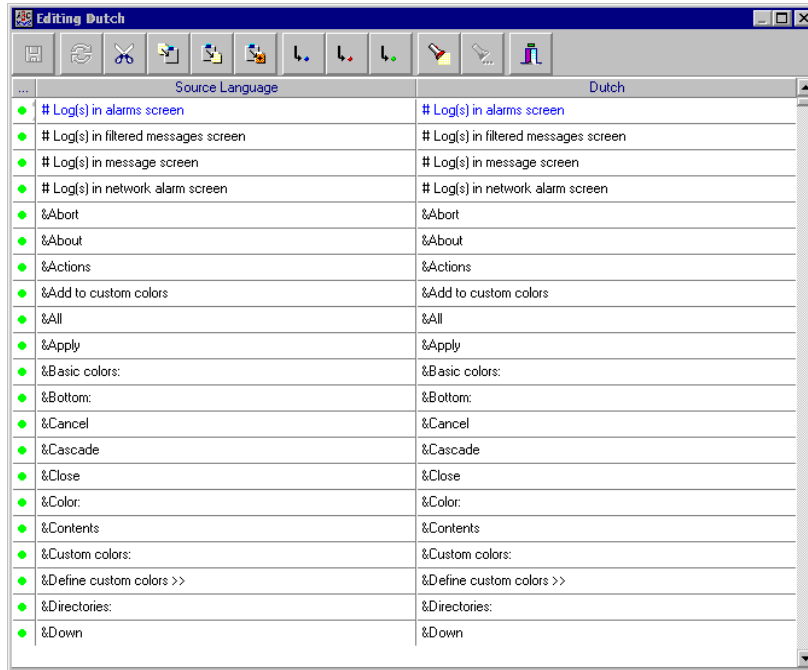


- 3 Select **Edit**  to view the vocabulary database table.





- In the Vocabulary Editor window, click the **Edit** button to start translating the software vocabulary. The system displays the dictionary database.



NOTE: You must make sure that the Customdictionary directories are regularly backed up (C:\ProgramFiles\Kantech\Vocabulary Editor\CustomDictionary\files.xxx.ath) or C:\ProgramFiles\Kantech\ "Application type" \CustomDictionary\files.xxx.0

The table below shows the value of the Vocabulary Editor color codes.

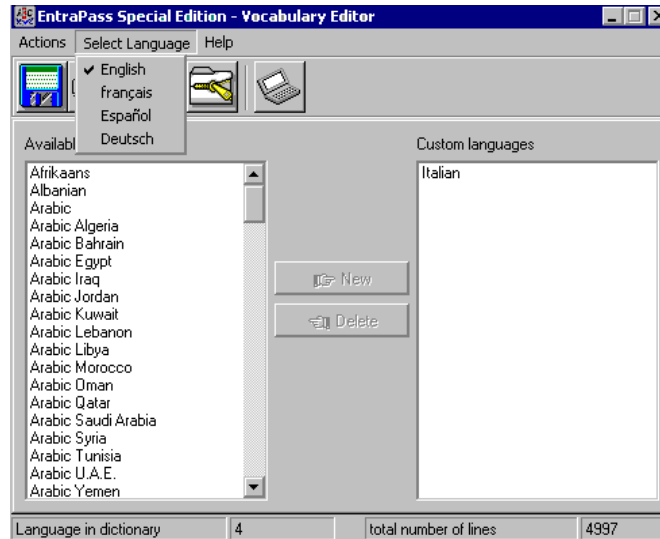
VOCABULARY EDITOR COLOR CODES	VALUE
Green	Valid text string.
Blue/Green	New text string.
Red	Obsolete text string.

- The "Source language" column contains text based on the basic language that was selected during the creation of the vocabulary. This column will serve as a "source" for the translation. Software language columns cannot be modified by the user.
- Use the right-click to enable a contextual sub-menu or use the **Language editor** toolbar. A hint appears when you position the mouse over a button.

To Integrate your Custom Language in Entrapass

Once the translation is finished, you have to integrate the new dictionary into the system dictionary so that system operators can use it.

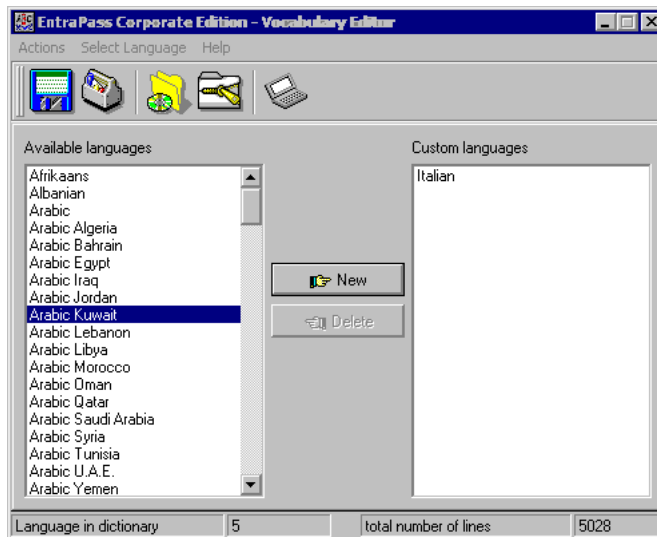
- 1 Start the Vocabulary Editor. The Vocabulary Editor window toolbar displays five buttons.






NOTE: The Graphic User Interface will only appear in one of four languages: English, French, German or Spanish.

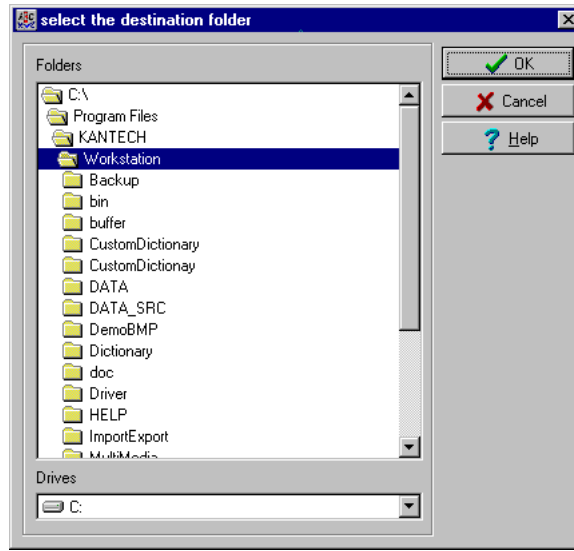


2 Select a newly translated vocabulary.



- You may choose to **Apply changes to the Operational dictionary**:  this option is useful when you want to test your changes before you update the whole system.
- **Restore the operational vocabulary**:  this option allows the user to easily restore the default languages. It creates a self-extracting file which restores the original dictionary.
- **Scan dictionary for new entries**:  this option is useful when the software was updated for example.

- 3 If you decide to implement the new vocabulary, select the **Actions** menu, then choose **Create self-extracting file for update** option. The system creates the **Updatedictionary.exe** file, and prompts you to select a destination folder for the file:



- 4 Select the destination folder for **Updatedictionary.exe**. By default, the Self-extracting file is stored in C:\Program Files\Kantech (application).



NOTE: It is recommended to copy the *Updatedictionary.exe* file on a network folder if you want operators to access the file to update their software application.

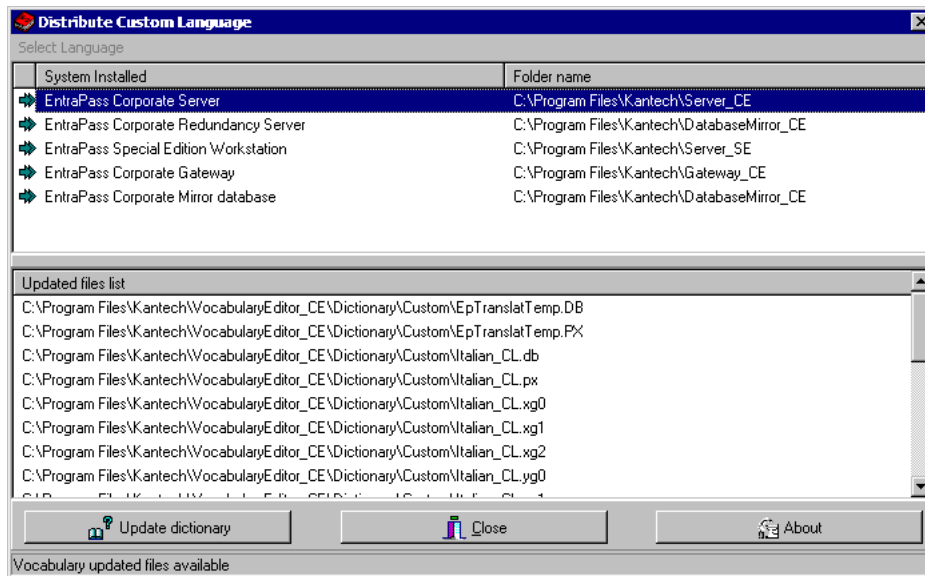
To Distribute the New System Vocabulary

Before you run the file, make sure to exit the Entrapass software; otherwise the operation will not work.

To Update the Server Vocabulary

- 1 Exit all Entrapass programs.
- 2 Start **Windows Explorer > Kantech > (Entrapass application)**, then copy the **Updatedictionary.exe** on the server.

- 3 Double-click **Updatedictionary.exe**. The system displays the Entrapass applications that are installed on the computer.



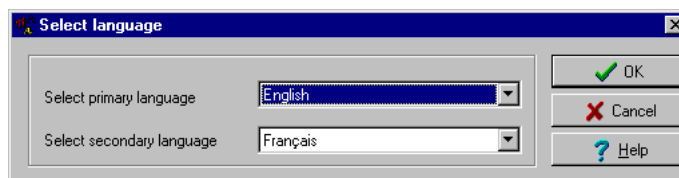
- 4 Select each application, then click the **Update dictionary** button.
- 5 You have to copy **Updatedictionary.exe** on every computer where Entrapass is installed, and then double-click it in order to launch the language update. To do so, you have first to exit all Entrapass applications before you run the self-extracting file.
- 6 Select the application you want to update (one at a time) and click **Update dictionary** button. The system will automatically copy the vocabulary to the **Custom Dictionary** directory then merge the custom directory with the application dictionary.



NOTE: You *MUST* update all the applications in the system.

NOTE: To restore the dictionary back to original default values, follow the same procedures as for updating the dictionary.

- 7 Select the **Options** tab, then select the **Select language** icon.



- 8 In the **Select the language** window, select the primary language and the secondary language. The newly integrated language is displayed in the list. It is important to select the language at this stage, otherwise the operators of the system will not be able to use it.



NOTE: For example, if your primary language is “English” and your secondary language is “French”: if you select your new language (i.e. Russian) as primary, all operators who have “English” as their display language in the **Operator** menu will be modified to “Russian”. On the other hand, if you change the secondary language to “Russian” and operators are using “English”, you will have to manually select “Russian” in the **Operator** definition menu”. To assign the desired language to an operator, use the **System** definition menu, then select the **Operator** definition menu.



NOTE: For every language you are installing, be sure to select the correct keyboard (**Start** > **Settings** > **Control panel** > **Keyboard**). The selected keyboard is displayed in the system tray.

To Upgrade the System Vocabulary

When you upgrade your system, the new or modified strings are automatically inserted in the system vocabulary and also in the custom dictionary.

If you have added a custom language to your system, you have to translate the new/modified strings following a system upgrade. Therefore, you have to re-edit the vocabulary and create a new self-extracting file.

When you re-open the vocabulary table, new strings are indicated by a green point. Obsolete strings (no longer used) are tagged red.

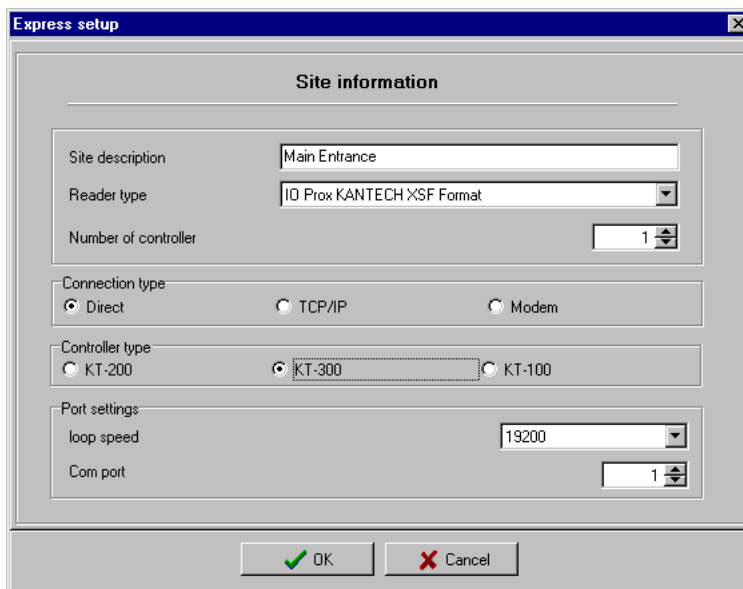


NOTE: For easier management, we recommend that you always edit your vocabulary from the same computer and integrate it to the system using a self-extracting file.

Express Setup Program

The Express Setup program offers a quick and simple way to configure all the components of a system Gateway: type of readers used, number of sites, site name, number of controllers on a site, etc. For example, it enables users to modify a door's name by automatically applying default settings to all relays and inputs of controllers connected to the selected door.

- 1 Enter the Site name in the **Site description** field, then select the reader type.



- 2 Set the number of controllers.
- 3 Specify the connection type. This indicates how the site communicates with the gateway computer.
 - Select **Direct**, if the site is integrated to the gateway computer and connected to it by an RS-232 serial port. If the connection type is direct, then you have to specify the serial port (com:) as well as the controller site baud rate (usually set at either 9600 or 19200). The default value is 19200.
 - Select **TCP-IP** if the site communicates with the gateway through a terminal server device using a port number. Then you have to specify the terminal server's IP Address and Port number. If the connection type is TCP/IP, the port settings section is disabled. To configure the terminal server, follow the manufacturer's instructions or refer to the terminal server documentation.
 - Select **Remote site Modem** if applicable. The modem option is enabled only when this option is installed.



4 Select the **Controller type** for this site.



NOTE: Click **OK**. When the system is updating the database, the second status flag turns red, indicating that the system database is locked. When you try to access another system menu while the database is locked, an error message appears. Simply wait until the system database becomes available.

The following are default values assigned to controllers by the Express Setup utility.

Controller	Door	Relays	Input zones	Aux. output
KT-100	1	4	4	2
KT-200	2	2	16	4
KT-300	2	2	8	4

The following table summarizes how input zones are used by the system.

Input zones	System use	Controllers
1	Door 1 contact	All
2	Door 1 Rex	All
3	Door 2 contact	KT-100 & KT-300
4	Door 2 Rex	KT-100 & KT-300
9	Door 2 contact	KT-200
10	Door 2 Rex	KT-200

The following table summarizes how output zones are used by the system.

Aux. output	Use	Controllers
1	LED (Door 1)	All
2	Buzzer (Door 1)	All
3	LED (Door 2)	KT-200 & KT-300
4	Buzzer (Door 2)	KT-200 & KT-300



NOTE: The remaining components (relays and input zones) are undefined, that is, they have been created but not yet defined. Components that are defined are grayed out. You cannot select them or change their description. You can change their description in their respective definition menu (Devices > Relays/Input zones).

By default, the system assumes that:

- The reader is IoProx Kantech 26 XSF Format,

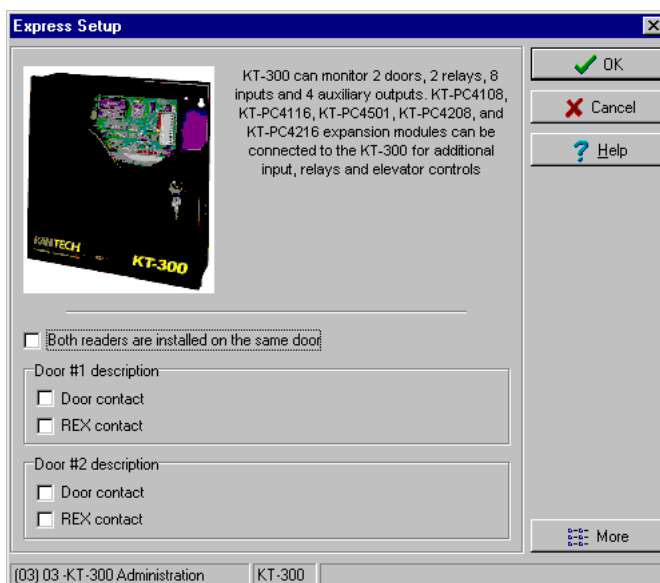


- The power supervision schedule is always valid,
- The failsoft delay is enabled for 45 seconds,
- The resistor type is single (KT-100 and KT-300),
- The wait for second card delay is 30 seconds.

To Configure a Controller Using Express Setup

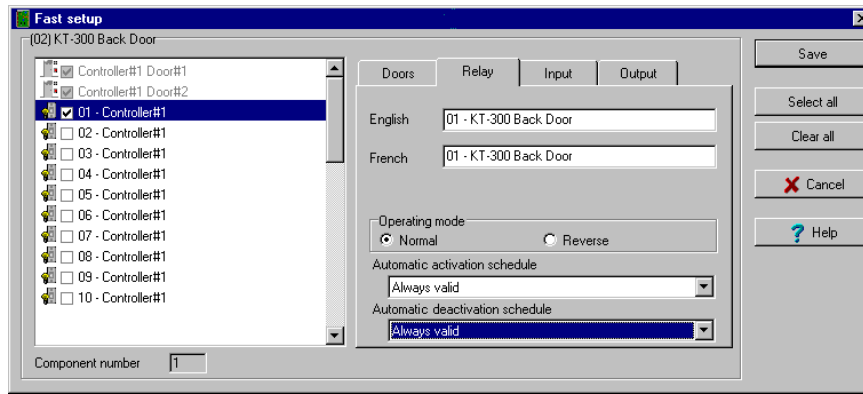
When you add a controller to a site, the system prompts you to use the Express Setup tool to define the controller. You may also launch this tool by selecting a controller and clicking the Express Setup icon in the controller window toolbar.

- 1 From a controller definition window, click the **Express Setup** icon or click **Yes** in the system message box.



- 2 Specify if **Both readers are on the same door** if this is applicable. If two readers are installed on the same door, the REX contact option is disabled.

- Click the **More** button to define the other devices, such as doors, inputs, relays and outputs.

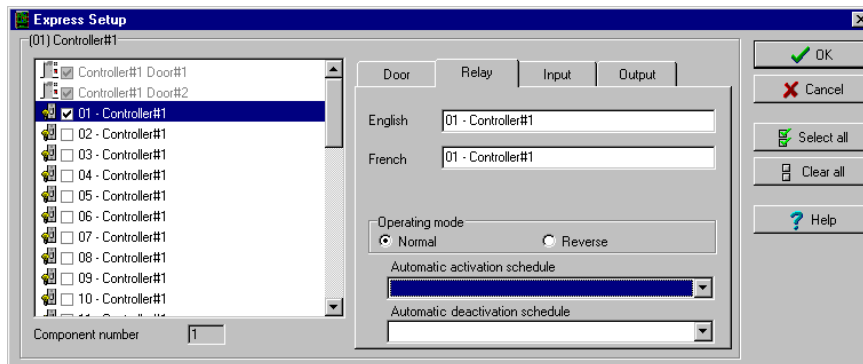


NOTE: Components are listed in the left-hand pane. The related tabs are displayed in the middle of the window. When you select a component, its default name, number and default settings are displayed in the language section. Select a component to enable its tab. Components that are assigned are gray. You cannot modify their description at this stage. You have to go in their definition menu. However, you may later modify any component description in its definition menu (Devices > Relay/Input/Output, etc.).

Defining Relays

You may configure relays to define their operation mode, activation and deactivation schedules. If you want to assign a name to the relay, you have to select it. When you use the Select All button, the default names are kept.

- Select the first relay if you want to modify its description. The relay tab is enabled. You have to check the box beside the relay name in order to enable the language section.



- Check the appropriate options for the **Operating mode** and for the **Activation mode**.

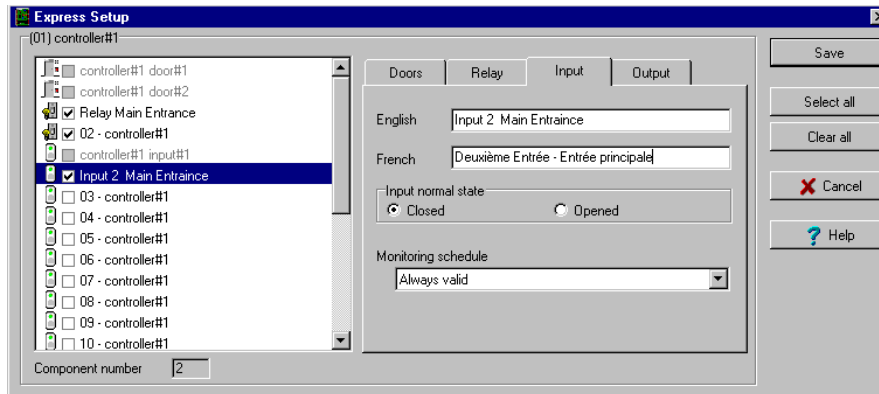


- 3 In the **Automatic activation schedule** drop-down list, choose the appropriate activation Schedule.

Defining Inputs

By default, the response time for a REX is 250 ms; it is 500 ms for other input zones. The alarm restore time is 150ms by default. The Express Setup program allows you to define the **Input Normal State** and **Monitoring Schedule**.

- 1 Select the first undefined input (its checkbox is not gray). Check its box to enable the language fields, then assign names to it.



- 2 Select the **Monitoring schedule** from the drop-down list. If you want to assign a custom schedule to the selected input, you have to define it. (Definition > Schedule).

Defining Auxiliary Outputs

By default, all outputs are defined, as follows:

- Auxiliary output 1 is used as a LED for door 1 (all types of controllers)
- Auxiliary output 2 is used as a buzzer for door 1 (all types of controllers)
- Auxiliary output 3 is used as a LED for door 2 (KT-200 and KT-300)
- Auxiliary output 4 is used as a buzzer for door 2 (KT-200 and KT-300).

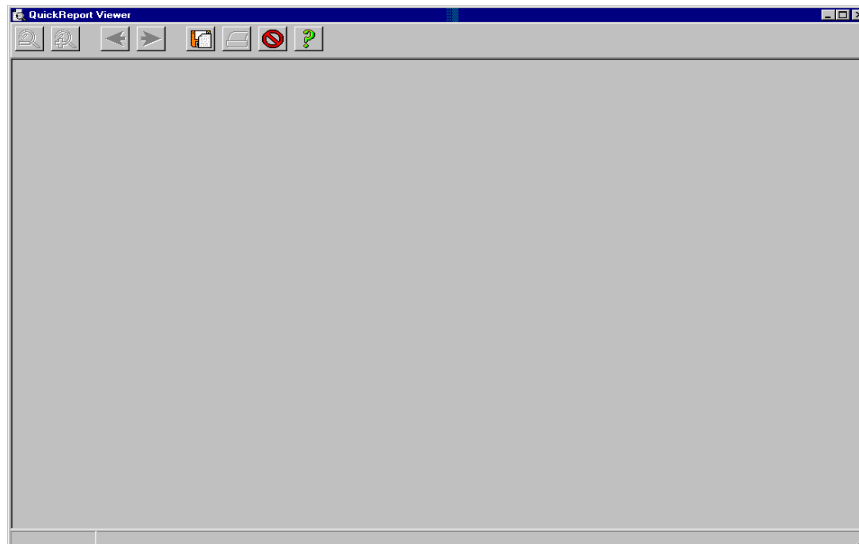
If you want to change their definition, you may do so while defining a controller or in their definition menu (**Devices > Auxiliary Outputs**)


Quick Viewer

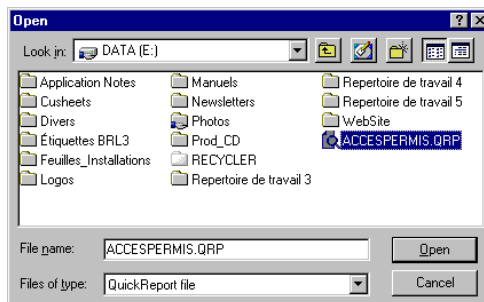
The **Quick Report Viewer** program allows operators to view previously saved reports without having to start Entrapass. It is used to view / display / load reports that were previously saved (in a.QRP format) during a print preview or Quick reports. For details on requesting and generating reports, see "Reports" on page 267.

This program is useful when Entrapass is off-line and when a report must be displayed for specific purposes.







- 1 From the Windows task bar, click **Start > Programs > Entrapass >Workstation/Server >Quick Viewer**.



- 2 Click the  button to open a report. The system displays the **Open** window:



- 3 By default, when a report is saved in a QRP format, the system automatically saves it in “My Documents” folder. If you have saved the report in another folder you have to browse to the folder to select the report.
- 4 Click **Open** to preview the report. Once you have selected the requested report, the system will display your report:
- 5 Use the toolbar buttons to preview the report:

Button	Description
	Use the Zoom out button to zoom out the report view.
	Use the Zoom In button to display details (view closer).
	Use Previous Page and Next Page buttons to change pages.
	Use the Open button to open a report located in any folder on your computer.
	Use the Print button to print the report. There will be no printer setup dialog box, the report will automatically print, to cancel the printing, click Cancel .
	Use the Quit button to quit the application.

Chapter 16 • Animated Icons

Animated icons indicate the status of physical or logical components in the windows of EntraPass software. They represent the component status in real time and simulate a movement by displaying a series of pictures associated with the component.

If a particular component status is difficult to identify, use this section to identify it.



Controllers

Controller animated icons indicate the status of a door controller in the graphic window (Desktop > Graphic desktop) or in the “Operation” window.

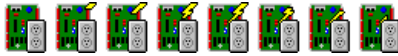
Status unknown



Appears when the EntraPass application has not received the component' status after four (4) attempts. It is displayed in:

- the Operation window (alarms, door, elevator door, relay, input, reload data)
- or the “Graphic” window (Desktop—graphic).

Controller AC failure



Appears when the controller is in AC failure. It is displayed in:

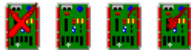
- the Graphic desktop (Desktop > Graphic desktop window)
- the “Operation” — “Controller Reset” Controller AC failure and Tamper Switch in “alarm”



Appears when the controller is in AC failure and the tamper switch is in alarm. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset

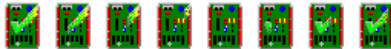
Controller is not communicating



Appears when the controller is not communicating. It is displayed in:

- the “Operation” — “Controller Reset” windows.
- the “Graphic” window (Desktop—Graphic desktop).

Controller communication is regular (no problem)



Appears when the controller is communicating and the communication is regular. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset.

Controller status is not yet known



Appears when the status of the controller is not yet known. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)

Controller is in “Reset” and AC failure



Appears when the controller is in “reset mode” and in “AC failure”. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset.

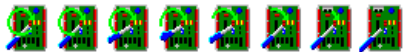
Controller is in “Reset”, “AC failure” and “Tamper in alarm”



Appears when the controller is in “reset mode”, in “AC failure” and the tamper is in alarm. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset

Controller is in reset and tamper in alarm



Appears when the controller is in “reset mode” and the tamper is in alarm. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation” > Controller Reset.

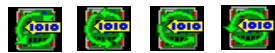
Controller tamper in alarm



Appears when the controller tamper is in alarm. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the “Operation” “Controller Reset” when the controller tamper is in alarm.

Controller reloading firmware



Appears when the controller is reloading firmware. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the “Operation” “Controller Reset”.

Doors

Icons representing a door state indicate the status of door within the graphic window (from the desktop) or within the “Operation” window.

Door forced open



This animated icon appears when the door is opened and that no access granted nor request to exit was permitted. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the “Operation” “Door, Elevator Door”

Door forced open (reader disabled)



This animated icon appears when the door is opened and that no access granted nor request to exit was permitted and the reader is disabled. It is displayed in:

- the “Graphic” window (desktop—graphic)
- the Operation > Door, Elevator Door

Door closed and locked



This animated icon appears when the door is closed and locked. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door

Door closed and locked (reader disabled)



This animated icon appears when the door closed and locked and that the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the “Operation > Door.

Door status unknown



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the status of the door is not yet known.

Door open too long



This animated icon appears when the door is opened more than the permitted delay set in “open time”. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the “Operation >Door, Elevator door”.

Door open too long (reader disabled)



This animated icon appears when the door is opened more than the permitted delay set in “open time” and that the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the “Operation” “Door, Elevator door”.

Door open and unlocked manually



This animated icon appears when the door is opened and it was unlocked by an operator. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation >Door > Elevator door”.

Door open and unlocked manually (reader disabled)



This animated icon appears when the door is opened and it was unlocked by an operator and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation >Door > Elevator door”.

Door is opened and unlocked by schedule



This animated icon appears when the door is opened and it was unlocked by a schedule. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation >Door > Elevator door”.

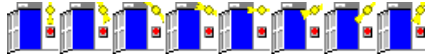
Door is opened and unlocked by schedule (reader disabled)



This animated icon appears when the door is opened, and it was unlocked by a schedule and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door”.

Door pre-alarm on open too long



This animated icon appears when the door is opened more than half the time permitted delay set in “open time”. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door”.

Door pre-alarm on open too long (reader disabled)



This animated icon appears when the door is opened more than half the time permitted delay set in “open time” and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door”.

Door still opened schedule invalid



This animated icon appears when the door is opened and the unlock schedule is invalid. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door”.

Door still opened schedule invalid (reader disabled)



This animated icon appears when the door is opened and the unlock schedule is invalid and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/ Elevator door”.

Door unlocked by an operator



This animated icon appears when the door is unlocked by an operator (manually). It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door”.

Door unlocked by an operator (reader disabled)



This animated icon appears when the door is unlocked by an operator (manually) and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door”.

Door unlocked by a schedule



This animated icon appears when the door is unlocked by a schedule. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door”.

Door unlocked by a schedule (reader disabled)



This animated icon appears when the door is unlocked by a schedule and the reader is disabled.

It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door”.

Elevator door unlocked and closed



This animated icon appears when the elevator door is closed and unlocked. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door”.

Relays

Relays icons indicate the status of a relay within the graphic window (from the desktop) or within the “Operation” window.

Relay activated by an event



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is triggered by an event.
- the “Operation” “Relay” when the relay is triggered by an event.

Relay temporarily activated by an event



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is temporarily activated by an event.
- the “Operation” “Relay” when the relay is temporarily activated by an event.

Relay activated by an input



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is triggered by an input.
- the “Operation” “Relay” when the relay is triggered by an input.

Relay temporarily activated by an input



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is temporarily activated by an input.
- the “Operation” “Relay” when the relay is temporarily activated by an input.

Relay activated by an operator



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is activated by an operator.
- the “Operation” “Relay” when the relay is activated by an operator.

Relay temporarily activated by an operator



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is temporarily activated by an operator.
- the “Operation” “Relay” when the relay is temporarily activated by an operator.

Relay activated by a schedule



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is activated by a schedule.
- the “Operation” “Relay” when the relay is activated by a schedule.

Relay deactivated



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is not activated.
- the “Operation” “Relay” when the relay is not activated.

Relay status unknown



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the status of the relay is not yet known.



Inputs

This section is used to indicate the status of an input within the graphic window (from the desktop) or within the “Operation” window.

Input in alarm—Not supervised



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in alarm and the monitoring schedule is invalid.
- the “Operation” “Input” when the input is in alarm and the monitoring schedule is invalid.

Input in alarm—Shunted by operator



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in alarm and it is shunted by an operator.
- the “Operation” “Input” when the input is in alarm and it is shunted by an operator.

Input in alarm—Supervised



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in alarm and the monitoring schedule is valid.
- the “Operation” “Input” when the input is in alarm and the monitoring schedule is valid.

Input in alarm—Supervised by operator



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in alarm and it is supervised by an operator (continuous supervision).
- the “Operation” “Input” when the input is in alarm and it is supervised by an operator (continuous supervision).

Input OK—Not supervised



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in normal condition and the monitoring schedule is invalid.

- the “Operation” “Input” when the input is in normal condition and the monitoring schedule is invalid.

Input OK—Shunted by operator



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in normal condition and it is shunted by an operator.
- the “Operation” “Input” when the input is in normal condition and it is shunted by an operator.

Input OK—Supervised



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in normal condition and the monitoring schedule is valid.
- the “Operation” “Input” when the input is in normal condition and the monitoring schedule is valid.

Input OK—Supervised by operator



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in normal condition and it is supervised by an operator (continuous supervision).
- the “Operation” “Input” when the input is in normal condition and it is supervised by an operator (continuous supervision).

Input status unknown



This animated icon appears in the “Graphic” desktop when the status of the input is not yet known.

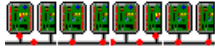


Sites and Gateways

These icons indicate the status of a site, or gateway within the graphic window (from the desktop) or within the “Operation” window.

Controller Site:

Site status is not yet known



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the status of the controller site is not yet known.

Controller site connected



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the site is connected and communication is OK.
- the “Operation” “reload data” when the site is connected and communication is OK.

Controller site connected and in “Reload Data”



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the site is connected and is in “reload data” state.
- the “Operation” “reload data” when the site is connected and is in “reload data” state.

Controller site—Communication Failure



This animated icon appears in:

- the “Graphic” window (Desktop—graphic) when the site is disconnected and there is a communication failure.
- the “Operation” “reload data” when the site is disconnected and there is a communication failure.

Gateway:

Gateway—Communication Failure



This animated icon appears in:

- the “Operation” (door, elevator door, relay, input, reload gateway) window when the gateway is in communication failure.

- the “Graphic” window (desktop—graphic) when the gateway is in communication failure.

Gateway in “Reload Data”



This animated icon appears in:

- the “Graphic” window (Desktop—graphic) when the gateway is being reloaded.
- the “Operation” (door, elevator door, relay, input, reload gateway) when the gateway is being reloaded.

Gateway—Communication Failure during Reload Data



This animated icon appears in:

- the “Operation” (reload data gateway) window when the gateway loses communication during a reload data operation.
- the “Graphic” window (desktop—graphic) when the gateway loses communication during a reload data operation.

Gateway communication is regular (no problem)



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the gateway is communicating and the communication is regular.
- the “Operation, reload data gateway, communication is regular.”

Gateway Trouble



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the gateway is not communicating.
- the “Operation” “reload data gateway”, the gateway is not communicating.

Gateway Trouble when Reloading



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the gateway is not communicating.
- the “Operation” “reload data gateway” is not communicating with the gateway during a reload data operation.



Gateway (Gateway Software Interface):

Gateway OK—communicating



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the gateway is communicating.
- the “Operation” “reload data” when the gateway is communicating.

Gateway in “Reload Data”



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the gateway is being reloaded.
- the “Operation” “reload data” when the gateway is being reloaded.

Gateway—Communication Failure



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when gateway is not communicating.
- the “Operation” “reload data” when the gateway is not communicating.

Entrapass Application

Application status is not yet known



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the status of the application is not yet known.

Application attempts communication



This animated icon appears in:

- the startup window when the workstation attempts to communicate with the server.

Application—Communication Failure



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the workstation is in communication failure.
- the “Operation” window (alarm, door, elevator door, relay, input, reload gateway) when the workstation is in communication failure.

Others

Database Initialization



This animated icon appears in:

- the startup window when the workstation initializes the database.

Data not available



This animated icon is used to indicate a transient stage. This could indicate that the requested information is not currently available.

No state available



This animated icon is used to indicate a transient stage. This could indicate that the requested component status is not currently available.



Output status is not yet known



This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the status of the output is not yet known.

Status unknown



This animated icon appears in:

- the “Operation” (alarms, door, elevator door, relay, input, reload) window when the workstation has not received the component' status after four (4) attempts.
- the “Graphic” window (desktop—graphic) when the workstation has not received the component' status after four (4) attempts.

Error in process



This animated icon appears in:

- the “Operation” (alarms, door, elevator door, relay, input, reload data) window when a specific error is detected.
- the “Graphic” window (desktop—graphic) when a specific error is detected.

Undefined Component



This animated icon appears in:

- the “Operation” window (alarm, area door, elevator door, relay, input, reload data gateway) when the component does not exist.
- the “Graphic” window (desktop—graphic) when the component does not exist.

Index

A

Access Levels

- Administrator 45
- Create groups 200

Access levels

- Bad 89

Acknowledging Alarms

- Acknowledge schedule 226
- Alarm sound 304
- Automatic 215
- Set priority 227

Acknowledging alarms

- Definition and purpose 261
- Using the alarm message box 53

Advanced schedule capability 307

Alarm Message Box 53

Alarm Sound 304

Alarms Desktop 256

Animated Icons

- Controllers 344
- Doors 346
- Inputs 352
- Others 357
- Site and gateway 354

Animated icons

- Relays 350

Apply user parameters 51, 53

Assign picture from file 139

Auto Acknowledge 215

B

Backup 320

Badging 2, 129

- Get picture from file 139
- MCI 139
- Paste picture 139
- Video images 139

Bullet

- Next to a name 57

Buttons

- Cancel 35
- Enable Animation 36, 108
- Enable Graphic 36, 108
- OK 36
- Select All 108
- Unselect All 36, 108

C

Card access group definition 180

Card format 297

Card use reports

- Schedule mode 277

Cards

- Assign a card access group 136
- Assign a picture 138
- Assign access levels to cardholders 136
- Card format 298
- Change format 298
- Create access level groups 180
- Delete when expired 137
- Information #1 to #10 130
- Keep picture on desktop 246
- Last transactions 178
- Modification date 130
- Modifications count 130
- Number 130
- Print a list of cards 174
- Show cardholder information with picture 51
- Start date 137
- State 137
- Trace 138
- User name 130
- Validate Card Access 172
- Wait for keypad 137

Change card format

- Decimal 298
- Hexadecimal 298
- Octal 298

Clear messages / alarms 51, 53

- Communication timing 58
- Components physical address 219
- Configure system devices 47
- Controller
 - Definition 66
- Controller's Loop baud rate 59, 336
- Controllers 47
 - Animated icons 344
 - Create groups 196
 - Reset 114
 - Status (graphic view) 207
- CSV files 53
- CSV Import/Export 184
 - Create patterns 185
 - Exporting procedure 186
 - Importing procedure 189

D

- Database
 - Logical components (view) 236
 - Structure 236
- Database Integrity 297
- Database Output Type 270
- Database Status 209
- Define E-mail Parameters 285
- Define E-mail parameters 285
- Desktops
 - Alarms Desktop
 - Acknowledge 259
 - Delete log 259
 - Display graphic screen 265
 - Display instruction screen 263
 - Flag 259
 - Print log 259
 - Purge deleted log 259
 - Historical Reports 253
 - Messages Desktop
 - Auto-rescroll delay 247
 - Background color 247
 - Delete all 248
 - Display events in bold 246
 - Display last message on top 246

- Display message (in full) 246
- Display toolbar 246
- Keep card picture 246
- Manual properties 246
- Message type 244
- Multi-line 245
- Send to back 249
- Show icons 245
- View parent 248
- Dial up modem 63
- Dial-up modem 63
- Directory 270
- Disable Door Reader 119, 123
- Door
 - Return to schedule 117, 120, 124
- Door contact 84
- Door Group 197
- Doors 47
 - Animated icons 346
 - Create groups 197
 - Door contact 84
 - Door unlock reading 84
 - Elevator cab 82
 - Lock mode 81
 - Open time 82
 - Pre-alarm on door opened too long 84
 - Re-lock on door closing 84
 - Re-lock on door opening 84
 - REX contact 85
 - Time and Attendance 82
 - Unlock on REX 85
 - Unlock time 82

E

- Elevator Control
 - Create floor groups 201
 - Create floors 100
 - Elevator cab (door) 82
- Elevator control
 - REB-8s 70
 - Select cab for floor group activation 93
 - Unlock schedules (elevator floors) 87

- Elevator controllers 69
- e-mail
 - Options 53
- Enable Door Reader 119, 122
- Enable/Disable Card Readers 117
- Enable/Disable card readers 117, 120
- Ethernet Kantech IP Link 59
- Ethernet polling 62
- Event buffer
 - Controller 65
- Events
 - Acknowledge schedule 226
 - Color 226
 - Deleting and restoring associations 228
 - Display (schedule) 226
 - Instructions (assign to events) 226
 - Parameter definition 225
 - Print parameters 229
 - Print schedule 226
 - Set priority 227
 - Viewing associations 227
- Expired 138

F

- Fail-Soft 235, 245
- Filtered Messages Desktop 252
- Floor
 - Confirmation 74
 - Definition 100
 - Group 201

G

- Gateway
 - Animated icons 354
 - Data reload 111
- Graphic Status (controller view) 207
- Graphics
 - See also Animated Icons 343
- Groups
 - Access levels 200

- Controllers 196
- Doors 197
- Floors 201
- Inputs 199
- Relays 198

H

- Hardware
 - Definition 57
- Historical Reports
 - Automatic filename 281
 - Automatic report schedule screen 276
 - Desktop 253
 - Destination 281
 - Filter mode 272
 - Output process 279
 - Output type 278
 - Preview 294
 - Report language 281
 - Schedule mode 277
 - Selected components 273
 - State 254
- Historical reports 271
- Holiday definition 105

I

- Icons, see Animated Icons 343
- Import/Export 184
- Information #1 to #10 130
- Inputs
 - Animated icons 352
 - Continuous supervision 127
 - Create groups 199
 - Group 199
 - Monitoring schedule 92
 - Normal 127
 - Normal condition 92
- Installing the system 12
- Instructions
 - Assign to events 226

Definition 231
Interlock options 86

K

Kantech IP Link 59
Keypad Escape key 69
KT Controllers 66
KT-100 68
KT-100 controller 68
KT-200
 Expansion devices 70
KT-2252 elevator controllers 70
 Program 71
KT-300 68

L

Language (operator) 215
Lock/Unlock
 Door 117
 Door temporarily 117
 Elevator door 120
 Elevator door temporarily 120
Login
 Name 215
 Schedule 215
Logout on idle 49

M

Mantrap 86
Manual Operations
 Disable reader 117, 120
 Enable readers 117, 120
 Lock door 117
 Lock elevator door 120
 Temporarily lock door 117, 120
 Temporarily unlock door 117, 120
 Unlock doors 117, 120
Messages Definition (Filters) 233

Messages Desktop 244
Modem dial-up 63
Multimedia Devices 297, 304
 Alarm sound 304
 Signature capture 306
 Video options 305

N

Normal condition 92

O

Online help 4
Operator definition 214
operator name 214
Operators
 Allow login on server 219
 Definition 214
 Language selection 215
 Login name 215
 Login Restrictions 219
 Operator login schedule 215
 Password 215
Output definition 95
Output filename 270
Outputs
 Activation period 95
 Associating door events to auxiliary outputs 96
 Flash 96
 Flash timed 96
 Operating mode 95
 Steady 96
 Steady timed 96

P

Passback
 Option 138
Password
 Operator 215

- Pending 138
- Picture 139
- PIN number 69, 137
- Port number 336
- Power supervision schedule 68
- Print a log 259
- Print cards 174
- Print Event Parameters 229
- Printer, see Log printer 301

R

- REB-8 Elevator controllers
 - Program 72
- REB-8 relay expansion board modules 69
- Relay
 - Activate 124
 - Deactivate 124
 - Temporarily activate 124
- Relay Group 198
- Relays 47
 - Activation schedule 90
 - Animated icons 350
 - Create groups 198
 - Operation mode 90
 - Temporary activation timer 90
- Remote modem delay 65
- Reset, see Controllers 114
- REX 69
- REX (Request to EXit) 85
- REX contact 85
- REX options 85
- rpf files 53
- RS-232 serial port 58, 336

S

- Schedule definition 98
- Schedules
 - Acknowledge schedule 226
 - Days 99
 - End time 98

- Login schedule (operators) 215
- Monitoring schedule (inputs) 92
- Printing events 226
- REX schedule 85
- Start time 98
- Unlock schedule # 1 (elevator doors) 87
- Security Level
 - Assign to operator 216
 - Read only - (View components) 219
- Security level definition 217
 - Administrator 214
 - Installer 214
 - Restricted 214
- Security parameters 49
- Server
 - Database Utility Program, see Database 324
 - Server's IP Address 336
- Shunt delay 92
- Signature capture 306
- Site
 - Retrieving site events 64
- Sound Notification 304
- Start a session 30
- State (cards), see Cards 137
- Status icon
 - Refresh delay 51
- Suspend messages 49
- System data 320
- System Date & Time 303
- System Options 307
- System parameters 297

T

- TCP-IP 62, 336
- Terminal server 62
- Time & Attendance Reports
 - Add transactions 290
 - Automatic Report output definition 288
 - Preview 295
 - Select doors 286
 - Use specific card range 286
- Time and Attendance 81

Trace
Option 138

U

UDP 62
Unlock schedules (elevator floors) 87
Upgrading the system 22
User Datagram Protocol (UDP) 62
Users 129

V

Validate Card Access 172
Video 305
View Last Transactions 178
Visual feedback
see Reader 66

W

What is access control? 1
Window
Description 49
Workstation
Automatic logout on idle 49
Suspend messages 49

KANTECH

© 2006 Tyco Safety Products, Canada, Ltd.
Tel.: +1 (450) 444-2030 • Toll Free: +1 888 222-1560 • Fax: +1 (450) 444-2029
Internet: www.kantech.com • E-mail: kantechsupport@tycoint.com
DN1420-0612
