ENTRAPASS™
CORPORATE EDITION

High Performance Access Control and Integrated Security System

Reference Manual

KANTECH | access control and integrated systems

DN1415-0401 / Version 3.12

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 JURISDICTIONS 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

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:

- Remote communication capability (with Corporate Gateway only),
- Configurable desktops,
- Integrated Badging capability,
- Multiple reader technology,
- Interactive floor plans,
- Time and Attendance reporting,
- Visual diagnostics,
- SmartLink interface,
- Elevator control,
- Live video,

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.

Some EntraPass Features

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.

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.

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.

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.

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.

SmartLink feature. EntraPass enables organizations to interface to most intelligent devices such as CCTV multiplexers, alphanumeric pager systems, LCD panels, video matrix switchers, etc., using an RS-232 link cabled between one of the EntraPass SmartLink workstation and the external device. This feature can also be used to create, in real time, text or CSV files containing specific information concerning an event. These files can then be used with third party Time and Attendance systems, spreadsheet programs, etc.

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.

This indispensable feature in a multi-tenant building allows facility managers to restrict specific floor access to authorized cardholders.

Live Video feature. EntraPass adds real-time monitoring capability to the Corporate and Global series as a response to the growing importance of video in access control systems. From EntraPass Corporate and Global Edition user interfaces, operators can configure viewing parameters for digital video applications.

Redundancy Server & Mirror Database. The Redundancy Server & Mirror Database option provides an alternative duplication mechanism in case of failures and errors of the Primary Server.

Using KT-100, KT-200 and KT-300 controllers. EntraPass is compatible with Kantech's KT-200 controller, KT-100 and KT-3000 controllers when using a Corporate Gateway. 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.

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 a Corporate Gateway. This allows EntraPass to easily integrate with an external alarm system.

EntraPass Manual and Help

Using this 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 screens. You may also use the right-click option; it may either display a shortcut menu or the help file of the active window.

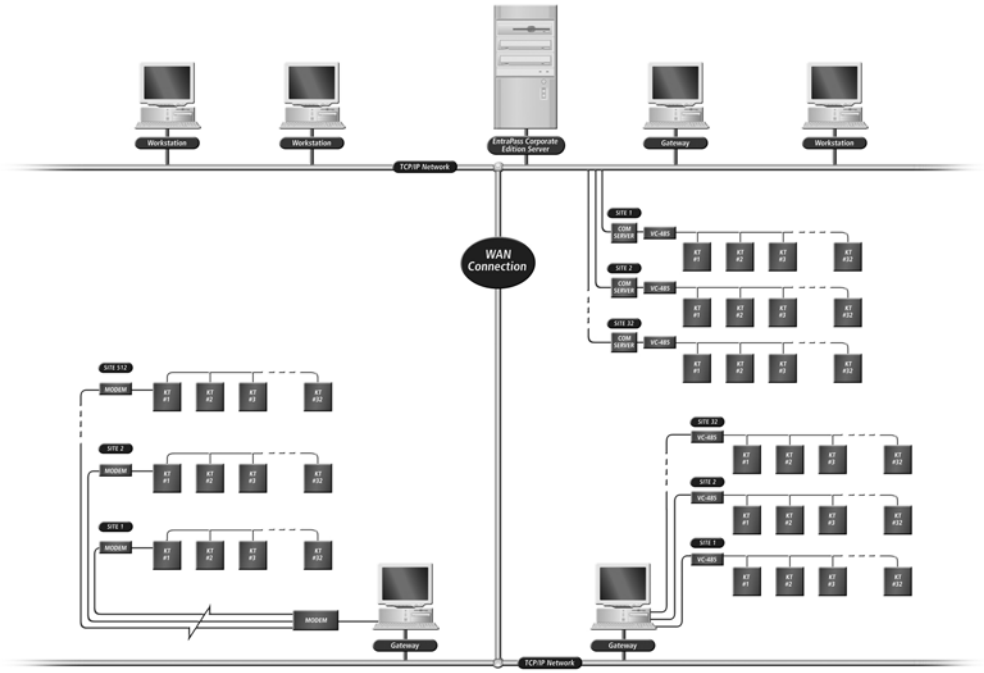
Technical Support

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 Customer Assistance Service, 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 devices.

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:

- Windows 98/NT/2000/Me/XP operating systems,
- Pentium III processor at 800 MHz (minimum),
- 128 MB RAM,
- 4 GB HDD minimum,
- 800 x 600 (256 colors) screen resolution,
- 4 MB Graphic adapter card,
- CD-ROM drive,
- 10/100 MBPS Ethernet TCP/IP Network card,
- Mouse and keyboard.

Live Video applications

- Pentium 3 with 256 M RAM recommended (minim supported 128 M),
- Windows 98, ME, 2000, NT, version 4, and Server 2003,
- Microsoft XP Home and Professional,
- Video card with at least 4M of RAM,
- Monitor with a resolution of at least 800 x 600.

For some 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*. 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 Server and 1 Workstation
- 1 SmartLink

The installation CD also contains system advanced options. These are subject to an additional license:

- 6 additional workstations (for a maximum of 20),
- 40 Gateways ,
- Redundancy Server & Mirror Database option,
- Oracle/MS-SQL HR Interface option.

NOTE: *Additional options can only be installed after the Server has been registered. They require an additional license.*

Installation Steps

It is easy to install EntraPass. An installation assistant guides you through the 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.

Installing EntraPass Software

The system is up and running in only three stages! Installers need to:

1. Install the software using the **System Installation Code** located in the CD pocket.
2. Register the system using the **Registration Confirmation Code** provided by Kantech Customer Assistance.
3. Install the first components that are part of the installation kit (5 workstations and 1 gateway; the first workstation is automatically installed during the installation of the EntraPass Server).

NOTE: *The software is fully functional even before it is registered. However, an unregistered system is restricted to ten cards. Moreover, there is an automatic logout after 1 hour of idle time, that is, when there is no action on the keyboard. After an automatic logout, operators need to enter a 20-character password; it is displayed in the lower part of the screen.*

Adding Optional Components/Features

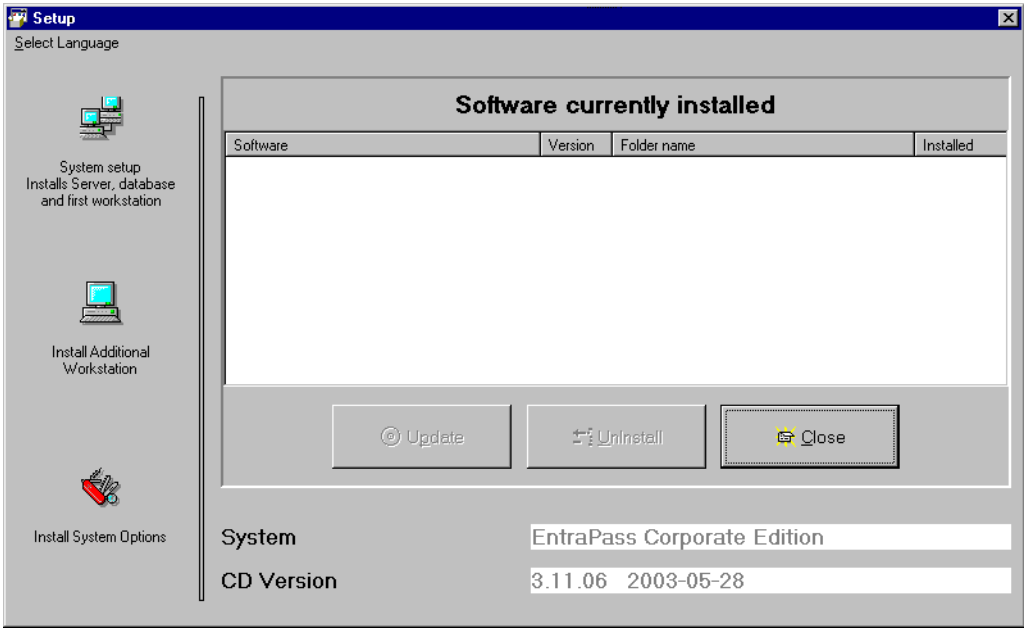
This stage is executed in four steps. Installers need to:

1. Add components or options from the Registration screen:
   - **Server** > **Connection list** > **Registration** icon or
   - **Workstation** > **Options** > **Registration** icon.
2. Call Kantech to obtain or register the component/option **Option Code** (located on the Option Certificate) and get the Registration Confirmation Code.
3. Enter the **Registration Confirmation Code** in the Registration screen and activate the option.
4. Install the component or option using the **Installation Code** (if applicable). The **Installation Code** is generated by the system; it is displayed in the Registration screen.

NOTE: *You need to establish communication between the EntraPass Server and the computer where the new component/option is installed (if applicable). You need to perform this step only when the component/option is installed on a computer different from the EntraPass Workstation.*

Installing the System

1 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:



2 Click the **Select Language** menu option to change the installation language, if necessary.

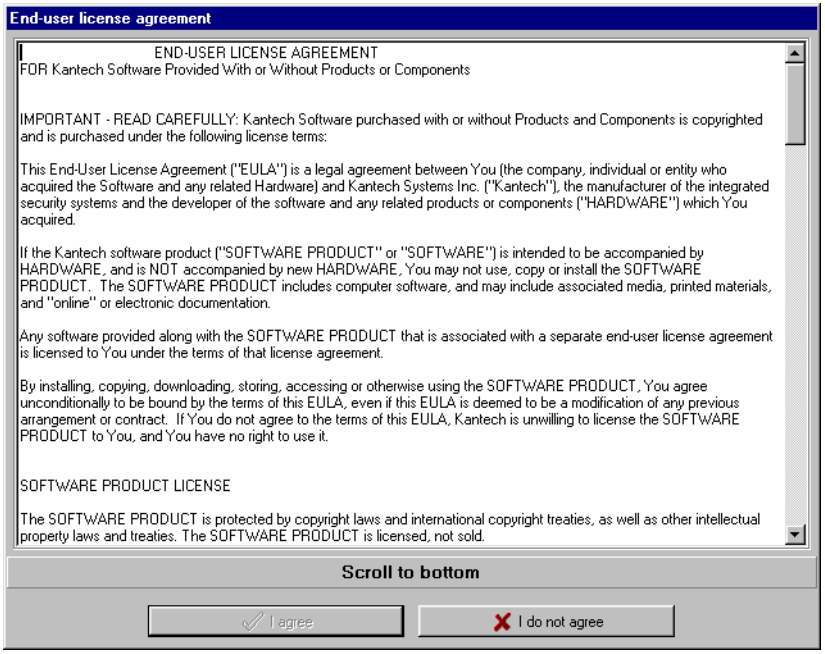
3 Select the **System Setup** icon on the left. The system prompts you for the **System Installation Code**.

4 Enter the **System code** located in the CD pocket. Make sure to enter the correct digits. The **OK** button is only enabled if the installation code is correct.

5 Click **OK**. The system prompts you to select the installation language. English is the default language.

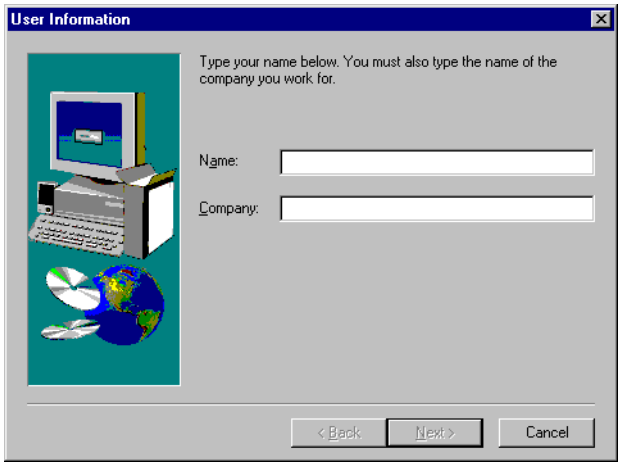
NOTE: *The system language depends on the language you select when installing the software. For example, if you select "French", the system default language at start up.*

6 Make the appropriate choice, then click **OK** to continue. The system displays the Setup window indicating the installation progress. Once completed, the system displays the software End-user license agreement:



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

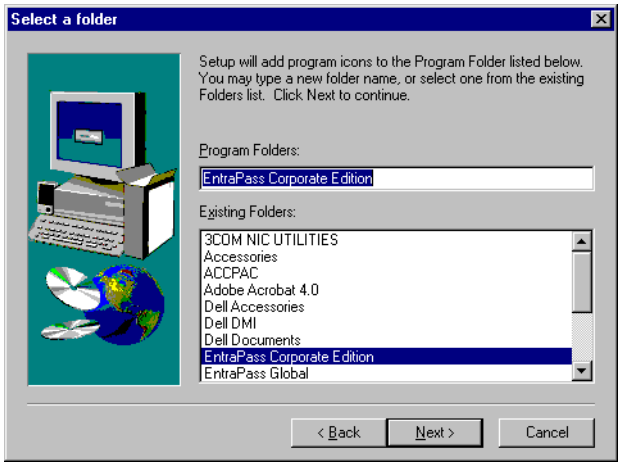
NOTE: *You have to scroll to the end of the screen to enable the* ***I agree*** *button.*



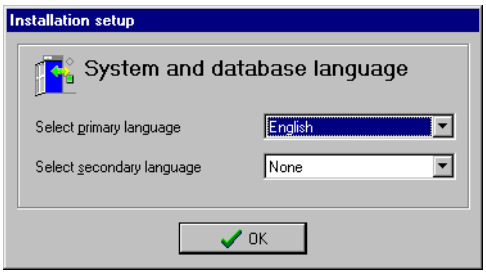
8 Follow the instructions displayed on-screen.

9 Enter the user name, the company name and click **Next** to continue. The system prompts you to confirm the registration information. Click **Yes** to confirm the displayed information and to continue the installation; or click **No** to return to the previous screen.

10 Click **Next** to accept the default installation folder or click **Browse** to select a different installation path. Once you have clicked **Next**, the system displays the default program folder.

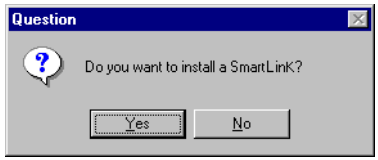


11 Click **Next** to accept the default program folder or click **Back** to modify it. Once you have clicked **Next**, the system starts the installation and displays the installation setup screen. At some point during the installation, you will be prompted to enter the system and database primary and secondary languages.



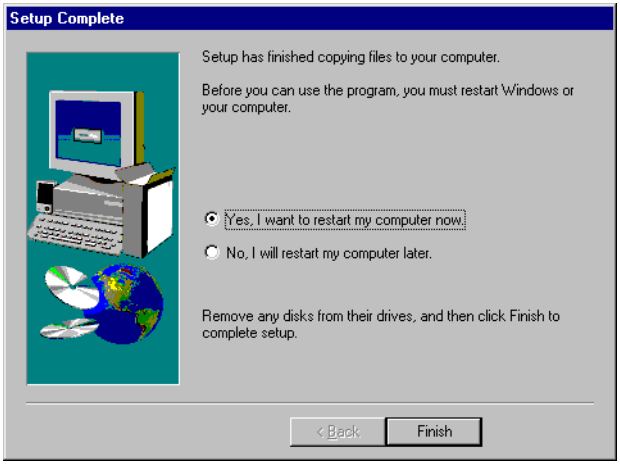
12 Select between English, French, German or Spanish as your primary working language, then select a second language if needed. These selections will allow users to personalize their work environment to one of the two language selections. Click **OK** to continue.

13 Next, you will be prompted to install a SmartLink.



14 To install a SmartLink, on the same computer during Server installation, click **Yes** and choose the default options.

15 Next, you will be prompted to choose your final options.



- Check the **Launch Server automatically with Windows** option if you want the application to start automatically when Windows starts up.
- Check the **Install Automatic Server Updater** option to allow the server to automatically update all EntraPass software components over your global network whenever software updates become available.

NOTE: *When installing the Server on Windows NT/XP/2000 the* ***Install Server in Windows Service*** *option is displayed. Select this option for the application to automatically started up with Windows NT/XP/2000.*

16 You may click the **View** button to view the latest information about the software, then click **Next**.

17 The system prompts you to restart the computer. Click **Finish** to complete the installation.

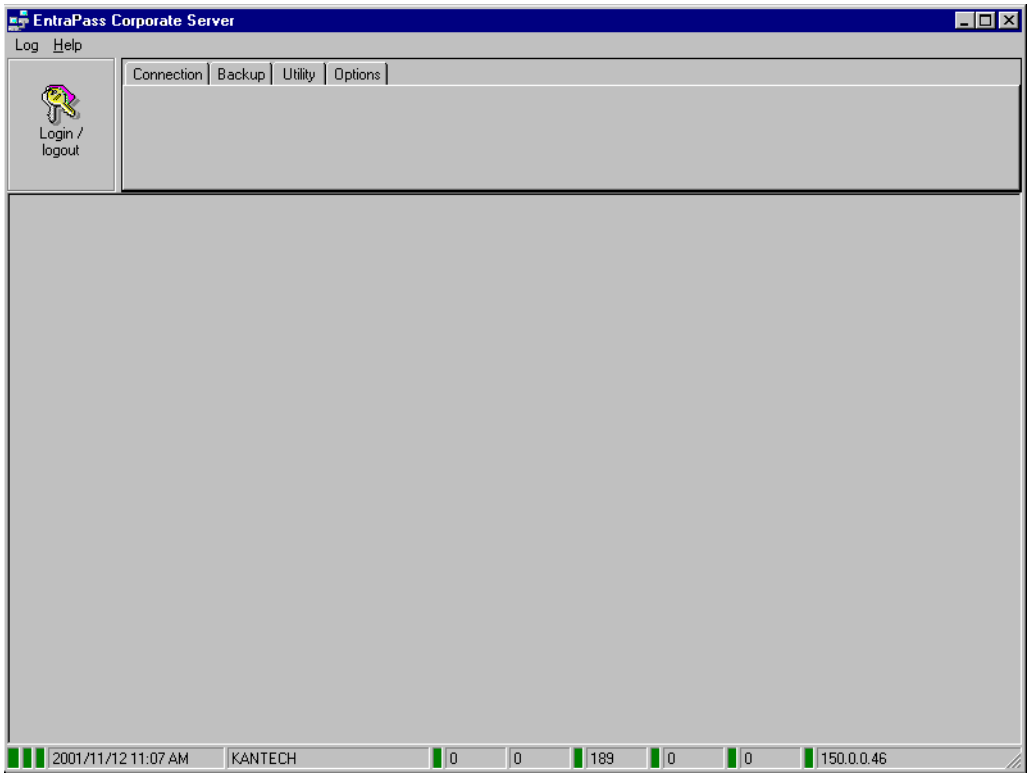
NOTE: *You must restart the computer after the installation.*

Registering the System

It is recommended to register the system as soon as possible so that users can install additional options and use the access system with no restrictions. In fact, though the system is functional even before the system registration, it is limited to only 10 cards. Moreover, when the system is not yet registered, operators are logged out after one hour of idle time; then they have to enter the randomly-generated 20-character password each time they are logged out.

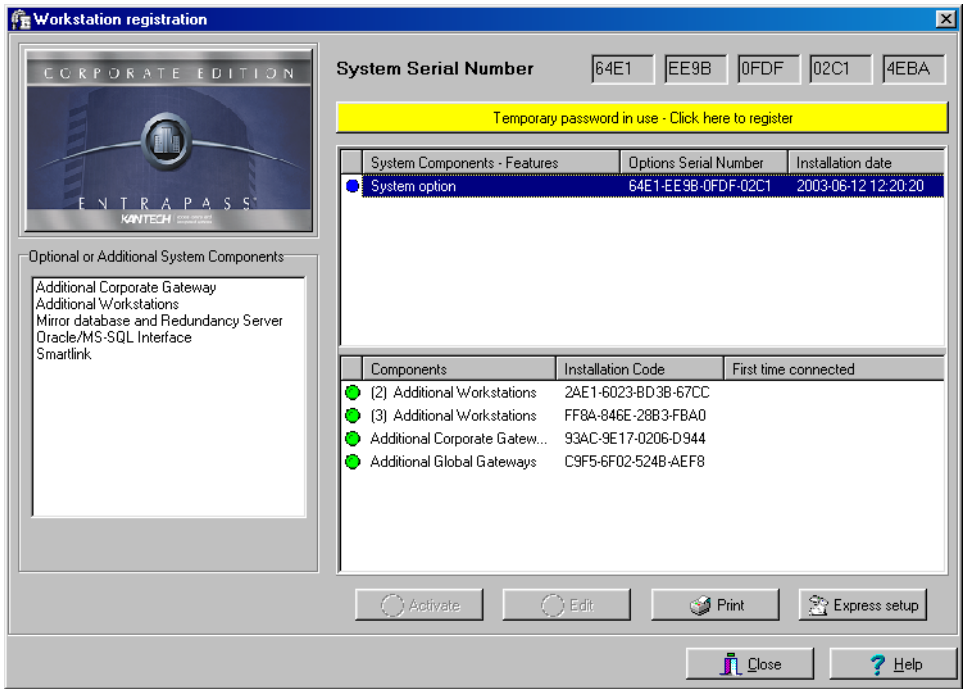
To register the system:

1 Click the **Server** icon on the computer desktop. You may also start the EntraPass Server from the Windows Start menu (**Start** > **EntraPass Edition** > **Server)**.

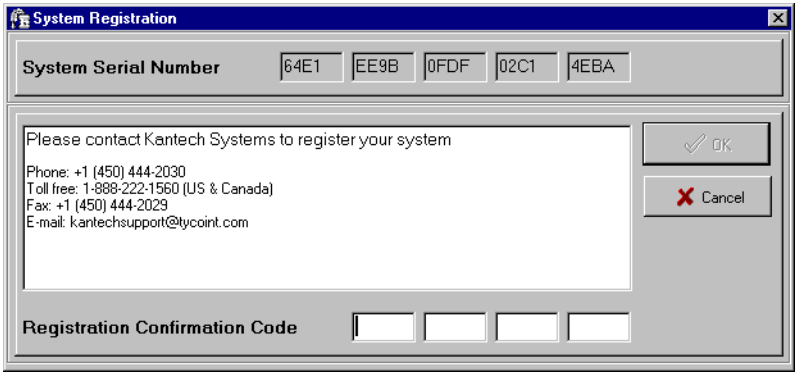


2 Click the **Login** / **Logout** button. The Operator Login screen appears.

3 Enter Kantech in the **User name** field (not case sensitive). Enter the temporary 20-character password displayed at the bottom of the Operator login screen. The Workstation registration screen appears.



4 Click the **Temporary password in use (...)** yellow button to register the system. The System Registration screen appears.



5 Enter the **Registration Confirmation Code** provided by Kantech, then click **OK**. The **OK** button is only enabled when you have entered the correct information.

NOTE: *If you exit the Server main window without registering the system, the Change Master Password screen is displayed. It is no longer displayed when the system has been registered.*

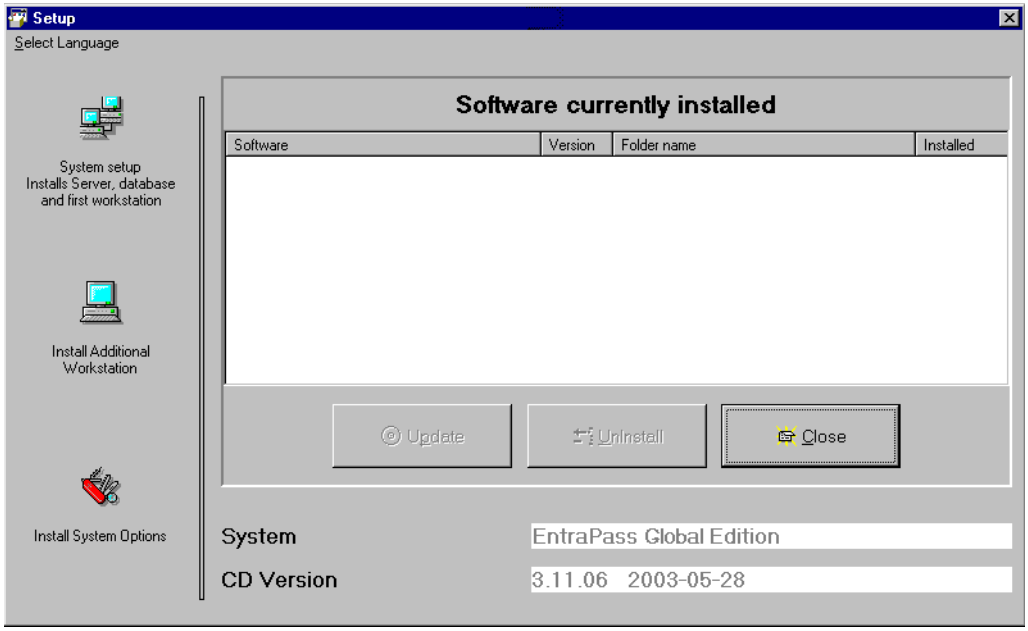
Installing Additional Workstations and Gateways

Once the Server has been registered, you may install additional workstations and options. Before you install system components, make sure that the designated computer meets the minimum requirements.

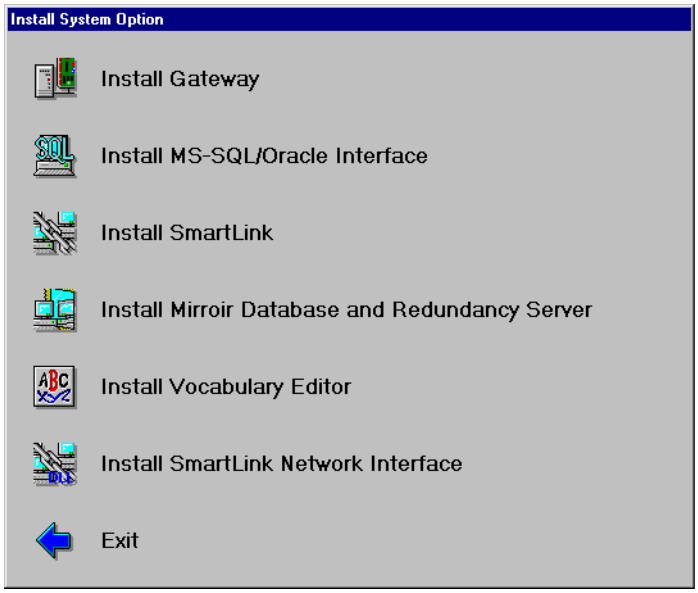
You do not need to call Kantech Customer Assistance to install the first two workstations and the Gateway. These are part of the installation package.

To install the first workstations and gateway:

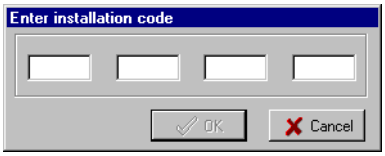
1 Insert the software CD into the CD-ROM drive of the computer where you want to install the workstation or gateway. The Setup screen appears.



2 From the Setup screen, select the **Install System Options** icon. The Install System Option screen appears.



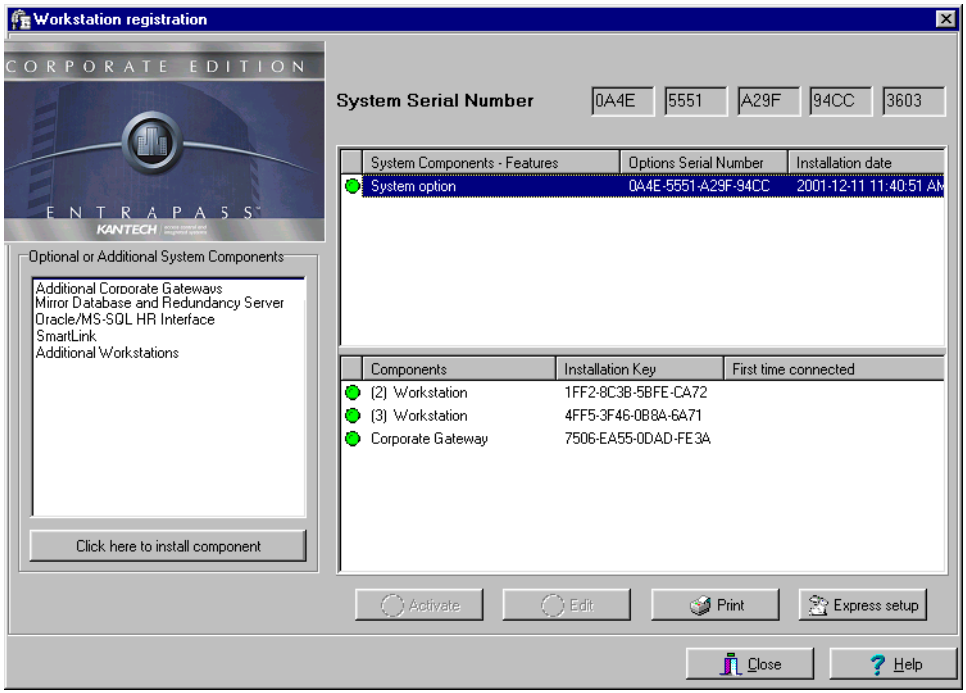
3 From the Install System Option screen, select the **Install Gateway** icon (or any other system option you want to install). The system prompts you for the installation code.



4 Enter the **Installation code** (it is displayed in the System registration screen). The **OK** button is enabled only when a correct code has been entered.

Adding Advanced Options

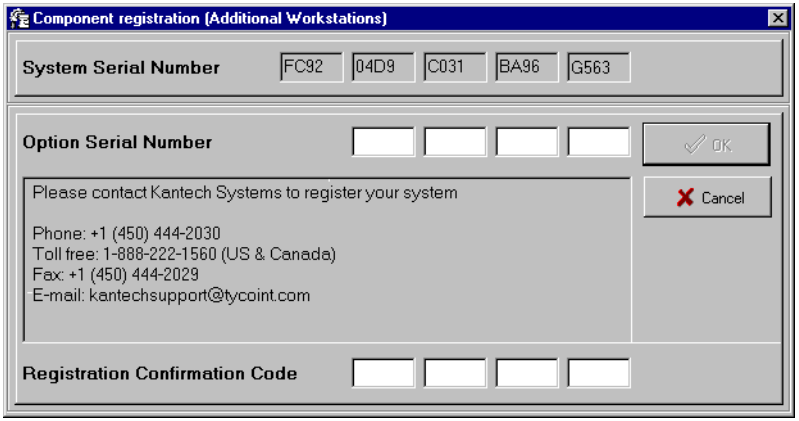
1 In the Server main window (or Workstation option screen), click the **Registration** icon. The Workstation registration screen appears.



NOTE: *One workstation is automatically installed when the Server is installed. It is used for configuration purposes. It does not appear in the lower pane because it is automatically installed and registered. Use the installation CD and the Installation Codes to install the four additional workstations. Make sure that the computer on which they are installed meets the minimum requirements.*

2 Click the **Print** button to print the Installation Codes, so that you can take the codes where you are installing the workstations or the gateway. To avoid errors, do not copy the codes on a piece of paper.

3 From the Workstation registration screen, select the component you want to install. Then select the **Click here to install component** button (left pane). The Component Registration (Name of component) screen appears.



4 Enter the **Option Serial Number** (located on the Option Certificate) then call Kantech Customer Assistance (phone numbers are displayed on-screen) to get the **Registration Confirmation Code**.

5 Enter the **Registration Confirmation Code**, then click **OK**. The **OK** button is only enabled when the correct Registration Confirmation Code has been entered.

NOTE: *When you have entered the correct Registration Confirmation Code, the system generates an Installation Code. Blue flags identify components that have been created, but not yet activated. Green flags indicate components that have been activated.*

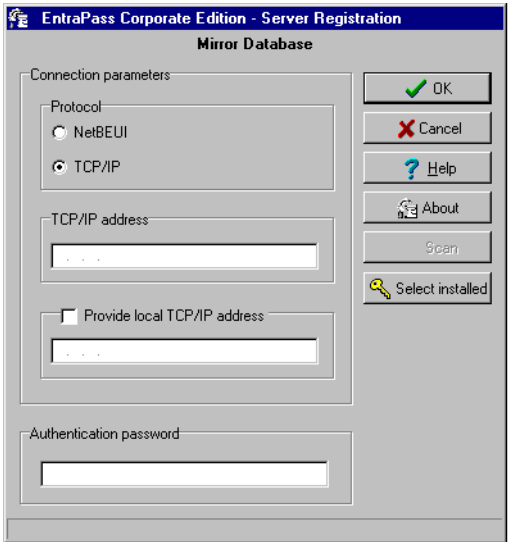
Establishing Communication with the Server

After a workstation has been installed, you have to establish communication with the Server. The following steps will assist you in configuring and establishing the first communication between the workstation and the Server using the proper protocol.

NOTE: *Before you proceed, make sure that the Server is online. If it is not, launch it.*

To establish communication with the Server:

1 From the Windows Start menu, click on **Start** > **Programs** > **EntraPass Corporate Edition** > Workstation application (x) > **Register to Server** utility. You may also start the workstation; the system automatically launches the registration program when a workstation attempts to connect to the Server before it is registered.



NOTE: *The Registration screen also appears when you launch a workstation before the Server is online. When this happens, simply start the Server.*

2 Click to select the communication protocol that is used between the Server and the Workstation.

- **NetBEUI**: The NetBEUI protocol (NetBIOS Enhanced User Interface) uses the computer name to communicate with devices. Enter the name of the computer where the EntraPass Server software is installed (case sensitive). The name of the current computer is displayed in the status bar. You may use the **Scan**  button to browse and to display existing computer names;
- **TCP/IP**: Enter the TCP/IP address of the computer where the EntraPass Server program is installed. The EntraPass Server TCP/IP address appears in the Server status bar.

- **Local**: Enter Local when registering a component on the same computer as the EntraPass Server software is installed. This option will take the address from the Server software.

3 Check the **Provide local TCP/IP address** button if the workstation connects to the EntraPass server using a VPN (Virtual Private Network) connection. Type the IP address used by the VPN application. This address is provided by the VPN application and is usually accessible by clicking on the minimized VPN icon found in the system tray.

4 You may enter a **Authentication Password** if you want operators to use a specific password when they register workstations to the Server. If you do not specify a registration password, the master password (lower case, case sensitive) will be used as the default **Authentication Password**.

Updating the System

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) since the update may take a few hours—depending on the size of the system.

Before you update your software:

1. Perform a **complete backup of your system database.** For more information on how to perform a backup, see "Creating/Restoring Backups" on page 322.
2. If you have a Redundancy Server & Mirror Database option installed, you **MUST** shutdown the Redundancy Server **FIRST**.
3. Shutdown the EntraPass Server and all other EntraPass applications. **No applications should be running when you perform a system update**.
4. Update the EntraPass Server **FIRST**.

NOTE: *Once the upgrade is complete, DO **NOT** START THE SERVER YET.*

5. Update the Redundancy Server & Mirror Database application.

NOTE: *Once the update is complete, DO **NOT** START THE Redundancy Server and Mirror Database yet.*

6. Verify the system database (see "Creating/Restoring Backups" on page 322) to make sure that no errors are detected.
7. Once you have verified the database and no errors are present, start the EntraPass Server. Once the Server is up-and-running, start the Redundancy Server & Mirror Database. It is essential to start the Server **before** starting the Redundancy Server and the mirror database.
8. When the EntraPass Server and Redundancy Server are operational, update all other EntraPass applications (i.e. gateway, workstation, SmartLink, etc.). Once the update process is finished, you may start the workstation.
9. 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**).
10. You may also use the "View connected workstations" menu item to verify the status of all the system gateways and workstations. For details, see "The EntraPass Server" on page 317.

Chapter 3 • Getting Started

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

To start an EntraPass session, you have to launch the EntraPass Server, the gateway and the Entrapass Workstation.

The server is a dedicated computer on a network that manages the access control system database. It is used to receive and dispatch information from the gateways. Gateways receive information from sites and transmit it to the server.

EntraPass Workstations enable operators to access and program the system database and components.

NOTE: *In the EntraPass Global and Corporate Edition, the Redundancy Server & Mirror Database option may be enabled to monitor the activity of the Primary Server and to serve as an alternative if the Primary Server fails.*

The software allows operators to start the gateway and the workstation at the same time by clicking on the Gateway-Workstation icon located on the desktop.

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.*

Starting and Ending a Session

From the Windows Start menu, click **Start** > **Programs** > **EntraPass Edition** > **Server** / **Workstation** > (**EntraPass application**), where the EntraPass application may be a **Workstation only** application, a **Gateway** application, or any system stand-alone utility. You may also start the program from the EntraPass shortcut icon on your desktop.

On startup, the application attempts communication with the Server. The display language depends on the settings of the previously logged operator. English is the software default language.

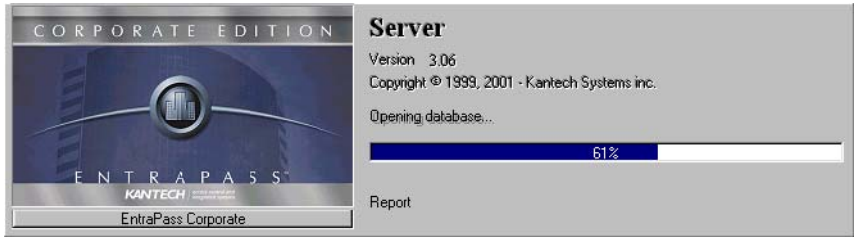
NOTE: *You have to start the EntraPass server first. If you start a workstation before starting the server, you are prompted to register your workstation to the server even when the workstation has already been registered. If your workstation has been registered, you just have to start the server.*

Starting the Primary Server

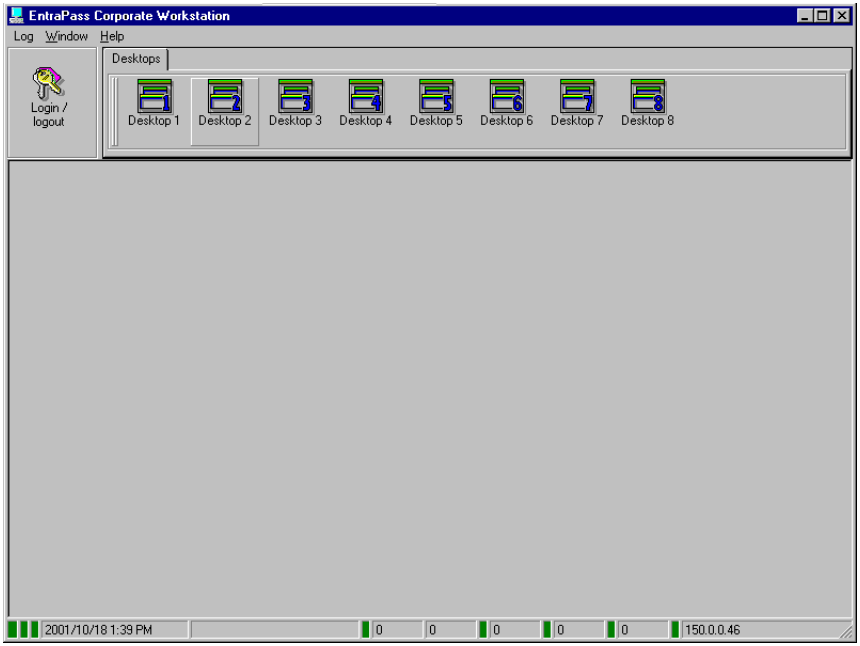
The EntraPass Server is used for:

- Displaying all the workstations connected to the server, the system event log and system error log,
- Registering new connections (workstation, gateway, client applications, etc.),
- Performing backups (Data, Archives, Time and Attendance databases),
- Restoring data (data, archive, Time and Attendance databases),
- Verifying database integrity,
- Changing the database language.

1. Start the Server (from Windows **Start** menu or from the desktop). The Server startup screen displays a progression bar as well as the information related to the server startup process.



2 From the EntraPass Server screen, select the **Login/logout** button to login.

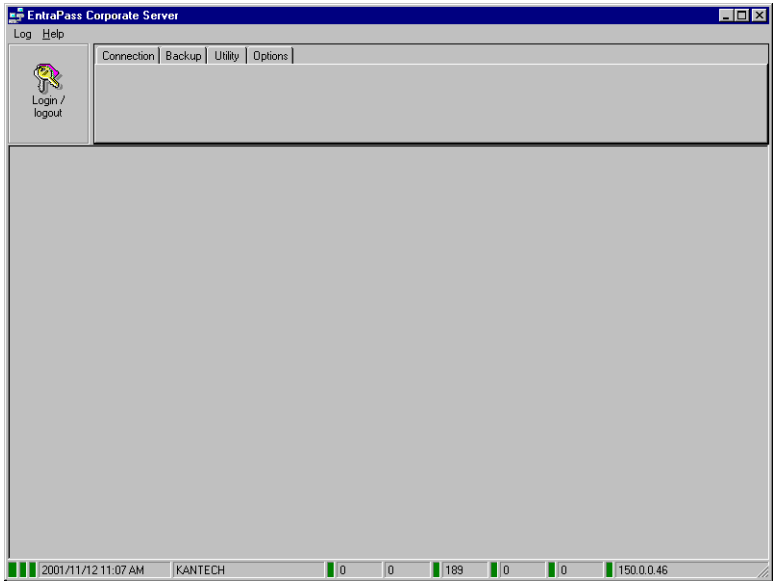


NOTE: *To allow an operator to login to the server, select the option "Allow login on server", during the "Operator security level" definition (**System** > **Security Level**). For more information, see Chapter 11 'Security Level Definition' on page 245.*

3 Enter the login information in the Operator login dialog box. The default **User name** is kantech. It is not case sensitive. The default **Password** is kantech, in lower case; it is case sensitive.

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.*

4 Once you have entered the correct login information, the EntraPass Server main window appears. Select the desired tab or the corresponding menu item to perform an operation or to display system information.



The status bar indicates the communication status: Green: Communication is OK, Red: Communication problems.

5 Point the cursor to the status flag (colored rectangle) to enable a hint describing the displayed information: the first two colored rectangles indicate the server database open state and the database locked state.

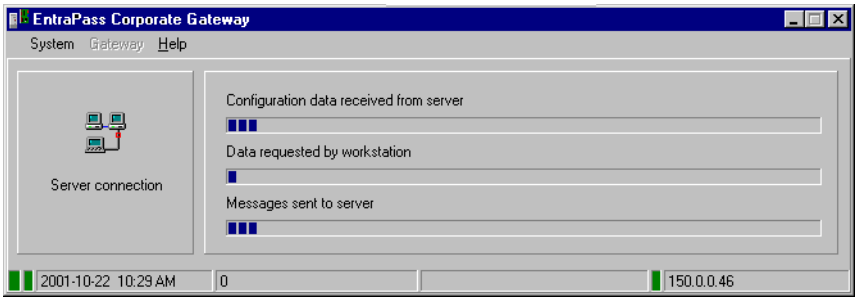
- If the first status flag is red, this indicates that the system database is not open. This could be due to a backup or a database verification in progress.
- If the second status flag is red, this indicates that the database is unavailable. This happens when the server is processing data or updating the database.

Starting the Gateway Program

The gateway program may be installed on the same computer as the server or workstation, but it is recommended to install it on a dedicated computer.

To start the gateway:

1 Start the Gateway (from Windows **Start** menu or from the desktop). You do not need to enter a password or a username. The EntraPass Edition main window appears.



The progress bars indicate:

- **Configuration data received from the server**: this indicates configuration data such as card modifications are being sent to the gateway from the server.
  - **Data requested by workstation**: this is requested data such as a status request.
  - **Messages sent to server**: these messages originating from a controller are sent to the server.

NOTE: *On rare occasions, you may use the* ***System*** *menu items to reload the gateway. This option is used to refresh all or some parameters of the network. You have to login in order to perform the reload operation.*

2 You may right click anywhere in the Gateway program screen to display a submenu:
   - **Minimize** minimizes the Gateway screen,
   - **Send to tray** sends the screen to the status (tray) bar.

3 You may select the **System** menu item to login, to logout, or to perform a gateway **reload**.

4 You may select the **Gateway** menu item if you want to choose a gateway. The number of gateways that are communicating with the server is displayed on status bar in the gateway main screen.

NOTE: *The status bar displays the communication status flags. The first status flag indicates the status of the communication with the server. If the first status flag is red, this indicates that the server is not communicating with the gateway. This can occur when the server is offline (you may then start the server). The status bar also indicates the system date and time, the number of gateways and the server IP address.*

Starting the EntraPass Workstation

EntraPass workstations enable operators to access and program the system database and components.

Make sure that the server is online when you start the workstation software.

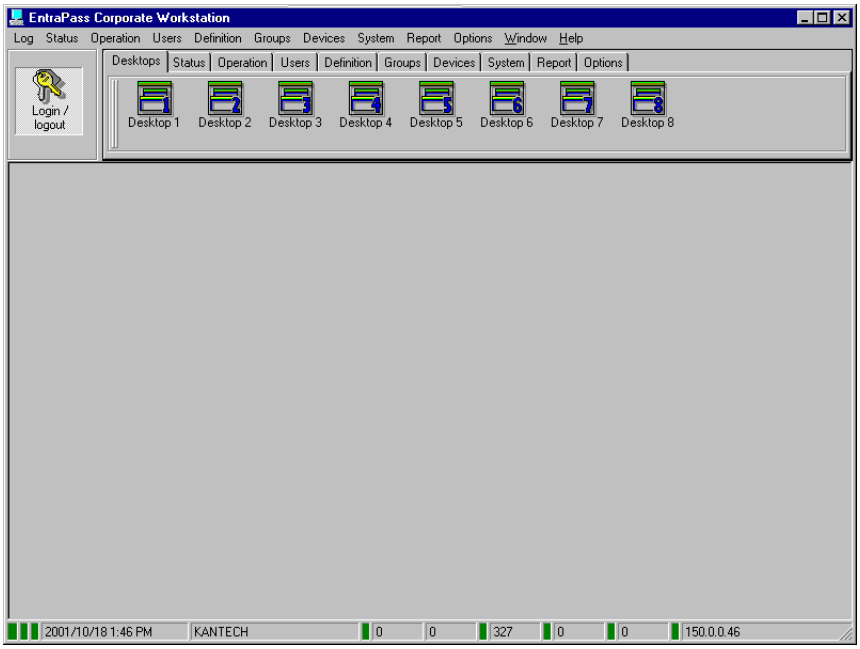
On startup, the application attempts communication with the Server. The display language depends on the settings of the previously logged operator. English is the software default language.

NOTE: *You have to start the EntraPass server first. If you start a workstation before starting the server, you are prompted to register your workstation to the server even when the workstation has already been registered. If your workstation has been registered, you just have to start the server.*

To start the workstation:

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

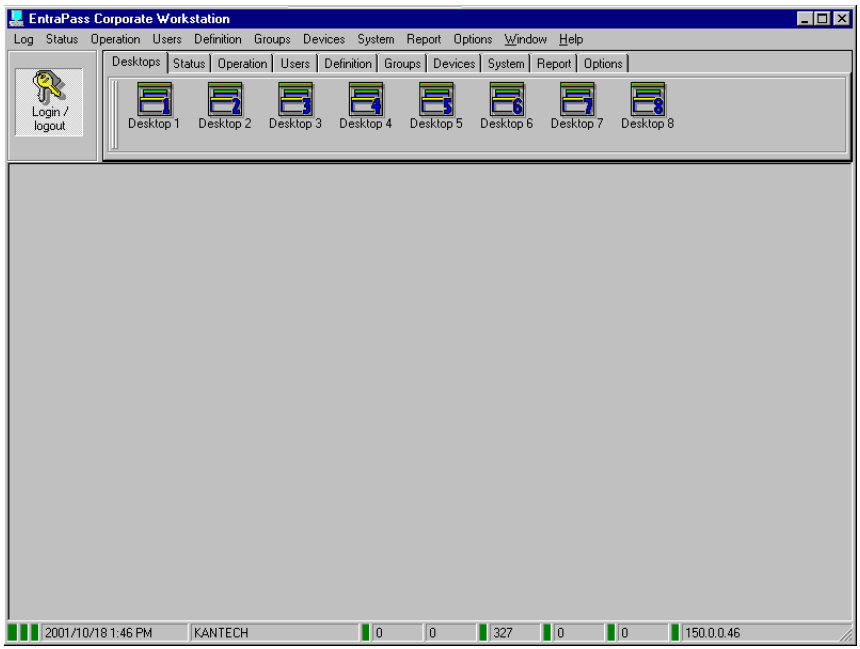
2 Click the **Login**/**logout** button on the toolbar.



NOTE: *When the server is off-line, the first status flag (colored rectangles of the status bar) turns red; the Login/logout button is disabled. If this happens, launch the server; the workstation will resume its operation.*

3 Enter you Operator **User name** and **Password**. The password is case sensitive; the username is not.

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. Operators are not allowed to login on more than one workstation at a time. However, an operator may login on a server and a workstation at the same time.*

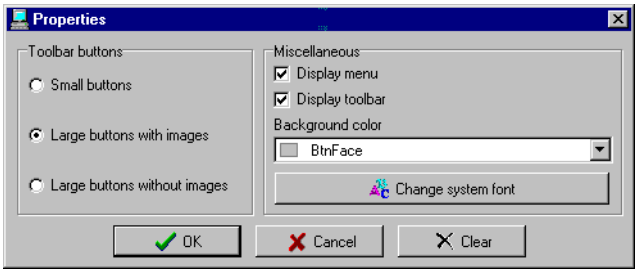


NOTE: *Click any tab to access the system toolbar or select a menu item to access the system menu. In the lower part of the screen, color coded rectangles indicate the communication status: Green, communication is OK; Red: communication problems; Blue: a report is pending. You may point the cursor to a rectangle or any number to display details.*

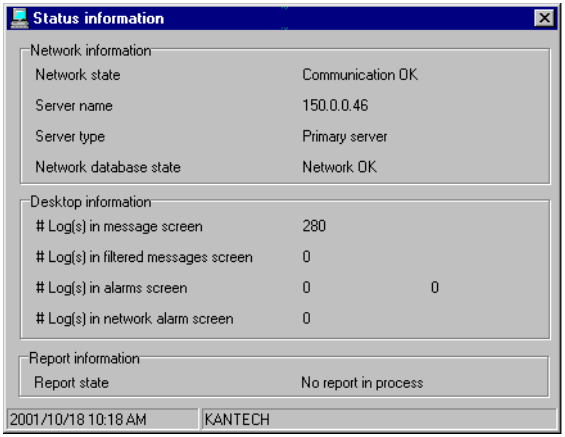
4 Move the cursor over the colored rectangles to show details about the network status, the network database status and the workstation report status.

5 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.

6 Right click anywhere in the main window to display the Properties screen. This allows operators to customize the screen buttons as well as the background color.



7 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 logout. This ensures that the system databases are shutdown properly.*

Express Setup

Express Setup allows you to configure system components such as sites and controllers, as well as devices associated with these components such as doors and inputs. This utility reduces programming to a minimum, allowing the installer to test the installation and system components. You may use it to configure a site or to define controllers associated with a site.

When used to configure a site, it allows installers to associate this site to a gateway. It also allows installers to configure the site rapidly, giving minimum configuration information about the controllers connected to it.

You may launch Express Setup from Windows Start menu: **Start** > **Programs** > **EntraPass Edition** > **Workstation/Server** > **Express Setup** or by clicking the **Express Setup** icon from a workstation or gateway toolbar.

NOTE: *There are two versions of the Express Setup program..*

When used to configure a controller, it allows operators to assign default values to a controller and to its associated devices (input, relays and output). In this case, it is launched at a system message box or from a controller definition menu.

NOTE: *You have to login to the server when you launch Express Setup. In fact, as the program allows you to modify the system devices configuration, it is essential to authenticate yourself before proceeding with any modification.*

For details on Express Setup, see “Express Setup Program” on page 345.

Other 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. This utility is run 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 sites, number of controllers in a site, etc.
- **PING Diagnostic:** Program used to diagnose network related problems.
- **System Report Viewer:** Program used by the operator to view reports without having to start a Workstation.
- **Vocabulary Editor**: Simple and easy program used to translate the software in the language of your choice.
- **Workstation (Configuration Program):** Program, similar to a standard workstation, used by the system administrator to configure the system logical and physical components.
- **Migration Utility**: Program used to transfer information relating to software and database for the upgrade from Special Edition to Corporate Edition or Corporate to Global Edition.

These utilities may be launched from the Windows Start menu of any computer where Entrapass Server or EntraPass Workstation are installed.

For details on EntraPass stand-alone utilities, see Chapter 15 ‘System Utilities’ on page 327.

EntraPass Workstation Toolbar

EntraPass windows display most of the following buttons. They are an easier 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 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.

- 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 “Viewing Components Links” on page 44.
- 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 “Finding Components” on page 40.
- The **Express Setup** button allows installers and system administrators to configure system devices by assigning default settings.
- 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 H**elp** button to view the help content on a specific subject.
- The **OK** button is used to save and accept the modifications, additions or deletions made to a record in the database of the system.
- The **Select all** button is used to select all the items or components displayed in a list.

- The **Unselect all** button is used to unselect all the items or components that were previously selected in a list of choices.
- 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.

In some 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.

- 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.
- 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.

Basic Functions

Following are the basic system operations:

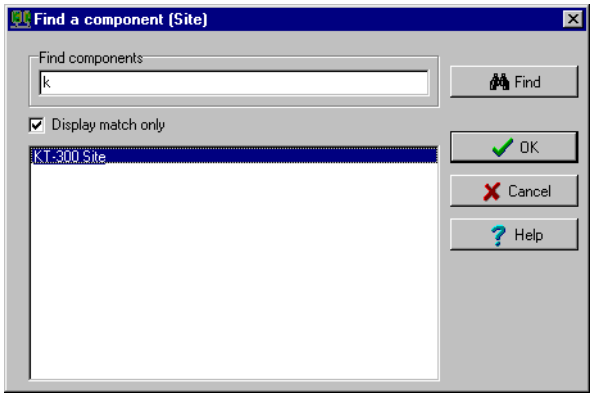
- Find components,
- Select components,
- Print lists or reports,
- View links between components.

Finding Components

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

To find a component:

1 From any EntraPass window toolbar, click the **Find** icon.



2 Check the **Display match only** option if you want to restrict the search result. If you do not select this option, the search results will be extended to any system component related to the string you have entered.

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

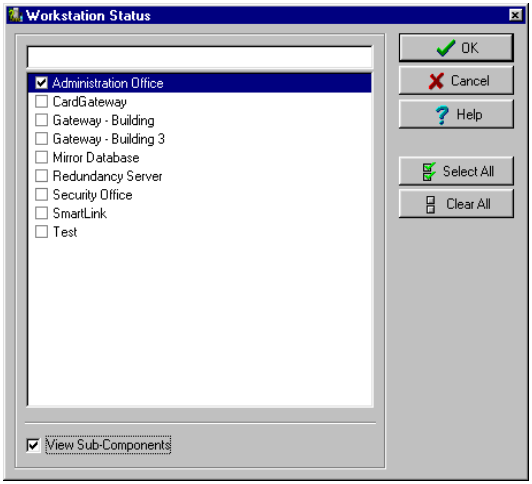
4 Select the component you want to display, then click **OK**.

Selecting Components

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

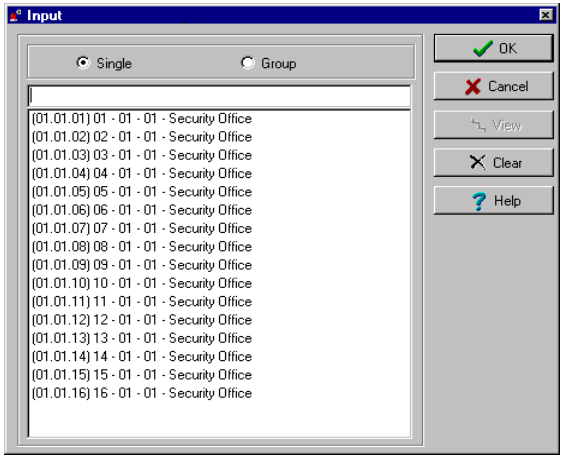
To select a component:

1. From the active window, click the 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.

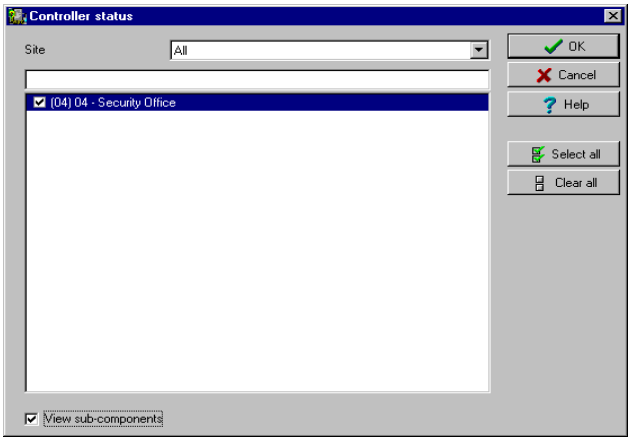


3. From the displayed list, select the component/group you want to display. You may check the **View sub-components** option to display the components associated with the selected components.

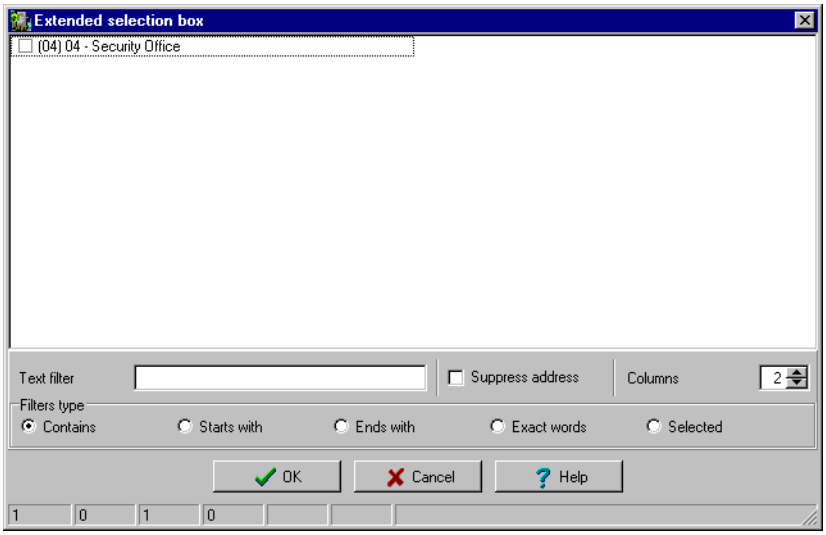
4 Where available, use the **Select all** button to select all the components, or use the **Clear all** button to remove the check marks from the selected components. Click **Cancel** to return to the previous screen without any selections or changes.



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



6 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.



7 Click **OK** to apply selections and return to previous screen.

Printing

Operators may need the Print function to:

- Print a list of cards,
- Print event parameters,
- Print event-relay association,
- Setup a report for printing.

To print a list or a report:

1 From any EntraPass screen, 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 353.

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 you want 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.

8 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 screen to preview your output before printing.

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

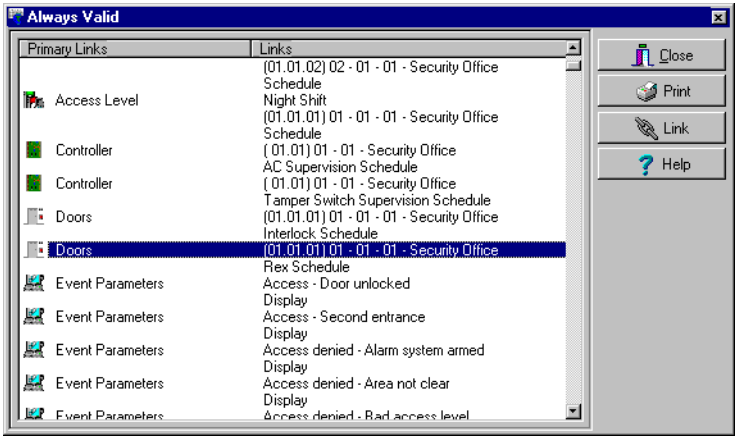
Viewing Components Links

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.*

To view component links:

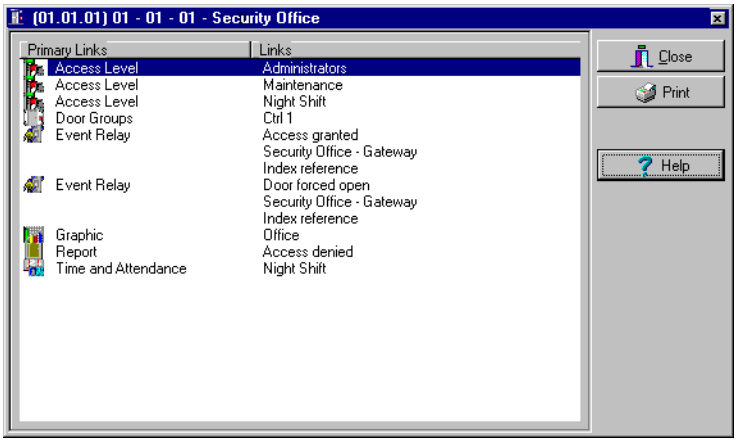
1. From any menu screen, select a component and click on the **Link** button. All the components that are associated with the selected component are displayed.
2. The icons that are located on the left side of the components indicate the component type. For example, if you select the **Always valid** 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.



In the highlighted example, the **Always valid** schedule is used as the REX (Request to EXit) schedule in the Door definition menu.

NOTE: *You can right-click on the screen 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:



The screen displays all the system components that are associated with the selected door. In this example, the “door” is used in the Administrator access level--meaning that users granted this access level are allowed access to the selected door.

4 Click the **Print** button to print the information displayed on the screen.

Chapter 4 • Configuring System Devices

After the installation of the system hardware and software, you have to configure the access system devices. These include software components (workstations, gateways, SmartLink, Redundancy Server and Mirror Database) and physical components (controllers, relays, doors, etc.).

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 for the first time or when you are defining controllers. You may launch the Express Setup utility from the Windows **Start** menu or from the Workstation Registration screen. You may also launch this utility from a system prompt, when, for instance, you are adding a controller to your system.

NOTE: *For detailed information about using the Express Setup utility, see “Express Setup Program” on page 345.*

Configuring EntraPass Workstations

Configuring EntraPass Workstations and Client Applications

The Workstation menu allows operators to configure computers where EntraPass is installed. This includes configuring computers where you have installed: the EntraPass Workstation software, the Gateways, the Redundancy Server and Mirror Database programs, as well as computers where you have installed the SmarLink Interface, if applicable.

To configure the EntraPass Workstation and client applications, you have to define:

- General parameters applicable to all computers where EntraPass is installed, including selecting the graphic,
- Security parameters (applicable to all the workstations where EntraPass Workstation, the Gateway as well as client applications are installed),
- Filters (to define which gateways and workstations will send messages to the workstation being configured),
- Message/alarm controls.

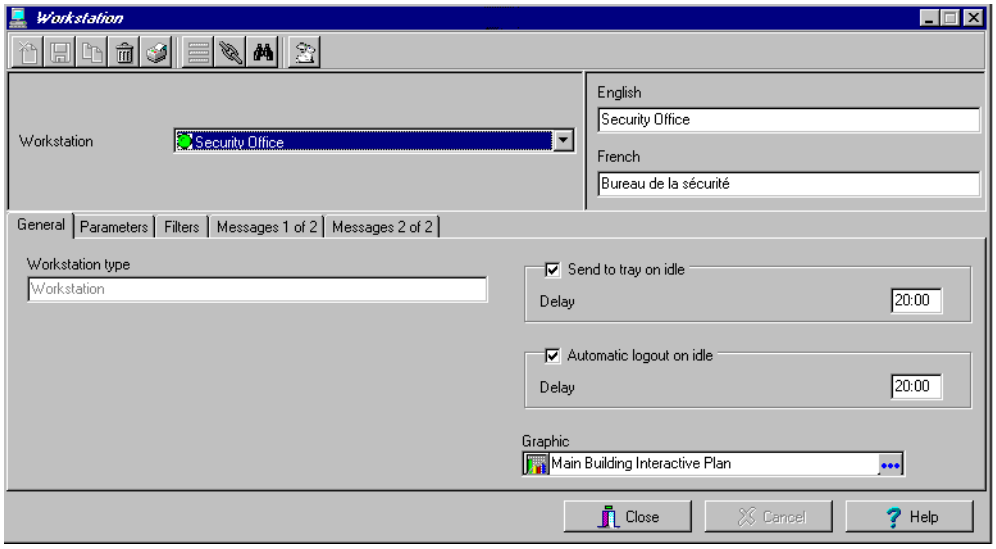
Defining Workstations General Parameters

The **General** tab allows you specify the system behavior when the operator is inactive, that is when there is no action on the keyboard (idle time). This feature provides additional security to prevent access to the system by an unauthorized person. The default delay is 20 minutes.

This menu allows you also to select a graphic into which the workstation will be displayed. For details on system graphics, see Chapter 7 ‘Defining Graphics’ on page 143.

To configure an EntraPass Workstation:

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



NOTE: The Workstation drop-down list displays default names assigned by the system. You have to customize these names according to your needs.

2 From the **Workstation** drop-down list, select the workstation application you want to configure. The **Workstation** drop-down list displays all Workstation and gateway applications that have been installed and registered. The **Workstation type** drop-down list displays the type of the selected item. It may display Workstation, Gateway, Redundancy Server & Mirror Database, etc.

3 Assign a name to the selected workstation. 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.

4 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 application 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 workstation application will be minimized and sent to the task bar.
- Select the **Logout on idle** option if you want the EntraPass application to logout when there is no action on the keyboard. If you do this, you have to specify the period after

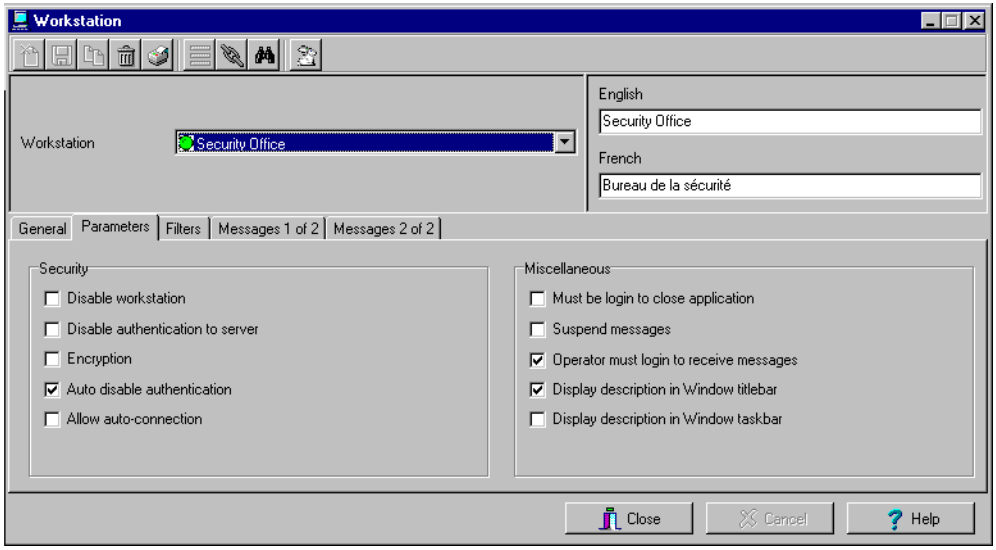
which the application will be minimized: in the Automatic logout on idle enter the delay after which the Operator will be automatically logged out, (the option has to be checked).

5 From the **Graphic** list, you may select the graphic to which the workstation is assigned, if applicable. For details on defining graphics, see "Defining Graphics" on page 143.

Defining Security Parameters for EntraPass Workstations

This section applies to all EntraPass applications (EntraPass Workstations, Gateways, SmartLink (if installed), Redundancy Server & Mirror Database, etc.).

1 From the Workstation screen, select the **Parameters** tab.



2 Make the appropriate choices:

- **Disable workstation:** if selected, the operator will not be able to start the workstation.
- **Disable authentication to server:** When this option is checked, it is no longer possible to register the workstation to the server.
- **Encryption:** select this option if all incoming or outgoing messages for this workstation should be encrypted.
- **Auto disable authentication:** if selected, the system will automatically disable authentication when the workstation has authenticated itself for the first time.
- **Allow auto-connection:** if selected, the workstation will automatically connect itself to the server.
- **Must be login to close application**: checking this option will oblige operators to login before they exit an EntraPass program.

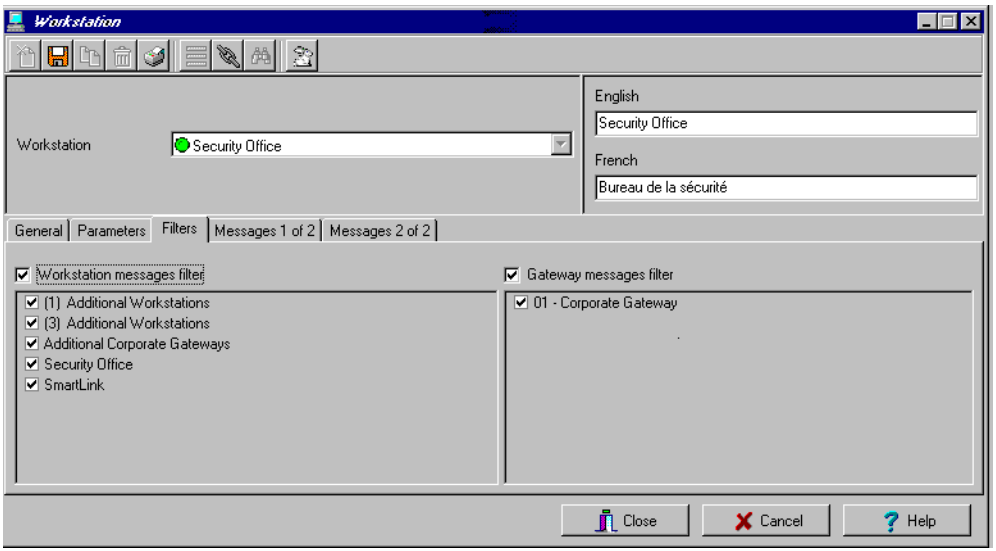
- **Suspend messages:** if this option is selected, all incoming messages for this workstation will be suspended. Use this option for a workstation that is used only to configure components or when messages are not required.
- **Operator must login to receive messages**: checking this option will oblige the operator to login with a valid username and password before system messages can be viewed.
- **Display description in Window titlebar**: check this box to display workstation information in the window titlebar (top).
- **Display description in Window taskbar**: check this box to display workstation information in the window taskbar (bottom).

Defining Workstation Filters

The filters menu allows you to define which messages the Server will send to the selected workstation. This feature provides the ability to restrict incoming messages for a computer.

To define filter incoming messages:

1 From the Workstation window, select the **Filters** tab.



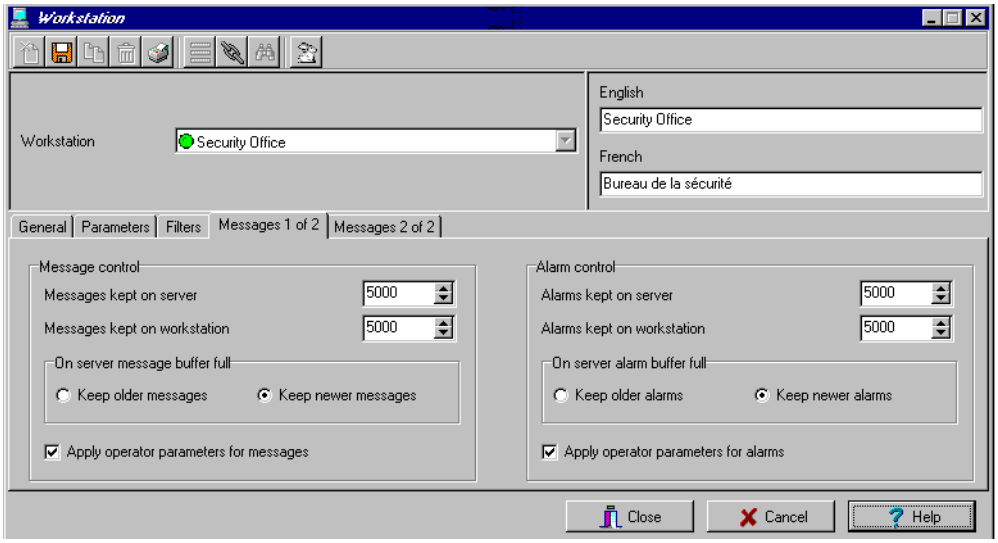
2 Select the workstation whose generated messages will be sent to the workstation being configured by the server.

3 Select the gateway whose generated messages will be sent to the workstation being configured by the server.

NOTE: *The basic configuration of a workstation consists of the workstations and gateways that are selected during its definition. This configuration indicates to the server that the workstation is authorized to receive events/messages that will be generated by the selected workstations or gateways.*

To define message and alarm controls:

1 Click the **Messages 1 of 2** tab to define how messages should be processed when the workstation is connected (or not) to the server .



2 In the **Message control** and **Alarm control** sections:

- Specify the number of messages that the server will buffer when the workstation is off-line, that is, when it is not connected to the server . The server buffers a maximum of 60,000 messages and 60,000 alarms per workstation (default: 5,000).
- Specify the number of messages that will be kept in the **Messages Desktop**. There is a maximum of 60,000 messages and 60,000 alarms per workstation. By default, it keeps 5,000 messages and 5,000 alarms.

NOTE: *The workstation will always keep newer events. To view older events, you have to request a historical report. For details on requesting reports, see Chapter 13 'Defining and Requesting Reports' on page 287.*

3 Specify if the Server should keep newest or oldest messages/alarms when its buffer reaches the defined maximum number:

- **Keep older messages/alarms:** the EntraPass Server will keep the oldest messages/alarms and archive the newest messages/alarms when the workstation is off-line and when the Server buffer is full.
- **Keep newer messages/alarms:** The EntraPass Server will keep the newest messages/alarms and archive the oldest messages/alarms when the 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 workstation configuration by checking **Apply operator parameters for messages**/**Apply operator parameters for alarms** options. When these options are enabled, operator settings have priority over workstation settings.

- When the **Bypass workstation message filter** option is checked in the **Operator** definition menu (**System** > **Operator**), the operator will receive all messages, regardless of the filters configured in the workstation definition.
- If the **Apply operator parameters for messages**/**Apply operator parameters for alarms** options are selected and if the **Bypass workstation message filter** is not selected, all events will be filtered according to the workstation configuration, and filtered again according to the security level of the operator who is currently logged on the workstation.

NOTE: *If the "Apply operator parameters for messages" and "Apply operator parameters for alarms" options are selected and no operator is logged in, or the workstation is off-line, events will NOT be buffered by the server.*

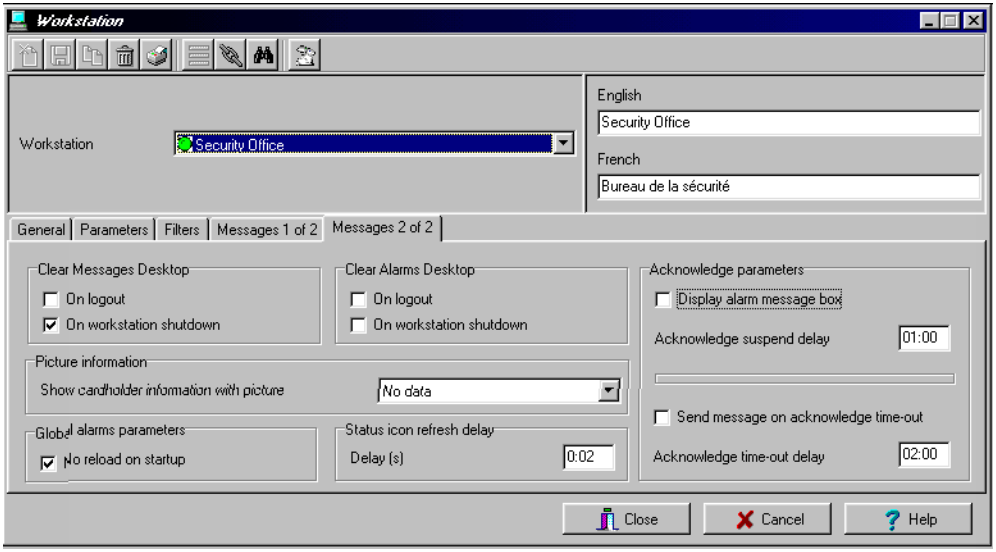
Defining Parameters for System Logs and Alarm Messages

The EntraPass software stores all system logs and alarm messages. System messages are displayed in the Message desktop; alarm messages are displayed in the Alarms desktop. System desktops display messages, alarms, instructions, etc. For details on EntraPass Desktops, see Chapter 12 'Working with Desktops' on page 263.

The **Message 2 of 2** tab allows you to specify when systems messages and alarms will be cleared as well as acknowledgement parameters.

To define parameters for system desktops:

1 Click the **Messages 2 of 2** tab to define additional parameters for the workstation being defined.



2 Specify when **Messages/Alarms desktops** are cleared:

- **On logout** (on a regular logout by an operator),
- **On network disconnection** (when the workstation is disconnected from server).

NOTE: *Messages and Alarms desktops are configured in the Desktop definition menu. For details, see Chapter 12 'Working with Desktops' on page 263.*

3 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 all the fields defined on a card.

NOTE: *By default, the fields display "card information #1" to "card information #10". These labels may be customized. For more information on renaming card information labels, see "Customizing Card Information Fields" on page 154.*

4 Specify whether all the system alarms (network alarms) will be reloaded on startup. System alarms are stored in the server database. If the **No reload on startup** option is checked, operators will have to manually reload the system alarms.

NOTE: *Manual reload of the system alarms can be done through the* ***Network Alarms*** *desktop. To do so, open the desktop, right click on an item and select* ***Refresh*** *from the contextual menu.*

NOTE: *You may want to check this option for fast startup; it is useful when the system has a slow connection.*

5 In the **Status icon refresh delay** section, specify the time interval at which the workstation 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.

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.

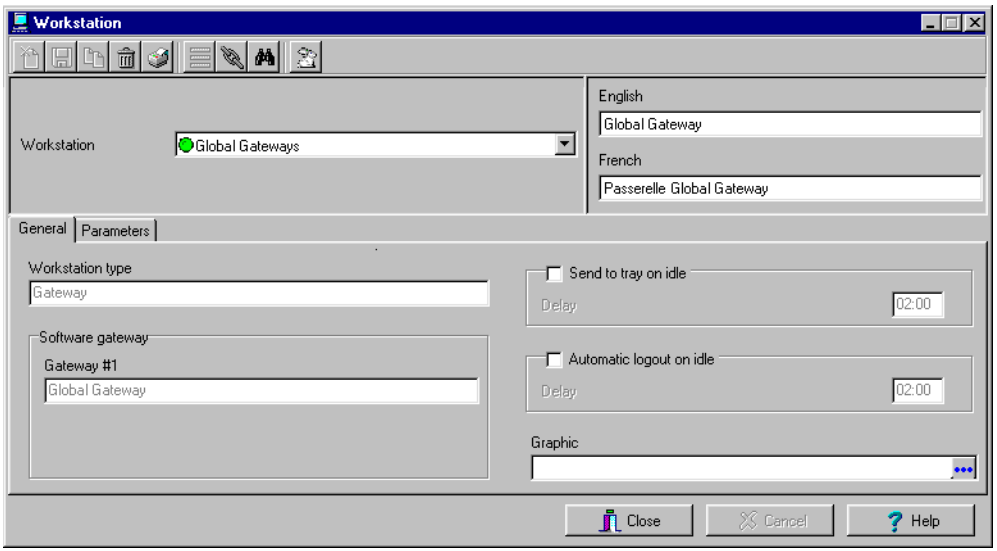
7 You may check the option **Send message on acknowledge time-out** to generate an "acknowledge time-out" event when the operator fails to acknowledge an event during the time-out delay specified in the **Acknowledge time-out** delay field. The message will be sent to the Message desktop and the Alarms desktop. For more information on EntraPass desktops, see Chapter 12 'Working with Desktops' on page 263.

Defining the EntraPass Gateway

The Gateway application allows you to monitor the controller sites connected to the gateway. You may add up to 40 gateways to your EntraPass software.

To configure a gateway program:

1 From the **Workstation** drop-down list, select the gateway application. When the selected workstation is a gateway type, the **Workstation type** field displays “Gateway”.



2 For details on defining the system behavior on idle, see “Defining Workstations General Parameters” on page 48.

3 To define security parameters for the gateway application, see “Defining Security Parameters for EntraPass Workstations” on page 50.

Configuring the Oracle/MS-SQL HR Interface

The Oracle/MS-SQL HR Interface creates a real-time mirror copy of the EntraPass card databases (Card database, Card group database, Card type database and Badge database) in MS-SQL or Oracle database formats. In addition, it allows operators to interact with the system card database from their MS-SQL or Oracle programs. Operators can add, modify and delete cards, or obtain card-related information in the EntraPass card database.

The card information is updated in all the databases, whatever the program used to modify or to update the database; the Oracle/MS-SQL HR Interface ensures that the modifications are conveyed in all the client applications.

NOTE: *The Oracle/MS-SQL Interface requires an additional license.*

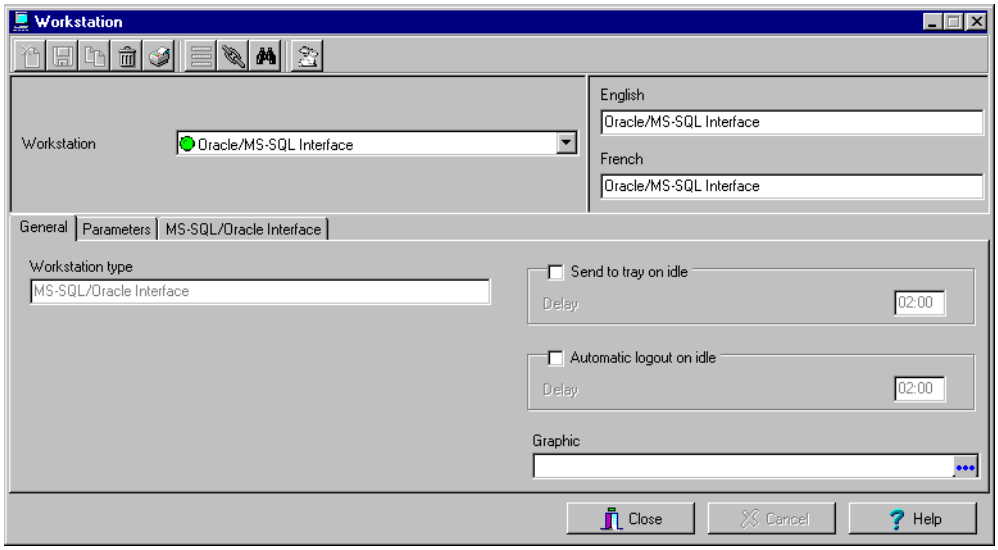
It is recommended to install the Oracle/MS-SQL HR Interface on a separate computer in order to facilitate the data exchange process between the EntraPass software and the Oracle or MSSQL server.

To configure the Oracle/MS-SQL HR database Interface you have to define:

- General parameters (applicable to the Oracle/MS-SQL HR Database Interface), including the workstation security parameters
- Database parameters, including the database access rights.

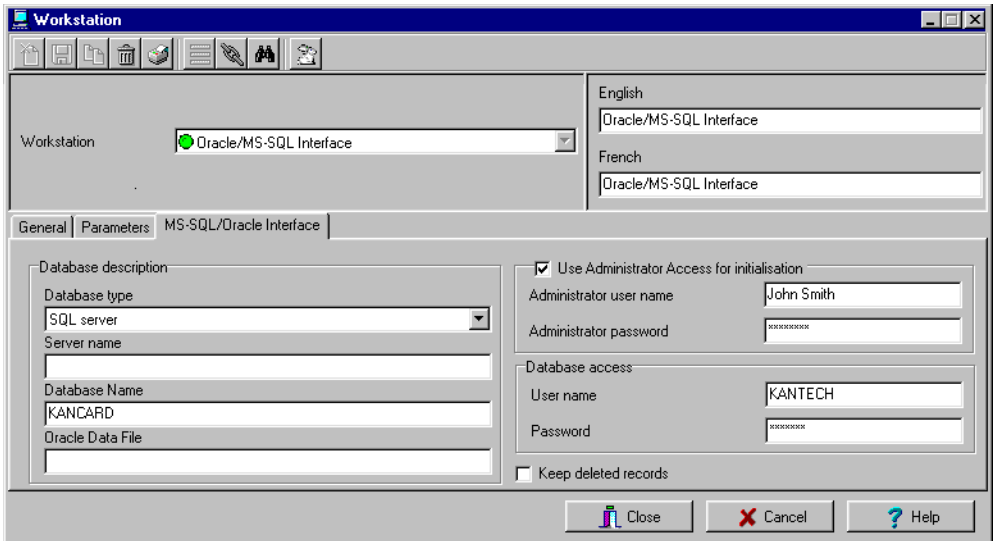
To configure the Oracle/MSSQL HR Interface:

1. From the **Workstation** drop-down list, select the Oracle/MS-SQL HR Interface from the **Workstation** drop-down list.



2. Define the workstation on which you have installed the Oracle/MS-SQL HR Interface. For more details, see “Defining Workstations General Parameters” on page 48.
3. Select the **Parameters** tab to define security parameters for the Oracle/MSSQL HR Interface. For details, see “Defining Security Parameters for EntraPass Workstations” on page 50.

4 Select the **MS-SQL/Oracle Interface** tab to indicate how the EntraPass software will communicate with the client database and to define the database access rights.



5 From the **Database type** drop-down list, select the database server: Oracle 8.0, Oracle 7.3 or Microsoft SQL. Be sure to select the correct server version since the database configuration is different from one version to another.

NOTE: *If the wrong version is selected, the Oracle/MS-SQL HR Interface will not communicate and will not be able to connect to the server.*

6 Enter the database server name in the **Server name** field.

7 Type the name of the requested Oracle or SQL database in the **Database Name** field.

8 If you are using an Oracle server, type the name of the data file which points to the data you wish to access in the **Oracle Data File** field.

NOTE: *Oracle and SQL servers may be configured to contain more than one database. Accessing an SQL database requires pointing to its name while accessing an Oracle database requires pointing to its name and specific data file. Refer to your network administrator for access parameters to the database specific to your application.*

9 Check the **Use administrator Access for Initialization** option, if applicable. Checking this option enables you to enter a valid administrator username and password.

NOTE: *It is important to check this box. If you do not, you must manually create the database, the username and password in the database server.*

10 Enter the username and password of the database administrator in the **Administrator user name** and **Administrator password** fields. The program will automatically create the database, username and password in the server database

11 In the **Database Access** area, enter a username and password which will be used by the card gateway to connect operators to the Oracle/SQL database.

NOTE: *The database access procedure does not allow the card gateway to create or modify an existing user profile on an Oracle/SQL server.*

12 Check the **Keep deleted records** option if you want to keep the record of a card, even when the card is deleted from the EntraPass database. The record will be kept in the Oracle/MS-SQL HR Interface database.

NOTE: *If you do not select this option, deleted records will be physically and permanently erased from the Oracle/MS-SQL HR database.*

NOTE: *When EntraPass creates the card database automatically in the SQL or Oracle Server, it allows a maximum of* ***50MB*** *for the card database. If you want to increase the size of the database, you must create the database manually, as detailed in the following section.*

Manually Creating Database Servers

In order to integrate the database with EntraPass, you have to create the database that will be used and then create the Kantech operator in the database. If your system is using an MS-SQL server, proceed as follows:

To manually create the operator in the MS-SQL/Oracle Server:

The first step in integrating MS-SQL/Oracle with EntraPass is to create the database that will be used.

1 Right-click the Database folder and select **New Database**.
2 Enter the database name in the **Database name** field.
3 Click **OK** once you have entered the name of the database.

To create the KANTECH operator for an MS-SQL Server:

You have to create an operator that the Oracle/MS-SQL HR Interface will use to log on the MS-SQL server.

1 Right-click **Logins** and select **New Login**.
2 Enter kantech (lower case) in the **Name** field.
3 Make sure that the **SQL Server Authentication** option is checked.
4 Enter **kantech** (in lower case) as the password in the **Password** field.
5 Click the **Database Access** tab.
6 Check the name of the database created in step 2. When you select this option, the bottom part of the screen displays “Database Roles - Permit in database role”.
7 In order to be able to modify the database, check the **Public and db_owner** options and click **OK** to save and exit. You will be prompted to confirm the password.
8 Enter kantech (lower case) and click **OK** to exit.

To create the KANTECH operator for an Oracle Server:

1. Log on the ORACLE server as the administrator. Default name “kantech” may be used.
2. Create a database. Default database name “KanCard” may be used.
3. Create a logon profile. Default username and password “kantech” may be used.
4. Assign the kantech operator the permission “Owner”.

NOTE: *If any defaults are changed, there must be a consistent Database name, User name and Password between the Database and EntraPass software.*

Configuring the Mirror Database & Redundancy Server

The Mirror Database monitors the communication between itself and the Primary Server. The Mirror Database is a real-time copy of the system database and Windows system registry entries.

When communication between the Mirror Database and the Primary Server fails, the Mirror Database automatically initiates the delay after which the Redundancy Server is automatically started to replace the Primary Server.

The Mirror Database & Redundancy Server program cannot run on the same computer as the Entrapass software server. The Mirror Database & Redundancy Server should be installed on a dedicated computer.

NOTE: *It is possible to operate the system with more than one Mirror Database & Redundancy Server.*

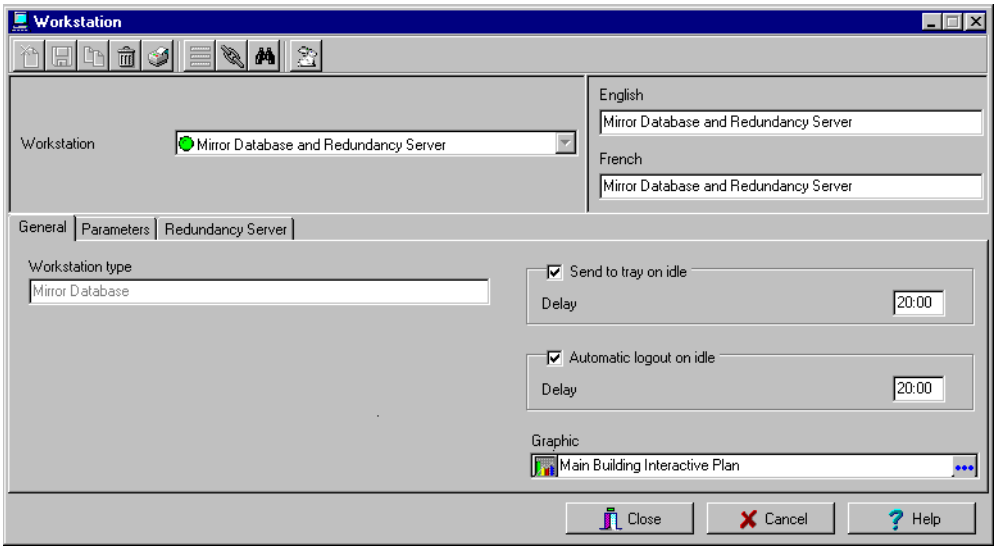
NOTE: *The Mirror Database & Redundancy Server feature requires an additional license.*

To configure the Mirror database & Redundancy server workstation, you have to define:

- General parameters applicable to the Mirror Database & Redundancy Server, including security parameters,
- Redundancy Server parameters,
- Security parameters.

To configure the Redundancy Server & Mirror Database:

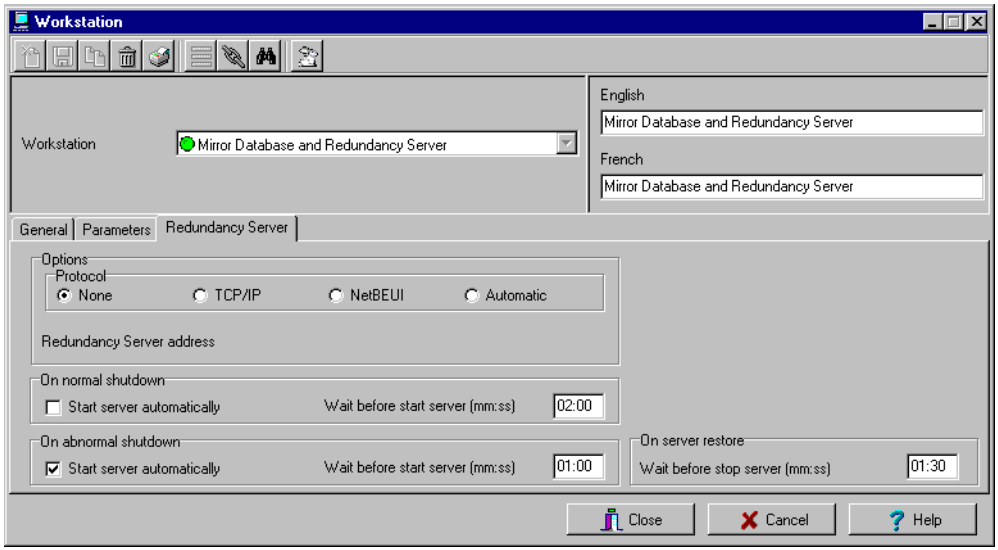
1 From the **Workstation** drop-down list, select the **Redundancy Server** application.



2 Define the workstation on which you have installed the Redundancy Server& Mirror Database. For more details, see “Defining Workstations General Parameters” on page 48.

3 Select the **Parameters** tab to define security parameters for the Redundancy Server& Mirror Database. For details, see “Defining Security Parameters for EntraPass Workstations” on page 50

4 To define communication parameters for the Redundancy Server& Mirror Database, select the **Redundancy Server** tab.



5 Select the protocol that is used to communicate with the computer where the Mirror Database is installed: **None**, **TCP/IP** (network server), **NetBEUI** (computer name) or **Automatic**.

NOTE: *When you select TCP/IP, the* ***Redundancy server address*** *field is enabled to allow you to enter the TCP/IP address of the computer hosting the Redundancy Server and Mirror Database. The field can be edited when you select NetbEUI.*

NOTE: *If* ***Automatic*** *is checked, the IP address of the computer hosting the Redundancy Server and Mirror Database will be sent to the server for broadcast to all workstations on the network. This option is particularly useful if you don't know the IP address or if the computer is set to a dynamic IP address.*

6 Specify the options for starting the Redundancy Server: this may be automatically on a normal shutdown or on an abnormal shutdown. The Mirror Database will start the Redundancy Server when the delay indicated in the **Wait before start server** field has expired.

NOTE: *If you do not check the* **Start server automatically** *option, the Redundancy Server* ***will not*** *start when the primary server is closed under normal conditions (i.e. operator shutdown). Therefore, it will be necessary to start it manually.*

7 Specify the system behavior when the server returns to normal (**On server restore**): enter the delay after which the Redundancy Server will be stopped when the primary server returns to normal functionality. During this time, the Redundancy Server will continue to prevail (maximum allowed: 59:59 minutes).

Configuring SmartLink

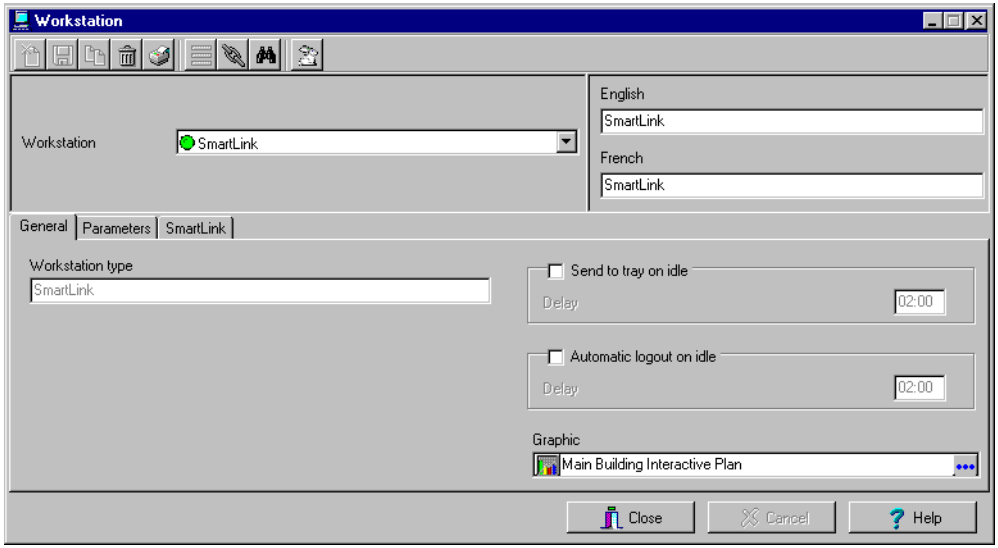
The SmarkLink application allows operators to interface the EntraPass access control software with any intelligent device such as video matrix switchers, paging systems, e-mail application, etc., using an RS-232 connection between one of the EntraPass workstations and the external device. Integration with other systems can also be accomplished through software DLLs. SmartLink can be used to connect to another computer to exchange information and update it automatically in real-time. It also enables EntraPass to receive and send messages or commands, and to communicate with client applications.

NOTE: *The SmarkLink feature requires no additional license.*

EntraPass allows you to configure the SmartLink communication mode. For more information on SmartLink and how it works, see your *SmartLink Reference Manual*.

To configure SmartLink general parameters:

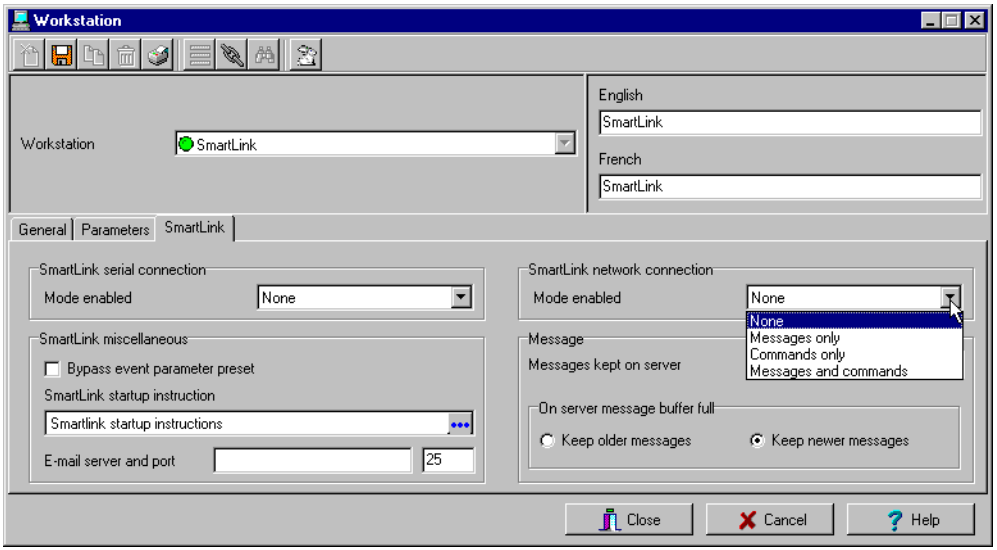
1 From **Workstation** drop-down list, select the system **SmartLink** application.



2 Define the workstation on which you have installed the Smartlink interface. For more details, see “Defining Security Parameters for EntraPass Workstations” on page 50.

3 Configure the SmartLink workstation security parameters. For more details, see “Defining Security Parameters for EntraPass Workstations” on page 50.

4 Click the **SmartLink** tab to view and setup the Smartlink connection parameters.



5 From the **Mode** enabled drop-down list, select the mode that is used:

- The **Unidirectional** or **Message mode** is used to process the contents of instructions that are generated when an event programmed with an instruction occurs. Instructions are defined in the **Instruction** definition menu and assigned to events in the **Event Parameters** menu. For details on defining instructions, see "Instruction Definition" on page 256.
- The **Bidirectional** or **Command mode** is used to process the requests corresponding to commands received by the serial port or by the network, and to return the appropriate response from the process to the sender.

NOTE: *When you start the SmartLink application, the connection options for the serial port and network modes are retrieved from the EntraPass Server. If the network connection mode of the SmartLink is different from "none", the SmartLink application will be started to allow a client application to connect to the SmartLink application, either to execute commands or to receive messages sent through the network or both process simultaneously.*

6 Check the **Bypass event parameter preset** option if you want to ignore all default settings of the **Event Parameter** definition menu (**System** > **Event Parameters**). By default, all events are programmed to be sent to all workstations (including the SmartLink workstation). Check this option to avoid receiving unnecessary instructions and events that are not intended for the SmartLink application.

NOTE: *You will have to "manually" create associations of events and instructions in the Event Parameter definition menu. For example, you could select the event "Door forced open" and send only a specific instruction to the SmartLink workstation that would send an e-mail.*

7 Click the button to select a SmartLink startup instruction. The instruction you assign will be processed automatically when the **SmartLink** application is started. For details on defining Smartlink and other system instructions, see Chapter 11 'Instruction Definition' on page 256.

8 To use the SmartLink option with the e-mail service, enter the E-mail server name and port in the **E-mail server and port** field.

NOTE: *The e-mail port value is set to 25 by default. You may leave as is or change this value to any available port on the network (between 0 and 65695) For information about setting of the e-mail server, contact the network administrator.*

9 In the **Messages** section, you may want to define the status of messages in the Server, or to modify the number of messages that are kept in the Server.

Configuring EntraPass Gateways

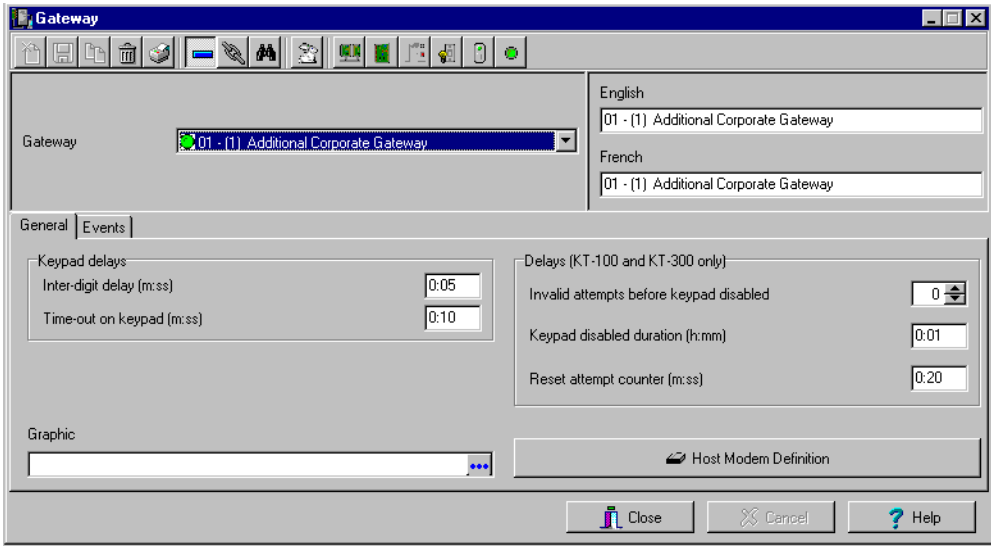
Entrapass Gateways convert the information received from a controller or a site and transmits the converted data to the Server; they also convert the information received from the Server and transmit it to controllers.

They may be installed on a dedicated computer, or it may be integrated with another EntraPass workstation.

Configuring a Corporate Gateway

To configure a Corporate Gateway:

1 From the **Devices** definition tab, select the **Gateway** icon.



2 From the **Gateway** drop-down list, select the Corporate gateway to be configured.

3 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 an operator.

4 Enter the **Time-out on keypad** delay time (m:ss). It is set in seconds. It represents the maximum time allowed for operators 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.*

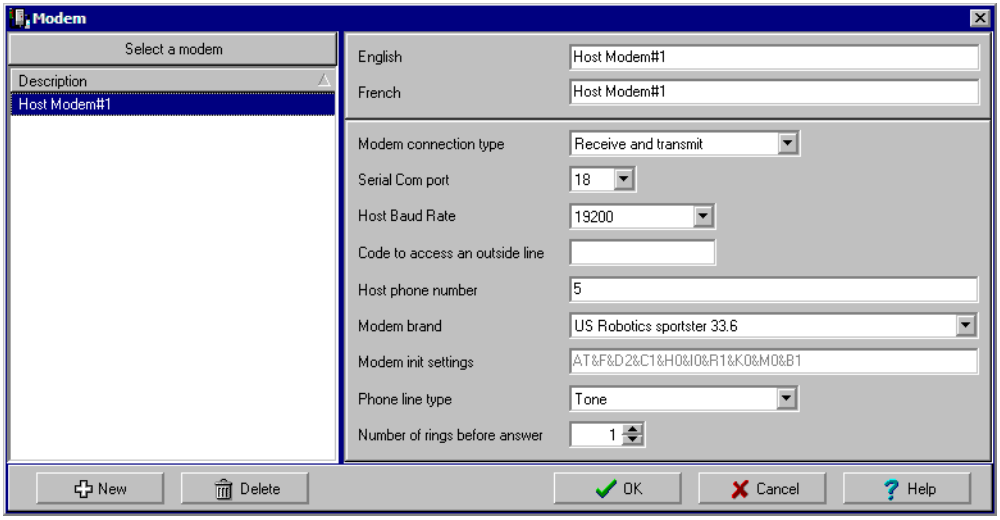
5 Select a Graphic to which the Gateway is assigned, if applicable.

6 Using the up and down controls, determine the number of **Invalid attempts before keypad is disabled**. Users have a maximum of 255 invalid attempts before the keypad is disabled.

7 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.

8 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.

9 If your Corporate Gateway connects to the first controller of a remote site via modem, click the **Modem definition** button to display the modem setup window.

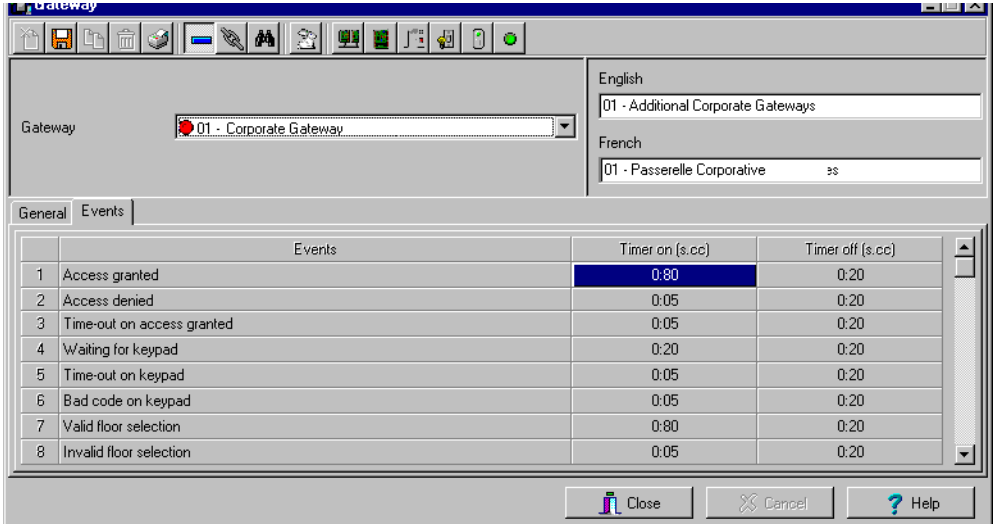


10 Click on the **New** button to add a modem to the modem selection list.

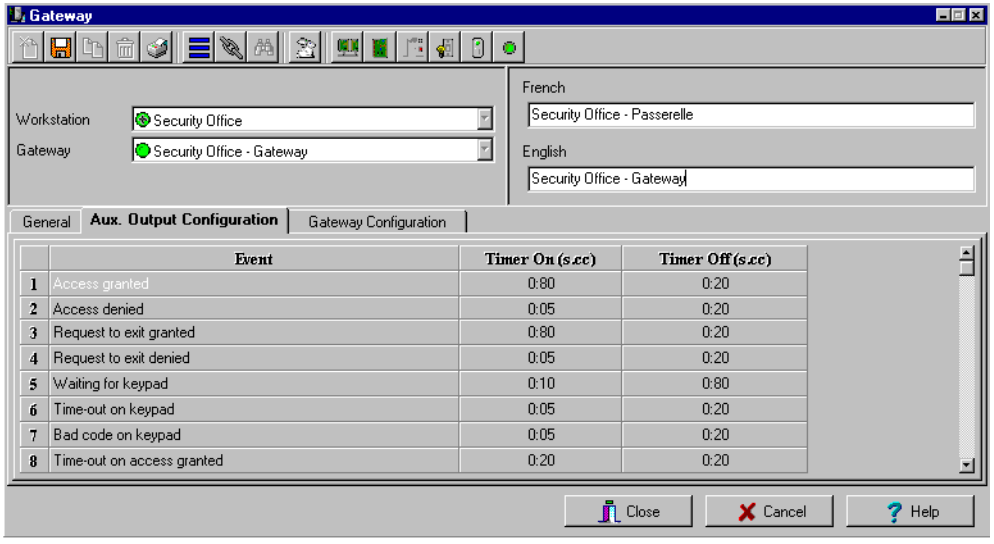
11 Configure the modem as per the example entries shown in the previous screen capture and click **OK** to return to the **Device** definition screen.

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.*

12 Select the **Events** tab to set the **Timer on** and **Timer off** for each event. A Corporate Gateway is configured to manage 30 events.



13 Select the **Auxiliary Output Configuration** tab to set the **Timer on** and **Timer off** for each event.



NOTE: *A Corporate Gateway-based system may support up to 40 Corporate Gateways. You may add up to 40 gateways to your access control system.*

Configuring Sites

A site is composed of controllers attached to the same serial port. The system can manage up to 256 sites (including remote sites) per Corporate Gateway .

Corporate Gateway sites are composed of KT-100, KT-200 or KT-300 controllers.

***NOTE:** It is suggested to use a site for each section of a building in order to provide easier system expansion and management.*

Corporate Site Definition

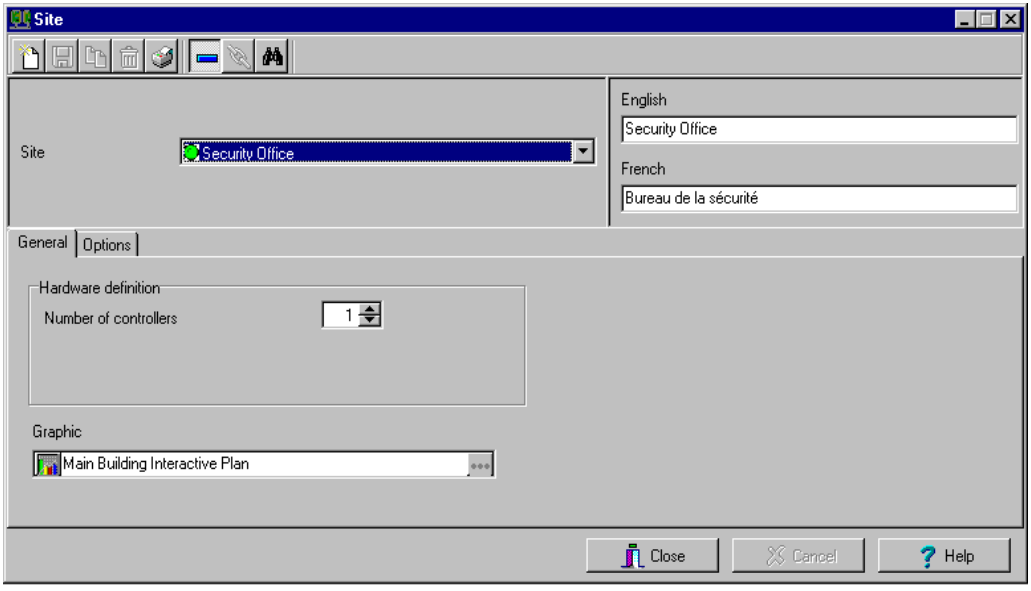
Under a Corporate gateway configuration, you have to specify:

- The gateway to which a site is connected,
- The number of controllers in the site,
- The connection type between the site and the gateway.

You may also define the controllers for that specific site by clicking the **Controllers** icon in the Site screen toolbar.

To define a site :

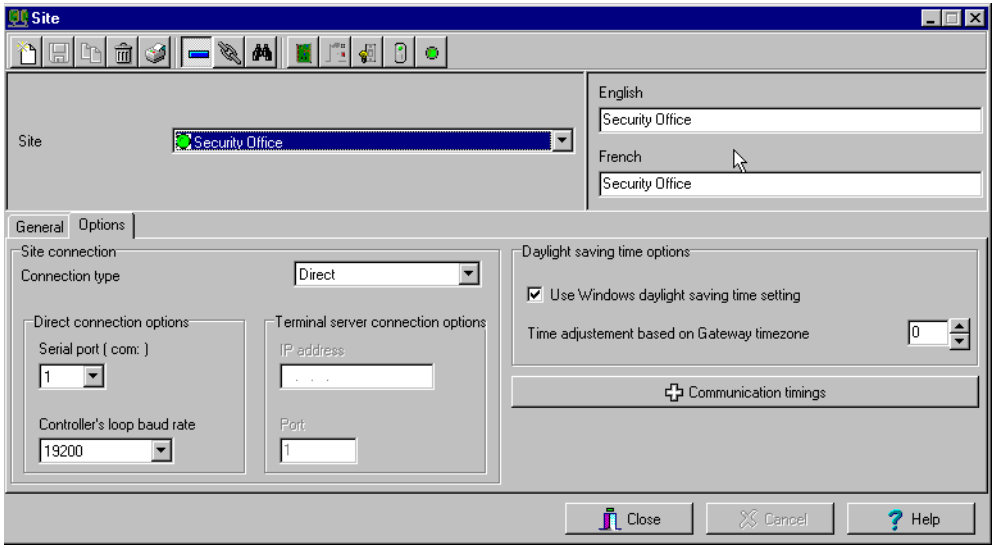
1 From the **Devices** window, click the **Site** icon.



2 If you are defining a new site, assign a name to the new site and click the **Save** icon. The bullet beside the site name turns green.

3 In the **Hardware Definition** section, specify the number of controllers in the site. There may be up to 32 controllers per site. If the number specified is greater than the maximum allowed, the system will use the existing value.

4 Select the **Options** tab to define the site connection options.



5 From the **Connection type** drop-down list, specify how the site communicates with the gateway computer. This may be through:

- A direct connection,
- A TCP/IP connection,
- A modem connection.

NOTE: *Selecting **Modem** adds three extra tabs to the Site configuration window. To configure these tabs, see "To define extra tabs on modem selection:" on page 71.*

6 Proceed as follows:

- Select **Direct**, if the site is connected to the gateway by an RS-232 serial port. Then you have to specify the **Serial port (com:)** as well as the **Controller site baud rate** (usually between 9600 and 19200). When the site communicates with the gateway using a direct connection, the **Terminal server connection options** section is disabled. You also have to select the **Daylight saving time options** (see the following step).
- Select **TCP/IP** if the site communicates with the gateway through a terminal server using a port number. Then you have to specify the terminal server IP address and **Port** number (maximum allowed is 99). 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.

NOTE: *You may install up to 32 terminal servers (per gateway).*

7 Check the **Use Windows daylight savings time setting** box to automatically switch to daylight saving time according to Windows standard settings. Leave unchecked if you want to do it manually.

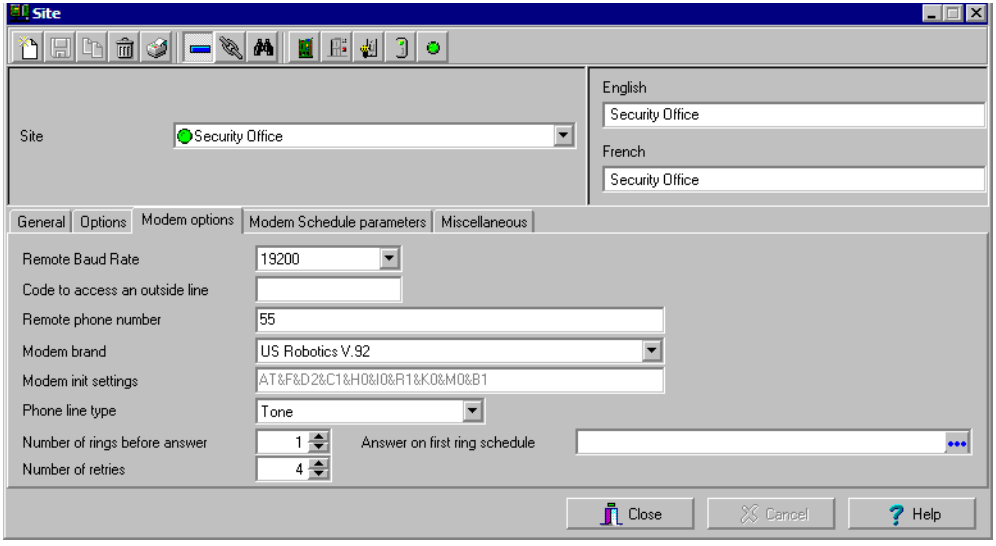
8 Type the time difference between gateway location and server location in the **Time adjustment based on Gateway timezone**. This setting will allow events to be displayed at local gateway time on workstations located in different timezones.

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 following screen capture shows the actual default settings. They must be preserved unless advised otherwise by Kantech Systems.

To define extra tabs on modem selection:

If you specified **Modem** from the **Connection type** drop-down list, you need to access two extra tabs.

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



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

3 Set the **Number of rings before answer** to set the number of rings before the modem picks up the call. This option is valid whenever ring schedules are not in effect.

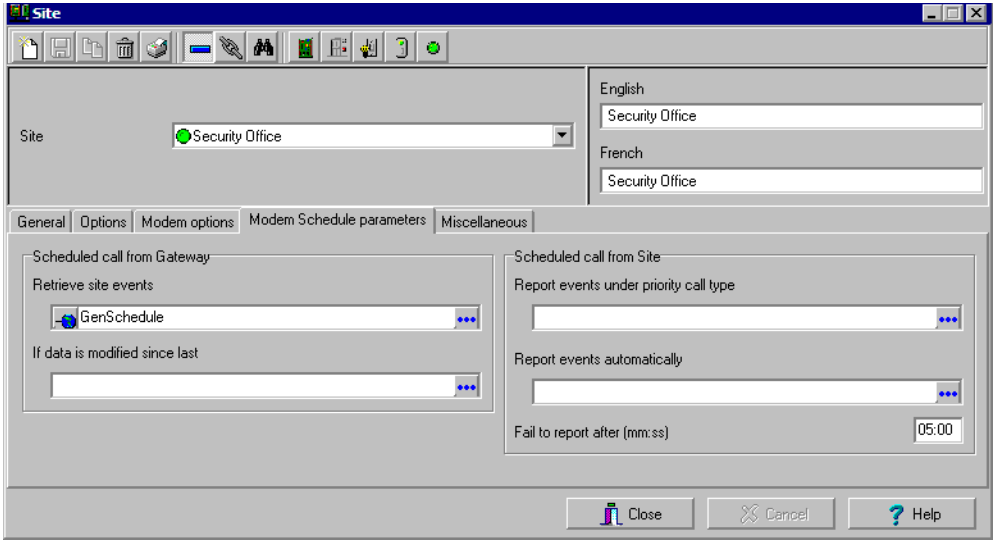
4 Set the **One ring schedule** option to configure the time interval during which site modem will be allowed to answer on one ring.

5 Set the **Number of retries**. This will set the number of calls the modem will attempt to make before giving up.

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

NOTE: *The **Modem settings** and **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.*

6 Once all modem options have been set, click on the **Schedule parameters** tab. This will allow you to set time intervals during which the gateway connects to remote sites (through modem calls) in order to perform specific tasks.

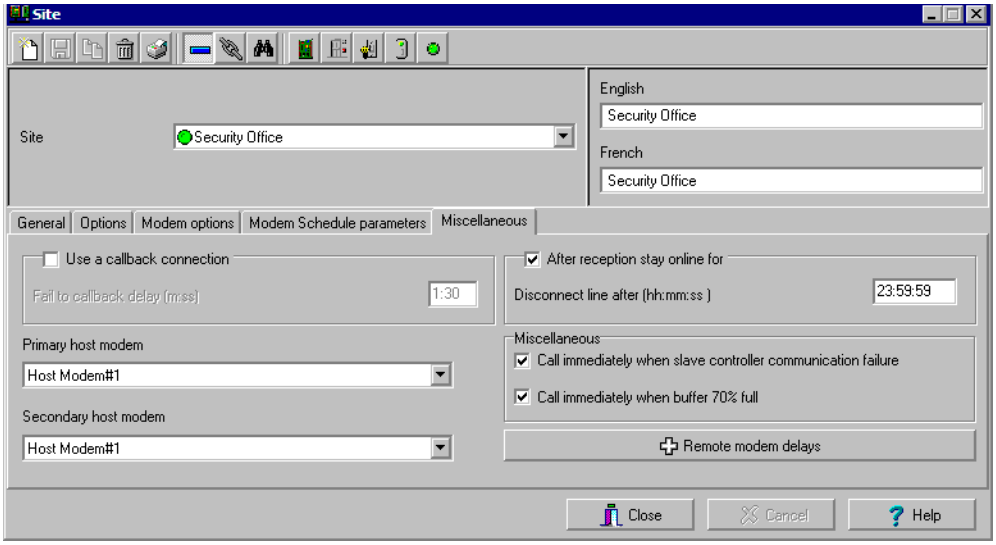


7 Click on the **Retrieve site events** browse button to bring up the schedule selection window. Select the schedule that best corresponds to the time requirements set out for this task. For more information on defining schedules, see Chapter 7 ‘Defining Schedules’ on page 140

8 Repeat this step for **If data is modified since last**, **Report events under priority call type** and **Report events automatically**.

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

9 Click on the **Miscellaneous** tab to set how modems handle site incoming and outgoing calls.



10 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 standby-for-acknowledgement time in the **Wait for security callback** factory set to 01:minute:30 sec.

11 Select primary modem in the **Primary host modem** 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.

12 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 00.03.09.

13 Check the **Call immediately upon 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).

14 Check the **Report 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 authorized by Kantech.*

Configuring Controllers

The controller definition tells the system how a controller is being used and what devices are associated with it: (door(s), 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 screen) or by using Express Setup (identified by the icon).

Corporate Gateways use 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:

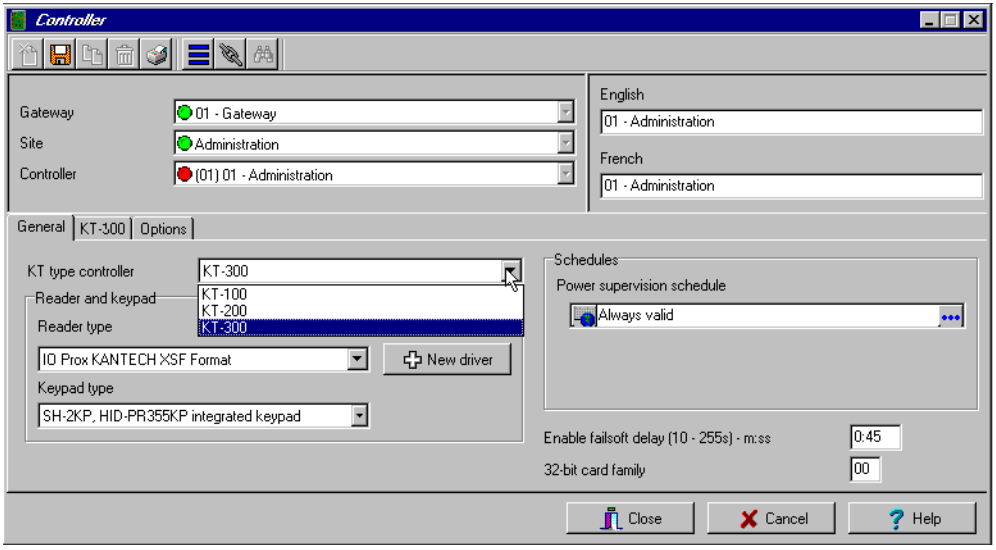
Type	Doors	Relays	Input Zones	Auxiliary Outputs
KT-100	1	4	4	2
KT-200	2	2	16	4
KT-300	2	2	8	4

NOTE: *KT-200 are used in both Global and Corporate Gateway configurations. Corporate Gateways support all Kantech controllers (KT-100, KT-200 and KT-300).*

Defining General Parameters for KT Controllers

1. From the **Controller** definition screen, 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 From the **Controller KT type** drop-down list, select the controller type.



5 Select the controller type and assign a name to it in the language section (English and French), then Click the **Save** icon. Once you save, the **Controller type** drop-down list is disabled.

6 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).

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

NOTE: *The **New driver** button 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.*

8 Select the applicable **Schedules** for the new controller:

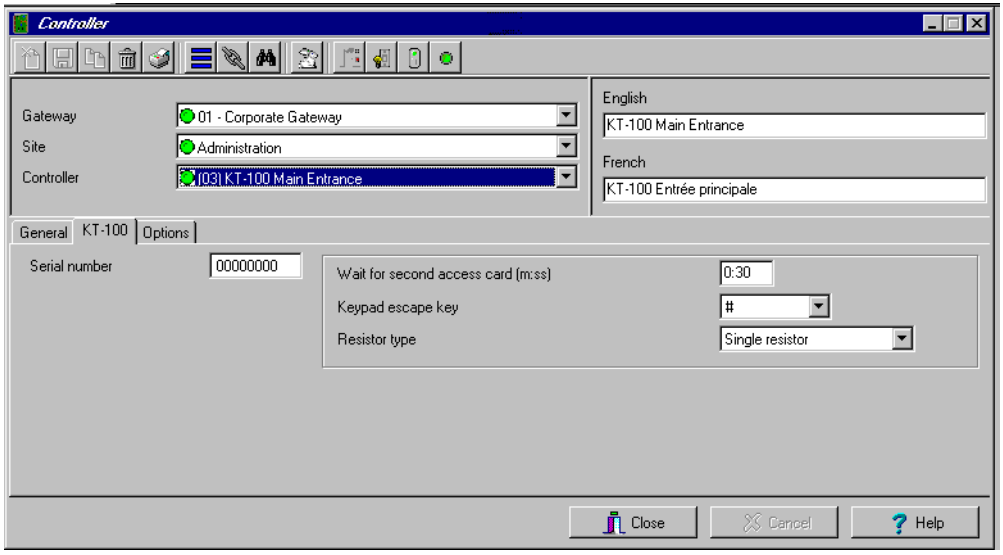
- When a KT-100 or KT-300 is selected: only the **Power supervision schedule** list is displayed.
- For KT-200, the **Power supervision schedule** and the **Tamper switch supervision schedule** lists are available.

9 Click the **Save** icon.

Configuring a KT-100 Controller

Once the general parameters are defined, the controller type tab is displayed on screen. A **KT-100** or **KT200** or **KT-300** tab appears beside the **General** tab.

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



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. 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 **Resistor type** drop-down list, select the resistor type used with your system. By default, this choice is set to **Single resistor**.

NOTE: *For details on defining options for KT-100 controllers, see "Defining Controller Options" on page 86.*

Configuring a KT- 200 Controller

KT-200 door controller provides 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.

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.

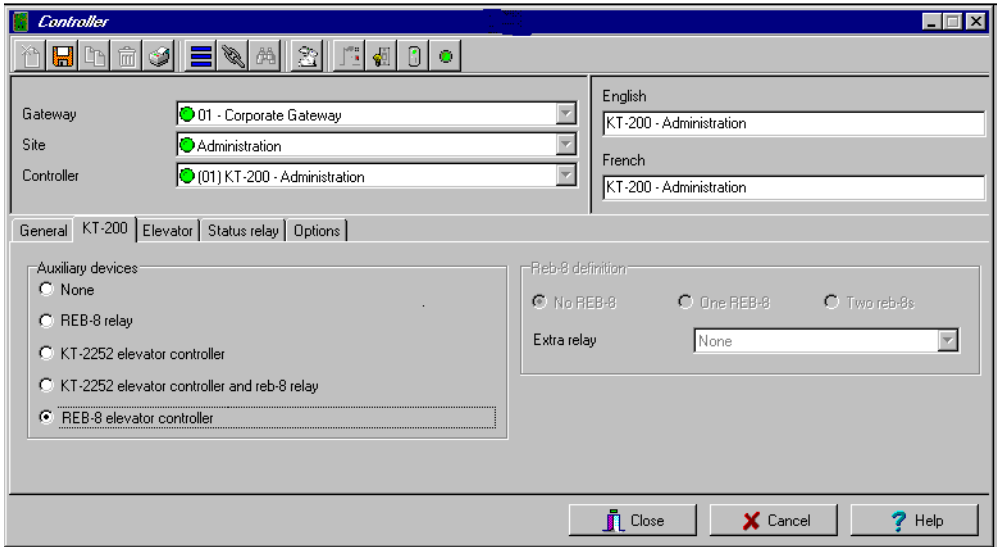
Defining KT-200 Expansion Devices

KT-2252 elevator controllers 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.

To define KT-200 auxiliary devices:

1 From the **Controller** definition screen, 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.

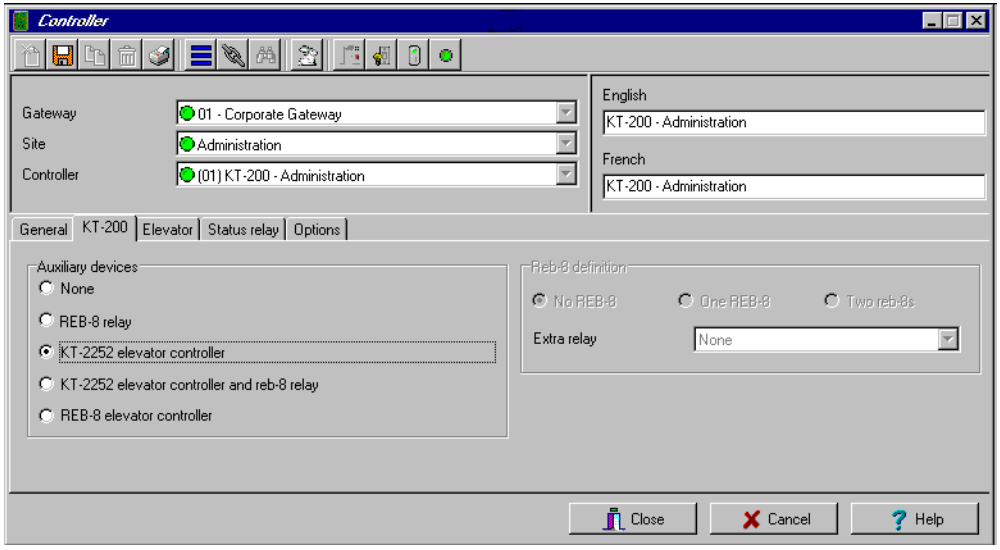
NOTE: *When an elevator controller option is checked, an Elevator tab appears beside the KT-200 tab.*

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

To program KT-2252 elevator controllers:

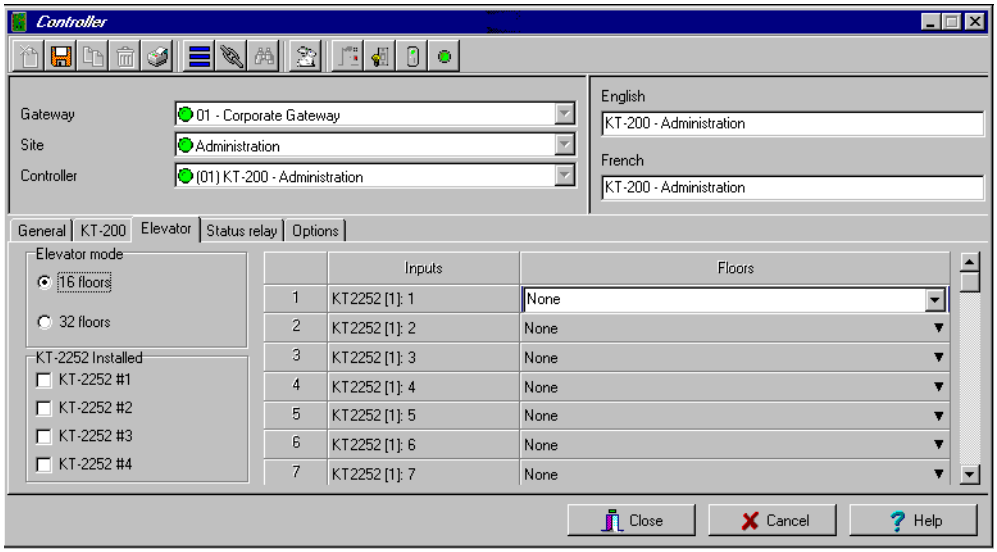
The **Elevator** tab allows you to specify which auxiliary devices are used with the KT-200 for elevator control and how they are used. Depending on the expansion board installed and on the option checked, the Elevator screen displays the **REB-8 Installed** or **KT-2252 Installed** section.

1 From the **Controller** definition screen, 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 (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

Number of cabs	Number of floors	Number of KT-2252
2	16	1
2	32	2
2	64	4

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

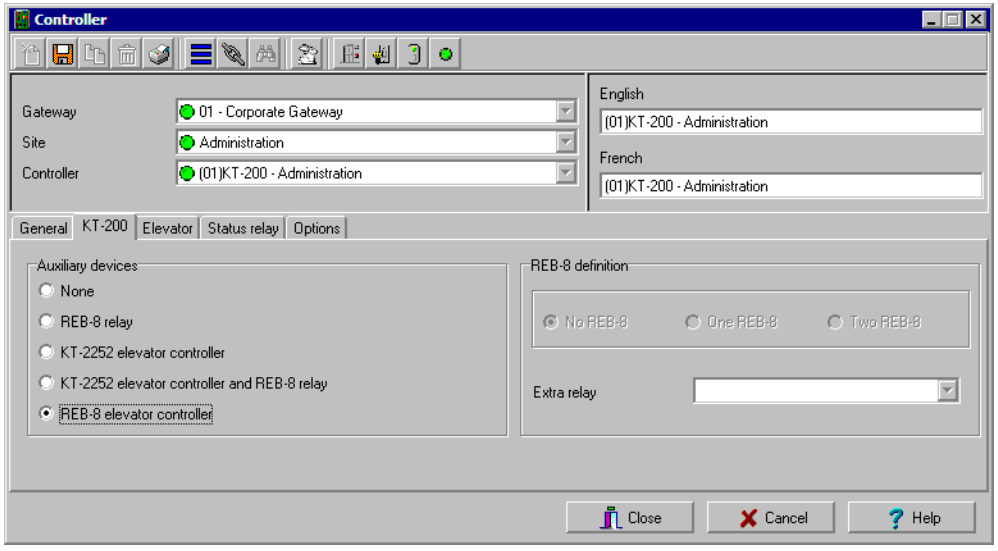
NOTE: *The Inputs column refers to the KT-2252 terminals. When floors have been defined (Floors menu), the Floors column contains the floors associated with the inputs.*

To program REB-8 elevator controllers:

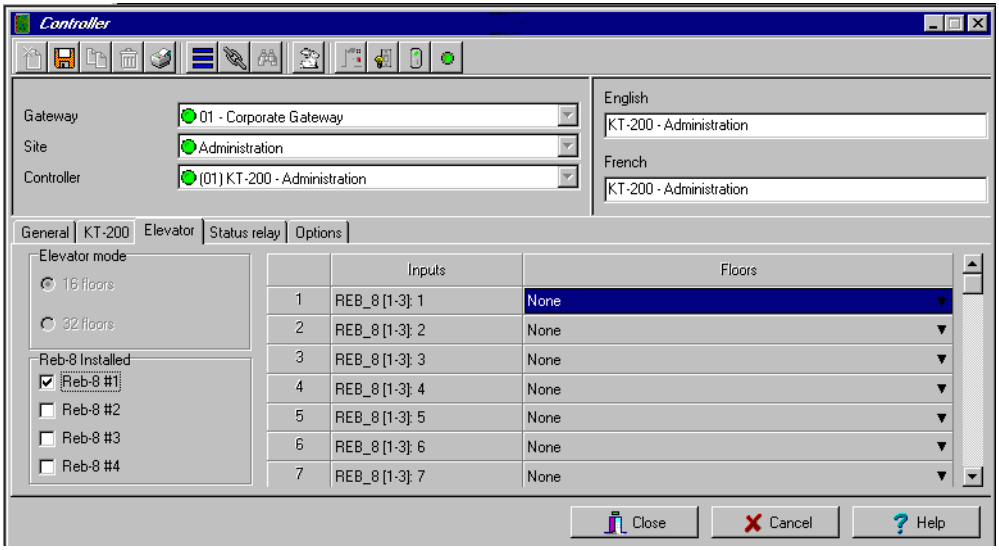
REB-8 relay expansion boards may be used as a cost-efficient alternative for elevator control. With an REB-8 expansion board added to a KT-200, the software may control up to two elevator cabs per controller.

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

1 In the **KT-200** definition screen, 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.



3 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

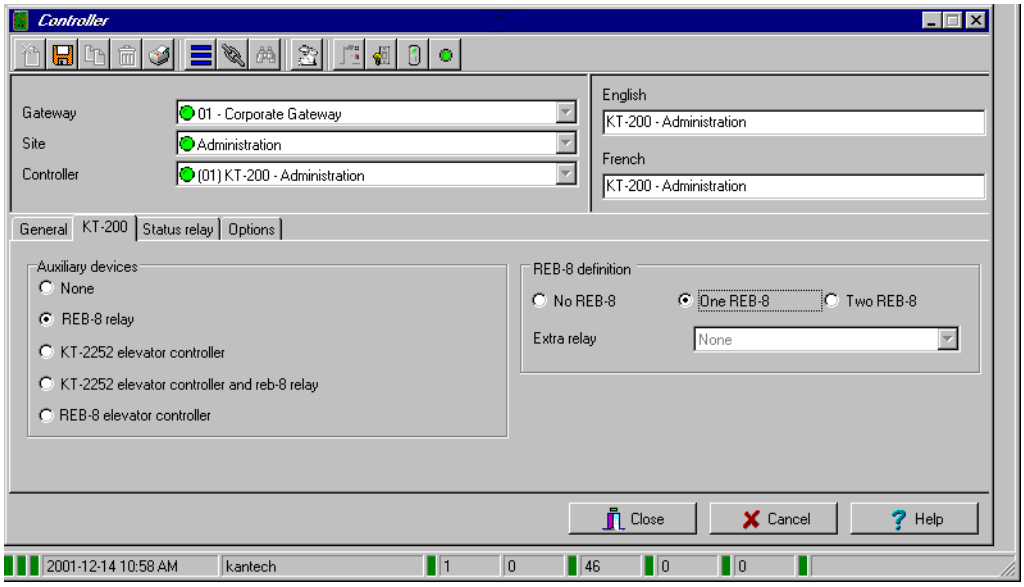
NOTE: *The Inputs column refers to the REB-8 terminals. When floors have been defined (Floors menu), the Floors column contains the floors that are associated with the inputs.*

4 In the Floors column, select the floors associated with REB-8 controller terminals. For details on floor definition and door group definition, see “Configuring Doors” on page 88.

To define 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.

1 In the KT-200 screen, select the **REB-8 relay** option if REB-8 are used as relays.



2 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.

NOTE: *For details on how to configure other options for KT-200 controllers, see* *"Defining Controller Options" on page 86.*

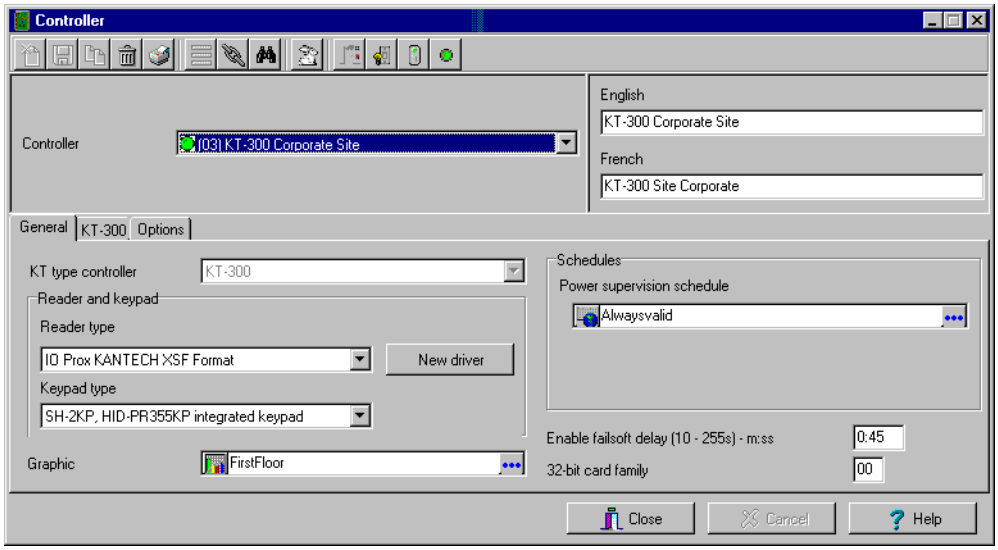
Configuring a KT-300 Controller The KT-300 constantly supervises battery condition and reports "Low battery/No battery condition" status to the system. It also supervises locking devices for short and open circuits to detect lock failures.

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. Four expansion modules can be connected to KT-300:

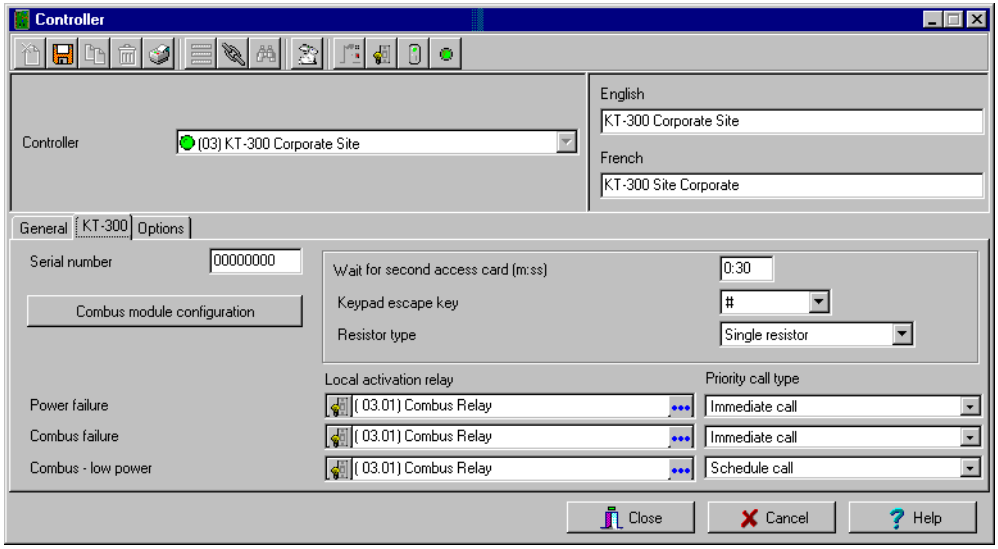
- KT-PC4108 (8-zone input expansion module). This module has a tamper contact input.
- KT-PC4204 (4-relay/power supply expansion module). It has a tamper contact input and also includes a built-in 12VDC, 1A power supply for field devices.
- KT-PC4216 (16-zone output expansion module). It can be used for elevator control, although additional hardware may be required.

- KT-LCD4501 (Kantech 32-character liquid crystal display). The LCD is *green* (normal status), *red* (power failure) and ***yellow*** (trouble).

1 From the Site menu, click the **Controller** icon.



2 In the **Controller** screen, select the **KT-300** tab.



3 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.

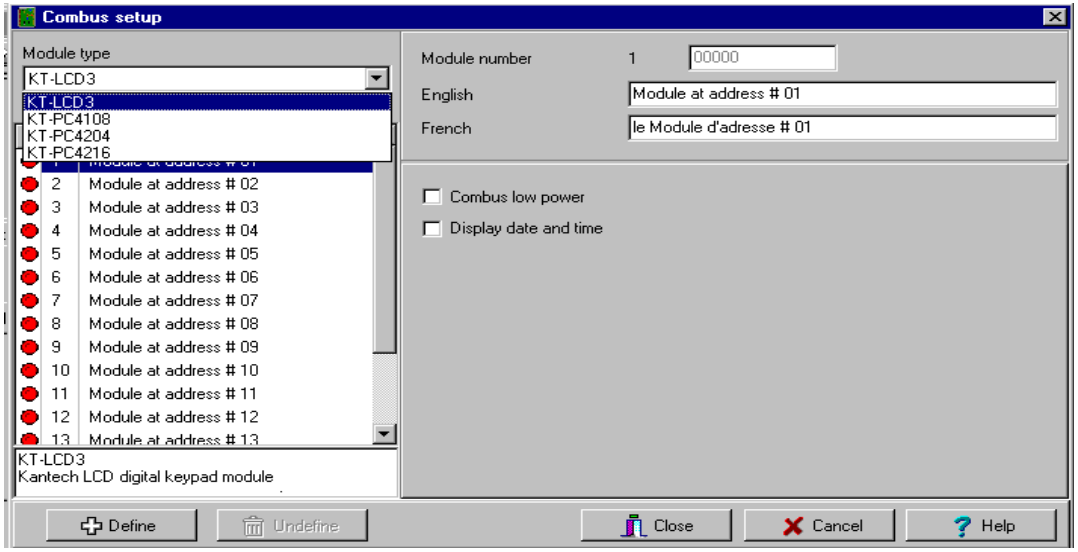
4 Enter the **Wait for second access card** delay. The maximum time allowed is two minutes and seven seconds. If the value entered is greater than the maximum allowed, the system will use the existing value. This feature is useful when access to a place is controlled by two cards.

5 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.

6 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:

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 screen). 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 screen).

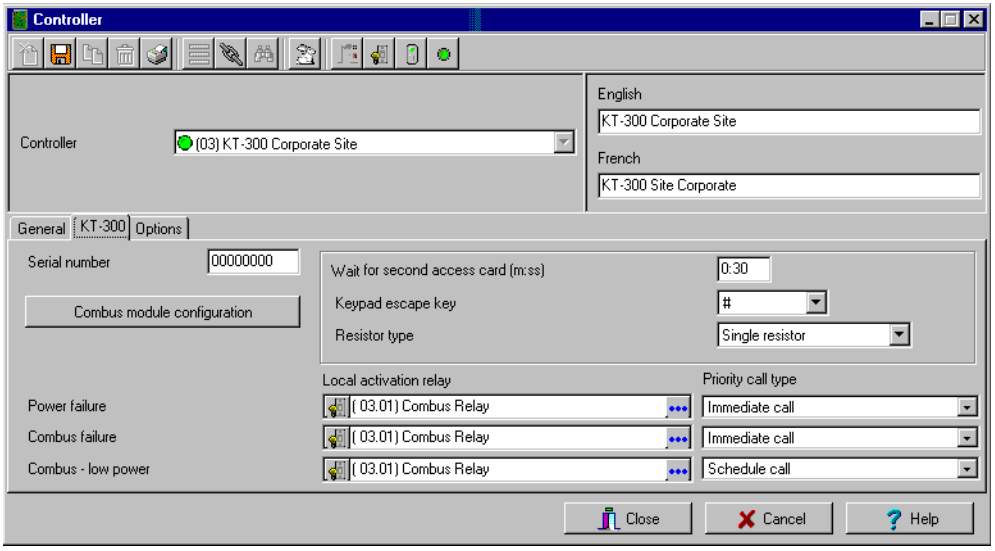
NOTE: *Usage options of a module vary according to the selected Combus module. For example, installing the KT-LCD3 and checking the options* ***Combus low power*** *and* ***Display date and time*** *will allow the KT-300 to report Combus low power conditions and to display the date and time.*

The following table summarizes the options associated with each module:

Combus type	Options	Additional options
KT-LCD3	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 When you have finished configuring the Combus module, click the **Close** button to go back to the KT-300 configuration screen.

7 Click the **Close** button to return to the KT-300 configuration screen.



8 Select the status and alarm relays for **Power failure**, **Combus failure** and **Combus low power**.If you want to assign a specific relay, you may click pop-up window icon (•••) and select a specific relay or group of relays.

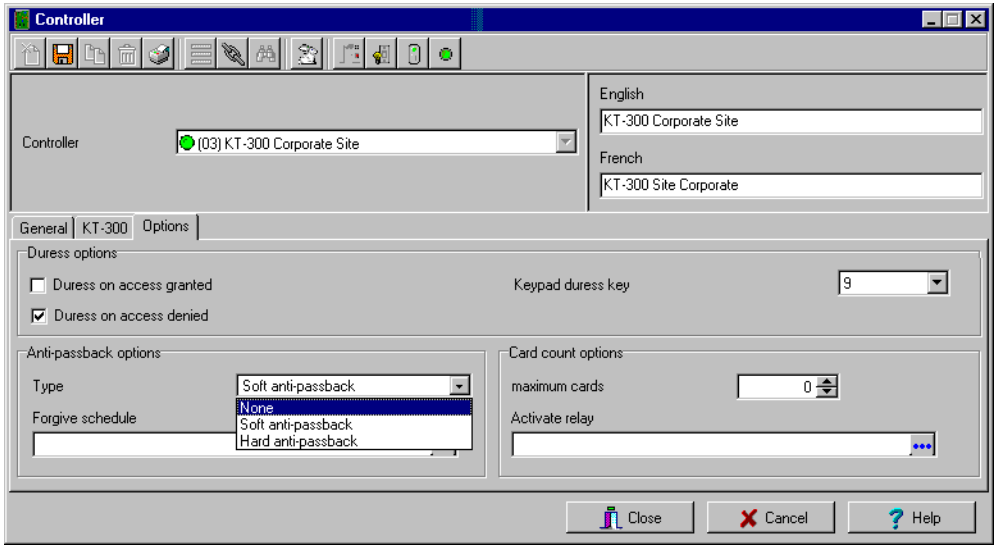
9 Under **Priority call type**, assign the call type option that best suits failure event reporting.

NOTE: *To access the Priority call type feature, the site connection type must be set to* ***Modem****. For more information, see "To define a site :" on page 69.*

Defining Controller Options

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

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 and 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 set count.*



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 button to set a schedule for resetting the anti-passback option on all other cards.
6 In the **Card count** option, use the up or down controls to set the maximum card count. The maximum allowed is 65535. 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.
7 You may configure the system to activate a relay when the maximum count is reached. Click the button to select the relay or relay group that will be activated when the number is reached.

Configuring Doors

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.

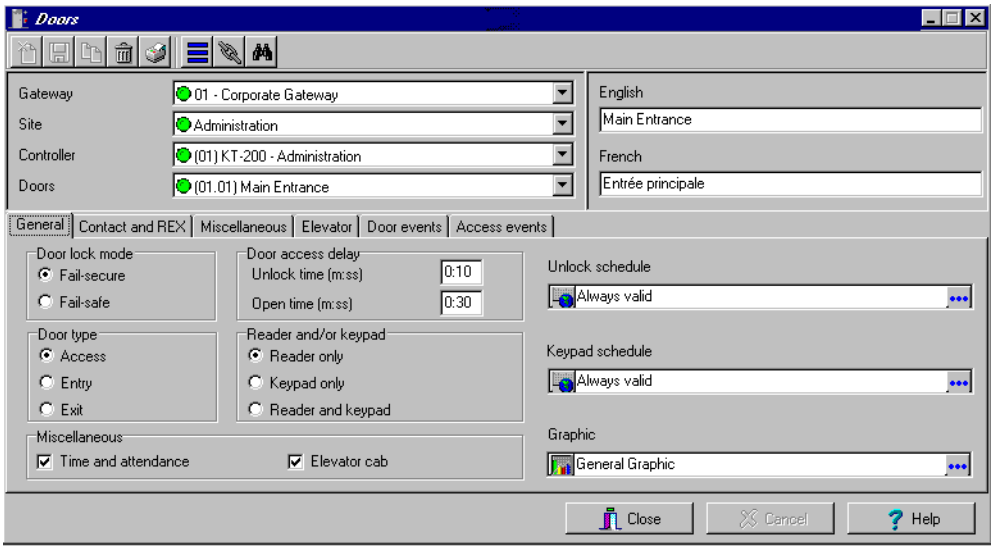
A door can be defined as an elevator door, a Time & Attendance door, an entry or exit door for anti-passback, or an access door.

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 main window, select the **Doors** icon.



2 In the **Doors** screen, select the appropriate Gateway to view the controller sites for a specific gateway, then 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 (electric 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 107.
- **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** screen, **Contact and REX** tab) to sound the door piezo when half of this delay has expired. It will continue to sound until the door is closed.

7 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. 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).
- **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.

8 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.

9 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.

NOTE: *For more information on how to program elevator control using REB-8 relays, see "Defining KT-200 Expansion Devices" on page 77.*

10 Specify the Unlock schedule: when the unlock schedule becomes valid, the door remains unlocked according to the specified time frames in the schedule. However, an alarm partition trying to arm can override this unlocking schedule if this door is programmed to stay "locked when armed".

NOTE: *For elevator control: using the unlock schedule will override the "Unlock Schedules #1 & #2". All floors assigned to this door will be available for selection. You can also use the "Unlock Schedules #1 & #2" to unlock specific floor groups during a certain time.*

11 Define the **Keypad schedule** during which users with the **Wait for keypad** option will need 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).

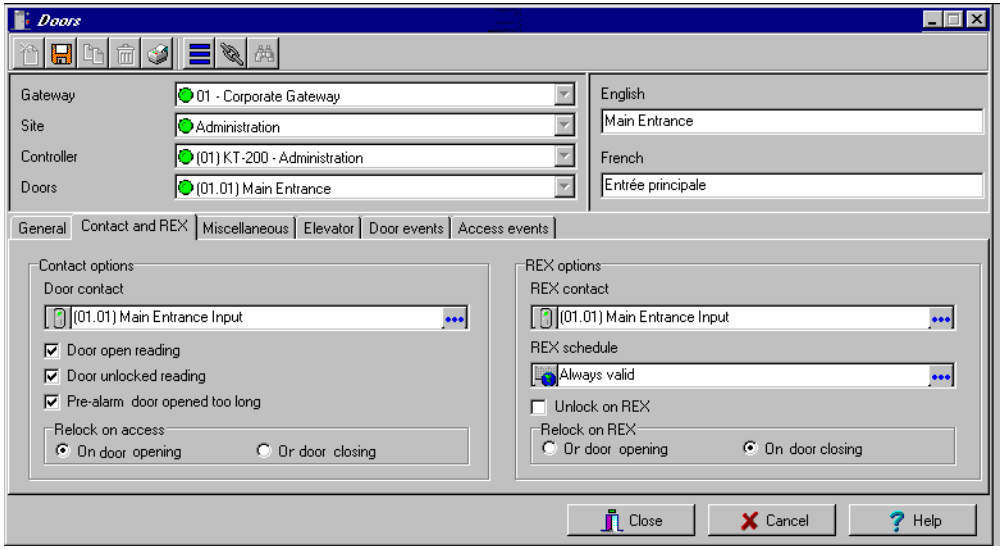
12 Select the graphic associated with the door, if applicable.

Defining Contact & REX 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.

To define the door contact and REX settings:

1 In the **Doors** screen, select the **Contact and REX** 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 permitted" is generated. Otherwise, the event "Access - Second entrance" 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 - Second entrance" 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 the door on a valid access, or relock the door when it closes.

5 In the **REX options** section, assign the REX contact: the input to which a “request to exit” detector can be connected. This input can only be one of the 16 inputs on the KT-200 controller operating the door.

6 Determine 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.

7 Select the **Unlock on REX** option to unlock the door when a valid request to exit is permitted by the controller. This option is usually used when a magnetic lock is installed and when the door is monitored with a door contact and has a reader on the other side. The system will permit the exit and show the “request to exit permitted” event rather than “door forced open” event.

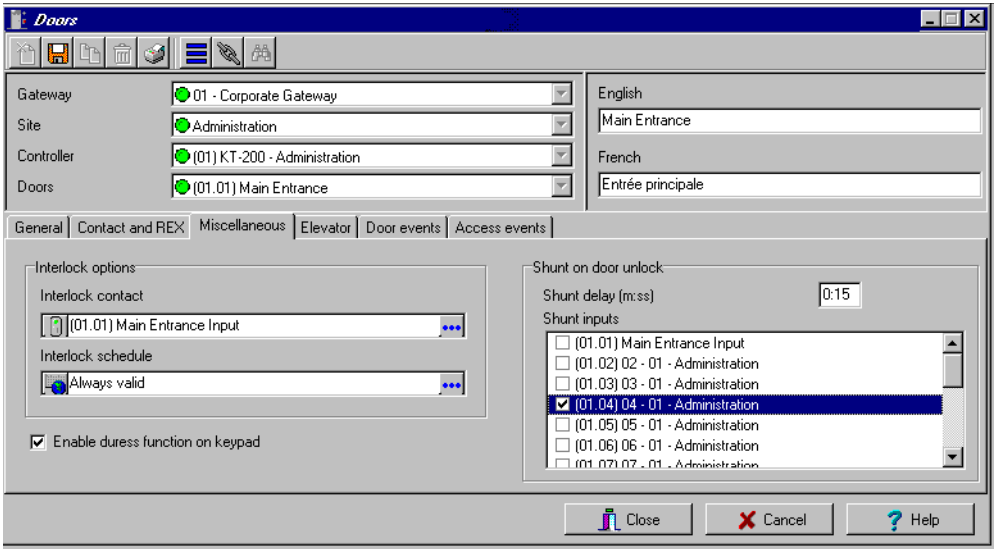
8 Check the appropriate Relock on Rex options: **Relock on door opening**, if you want the door device to re-lock following a valid access; or **Re-lock on door closing**, if you want the door device to re-lock when it closes.

Defining 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 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.

To define interlock options between two doors:

1 In the **Doors** screen, 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 first 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 **Enable duress function on keypad** option, if desired. (Corporate door only)

7 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 recommended to shunt a door contact since the system will automatically shunt it.

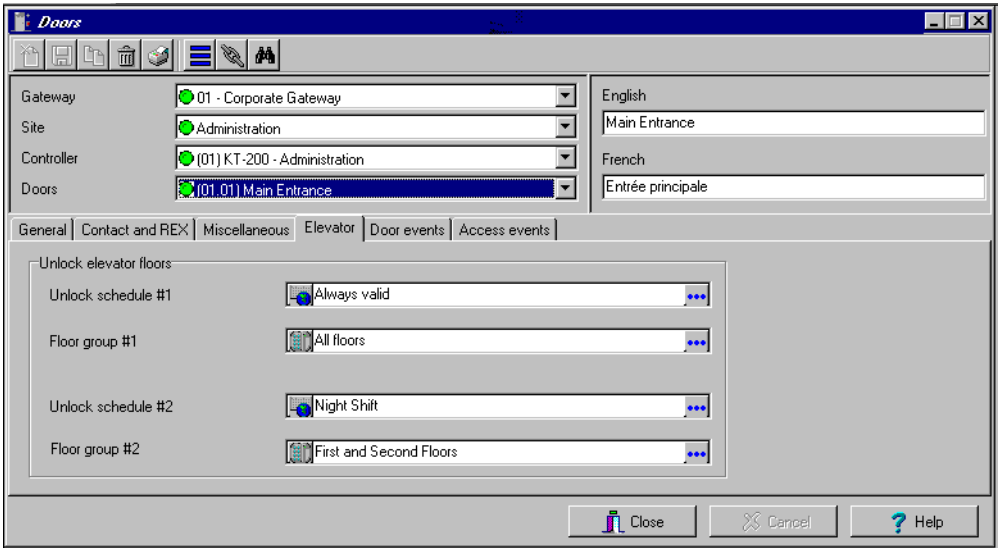
8 In the **Shunt inputs** scrolling pane, select inputs that will not be monitored when the door unlocks. Selected inputs will remain unmonitored for the delay defined in the **Shunt delay** field.

Defining Elevator Doors

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

To define settings for an elevator door:

1 From the **Doors** definition screen, 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 6:00 am to 9:00 am and the second schedule (Unlock Schedule #2) is valid from 7:00 am to 9:00 am, 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 8:00 am to 5:00 pm and the second schedule is valid from 4:00 pm to 9:00 pm, the gap (between 4:00 am and 5:00 pm) 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.*

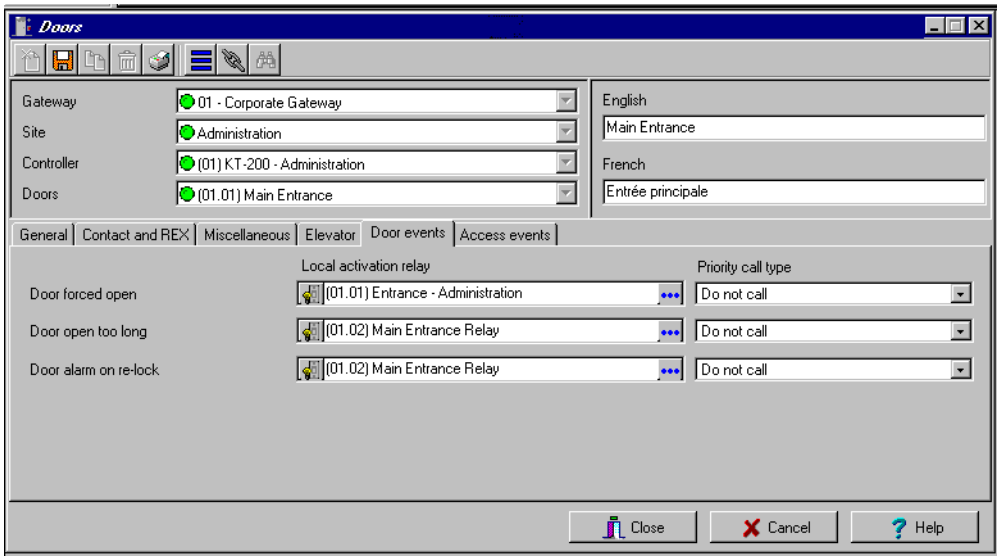
For more information on how to program elevator control using REB-8 relays, see "Defining KT-200 Expansion Devices" on page 77.

Configuring Door Events

This section relates to the definition of Corporate doors only.

To define door events:

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

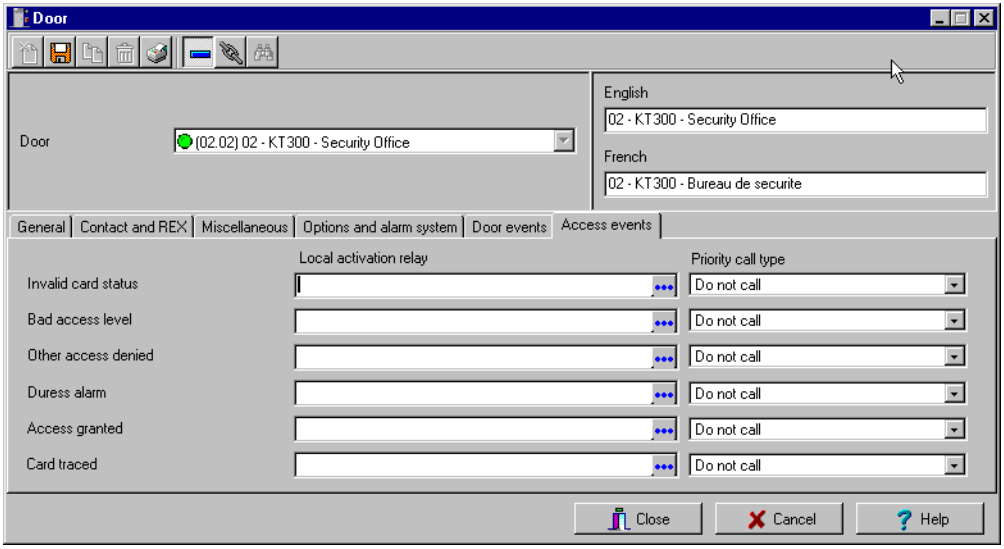


2 Select the relay that will be activated locally, on such events as: **Door forced open**, **Door open too long** or **Door alarm on relock**.

3 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**. *For more information, see "To define a site :" on page 69.*

4 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.



5 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**.

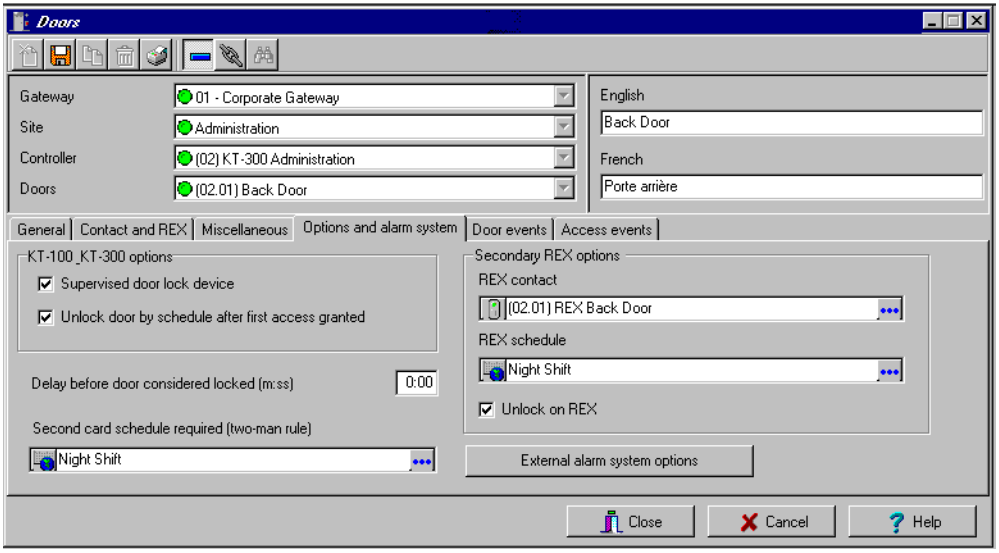
6 Under **Priority call type**, assign the call type option that best suits event reporting.

NOTE: *To access the Priority call type feature, the site connection type must be set to* **Modem**. *For more information, see "To define a site :" on page 69.*

To define options for a KT-100 and KT-300:

NOTE: *The following options are available with KT-100 or KT-300 controllers only.*

1 Select the **Options and alarm system** tab.



2 Check the **Unlock door by schedule after first access granted** option to unlock the door automatically when a first card is read.

3 If a second card read is required, select a schedule from the **Second card schedule required (two-man rule)** list.

4 You may define **Secondary REX** options: select a secondary REX contact as well as a secondary REX schedule from the pop-up menus.

5 Check the **Unlock on REX** option. The door will automatically be unlocked when a valid REX is permitted by the controller. This option is usually used when an electromagnetic lock is installed and when the door is monitored with a door contact and has a reader on the other side.

NOTE: *When KT-100 and KT-300 are installed, the system offers the possibility to interface with an external alarm system.*

Configuring External Alarm System Options

KT-100 and KT-300 offer the ability to interface with any external alarm system. When you add these Kantech controllers to an existing alarm system, cardholders can arm/disarm an existing system, simply by presenting a valid card on an entry/exit door. Adding a keypad will increase the system security since cardholders will be required to enter a PIN in addition to presenting a card.

There are five options to arm/disarm or postpone an external alarm system:

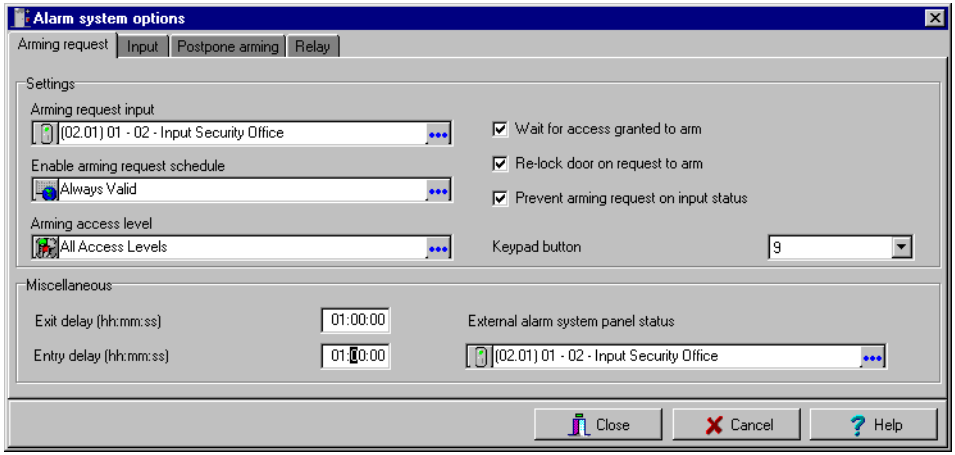
- On a valid card read on an arming reader,
- On a valid arming code entered on a keypad,

- By pressing a button on a keypad,
- By pressing a button connected to an input,
- By an automatic arming/disarming schedule.

There may be a combination of the three options. For example, an alarm system will be disarmed with a correct access code during a valid predefined schedule and after a valid card read.

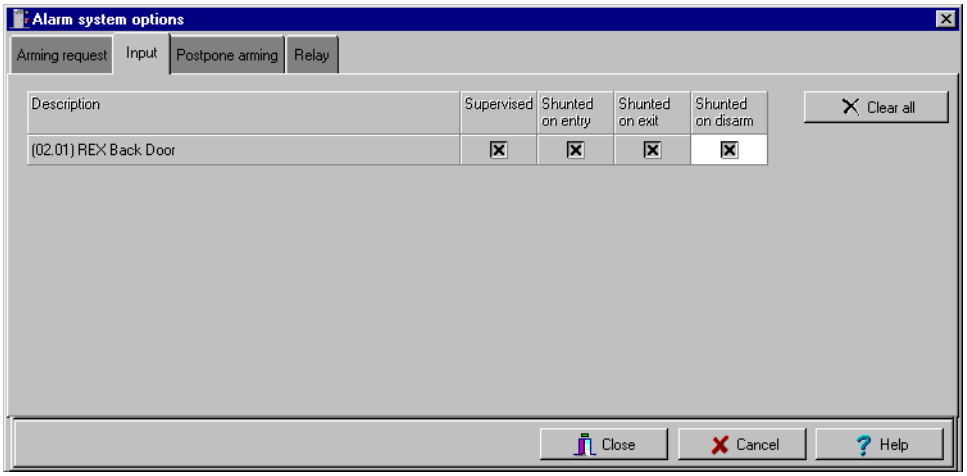
To configure external alarm system options:

1. Select the **External alarm system options** button (**Door** > **Options and alarm system** tab). The Options and alarm system tab appears when a KT-100 or KT-300 is selected.



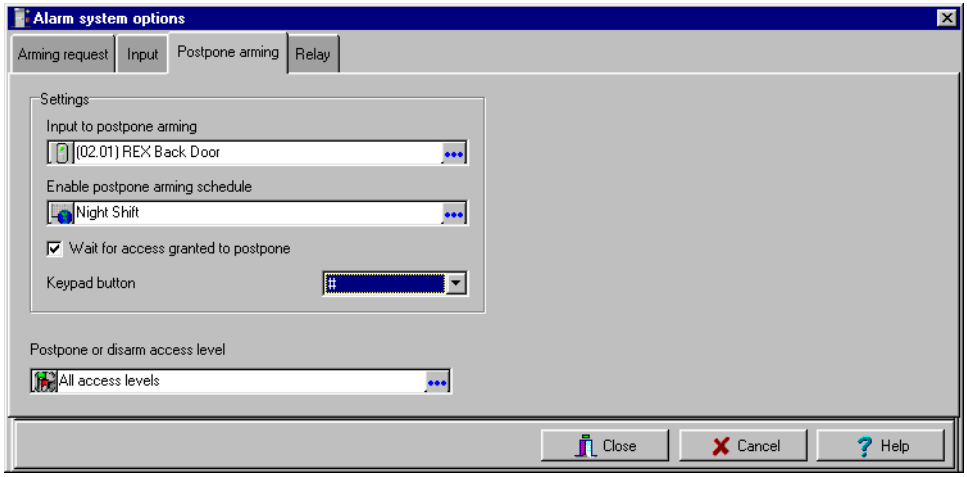
2. In the Arming request screen, select the **Arming request input**. This is the input that is activated on an external alarm arming request. Once you have selected an arming request input, you have to set the schedule during which the request will be valid.
3. If applicable, select an arming access level from the list. The **Group** option allows you to select all access levels. Choose **Single** if you want to select a specific level. If the level you want does not appear in the list, you may create a specific level to arm the external alarm system (**Users** > **Access level** definition).
4. Use the right-click menu to create a new access level.
5. To increase the security of your alarm system, check the **Wait for access granted to arm** option. This will oblige the user to present a valid access card before pressing the selected **Keypad button**. You may also check the **Lock door when system armed** option for increased security.
6. Specify the **Exit delay** and **Entry delay (h:mm:ss)**. The **Entry delay** is the time during which the alarm system is bypassed after an access granted event. The **Exit delay** is the period before which the system is armed. The maximum values are 9:06:07 for both the exit and entry delays. Usually the entry delay is shorter than the exit delay.
7. Select the input that will indicate the status of the external alarm panel. When the selected input status is “normal”, this indicates that the external alarm panel is armed.

8 Select the **Input** tab to define input devices that will be supervised or shunted (no supervision) when the alarm system is armed. The input description column contains all the inputs that are defined in the system.



9 Check the **Supervised** column for inputs that you want to be supervised by the external alarm system; check the appropriate column for input for which you want to suspend supervision (on entry, on exit, or when the alarm system is disarmed).

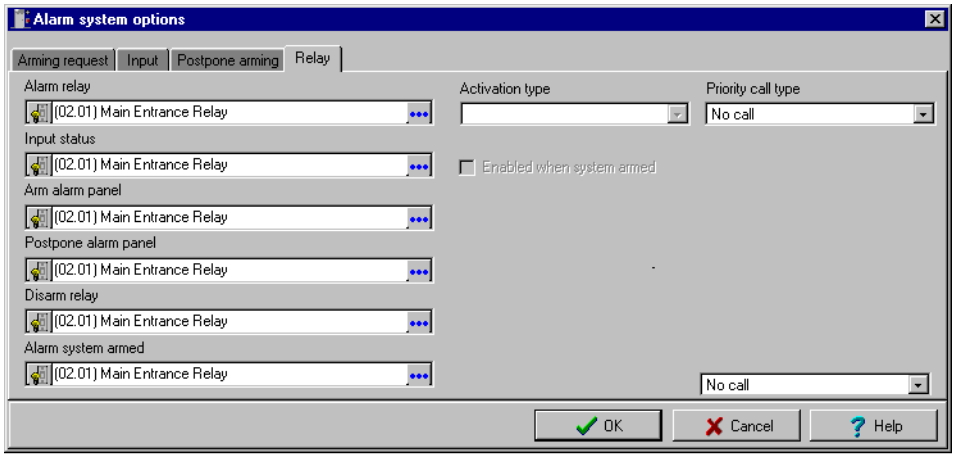
10 Select the **Postpone arming** tab to select the input that will be enabled to postpone arming. Select also the applicable schedule from the **Enable postpone arming schedule**.



11 You may check the **Wait for access granted to postpone** option. If this option is checked, the alarm system will be postponed only after a valid card read and the cardholder will then press the selected keypad button to postpone the external alarm system.

12 Select the **Postpone or disarm access level** from the list.

13 Select the **Relay** tab to define a relay or a group of relays and input status for the external alarm relays.



NOTE: *When you select an Alarm relay, you may specify its activation type. It may be activated permanently or temporarily.*

14 Under **Priority call type**, assign the call type option that best suits relay activation reporting.

NOTE: *To access the Priority call type feature, the site connection type must be set to* ***Modem****. For more information, see “To define a site :” on page 69.*

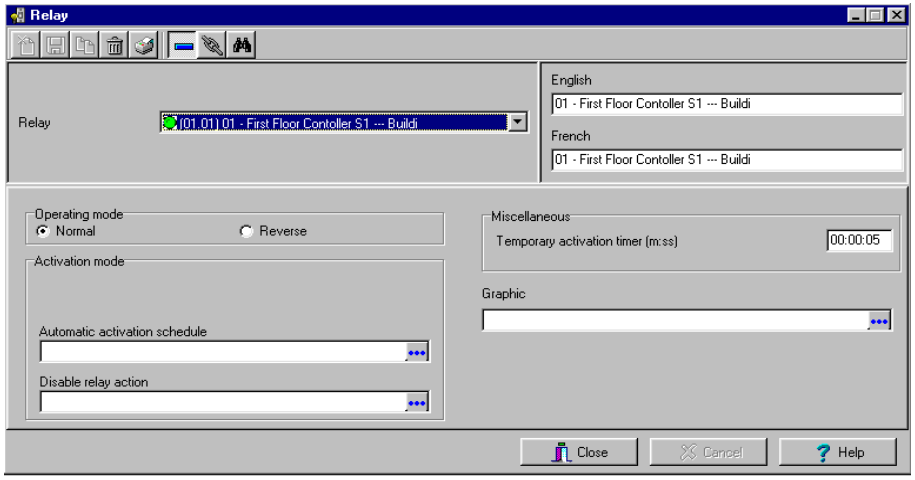
Configuring Relays

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, 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 **Gateway**, the **Site** and the **Controller** from the displayed drop-down lists.

3 In the **Relay** drop-down list, select the relay for which you want to define settings.

4 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.

5 Specify the **Automatic activation schedule**: when this schedule is valid, the relay will be triggered (activated or deactivated) according to the specified activation mode.

6 Specify the **Disable relay action**: when this schedule is valid, the relay will be deactivated (or activated) according to the predefined operating mode. (Corporate Gateway only)

7 Set the **Temporary activation timer** to indicate the delay during which the relay will be temporarily triggered following a temporary activation, whether it is manually, by an event or by any other system function.

NOTE: *When the timer is set to zero, the relay will follow the event or device condition even if it is programmed to be temporary activated. Maximum time allowed: 255 seconds (4 minutes 15 seconds).*

NOTE: *Only a manual operation can deactivate the relay.*

8 Select a graphic associated with the relay, if applicable.

Configuring Inputs

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.

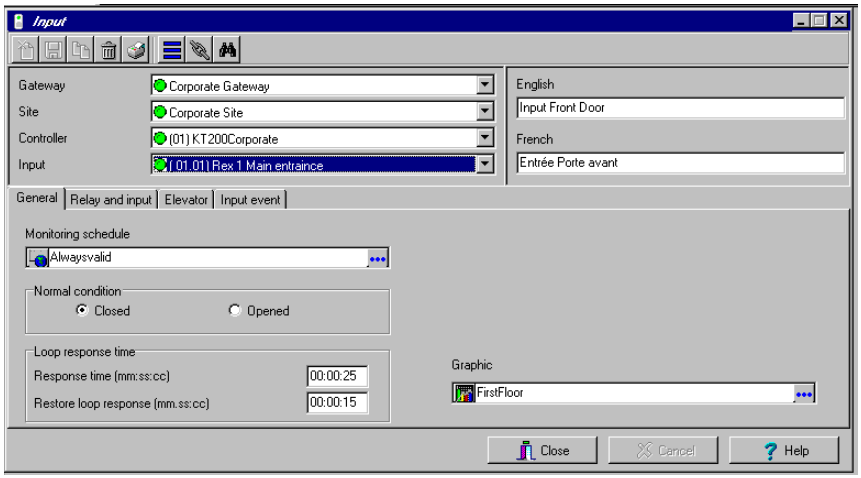
For KT-100 Controllers. Input 1 is reserved for door contact while input 2 is reserved for a request to exit device.

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 input under a Corporate Gateway:

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

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



2 Select a specific gateway (in 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 **Site 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.

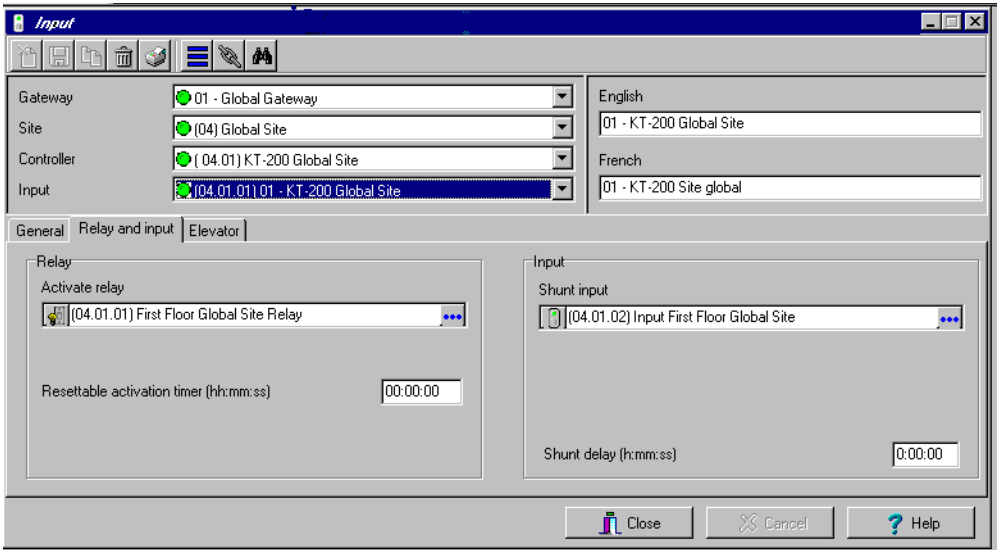
- **Response Time**—The delay before the system generates the input and alarm event.
- **Restore Site Response**—The delay before the system generates the input restore events

NOTE: *Specifying the site response time reduces bouncing when the contact changes state, and helps to generate only one event for each transition when this time is longer than the bouncing time. For example, a 100 delay requires that a condition remains stable for at least one second before it is reported. The range varies from 10 to 255 hundredths of a second.*

7 Select a graphic in which the input has been assigned.

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* ***Reset delay for shunt temporary*** *option has to be selected in the definition of the input that will reset the delay. For example, if Input 1 will temporary shunt Input 2, the* ***Reset Delay for shunt temporary*** *option has to be selected in the definition of Input 2 and the* ***Shunt delay*** *has to 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.

3 Check the **Activate relay temporarily** option, if applicable (Corporate Gateway only).

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

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

5 Check the **Shunt input temporarily** option and the **Reset delay for shunt temporarily**, if applicable (Corporate Gateway only).

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.*

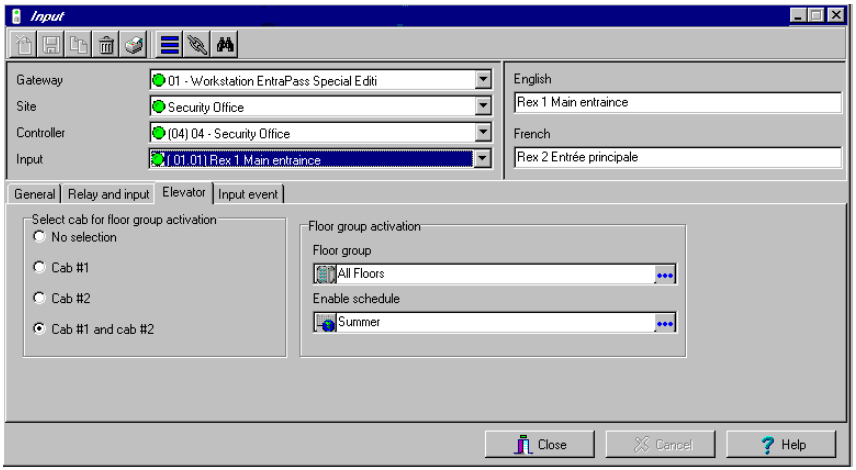
6 **In the Shunt delay (h:mm:ss)** field, specify the period during which an input is not monitored. Setting the timer to 0:00:00 will instruct the relay to follow the input state. The maximum value for the Shunt delay (h:mm:ss) is 9:06:07. (Corporate Gateway only)

To define an input for an elevator door:

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

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 screen, 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.*

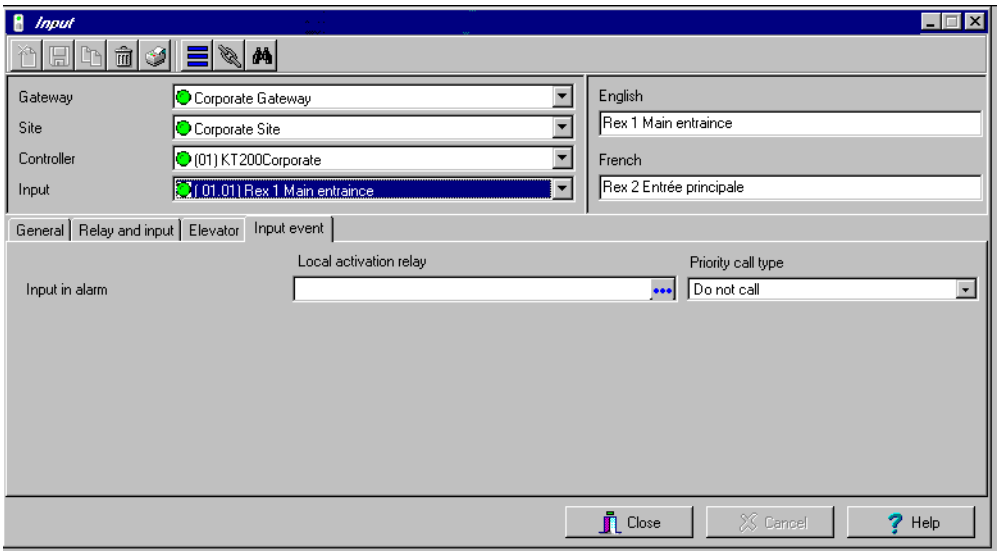
2 In the **Select cab for floor group activation** section, select the cab associated with the input.

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 (Corporate:

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**. *For more information, see "To define a site :" on page 69.*

Configuring Output Devices

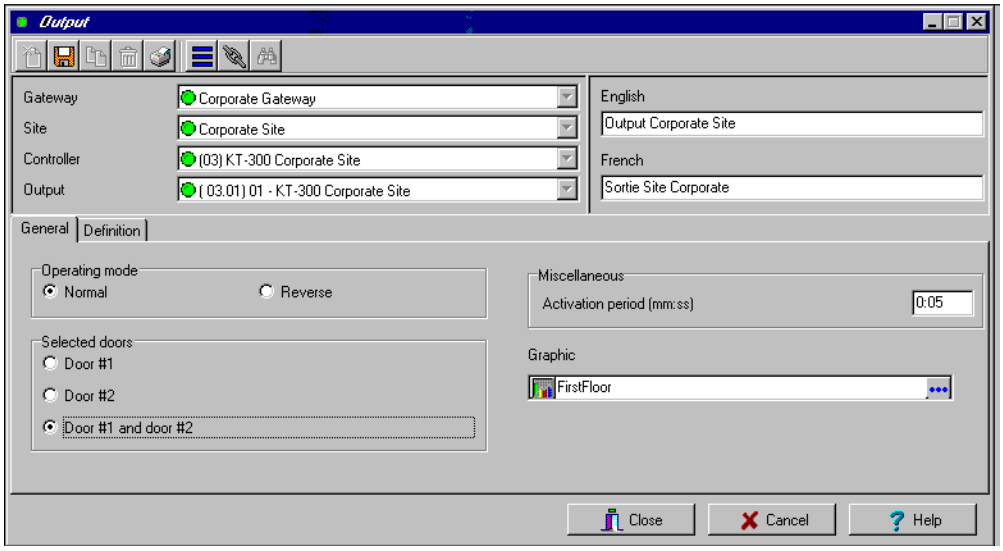
Outputs usually control the reader LED and buzzer. There are four outputs available per KT-200 and KT-300 controllers (2 per door). A KT-100 supervises the state of two outputs.

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.

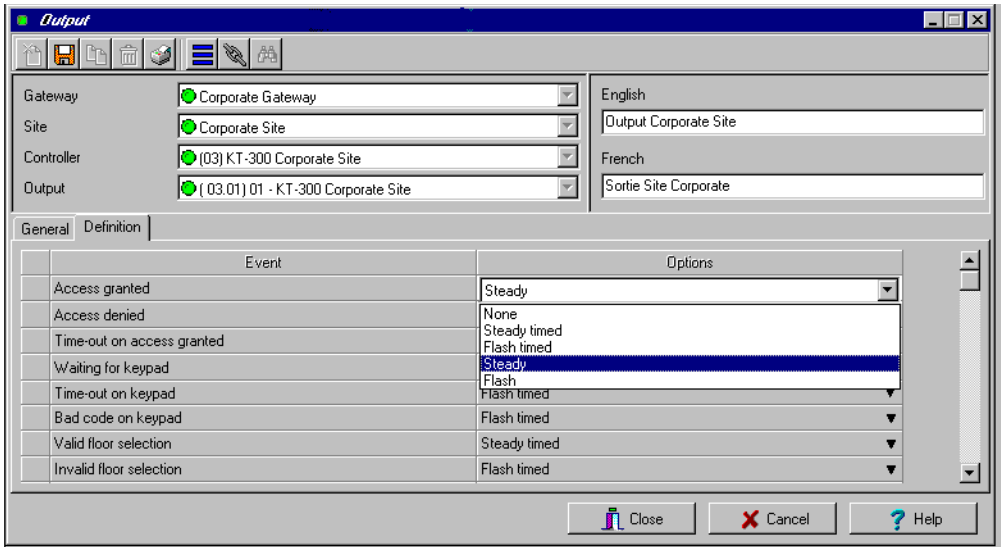
NOTE: *An activation period of zero will leave the output activated indefinitely, regardless of the activation type.*

To associate events with auxiliary outputs

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

To do this:

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.

NOTE: *The on-off delays for the outputs are pre-defined during the Gateway definition. For details, see “Configuring EntraPass Gateways” on page 66.*

Chapter 5 • Live Video

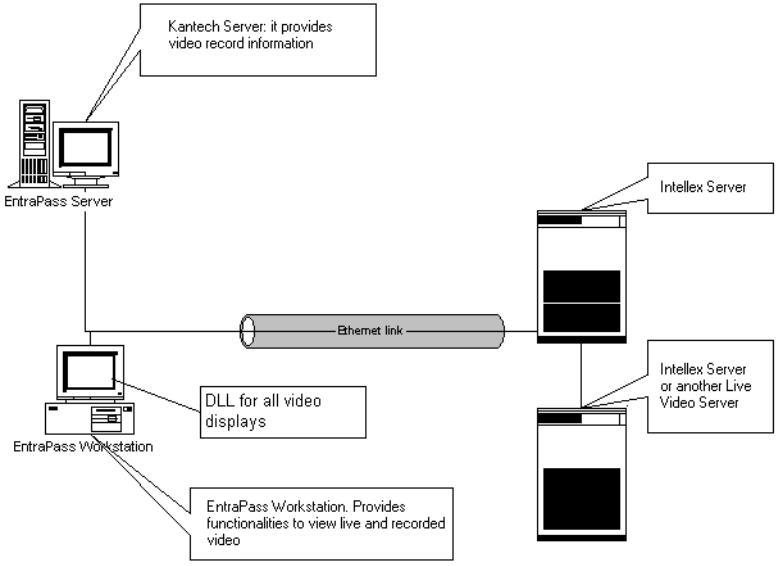
EntraPass adds real-time monitoring capability to the Corporate and Global series as a response to the growing importance of video in access control systems. The new feature allows operators to define Live Video viewing parameters from EntraPass Corporate and Global Edition user interfaces.

To install the Live video feature, EntraPass administrators have to:

- Define the Video server for use in EntraPass (identifying the Video source and specifying cameras connected to it),
- Define the Video view for Live video monitoring using EntraPass desktops,
- Assign appropriate operators' permission,
- Define a Live video desktop and/or assign a video view icon in graphics (such as floor plans).

NOTE: *Installing and using the Live Video feature may take a great amount of your company network bandwidth (LAN or WAN). The network administrator may control the use of the network bandwidth for Live Video transfer.*

The following diagram shows how the Live Video feature is integrated in EntraPass.

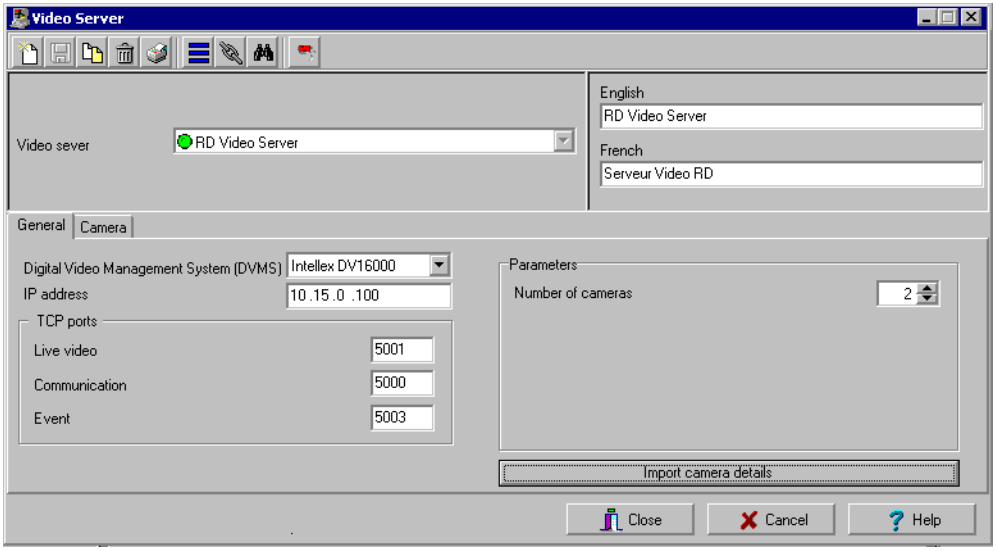


Defining the Video Server

A Video server is connected to a EntraPass through a specific IP address. The Video Server captures, stores and distributes video images to the EntraPass desktops for monitoring and surveillance purposes. The live video can then be accessed by any EntraPass workstation (with appropriate permission) through the network.

To define the Video Server parameters:

1 From the EntraPass main screen, click the **Video Server** button.The Video server window appears with the **General** tab enabled.



2 From the **Video server** drop-down list, select the DVMS you want to configure (or click the **New** icon to create a new one), then assign it a meaningful name in the language section. It is recommended to supply a name in the two languages if you are running the application in two languages.

NOTE: *The Camera tab appears only when you have set the number of cameras. The* ***Import camera details*** *button is enabled when you enter the data in* ***General*** *tab (DVMS name, IP address and TCP ports information).*

3 From the **Digital Video Management System (DVMS)** drop-down list, select the DVMS for the video server you are configuring.

NOTE: *The current version of the software integrates Intellex only. Other digital video management systems will be available in the future.*

4 In the **IP address** field, specify a static IP address for the DVMS. It is essential to select a static IP address; a dynamic address is not compatible with the live video feature.

NOTE: *Make sure that the Video server is set to a static IP address. For specific information about the DVMS IP address, contact your network administrator.*

5 In the TCP Ports section, specify the ports for the Video server. The ports numbers vary depending on the selected DVMS.

NOTE: *The TCP port (Transmission Control Protocol) is used by the Live video application to communicate with EntraPass. Options displayed in the TCP port section depend on the device you are configuring. For details about ports and their settings, contact your network administrator or the documentation provided by your DVMS vendor.*

6 Using the **Up/down** controls, specify the number of cameras connected to the video server. defining. When you do this, the **Camera** tab appears next to the **General** tab.

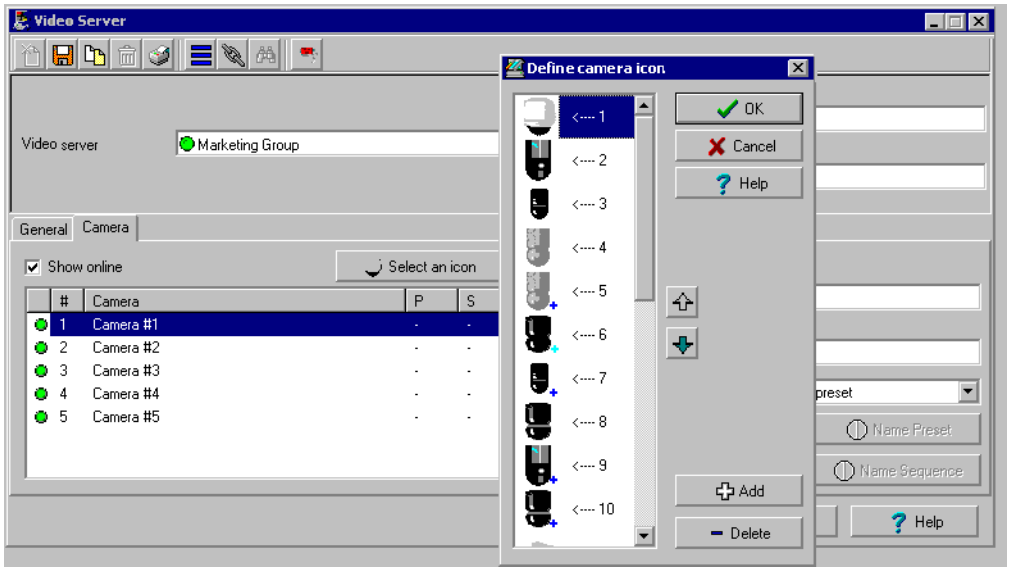
7 Click the **Select an icon** button to display the icons for use while defining your cameras. The **Add** button to select icons from a server and to add them to the default list. You can use the Up/down arrows to scroll down the displayed icons. You can remove an icon by selecting it and then clicking the **Delete** button.

8 Click the **Import camera details** button Import camera details to retrieve the number and default names for the cameras connected to the selected DVMS. When you click this button, the Live video feature will connect to the server and get default information about the connected cameras.

Identifying Camera Presets and Sequences

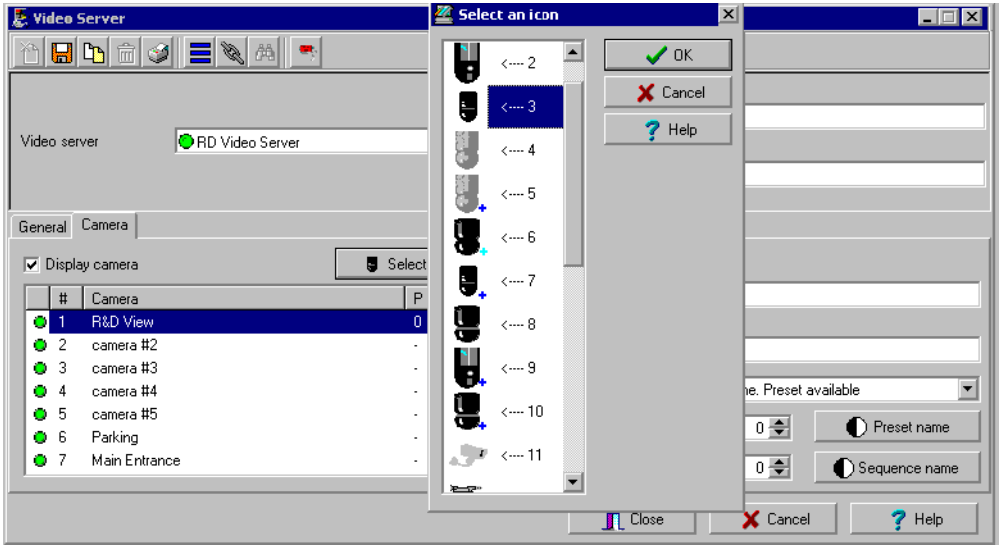
To define cameras:

1 Select the **Camera** tab to define cameras connected to the video server.Cameras appear with their default names. EntraPass offers you the ability to assign names to your cameras for easy identification in the Live video desktop.



NOTE: *A green flag next to a camera name indicates that the camera is available for display in the Live video desktop; a red flag indicates that the camera is unavailable for display. Double-clicking a camera allows you to toggle from available/unavailable.*

2 Select a camera, then assign a name in the enabled language fields. It is recommended to assign a name both in the primary and secondary language if the system is running in two languages.



NOTE: *If you select a camera and then click the* ***Display camera*** *checkbox, a red flag appears next to the camera name; making it a hidden (covert) camera. A hidden camera is represented by a plain cell in the Live video desktop. You may also double-click a camera to make it unavailable for view in the Live video desktop.*

3 To associate a specific icon with a camera for view in the Live Video desktop, select the camera, then click the **Select an icon** button, then click **OK** to close the Select an icon window.

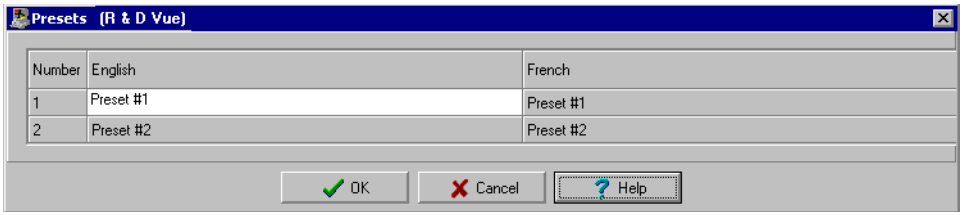
4 In the Video Server window, select the **Camera type** from the drop-down list.

- **Fixed, no preset**: operators cannot control a fixed camera. When this option is selected, the **Number of presets** scroll-down list and the **Preset Name** button are disabled.
- **Dome, preset available**: selecting this option allows operators to control the camera. If you select this option, assign meaningful names to the camera presets.

5 Set the **Number of presets** and the **Number of sequences** using the **up/down** controls. When the number of presets/sequences is greater than zero, the **Preset name** and **Sequence name** buttons are enabled.

NOTE: *Defining these parameters does not impact video server programming. They just allow you to identify components for use in the EntraPass environment.*

6 Click the **Preset Name** (or **Sequence name**) button to call the Preset (Sequence) window. The camera being defined is identified in the window's title bar.



7 Select a table cell, then overtype the default name. If you are running the system in two languages, enter the name in both the primary and secondary language.

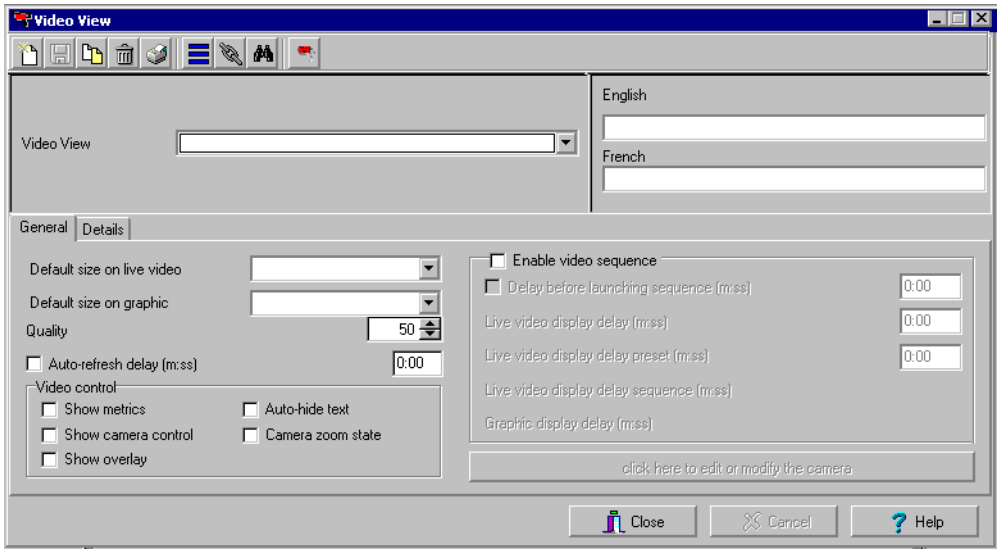
8 Click **OK** to close the Preset window.

Defining Video Views

Once the video server is defined and its cameras identified, operators have to define video views that will be displayed in Live video desktop for viewing and monitoring purposes.

To define video view options:

1 Select the **Video View** button from the Live Video window. The Video View window appears.



2 From the **Video View** drop down list, select a video view (or click the **New** icon to create one), then assign it a name in the language section. If the system is running in two languages, you have to give a name in each language.

3 From the **Default size on live video** drop-down list, select an appropriate size for the image that will be displayed: you may choose to select a smaller size if you have to display the Live video window with another window.

- **Large**: 1024x768
- **Medium**: 800x600
- **Small**: 640x480
- **Tiny**: 400x300
- **Last used**: displays the size that was previously displayed in the Live Video desktop.

4 From the **Default size on graphic** drop-down list, select a size for the image that will be displayed on the system graphics: (Large, Medium, Small, Tiny, Last used).

5 From the **Quality** scroll down list, set the quality for the video image. This options allows you to increase or decrease the image quality.

NOTE: *The image quality impacts the system performance: the higher the quality, the lower the compression and the lower the system performance. If you set the quality to high (> 80), the compression will be low. As result, the application will use a larger network bandwidth. This may result in a slower process. The following table shows the recommended options:*

Quality	Description
100	Maximum size
80	Super quality
60	Normal
50	Default
40	Low quality

6 Check the **Auto-refresh delay (m:ss)** if you want the system to refresh the displayed image. If you check this box, the displayed image will be automatically updated when the specified delay is elapsed.

7 From the Video control section, make the appropriate choices:

- **Show metrics**: this option enables the system to display the number of frames per second (Fps) and the number of bits per seconds (Bps) for the selected camera. The information appears in the upper section of the Live video window (and in the Live Video desktop).
- **Show camera controls:** check this option for use dome cameras. Selecting this option allows operators to control a dome camera. This option is not available with fixed cameras.
- **Show overlay**: check this option if you want the camera identification (camera name and server) to appear in the Live Video desktop.
- Auto-hide text: if this option is checked, the system will not display the information related to a camera.
- **Camera zoom state:** check this option if you want to display the zoom value for the selected camera. This option is not enabled in this release.

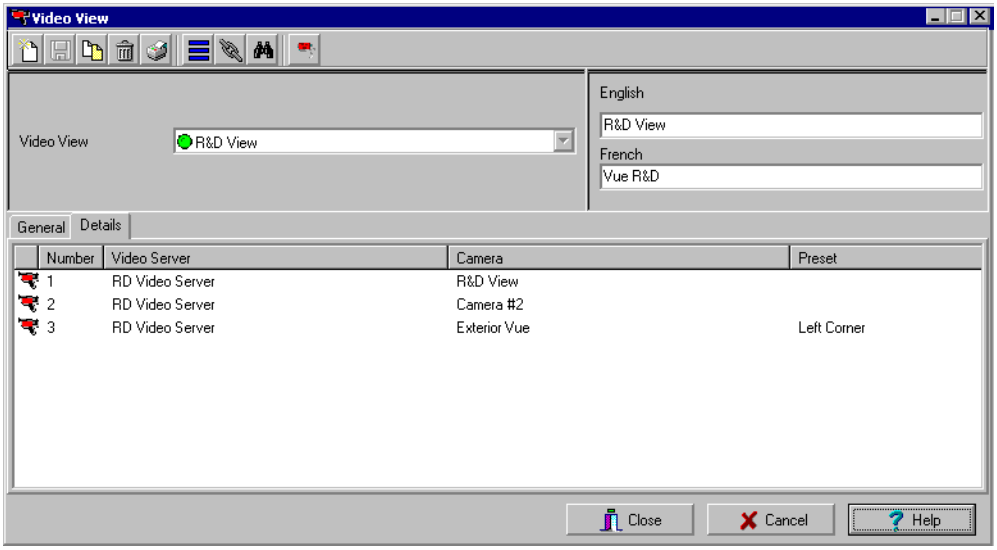
8 Check the **Enable video sequence** box to alternate video images in the Live video window. If you have defined a 2X2 view, then the video sequence will be composed of four images alternating in the video display according to the delay specified in the **Live video display** delay field. If you do not check this option, the video view will display a static image.

- Check **Delay before launch sequence** box to specify the transition delay before the images start alternating in the Live video window.

- Specify the **Live video and Graphic display and preset delays**: these delays indicate the time frame during which a video or graphic appears in the Live video display before it is replaced by another. Refer to the following table for presets and sequences minimum delays.

Delay	Minimum (seconds)
Delay before launch sequence	2 seconds
Live video display	3 seconds
Live video display preset	5 seconds
Live video sequence	20 seconds
Graphic display delay	5 seconds

9 Click the **Details** tab to view detailed information about the selected Video view.



10 Click **Close** to go back to the EntraPass main window.

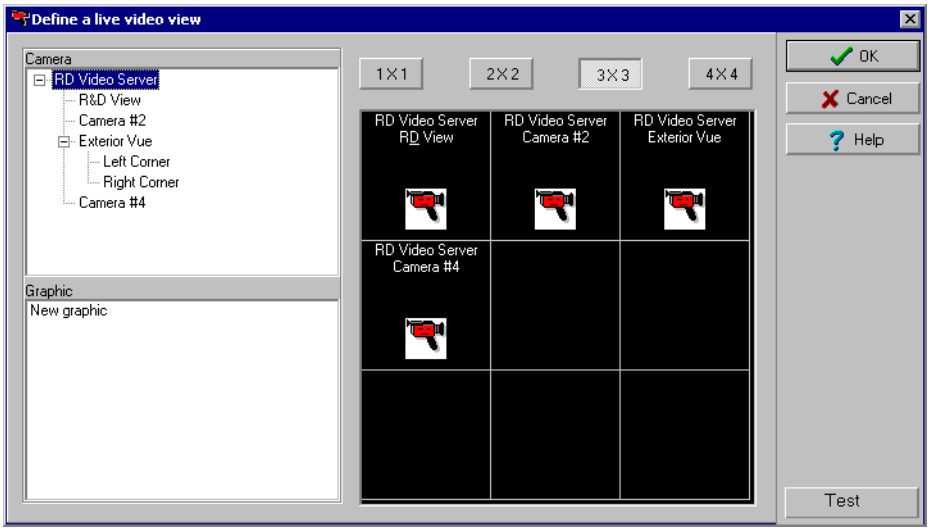
Defining the Live Video View

Video presets and sequences are configured for view in the desktop dedicated to Live video.

Later, a specific view (or graphic) is called in the Live video desktop with components updated in real-time.

To define a view:

1 From the Video view window, click the **Click here to edit or modify the camera** button to define the content of your video view.



NOTE: *The upper pane shows camera programmed in EntraPass. The lower pane shows graphics (floor plans, for example) defined in your system.*

2 From the left panes, select a camera preset, then drag it in a right pane cell. A camera is identified by its name and corresponding icon.

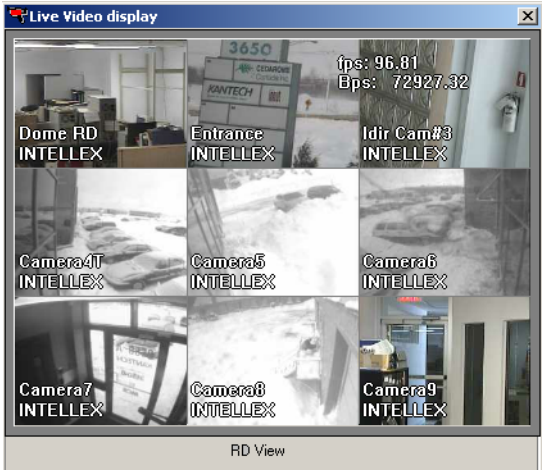
NOTE: *A specific camera and graphic can appear only in one cell. You can put cameras from different Video Server but the source must be from the same vendor.*

3 Click the button in the upper part of the right pane to specify the number of images you want to display:

- Click the 1 X 1 button to display 1 image
- Click 2 X 2 to display 4 images,
- 3 X 3 to display 9 images,
- and 4 X 4 to display 16 images.

NOTE: *The number of the images displayed influence the speed of the network bandwidth. For example, if you are displaying 4X4 images, the network bandwidth will be slower than when you are displaying a 1X1 image.*

4 Click the **Test** button to view the result of the selection. The displayed Live video view appears in the Live video desktop for video monitoring and surveillance.



NOTE: *To delete a camera from a cell, right-click it, then select* ***Delete*** *from the shortcut menu.*

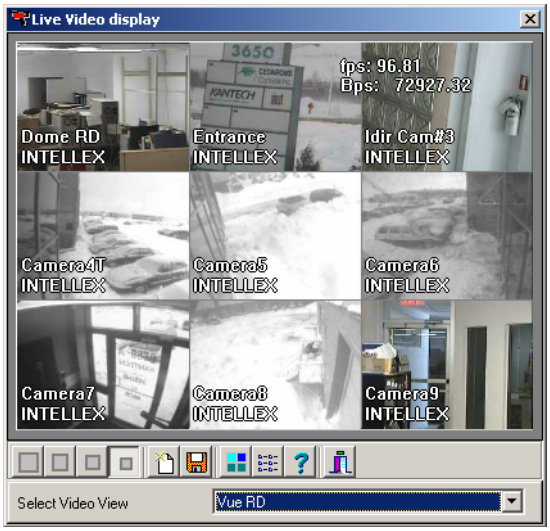
5 Click the **Close** button (the X) in the upper corner of the window to close the Live Video test window.

Using the Live Video Desktop

The Live Video Desktop allows operators to monitor live video using an EntraPass desktop. For details about configuring the Live video desktop, see “Live Video Desktop” on page 281.

To display a live video view:

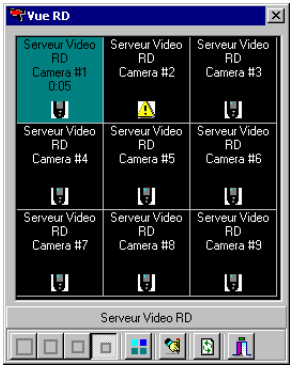
1 From the EntraPass main window, select the desktop dedicated to Live video. The Live video image appears in the desktop.



2 Click a button to resize the displayed images. Buttons in the lower part of the window allow you to perform various tasks:

Buttons	Description
	Use these buttons to select a size for the displayed video. **Note**: A bigger image requires more process power. Therefore, selecting a bigger image may result in lower process power.
	Use these buttons to copy and save new video views.
	Use this **Show view selector** button to display a mosaic view of all the camera defined in the system.
	Properties, Help and Close buttons. These are EntraPass standard buttons.

3 Click the **Show view selector** button to display the View selector window. This small window allows you to so select a specific view or to monitor a specific camera sequence. For instance, if you select a cell in the View selector, the sequence is interrupted to display the selected cell.



	Click the **Reset** button to go back to the Live video desktop and to display or select a specific view.
	Click the **Stop sequence** button to stop the sequence. To restart the sequence, click again the **View selector** button
	Click the **Bring to front** button if you want the Live video desktop to be on top of the displayed windows.

4 From the displayed view, you can click a dome camera icon to display control buttons for this camera (movement, zoom, focus). Available options depend on the Digital Video Management system connected to your system. Please refer to your DVMS documentation for additional information.

NOTE: *If your dome camera is set with preprogrammed movement patterns, you can define a view displaying a sequence composed of one or many of these pattern. For more details, see* *"Defining Video Views" on page 117.*

Chapter 6 • Operations

The **Operations** toolbar allows operators to perform manual operations on various system components. From the **Operations** toolbar (found on the workstation), manual operations are used to override schedules or process special requests when necessary.

When a manual operation is launched, it is possible to view in real-time, the status of the selected components. The following icons appear in most manual operation windows. Other icons also appear depending on the component that is displayed:

- The **Enable Graphic** button**:** When selected, this button 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.
- The **Enable Animation** button**:** When selected, this button automatically enables the **Enable graphic** button at the same time. This will activate the current component (i.e.: door) and will display its status in real-time.
- The **Select All** button: This button is used to select all the items or components displayed in a list of choices.
- The **Unselect All** button**:** This button is used to unselect all the items or components that were previously selected in a list of choices.

Manual Operations on the Gateway

The **Reload data** command allows operators to refresh system parameters with new data from the system database. After a reload operation, the gateway 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 gateway?

- 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).

To reload a gateway:

1. From the Workstation main screen, select the **Operations** tab and click the **Reload data** to open the following Reload data screen.

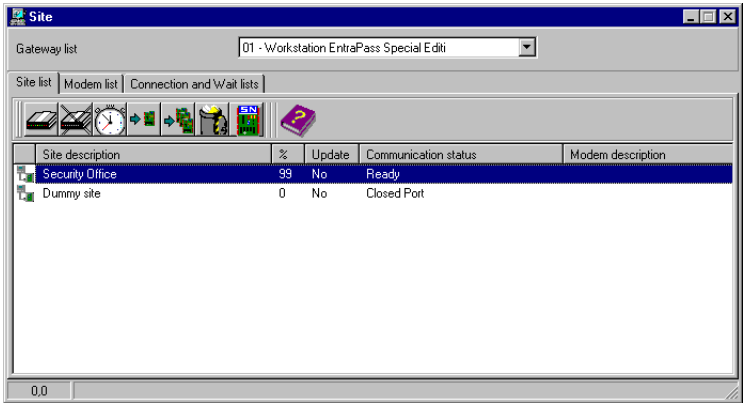
2. Select the desired gateway to reload. You may select the **Enable graphic** icon or the **Enable animation** icon in order to view real-time system animation on the gateway.
3. Click the **Reload gateway** icon to refresh data in the gateway.
4. You may select the **Help** icon to view more information about the gateway.

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. This applies to Corporate Gateways only.

To perform manual operation on a site:

1 From the **Operation** screen, click on the **Site** icon to open the following screen.



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.*

The following table identifies communication options available through the toolbar.

Tool	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 workstation and the remote site.
	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.

Manual Operations on Controllers

This menu is used to reset or reload a controller:

- **A 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);
- **A hard reset** will erase the existing controller database and reload it with new information in the controller database;
- **A reload** will reload the controller database; if for example a controller database is not reloaded correctly due to an erratic operation;
- **A reload controller firmware** will reload the firmware of the controller (KT-100 and KT-300).

From the controller reset screen, you may perform operations on the reader. For example, you may:

- Unlock the reader keypad (KT-100 and KT-300);
- Reset the power on the reader (KT-300);
- Rest the number of cards in the area, display the list of Cards in/Cards out (KT-100, KT-200 and KT-300 with Corporate Gateway only).

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

To reset a controller:

1 From the Operations screen, select the **Controller reset** icon.

2 From the Site list (left pane), select the Site (or Gateway) on which the controller is located.

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

3 From the **Controller** list displayed in the top right pane, select the controller on which the operations will take place. It has to be highlighted. To perform the operation on a group of controllers, select **All controllers** (lower right pane).

4 Select the appropriate operation: **soft reset** to refresh the controller; **hard reset**, to re-initialize the controller, **reload controller** and **reload controller firmware**.

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

5 To perform a manual operation on a reader:
- Select the **Unlock keypad** button if you want to unlock the keypad;
- Select the **Reset reader power** if there is a problem with readers (KT-300 only).

6 Select **Forgive** if you want to reset the **Cards in** and **Cards out** counters. When you select the Forgive option, card users will not be considered inside or outside until the next use of their card at an entry or exit reader.

7 You may want to know how many cards are in or out. To do this, use the **Cards in** and **Cards out** button. The passback option has to be enabled on the reader and the door has to be defined as an entry or exit door.

NOTE: *The Card in/Cards out operations are performed only on a door defined as an entry or exit door. If you have one or more controllers configured with anti-passback, this function allows you, for example, to view a list of cards that are considered inside or outside the area. The passback option has to be enabled; that is, it has to be either* ***soft*** *or* ***hard synchronization****. This operation is performed only on one controller at a time as it may be a lengthy operation.*

Manual Operations on Doors

This menu allows an authorized operator to manually modify the state of a door or group of doors.

Operators can manually:

- Lock/unlock a door (icons with a red/green flag),
- Temporarily look/unlock a door or group of doors (icons with an hourglass image),
- Enable or disable readers of selected doors (reader icons are red or green flag).

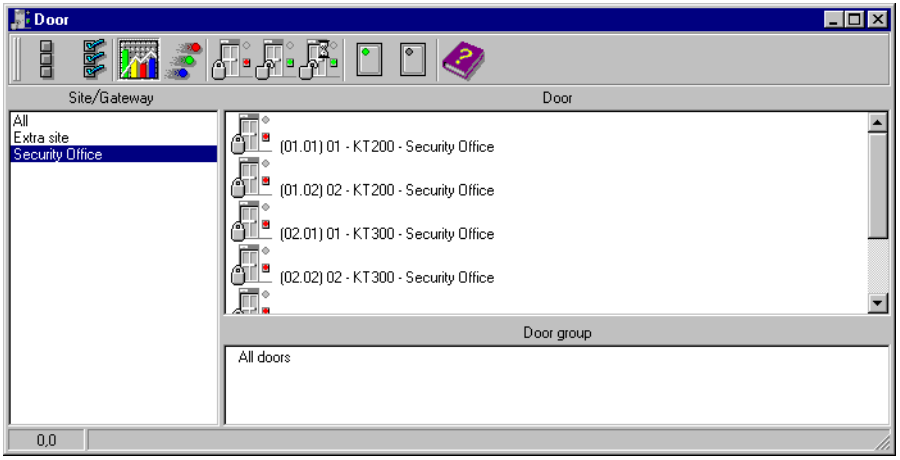
There are various reasons why you would want to perform one of these operations; for example you may need to “disable a reader” for a short period in order to deny access to the door, etc.

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 lock a door manually:

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



2 The left pane displays the site or gateway lists. You may select **All** sites/gateways or select a specific site or gateway. The doors are listed in the top right pane.

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

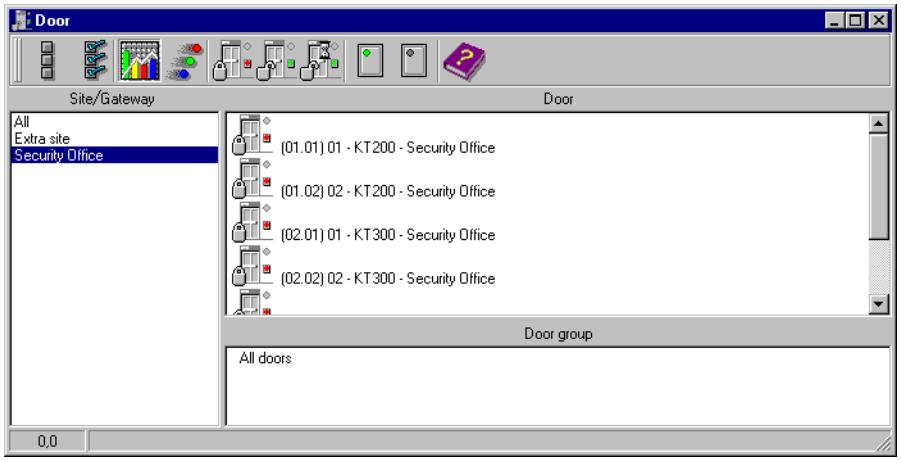
3 Select desired door(s) from top right pane or **All doors** from bottom right pane.

4 Click the **Lock-door** icon in the toolbar.

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

To unlock a door manually:

1 From the Operations window, select the **Door** icon.



2 The left pane displays the site or gateway lists. You may select **All** or select one site or gateway. The doors associated with the selected site or gateway are displayed in the right hand pane.

3 Select a door in the upper part of the right pane. You may also select **All doors** (bottom of screen).

4 Click the **Unlock-door** icon in the tool bar. The selected door will be manually unlocked. The system will prompt for operator confirmation. A door defined with an automatic unlocking schedule, it will remain unlocked until:

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

To unlock a door temporarily:

1 From the Operations window, select the **Door** icon.

2 The left pane displays the site or gateway lists. You may select **All** or select one site or gateway. The doors appear in the right hand pane.

3 Select door in the upper part of the right pane. You may also select a door group under the **All doors** (bottom of screen).

4 Click the **Temporarily unlock** icon.

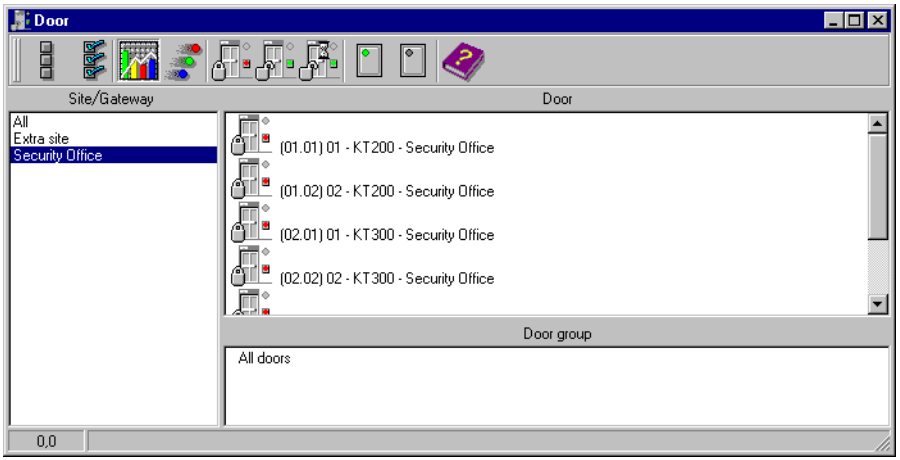
The selected door will be temporarily unlocked by an operator. The system will prompt the operator to enter the delay, when this delay expires, the door will re-lock automatically.

This option is often used to grant access to a user who does not have a card or has forgotten his/her card. Maximum unlock time: 4":15 (255 seconds).

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 enable a reader:

1 From the Operations window, select the Reader icon.



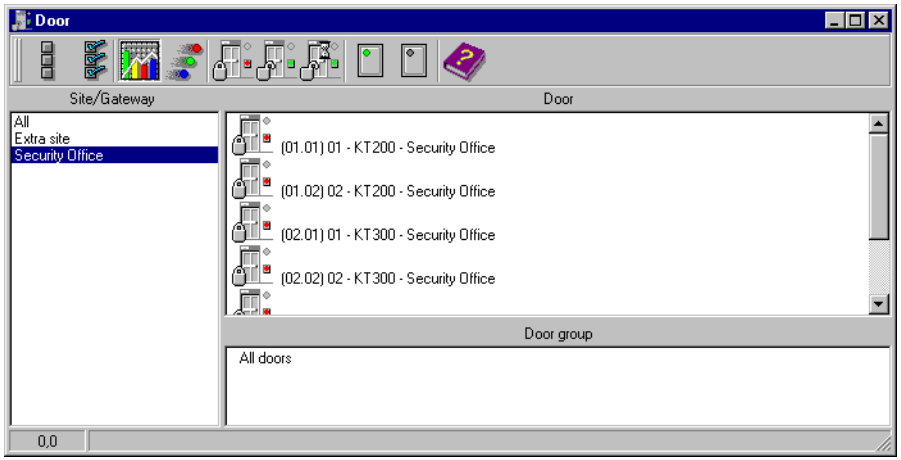
2 The left pane displays the site or gateway lists. You may select **All** or select a specific site or gateway. The Doors appear in the right pane.

3 Select a door in the upper part of the right pane. You may also select a reader group under the "All readers" (bottom of screen).

4 Click the **Reader-enable** button. This option enables a previously disabled reader.

To disable a reader:

1 From the Operations window, select the **Reader-disabled** icon.



2 The left pane displays the site or gateway lists. You may select **All** or select a specific site or gateway. The doors appear in the right hand pane.

3 Select a reader in the upper part of the right pane. You may also select a reader group under the **All doors** (bottom of screen).

4 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.

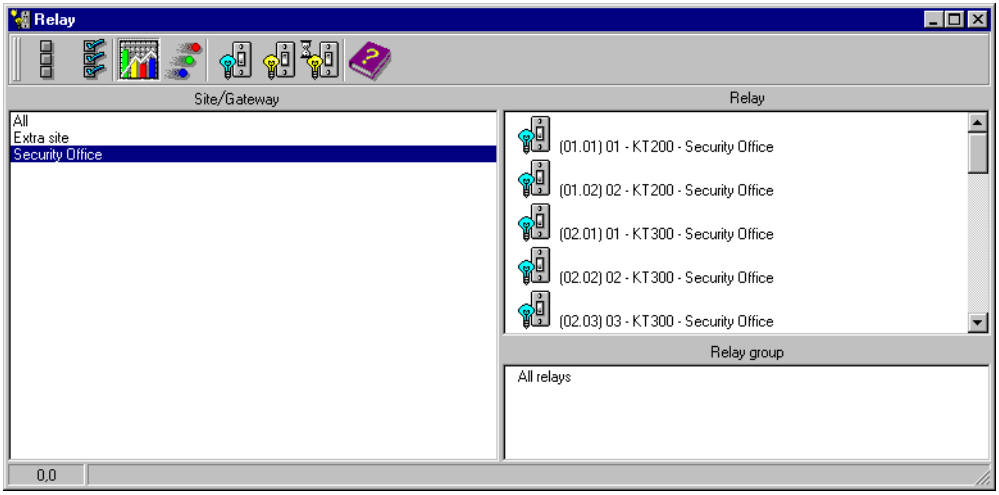
Manual Operations on Relays

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 screen 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.

To manually deactivate relays:

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

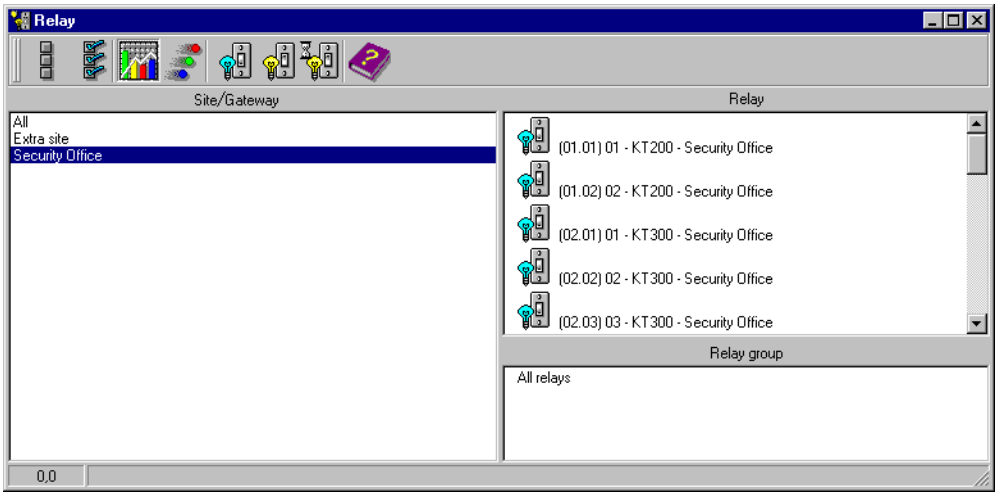


2. In the left pane, you may select a site or gateway, or you may select **All** to display all the relays.
3. In the right pane, you may select a relay in the upper part of the screen, or you may select **All** in the lower part of the screen.
4. Click the **Deactivate** relay icon.The selected relay(s) will be manually deactivated. This operation allows an operator to deactivate a relay which was previously activated by an operator, event, schedule or input in alarm.

NOTE: *If you manually de-active 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 From the Operation window, select the **Relay** icon.



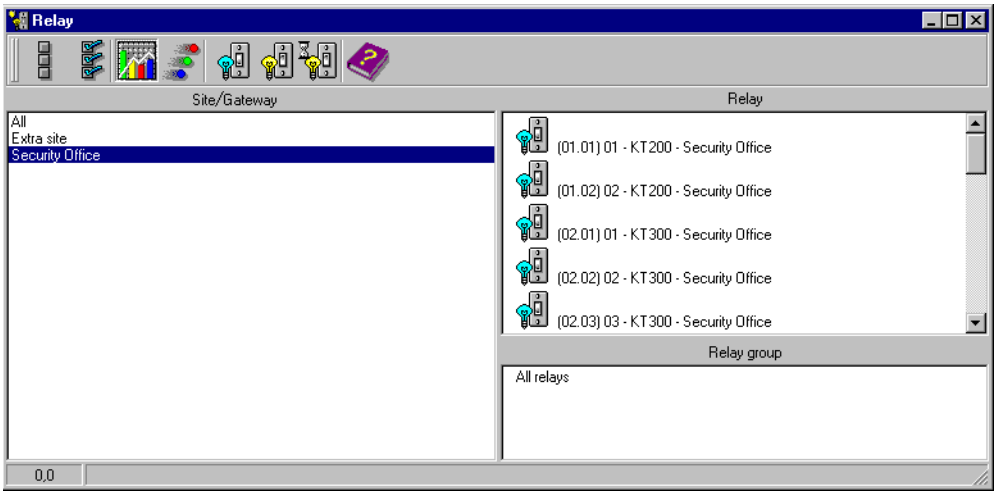
2 In the left pane, you may select a site or gateway, or you may select **All** to display all the relays.

3 In the right pane, you may select a relay in the upper part of the screen, or select **All relays** in the lower part of the screen.

4 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:

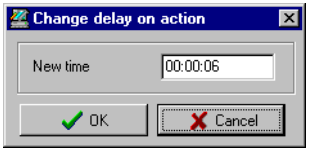
1 From the Operation window, select the **Relay** icon.



2 In the left pane, you may select a site or gateway, or you may select **All Relays** to display all the relays.

3 In the right pane, you may select a relay in the upper part of the screen, **All Relays** in the lower part of the screen.

4 Click the **Activate relay temporarily** icon to open **Change delay on action** screen.



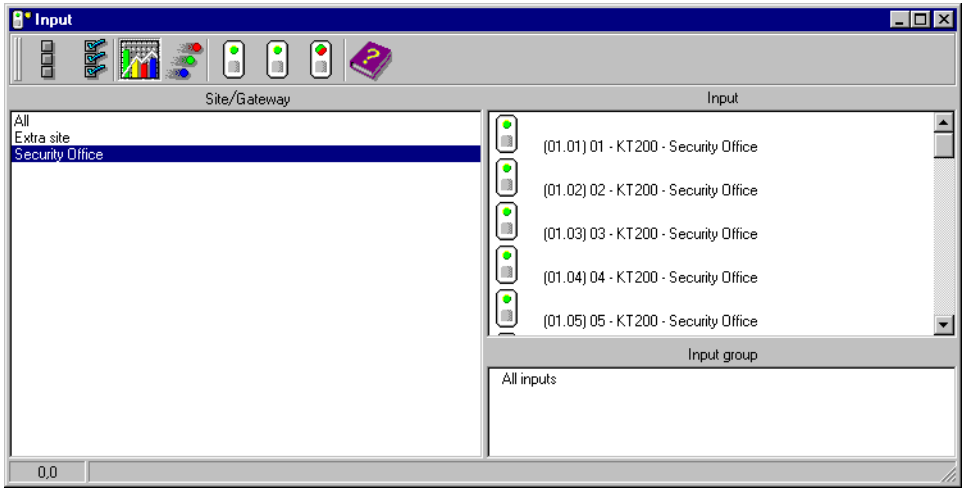
5 Enter the desired delay time and click **OK**.

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.*

Manual Operations on Inputs

To perform manual operations on inputs:

1 From the Operation window, select the **Input** icon. The Input window appears.



2 To return an input to its normal state, select the input, then click the **Input Normal state** icon. The selected input returns to its normal state as defined in the **Device** menu. 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.

3 To stop monitoring an input, select the input, then click the **Input no supervision** icon. The selected input is not supervised, regardless of its schedules (if defined). Only a manual operation can modify this condition.

4 To shunt temporarily an input, select the input, then click the **Temporarily shunt** icon. The input will not be monitored temporarily.

Chapter 7 • Definition

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

- Schedules,
- Floor,
- Graphics,
- Holidays.

Defining Schedules

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 need to be acknowledged or when to activate relays controlling different functions (lighting, heat etc.).

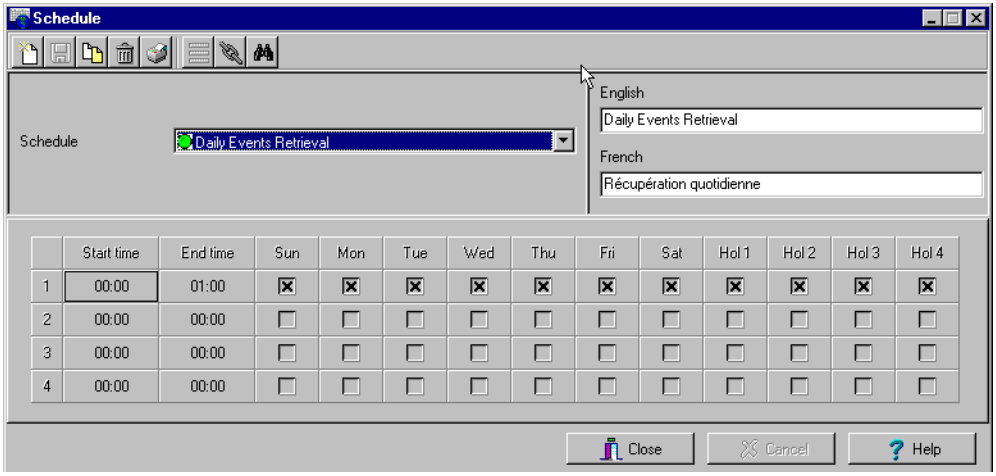
It is possible to use the same schedule in different menus, but it is recommended to create a different schedule for each application, because it is much easier to modify a particular schedule without affecting other applications.

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.

NOTE: *EntraPass offers you the ability to define four types of holidays.*

To define a schedule:

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



2. Select a schedule from the **Schedule** drop-down list, 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. 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.
5. 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.*

6 Check the **Days** during which this schedule interval will be valid. To do this, click in the check box below each day.

7 Check the **Holiday** 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;

2 Define a second interval for Tuesday from 00:00 to 08:00.

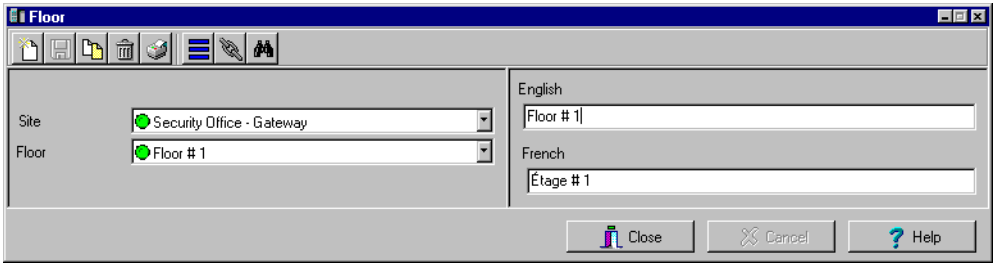
The system considers these two intervals as one continuous interval.

Defining Floors

The Floors definition menu 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.

To define floors:

1 In the **Definition** main window, click the **Floor** icon.



2 In the **Site** drop-down list, select the gateway/site workstation 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.

Defining Graphics

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

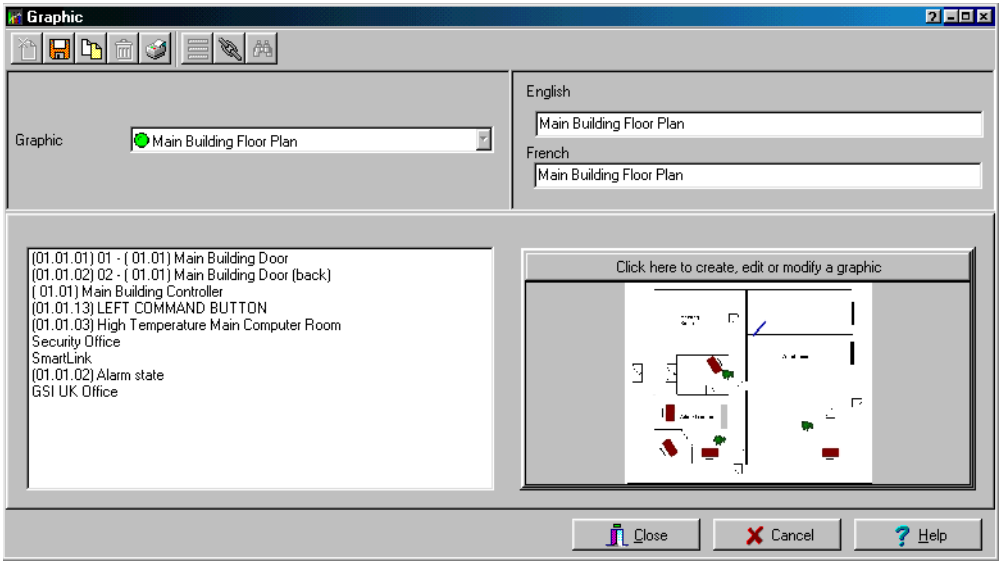
With graphics, operators can easily view the exact location of a component installed on a site, or the status of components and devices such as doors, contacts, motion detectors, controllers, assigned to the graphic. Operators can perform manual operations directly from the displayed component (for example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

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 is equipped with five built-in demonstration graphics. To view these demos, navigate to the EntraPass installation folder, then select the "Demobmp" folder.*

To create a background image:

1 In the Definition screen, select the **Graphics** icon.

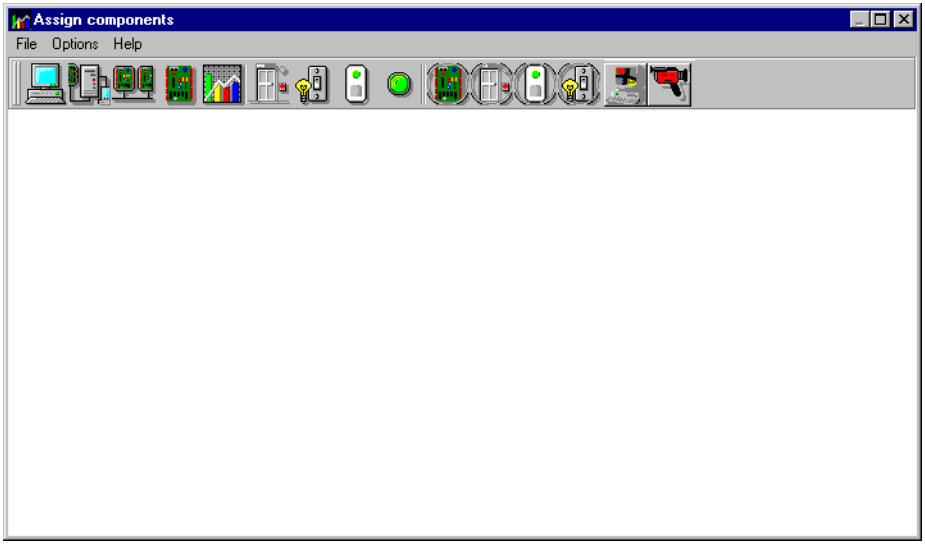


2 From the **Graphic** drop-down list, select the graphic you want to modify, or click the **New** icon to create a new one.

3 Assign a name to the graphic (or modify the existing name).

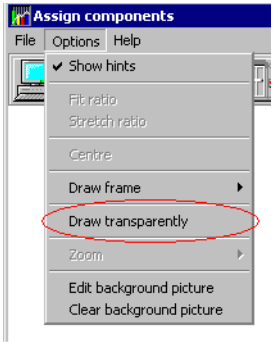
NOTE: *When you select a graphic, or when you create a new graphic, all the components that are assigned in your graphic are displayed in the left pane. The right part of the screen lets you view the selected graphic.*

4 From the **Graphic Definition** screen, click the Click here to create, edit or modify a graphic button to bring up the **Assign Components** window.



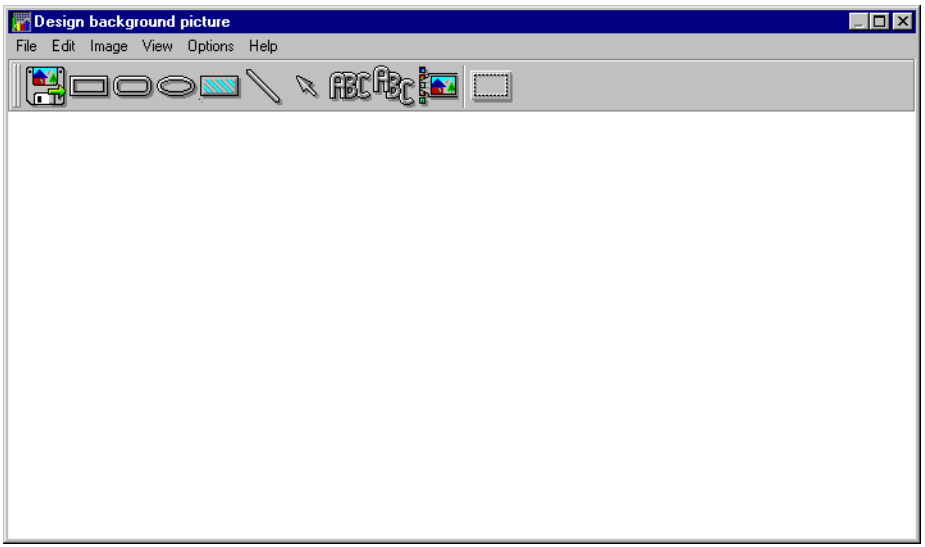
NOTE: *If the Live Video feature is enabled in your system, video components are added to the Graphics menu. These video components can be accessed from the graphic layout. The icon can be positioned on a graphic layout and its status can be retrieved by clicking on the video icon. In addition to standard option, the following Status option will be available for the video component: Video Server Online / Offline, Video Server Parameters (Related to a specific vendor) and Camera status.*

5 Click on **Options** to display pull down menu of drawing options.



NOTE: *The **Draw transparently** option allows you to place a transparent icon on top of a background picture for a blended effect.*

6 Double-click anywhere in the background to bring up the **Design background picture** screen.



7 Use this screen to import a graphic that was created with another application or create your own background using the drawing tool bar buttons.

- To import an existing graphic, click the diskette icon, then drag and drop the diskette in the work area. The system displays the **Open** screen. Make your selection and click **Open** to import your graphic.
- To create a background, select a form, drag and drop it to insert either a rectangle, a circle, a ellipse, etc. in your background. You can modify the background color only when the form selected is a rectangle. You can also insert a custom image in the background image.

- To import a custom static icon into the background graphic you may call up images from the **Custom image** button . The Select image window appears.

8 Select an image, then click **OK** to close the window and import the image in your design.

To add annotations and other features to the background image:

1 From the toolbar select an annotation, for example the pointer, click and drag where you want it to be.

2 Right-click on the arrow in the toolbar. From the displayed options, you can modify the properties (such as line width, color) and you can also specify if the arrow should be sent to the back or the front of the other annotations in your graphic.

3 When you are finished, click on **Image** from the File menu, save annotations. Annotations will be saved in a separate file.

4 Click **Clear** (following your save) to clear the annotations. If you save the graphic with the annotations, the annotations are permanent.

5 Select the **Load annotations** option to retrieve annotations that were previously saved to disk. When you add annotations to a graphic, you have the option of saving the annotations on a separate file in order to enter them later.

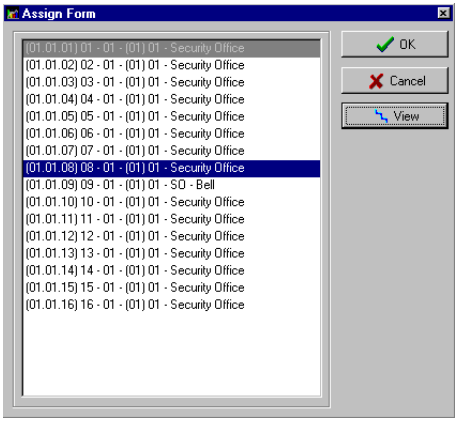
6 Select the **Save annotations** option to save annotations on a separate file from your graphic in order to retrieve them for later use.

7 Use the **View** menu to define how the graphic will be displayed on screen.

8 Use the **Options** menu to position and size the graphic in the Design background screen

To add components to the background graphic:

1 From the **Design** screen toolbar, click and drag the selected component to desired position. To drag an object across a screen, 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, you have to assign it to a component of your system: Right-click the component and select **Assign** from the contextual menu:

3 The system will display a component screen, select the component that corresponds to the image, then click **OK** to go back to the previous screen.

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.*

4 Select the **Options** menu to define the graphic:

- Select **Show hints** for the system to provide the component's name (component's address and name) when you point over that graphic. To show the hints, right-click on the component, select the **Show hint** option (a check mark will be displayed).
- Select **Draw frame** to draw a frame around the component.
- Select **Frame color** to change the color of the frame for the assigned components.
- Select **Edit background picture** to edit the background of the selected graphic. From this screen 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.

5 Right click on an assigned component to select or unselect it.

NOTE: *When an object is selected, sizing handles (square handles that are displayed along the sides of the object that surrounds the selected object) indicate the object is selected.*

Defining Holidays

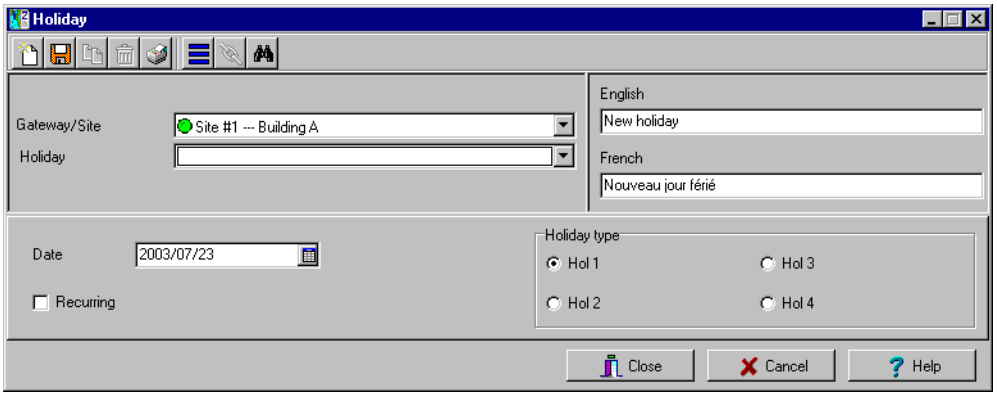
A holiday is treated differently than other days. It is recommended to program holidays at the beginning of the year; this helps to modify floating holidays for the current year (Easter, Thanksgiving Day, etc.).

To define a holiday for a Gateway:

A holiday may also 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.

To define a holiday:

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



2 To create a new holiday, select the **New** icon. By default, Global Holiday appears in the **Site** drop-down list.

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 calender.

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 8 • 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,
- Define and issue visitor cards,
- Define card types,
- Define and issue day passes,
- Modify groups of cards,
- 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.

Defining Cards

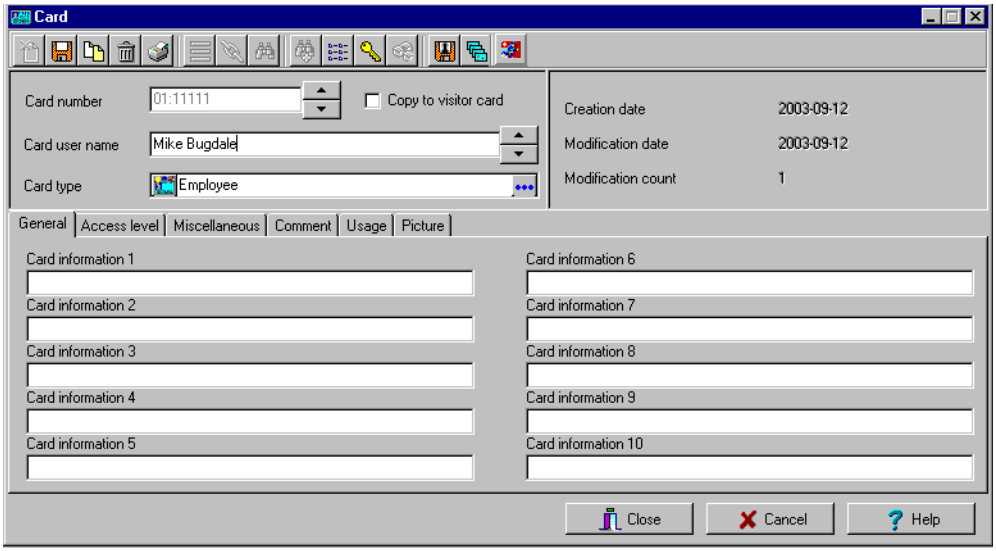
Cards are defined by the following properties: card number, cardholder name, access level and status (valid, invalid, pending, lost/stolen). Cards records can be searched, sorted and deleted.

The Users menu for card definition 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.
5. Check the **Copy to visitor card** checkbox. When this option is checked, card information fields are copied to the Visitor database (the card number is not copied). This feature enables you to archive profiles that are retrieved should you issue a temporary card.
6. Click on the **Card type** box to access the **Card type** menu. Select the card type for the new card. The card type is used to group cardholders; it is useful for modifying an existing card group

and creating reports, etc. For more information on how to create/modify card types, see "Defining Card Types" on page 209.

NOTE: *From the Card type screen, you can right-click the Card type field and choose New to create a new card type, choose Select to pick an existing card type or you can choose Edit to edit an existing card type.*

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

7 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.*

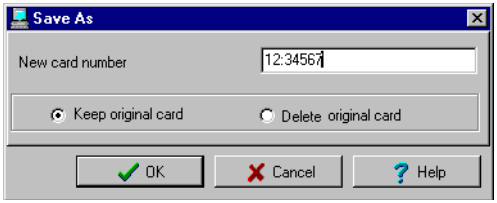
8 Click the **Save** icon.

Creating 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.

To create a new card using "Save as":

1 Type required changes into specific fields in the Card screen 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.

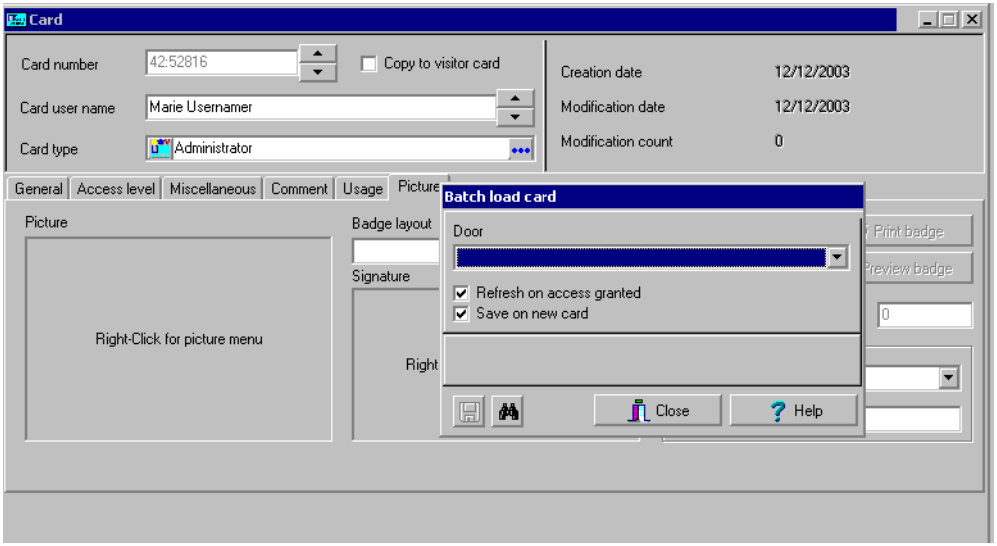
3 Select the **Keep/Delete original card** options to specify if the original card should be kept or deleted (usually kept), then click **OK** to save the new information. The Card screen is displayed.

Issuing Cards Using the Batch Load Feature

The Batch Load feature allows operators to issue cards on "access granted" and "unknown card" event messages.

To issue cards using the Batch Load feature:

1 From the card window, click the button.



2 From the **Door** drop-down list, select the Door that will be used to enter card numbers.

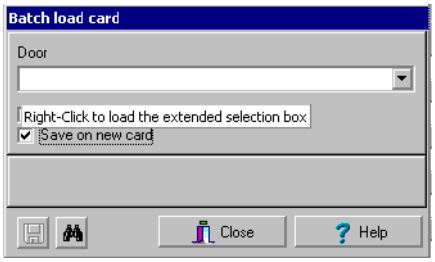
3 Check the following options:

- **Refresh an access granted**: if this option is checked, each time an access is granted the card database will be refreshed with data relative to the card.
- **Save on new card**: if this option is checked and the if the Save icon is enabled, new card data 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 data manually.

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.*
- *If an operator clicks the **Close** button 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 add more options to your selection.



Editing, Searching and Deleting Cards

Editing a card

To edit a card, do one of the following:

- 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.

Searching for a card

1. From the Card screen, select the **Binocular** icon.
2. Enter a keyword to start the search (For example, the cardholder's first name).
3. Check the **Display match only** option to restrict the search.
4. Click the **Find** button to launch the search.
5. Click the **Details** button to display detailed information about the cardholder.
6. Click the **Index** button to change the search field.

NOTE: *The system searches for "user name" by default. This may be changed with the Index button to search with any of the user definable fields.*

NOTE: *If you are searching for a visitor card, click the*  *from the Card screen.*

Deleting 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.

To delete a card:

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.

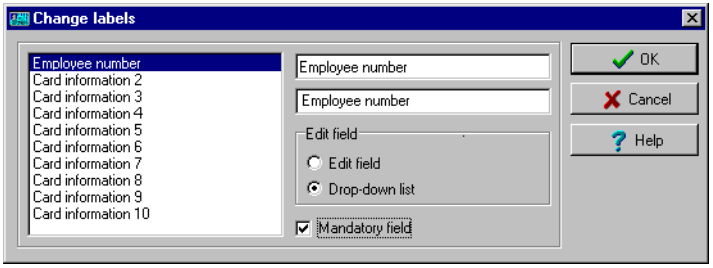
NOTE: *Although a deleted card is removed from the card database, it remains in the card history; all events involving that card remain in the event messages database. An event report locating past events that involved any deleted card can be performed.*

Customizing 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.

To customize card information fields:

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



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.*

Assigning Access Levels

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 "Defining Access Levels" on page 206.

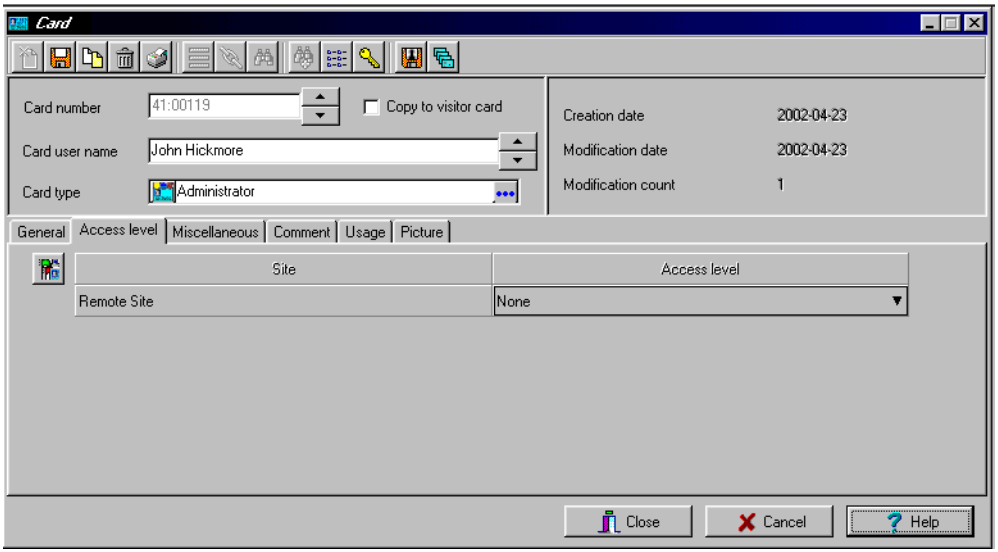
***NOTE:** When you modify the access level assigned to a card, you also modify the user's access permission to the doors and schedules associated to that access level.*

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 screen, select the **Access level** tab. The Access level screen appears, it displays the **Site** column and **Access level** drop down list.



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**.

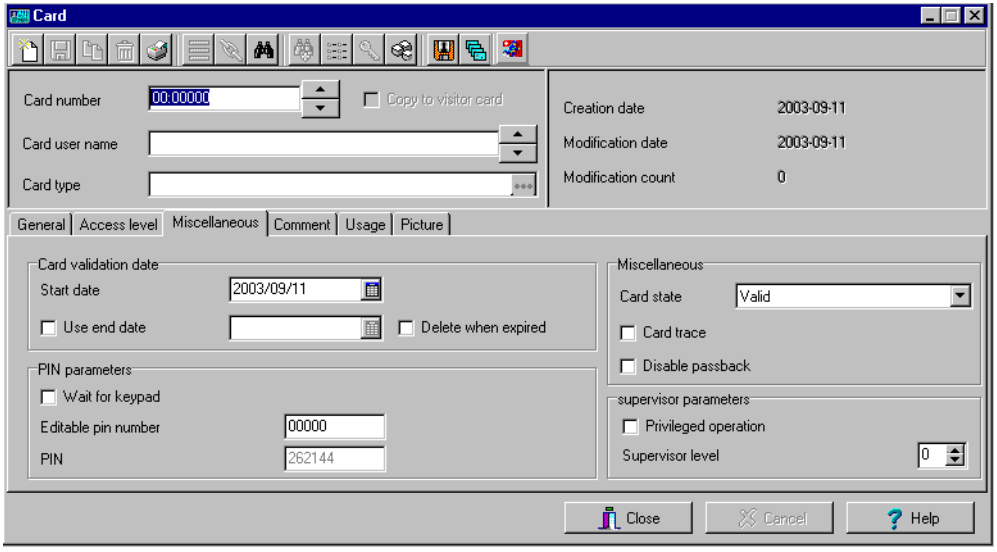
NOTE: *You have to create Access levels (**Users** > **Access Level**) to have them displayed in the **Access Level** drop-down list.*

Defining Card Use Options

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

To define card use options:

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 calender. 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 calender allowing you to select the end date. When the end date is reached, the **Card state** field is set to "Expired".

NOTE: *When creating a card with a time limited access of 24 hours of less, for example a **Day Pass,** the card will expire at midnight. This expiration may take up to one minute to register in the system.*

3 If applicable, check the **Delete when expired** option. 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 "Configuring Doors" on page 88.*

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 **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.

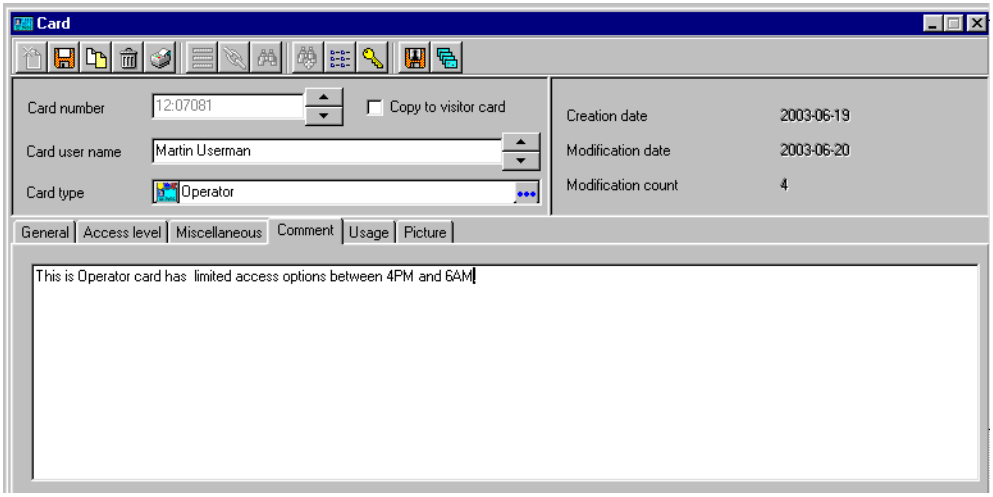
8 Set **Supervisor level** according to user privileges.

NOTE: *If required check the **Privileged operation** option to override any security measures regarding doors.*

Adding Comments to a Card

To add comments to a card:

1 From the Card screen, select the **Comment** tab.



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.

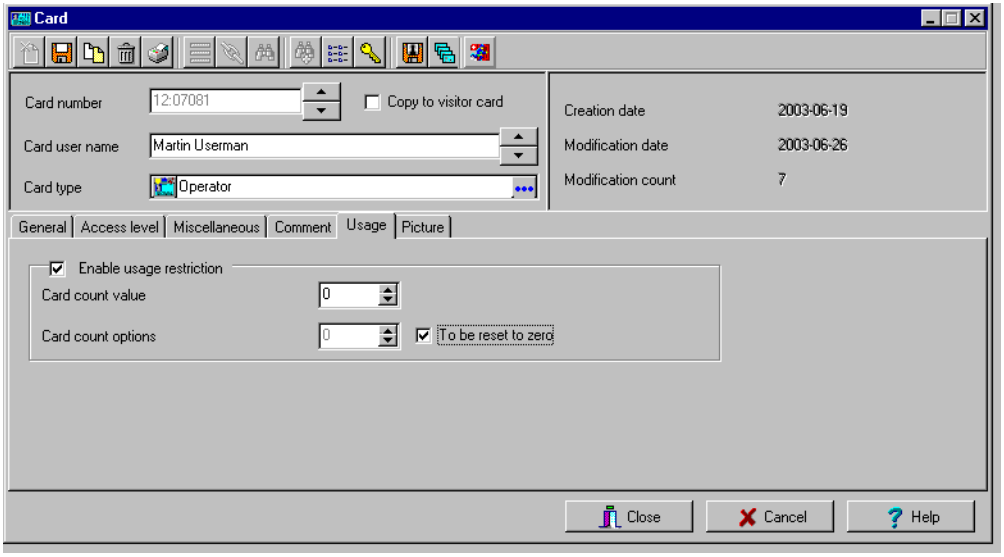
3 Click the **Save** button, then the **Close** button to exit.

Limiting Card Usage

EntraPass offers the ability to set card use count options so that you may limit the number of times a card can be used.

To set usage restriction:

1 From the Card screen, select the **Usage** tab.



2 Check the **Enable usage restriction** option in order to enable the card use count feature.

3 From the **Card count value** scrolling list, set the maximum number you want this card to be used. You may enter the number in the field or use the **Up/down** arrows.

NOTE: *Once you set the* ***Card use counter*** *feature, the* ***Card count option*** *field is automatically incremented each time the cardholder uses the card. After a certain number of uses, you may check the* ***Reset to zero*** *field if you want the counter to be reset to zero after the maximum value is reached.*

Assigning Pictures and Signatures

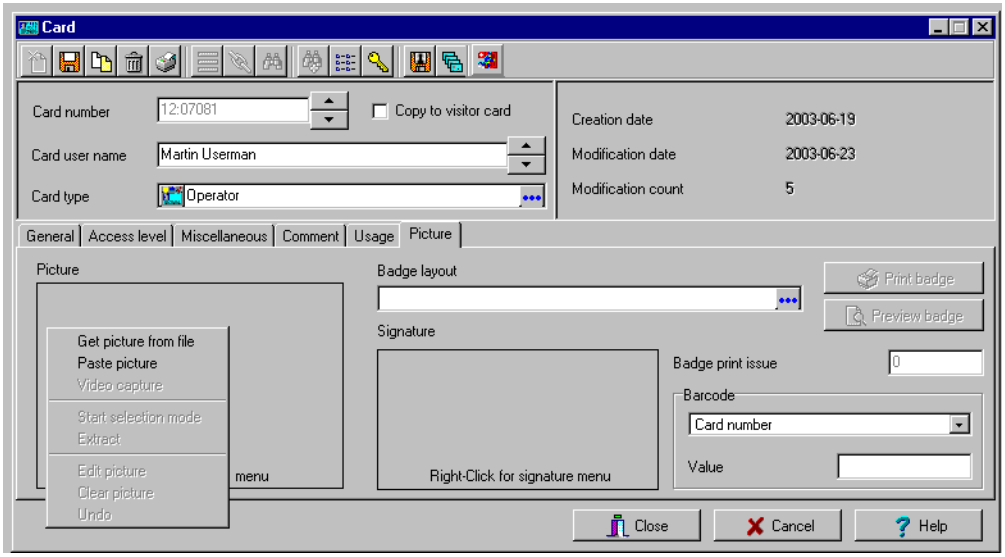
EntraPass offers the ability to associate photos and signatures with cardholders and to associate badge templates with cards as well as to print badges.

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 Saved or Pasted Images

To assign a picture from a file:

1 From the Card screen, 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 screen.

***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** screen.

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

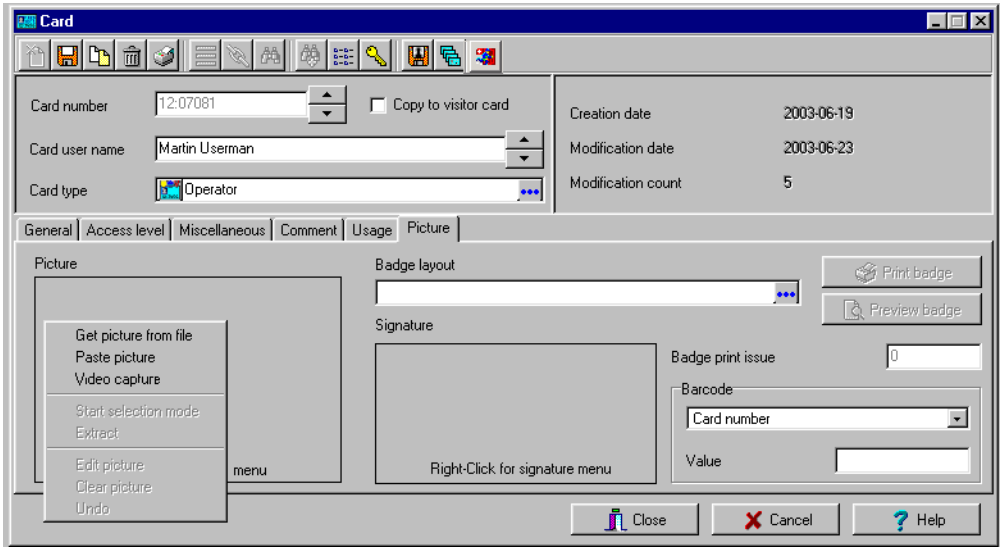
Assigning a picture using a video camera

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

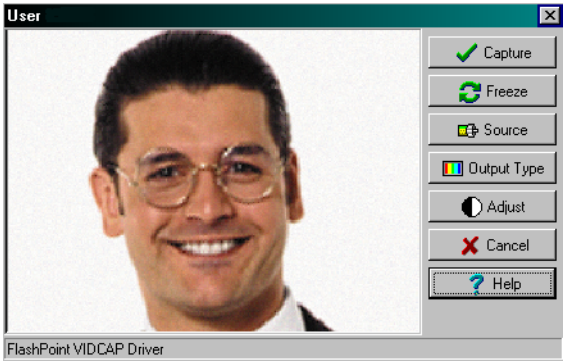
NOTE: *Before you can capture images using a video camera, all equipment needs to be properly configured. For more information, consult your manufacturer's device manual. If you have more than one video driver, you will need to specify the video driver to be used (**Options** > **Multimedia devices**>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

To incorporate a photo into a card using a video camera:

1 Right-click the picture area.

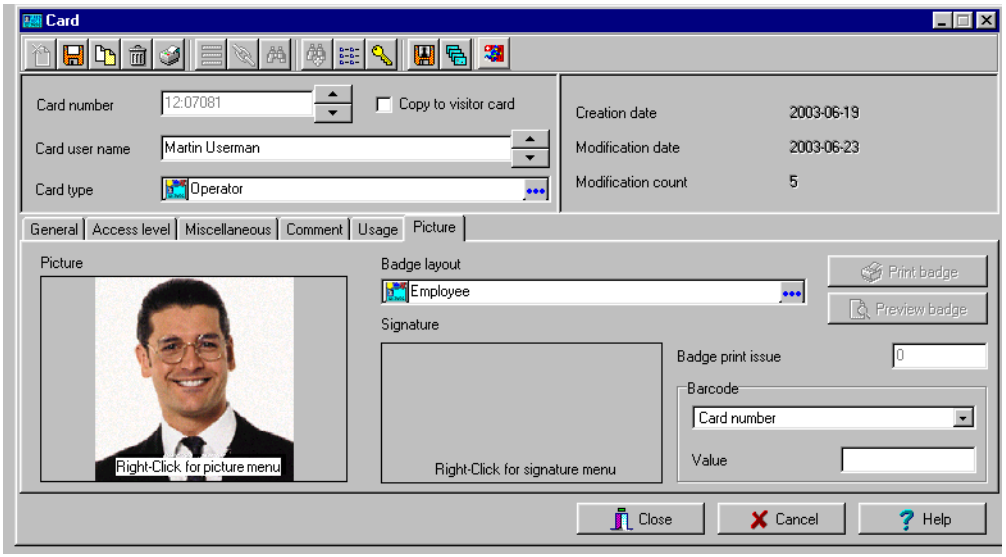


2 From the shortcut menu, select **Video capture**. This option is enabled only when the Video capture capability has been enabled in the Options menu (**Options** > **Multimedia devices** > **Video**).



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 Chapter 16 'Setting up Multimedia Devices' on page 368.*

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



4 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 “Designing Badges” on page 173.

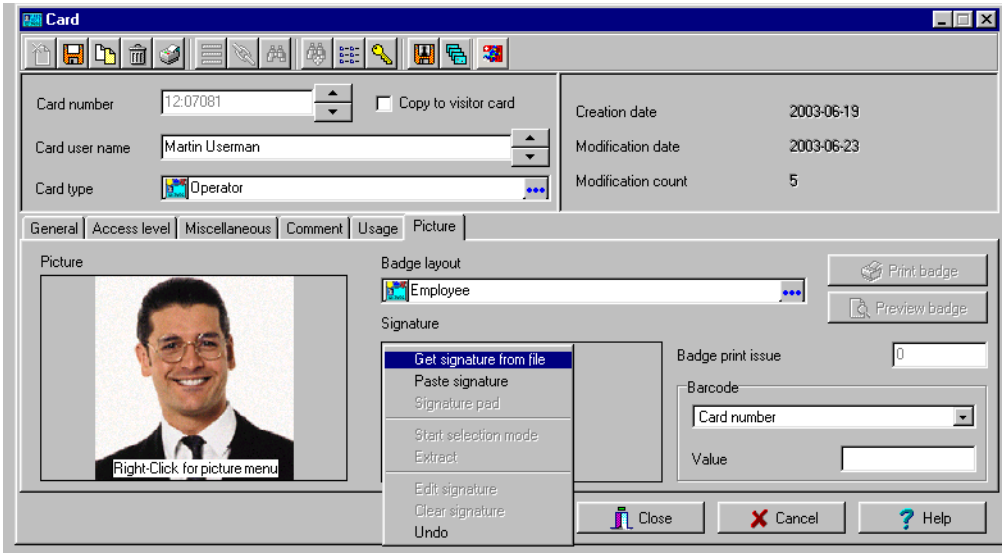
NOTE: *The **Print badge** and **Preview badge** buttons are enabled only when a badge printer and badge layout has been selected and the option Use badge printer checked: **Options > Printer>Badge printer**. If these buttons are enabled, you can preview and print the cardholder’s badge.*

Importing a Signature from a File

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

To import a signature:

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

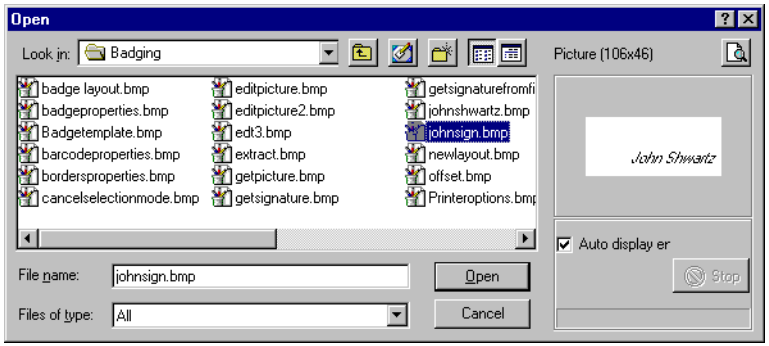


2 From the shortcut menu, make the appropriate choice:

- **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**.

Adding a Signature from a Signature Capture Device

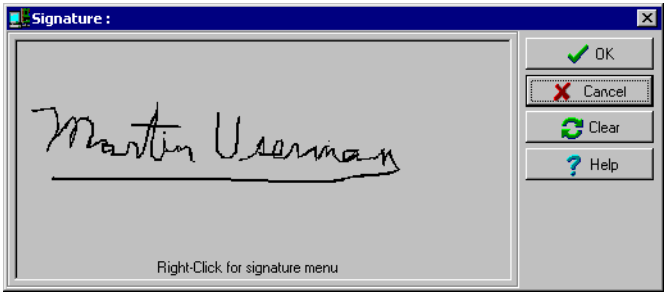
Use this option if a Signature Capture Device is installed and configured. The Signature pad option is enabled only when the appropriate device is enabled in the Options menu (**Options** > **Multimedia devices** > **Signature**).

To place a signature:

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

2 From the shortcut menu, select **Signature pad**. The Signature screen appears, allowing you to preview the signature.

3 Click **OK** to paste the signature in the card screen.



Working with Photos and Signatures

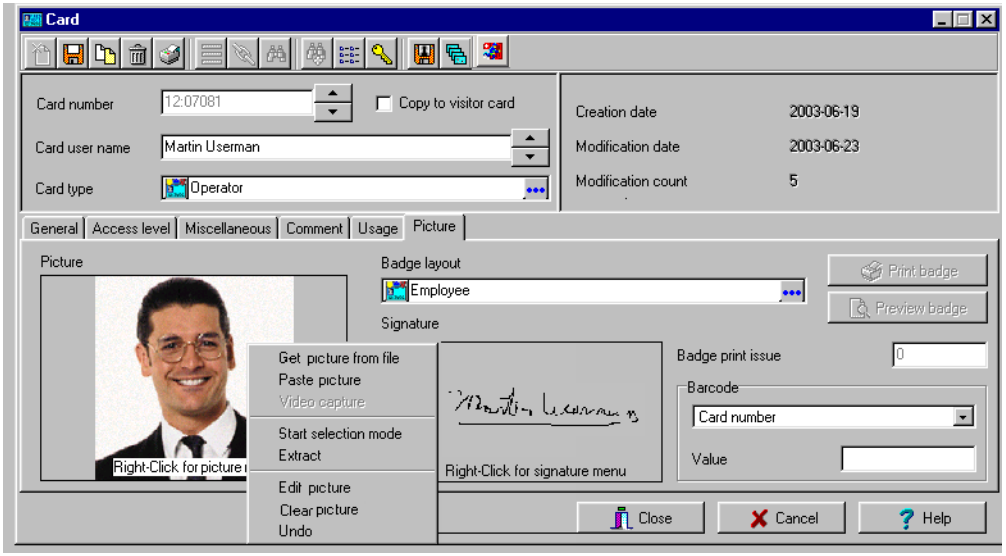
The EntraPass Integrated Badging feature allows users to extract part of an image or enhance images that are incorporated into cards.

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).

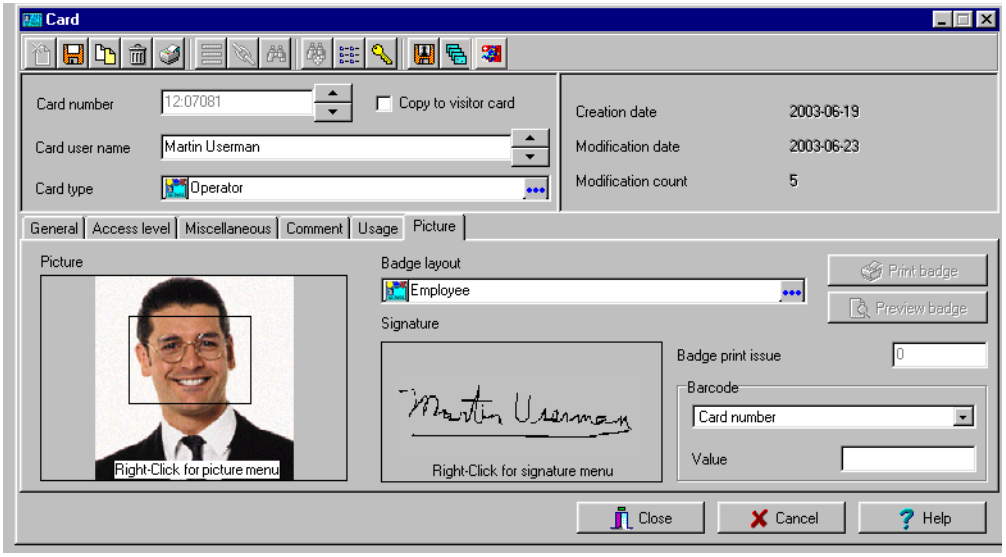
To extract part of an image:

1 Right-click the image you have just imported.



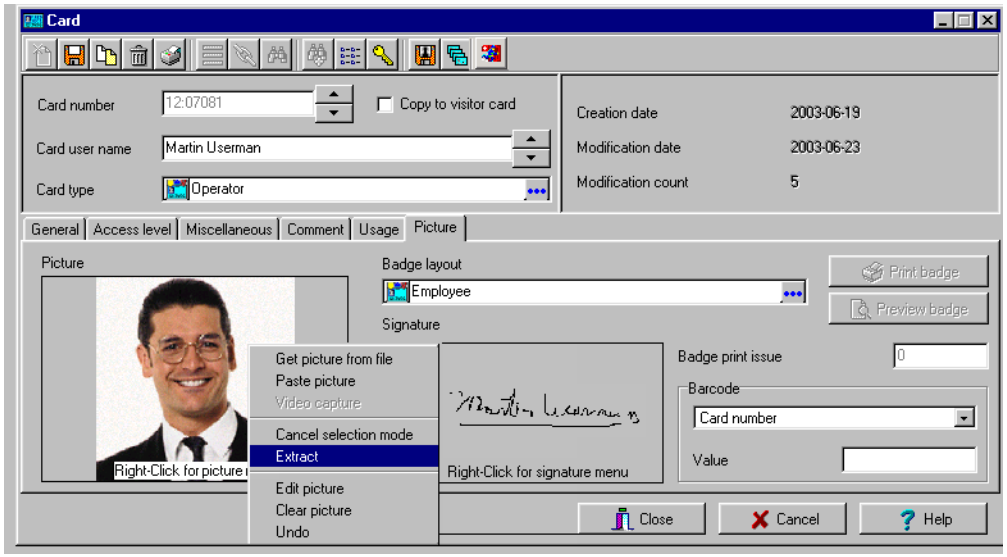
NOTE: *The* ***Extract option*** *is enabled after you have started the selection mode. Similarly, the* ***Undo*** *option is enabled only when an image has been pasted.*

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.

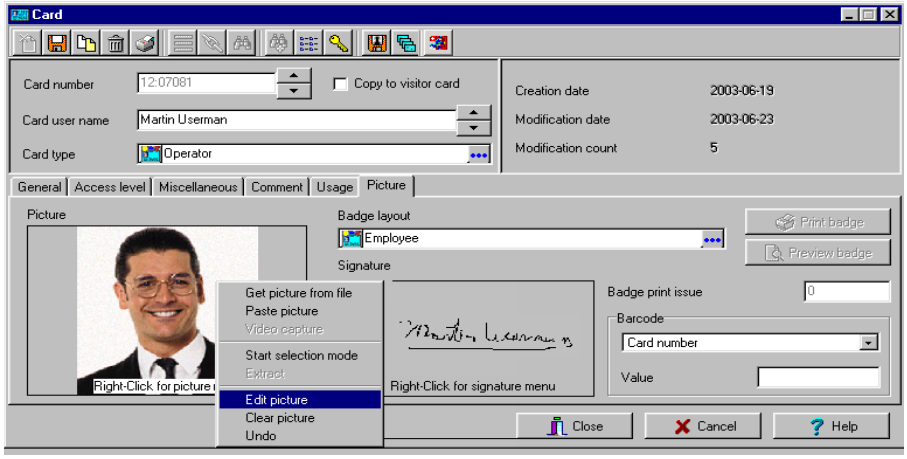


NOTE: *To disable the current selection, right-click the picture, then select* ***Cancel selection mode****. Select* ***Undo*** *to discard the changes. The* ***Undo*** *option is enabled only when you have pasted an image.*

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

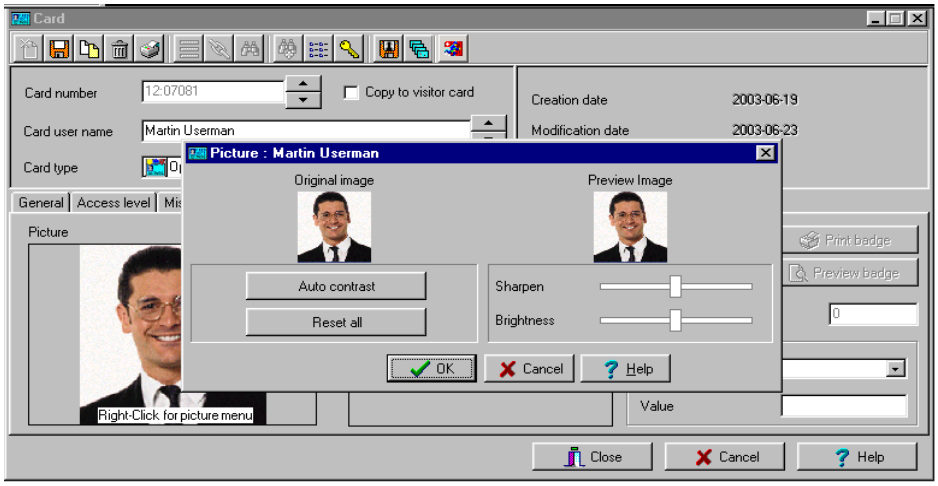
Editing a Picture/Signature

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 screen.

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 "Designing Badges" on page 173.

Printing Badges

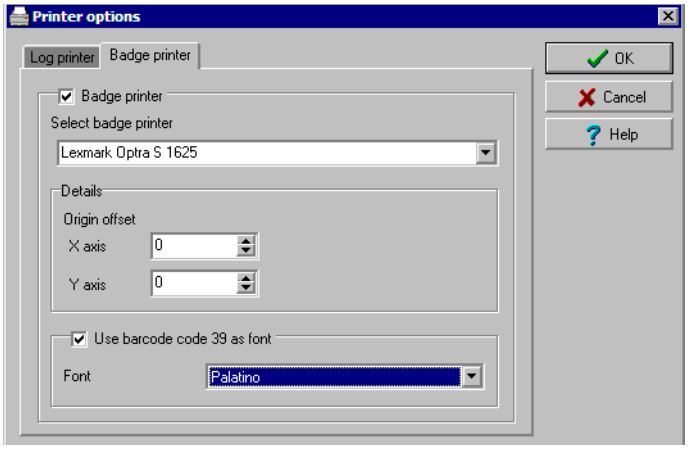
You may print badges from the Card menu, Visitor card menu, the DayPass menu or from all Badge preview windows. The software is set up to let you print one single or double-sided badges.

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 screen, 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, Visitor, and Daypass windows).

4 From the **Select badge printer** drop-down list, select the printer dedicated to badging.

5 Adjust the margins:

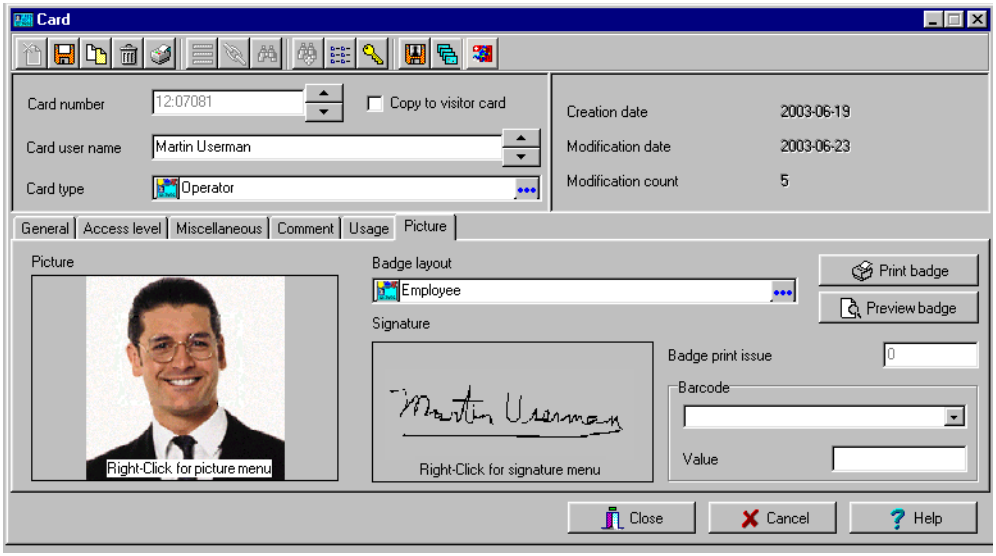
- Origin offset, X axis: indicates the left margin.
- Y axis indicates the upper margin.

Previewing and Printing Badges

The **Badge - Preview and Print** screen 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.

To preview badges:

1 From the Card, Visitor and Daypass windows, click the **Preview badge** button.



NOTE: *From the Badge design screen, 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 screen, choose a printing option:

- **Print front side**: only the front side (preview in the left pane) is printed.
- **Print back side**: only the back side (preview in the right 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.*

Designing Badges

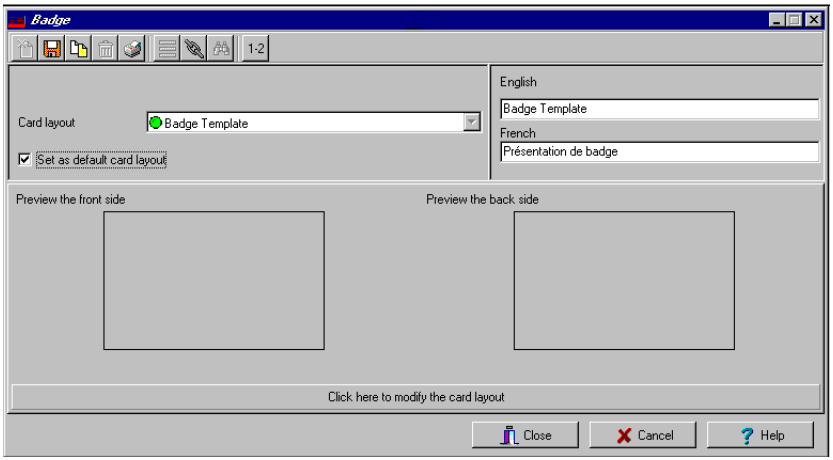
EntraPass contains a badge layout editor which enables users to create, save, edit or delete badge templates that are later selected and associated with cards for badge printing.

You can create and edit badge templates, add colored or graphic backgrounds, logos, text, barcodes, and place photo or signature holders.

Creating a Badge Template

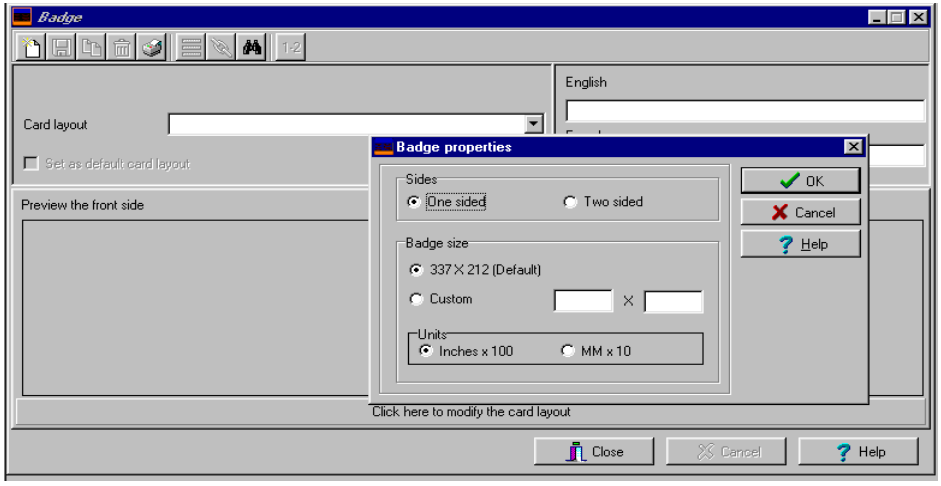
To create a badge layout:

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



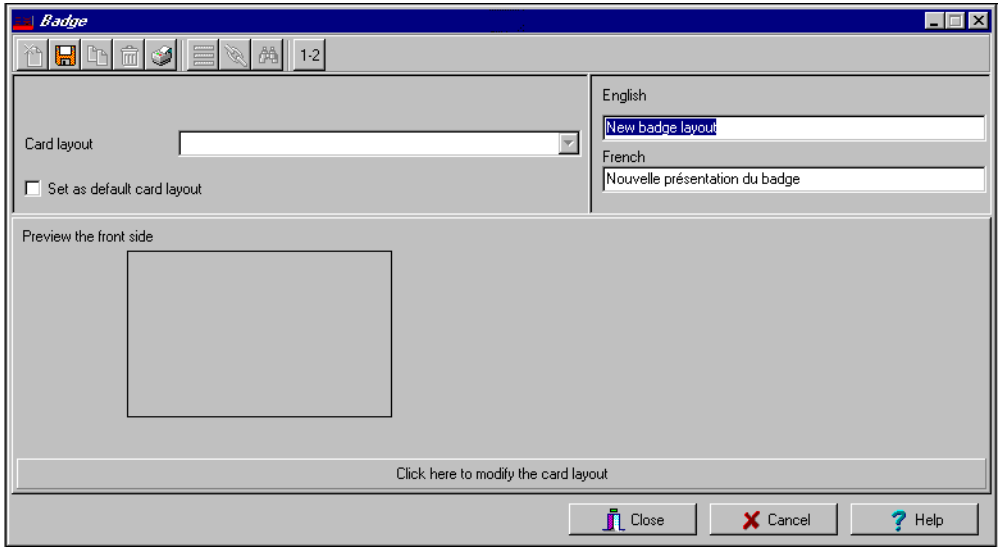
NOTE: *The Badge screen contains all the tools available in other EntraPass windows: new, save, copy, delete, print, links, search (the Hierarchy button is disabled). However, it contains an additional button* 1-2 *which allows to modify the number of sides assigned to a badge layout.*

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

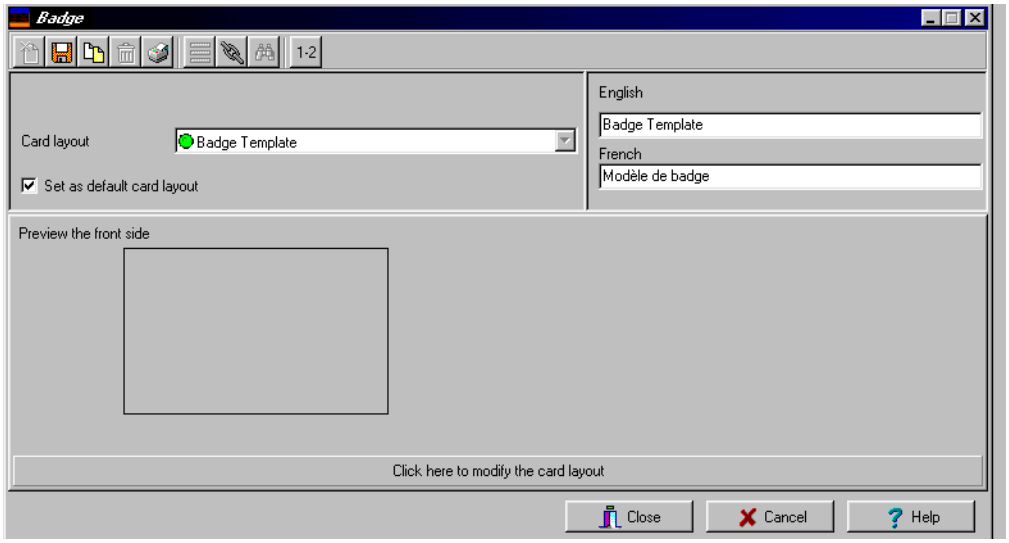


3 Indicate the number of sides for the badge, then select the desired size for the badge layout, then click **OK**.

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.*



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



5 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.*

6 Click the **Save** icon to save the badge template.

Editing a Badge Layout

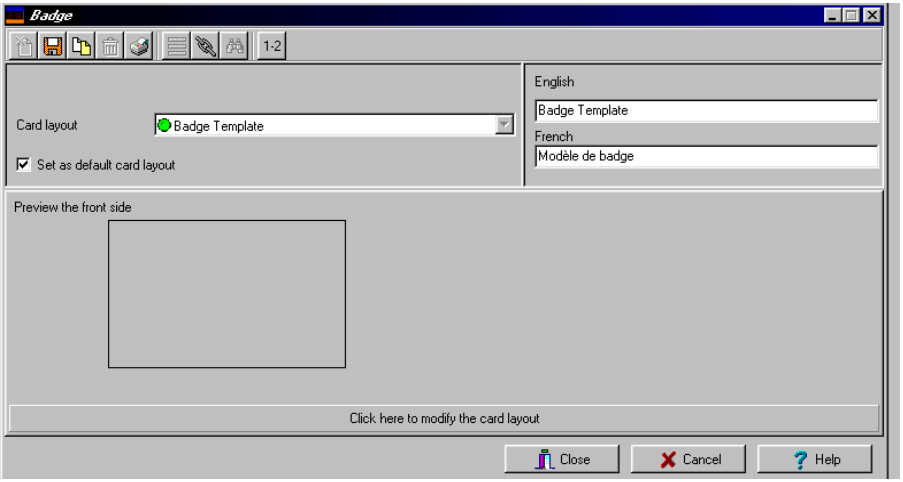
The Badge design utility allows users to edit the badge layout, to add background color or graphics, to modify the font, etc.

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 screen toolbar.*

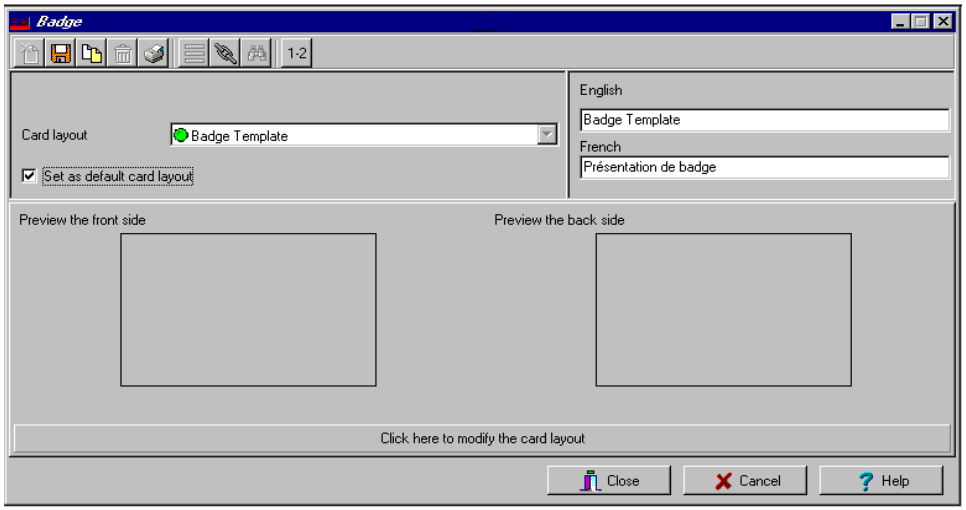
Modifying the Number of Sides

To modify the number of sides:

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



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

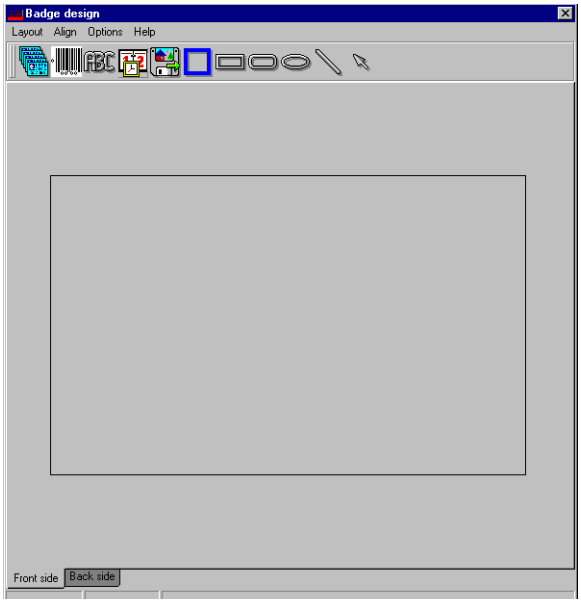


3 Click the **Save** icon to save the new badge information.

Modifying the background color

To modify the background color for your badge:

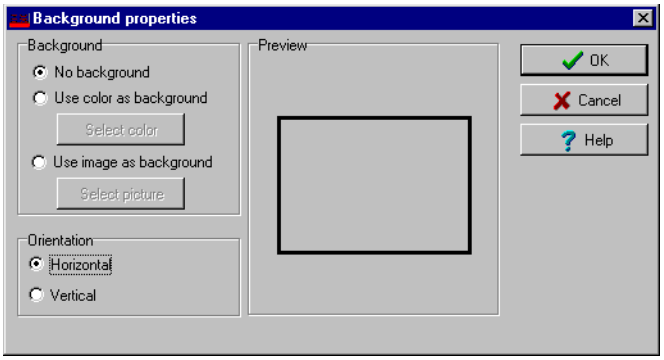
1. From the Badge window, select the badge you want to modify.
2. Click the **Click here to modify the card layout** button (located in the lower part of the screen) to open the Badge design screen.



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 screen 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

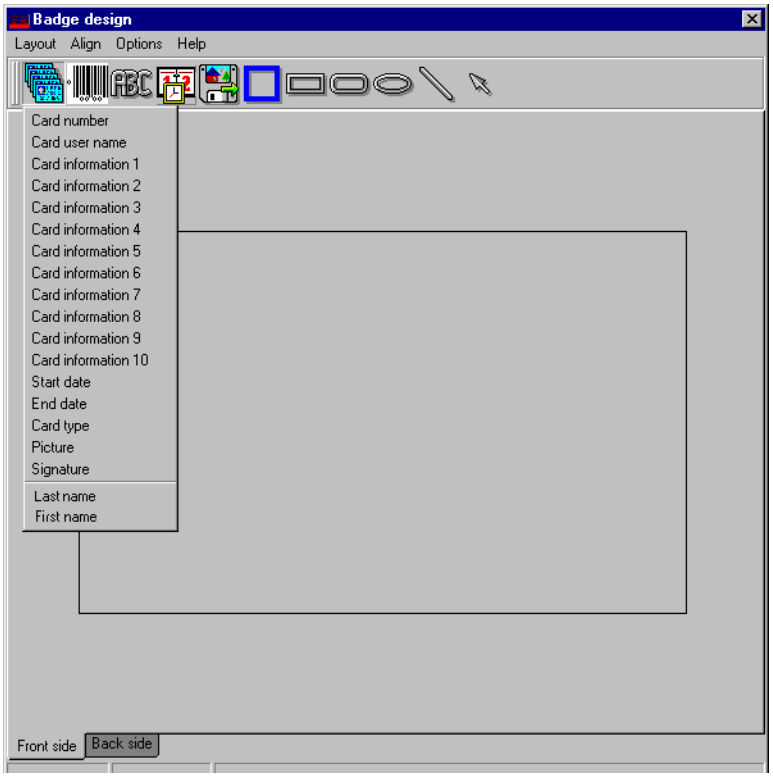
By a simple click and drop feature, the Badging utility permits you to incorporate objects into the badge template:

- 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.*

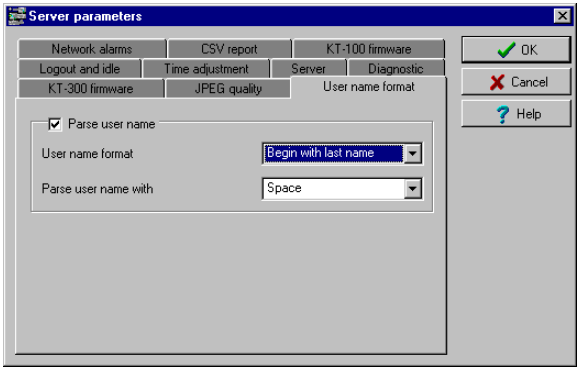
Incorporating Card Information Fields

1 To add card information fields to the badge template, click the **Card fields** icon. The **Card fields** submenu appears.

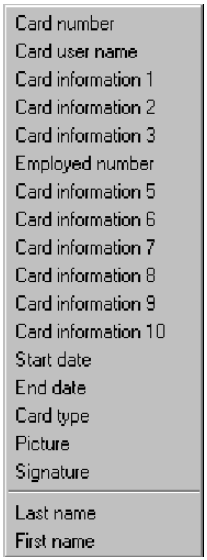


2 To modify an object property before you drop it, go to **Options** in the Badge design window, then choose **Show properties on drop**. If you do this, the Properties screen will open every time you drop an item in the template work area.

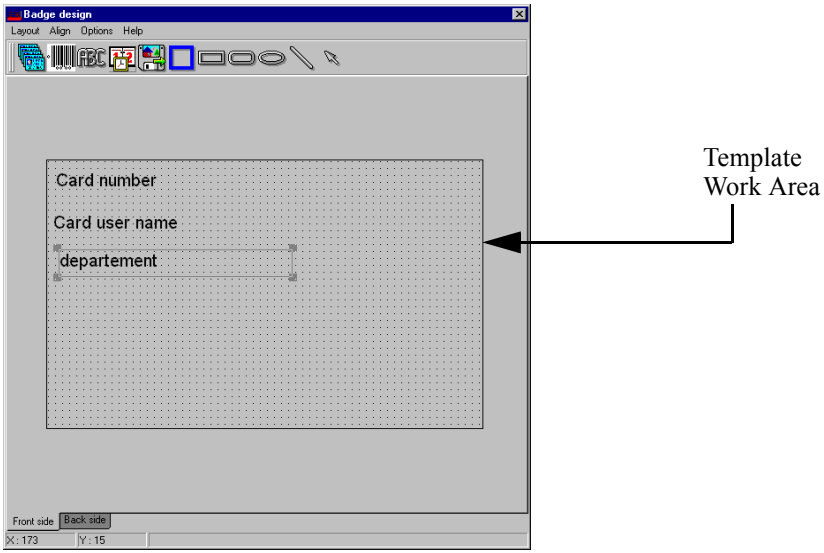
NOTE: *Icons may also be used to drag down information fields for barcode, text, date, pictures and border.*



NOTE: *To enable last and first name selection in the Card fields submenu of the Badge design window, go to the main* ***Options menu****, then choose* ***Server parameters,*** *click on the* ***User name format*** *tab and check* ***Parse user name*** *checkbox. For more information see "EntraPass Utilities (Options)" on page 359.*



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.



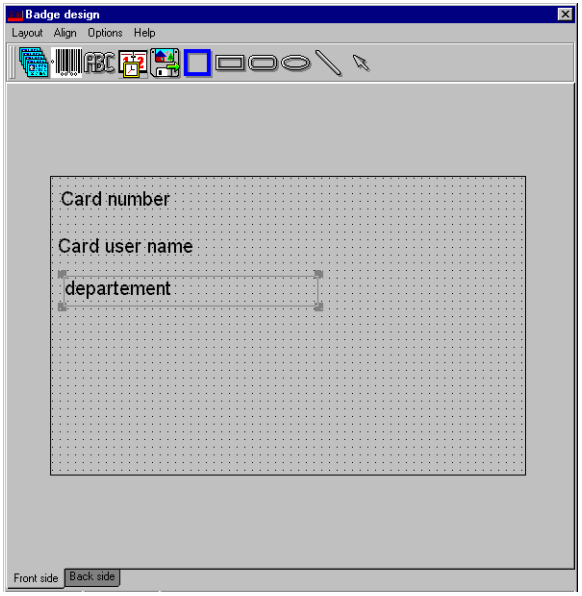
NOTE: *When you add a photo to a badge design template, the photo that appears is only a placeholder. It indicates where the cardholder's photo will be displayed. When a badge is assigned to a card, the appropriate cardholder's photo is displayed.*

Aligning Objects in the Template Layout

As you "click and drop" design objects in the template work area, they will not be properly aligned. The badging tool lets you align these objects, using the Align command.

To align items in the template:

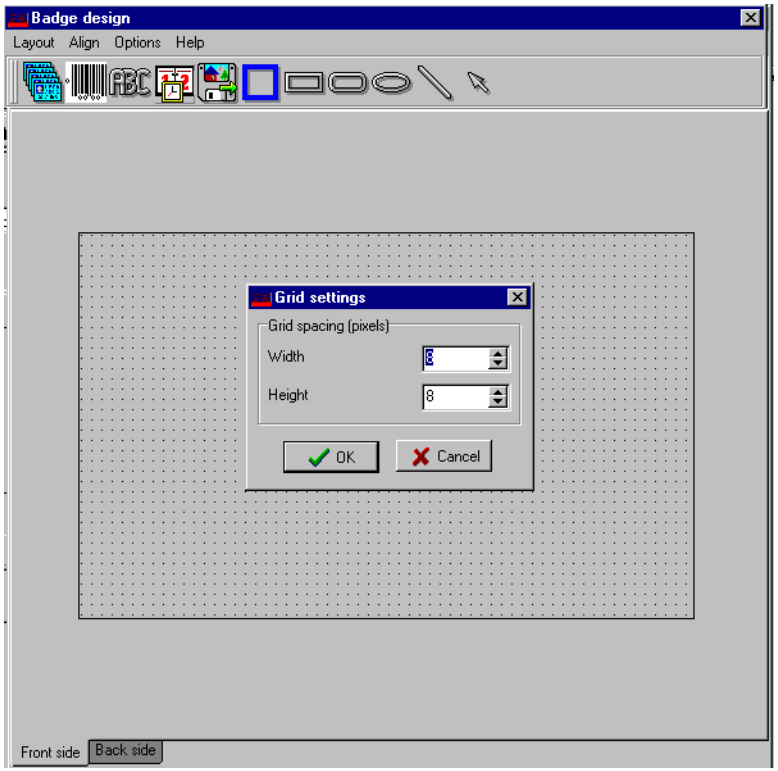
1 From the Badge design screen, select the **Align** menu, then select Show gridlines.



NOTE: *Grids assist you in aligning items in the badge layout template. It can be used as a visual aid to place items on gridlines. The* ***Snap to grid*** *option allows for more precise alignments of items. For example, when an item is moved close to a grid mark, it will be automatically aligned to the grid point.*

- **Show gridlines**: displays grid points to aid with object alignment.
- **Align to grid**: aligns all objects to the nearest grid point.
- **Grid settings**: allows you to specify the horizontal and vertical grid spacing (in pixels).

2 To adjust the space between the grid points, right-click the badge design work area to open the Grid settings screen.



3 Using the **Up/Down** arrows, select the desired spacing in pixels for the width and height, then click OK.

NOTE: *To disable the grid:* ***Align*** > ***Show gridlines***

Modifying Card Fields Properties

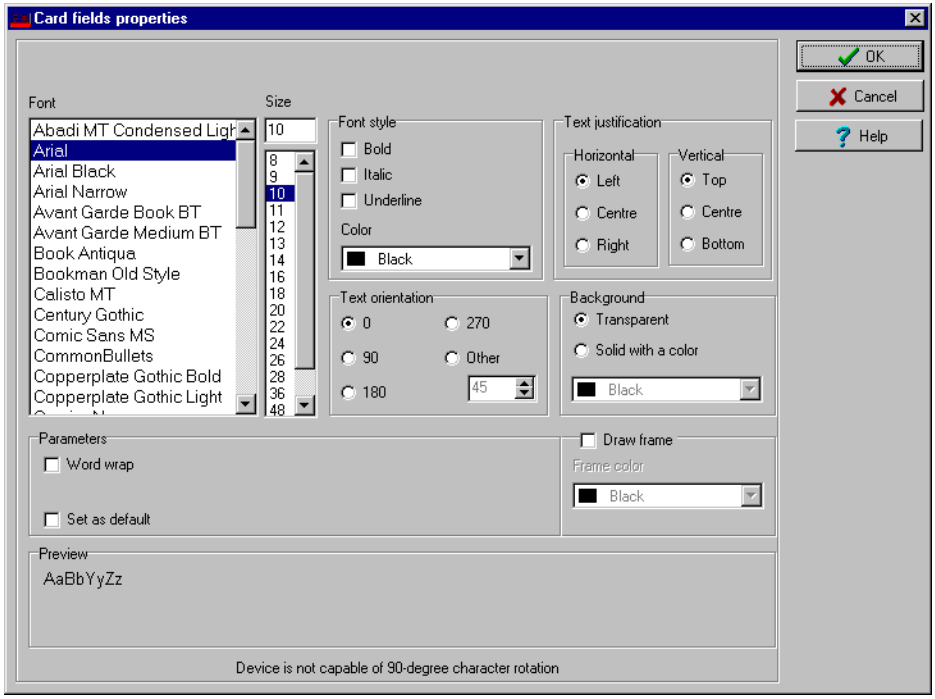
Objects are incorporated in the template with their default settings (font, color, etc.). You can modify the settings later. For example, you can modify the appearance of any text object, such as card field, static text, date, etc.

To modify an object (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 screen, 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.*

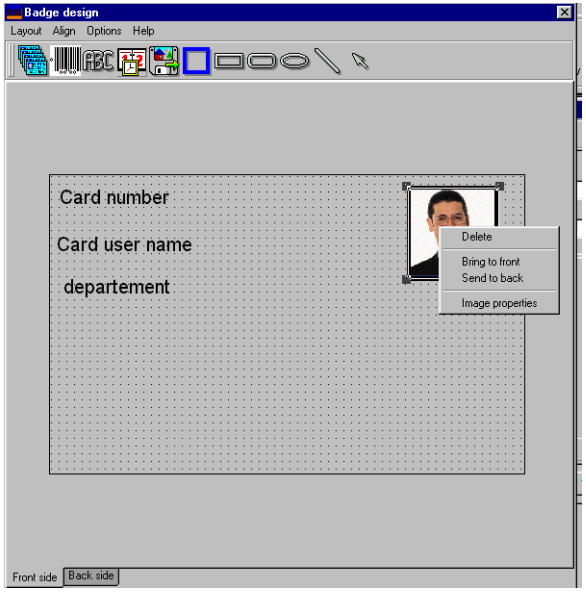
NOTE: *When Text Orientation is set to "Other" it is not possible to resize the field.*

Modifying Picture Properties

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

To modify the properties of a picture:

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.

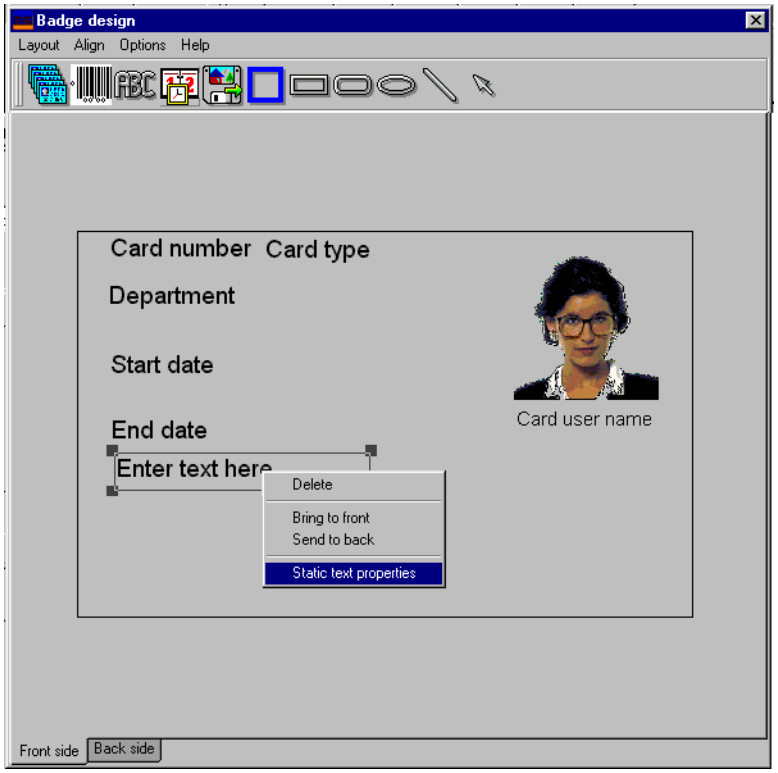
4 You may check the **Set as default** option if you want these properties to apply to all image objects you add in the badge template.

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.

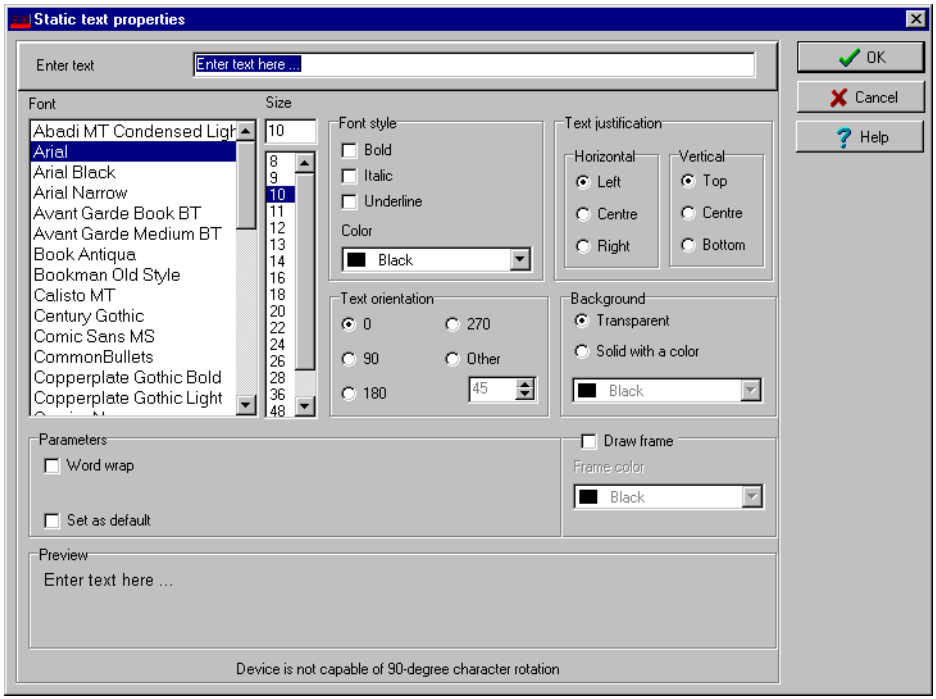
To add a static text box:

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 182.

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



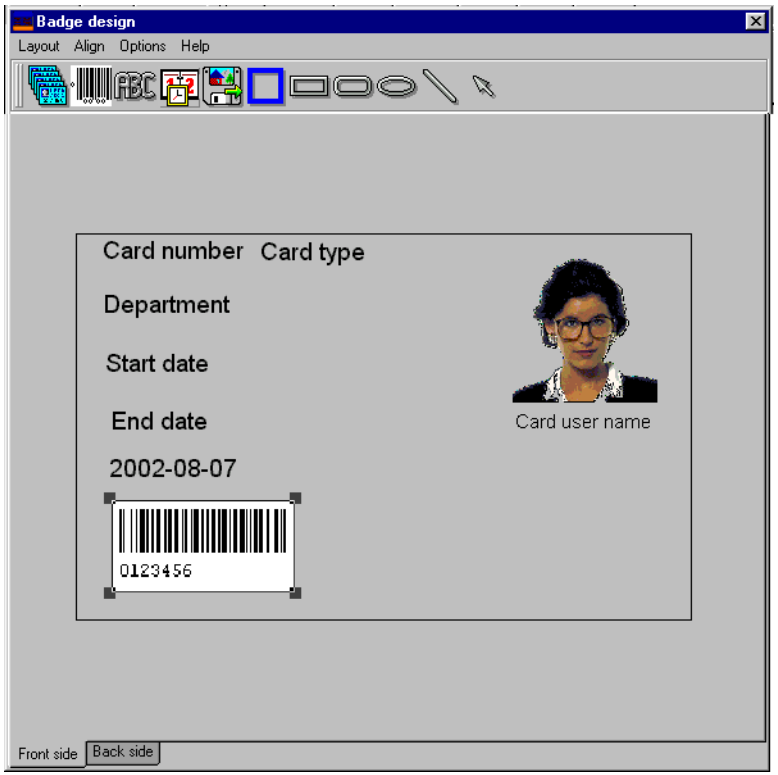
4 Enter text in the **Enter text** field; then modify the text properties as desired. The Preview section shows the result of the changes you apply to the text.

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.

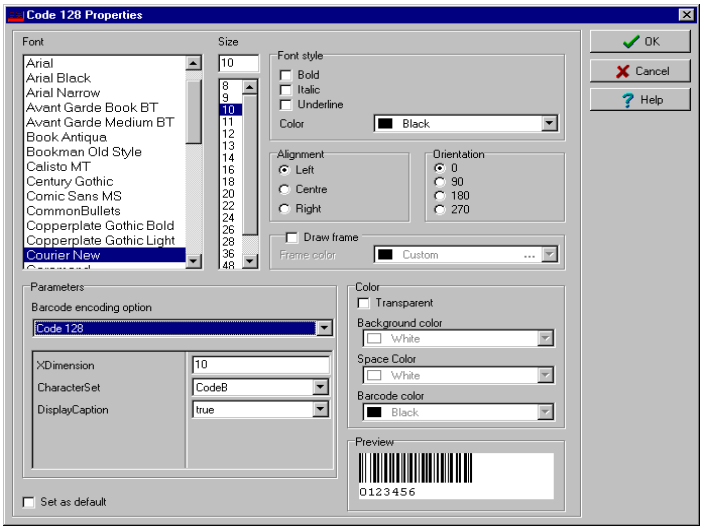
To add bar codes:

1 From the Badge design screen, 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 182.

3 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

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

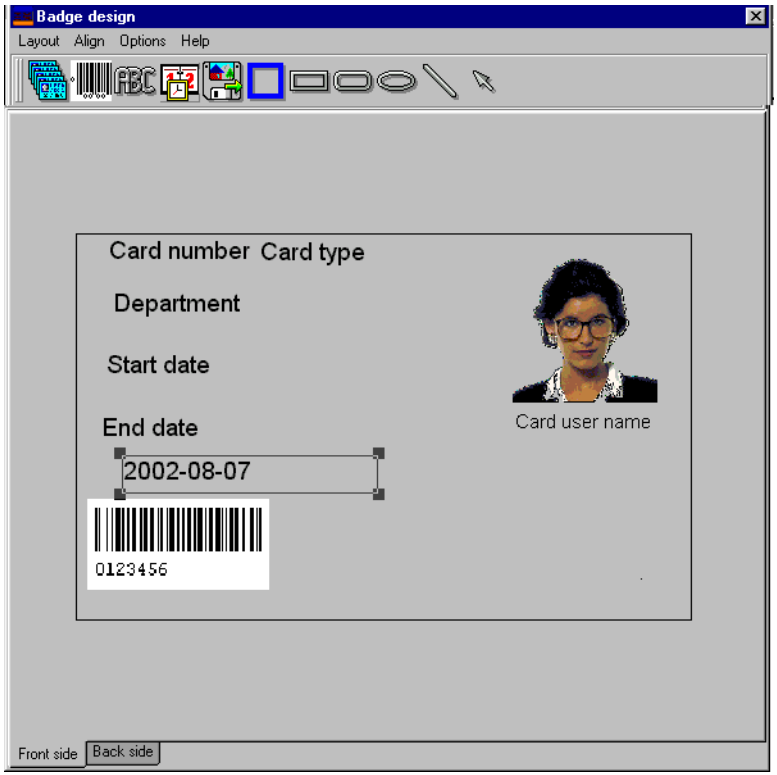
NOTE: *If it is necessary to set* ***Barcode encoding option*** *to Code 39-Modulo 43 set* ***Field Checksum*** *to true.*

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.

To Add the Current Date:

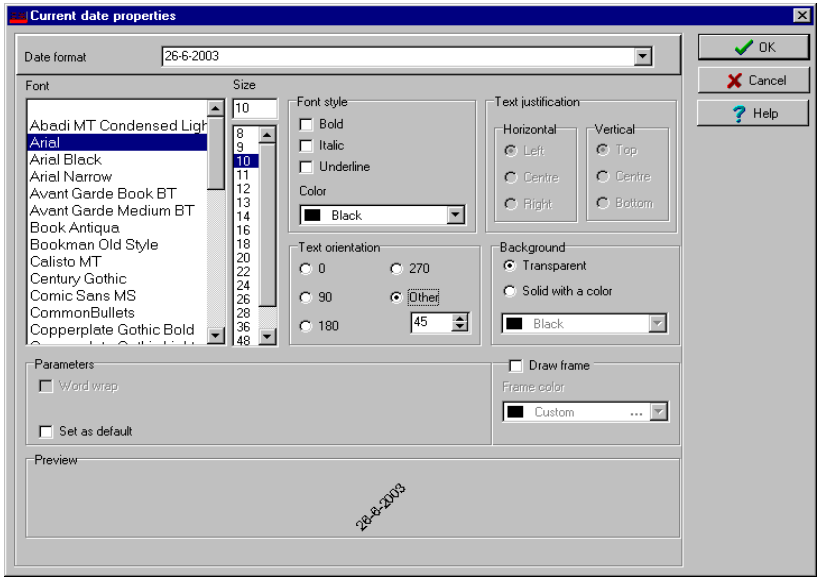
1 From the Badge Design template, select the **Current date** icon, then click in the Badge design work area.



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 182.

4 Select **Current date properties** from the shortcut menu.



5 From the Current date properties screen, you can:

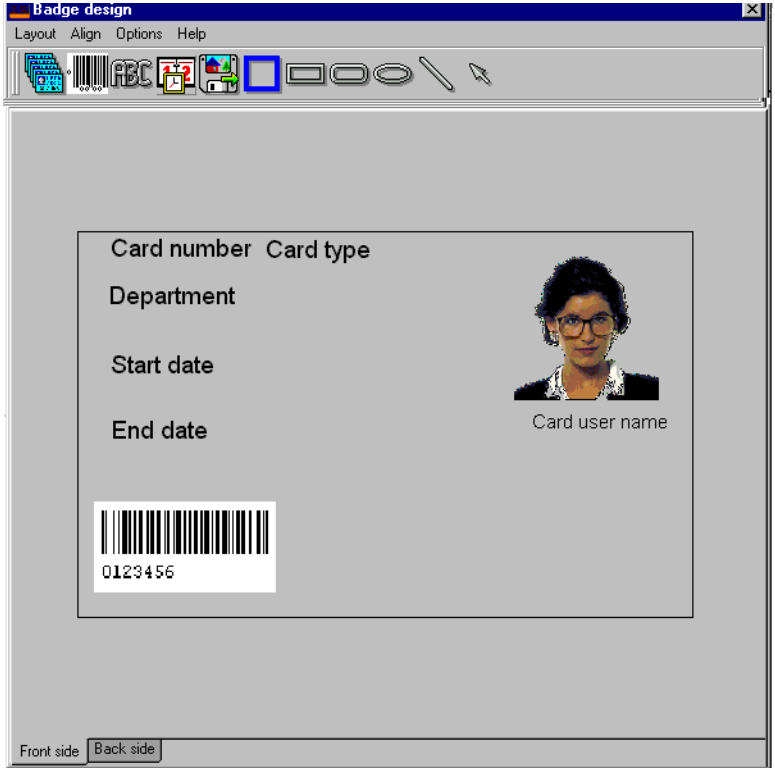
- Select the date format (top of the screen)
- Change the text properties: font, color, justification, orientation etc.

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.

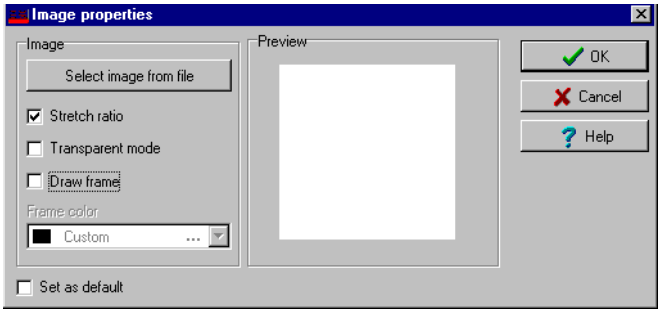
To incorporate an image into the design:

1 From the Badge design screen, select the **Picture** icon.

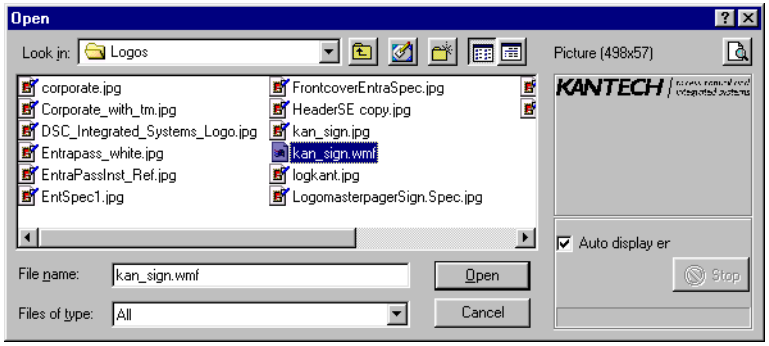


NOTE: The Badging feature supports most available image formats: BMP, JPG, EMF, WMF, GIF, PNG, PCD, and TIF.

2 Drop the **Picture** icon in the template work area. The Image properties screen appears.



3 Click the **Select image from file** button. The Open screen 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 position; you can use the grid to align it properly. For more information, see “Aligning Objects in the Template Layout” on page 182.

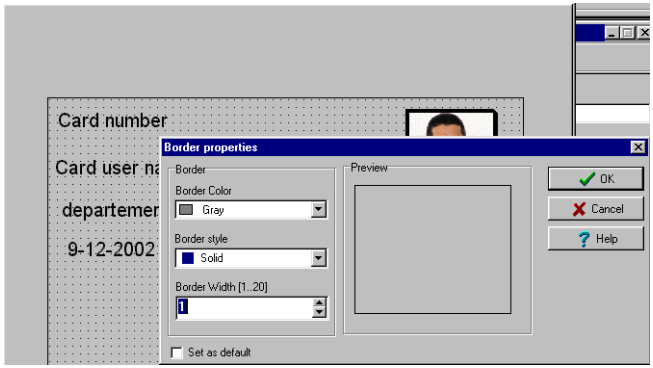
6 Right click the image to modify its properties. For details, see “Modifying Picture Properties” on page 186.

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.

To add a border, a pointer or a line:

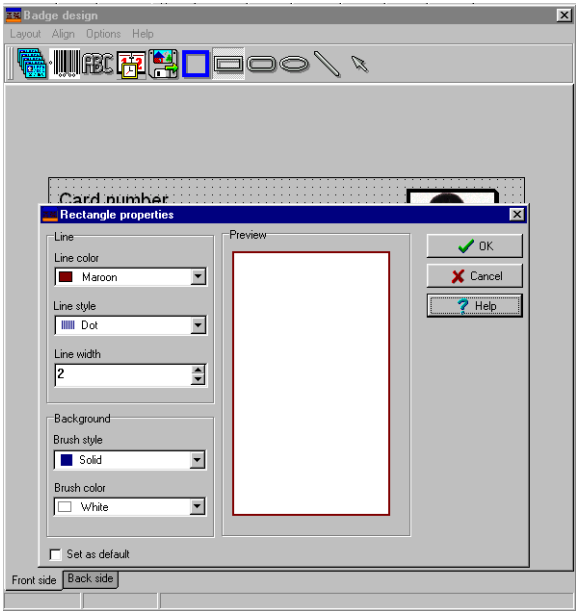
1 From the Badge design screen, select the object you want to add (next to the Diskette icon), then click in the Badge design work area" The Border properties screen opens.



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.

To place a rectangle:

1 From the Badge design screen, 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 screen, you may define the rectangle properties before importing it:

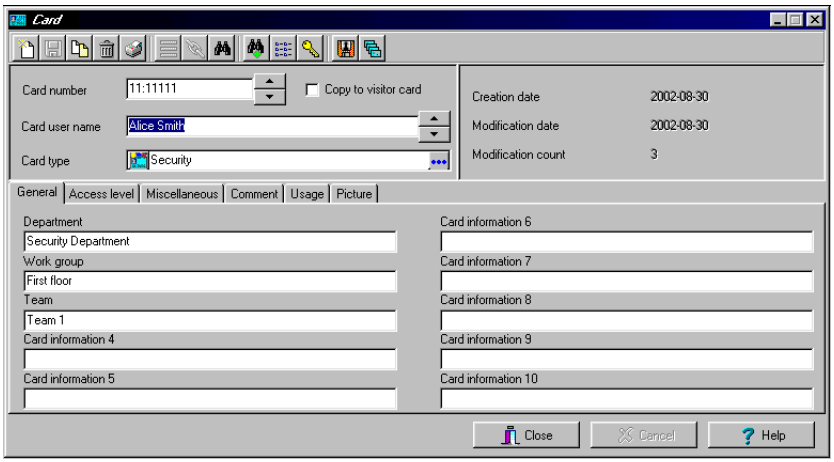
- Line color,
- Line style,
- Background (brush style and brush color).

Validating Card Access

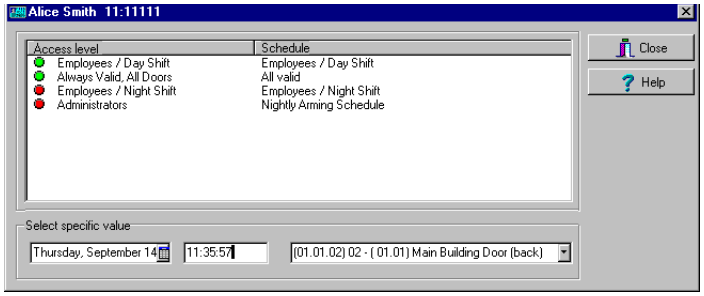
The Validate card access feature lets you view access levels that are assigned to a particular cardholder.

To validate user access:

1 From the Card screen, select a card.



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



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).

Printing Cards

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.

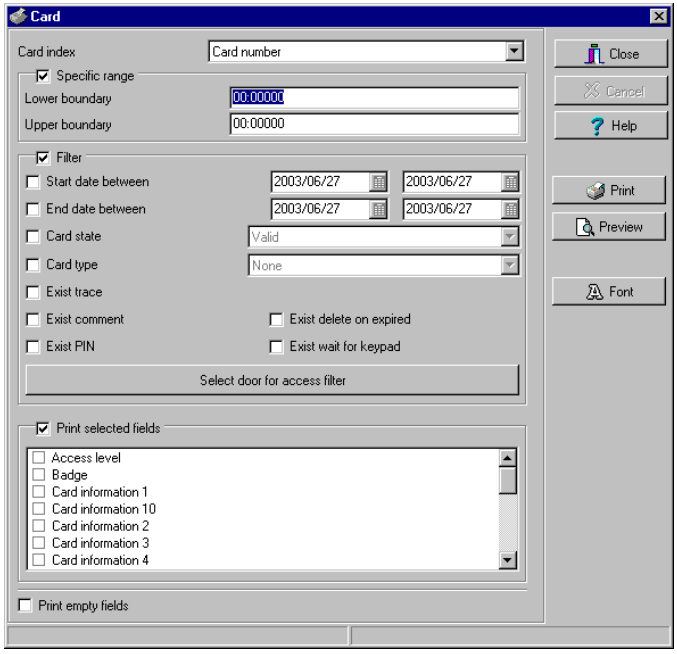
You can preview your list so that you can modify or verify the settings (fields) before printing.

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 screen, click the **Printer** icon.



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.

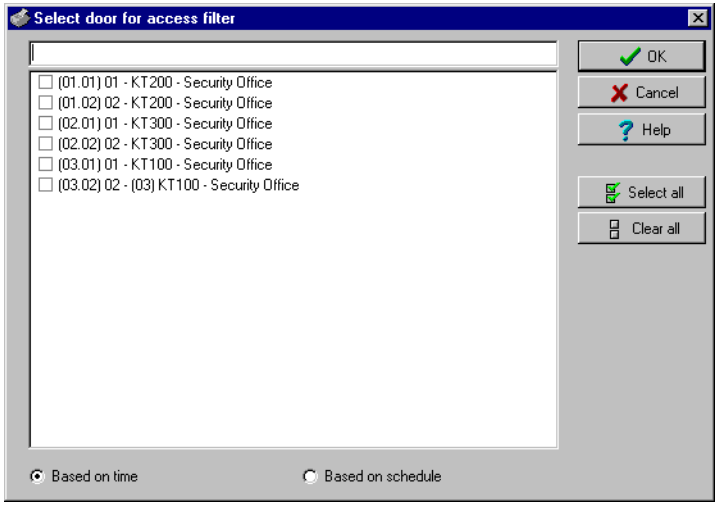
NOTE: *Only cards that match ALL the selected filters will be printed. For example, if you specify six filters, all the six criteria must be met. Cards that do not match all the six criteria will not be included in the range.*

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 screen (Miscellaneous tab).
- **Card type**—Check the option and then select the desired card type. The system will include cards that have this card type selected in the Card screen.
- Select the **Exist trace** for the system to include cards that have the "Card Trace" option in their definition (Card screen, Miscellaneous tab).
- Select the **Exist comment** option for the system to include cards that have information in the **Comment** field in their definition (Card screen, 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 screen, Miscellaneous tab).
- Select **Exist wait for keypad** for the system to include cards that have information in the **Wait for keypad** field (Card screen, Miscellaneous tab).

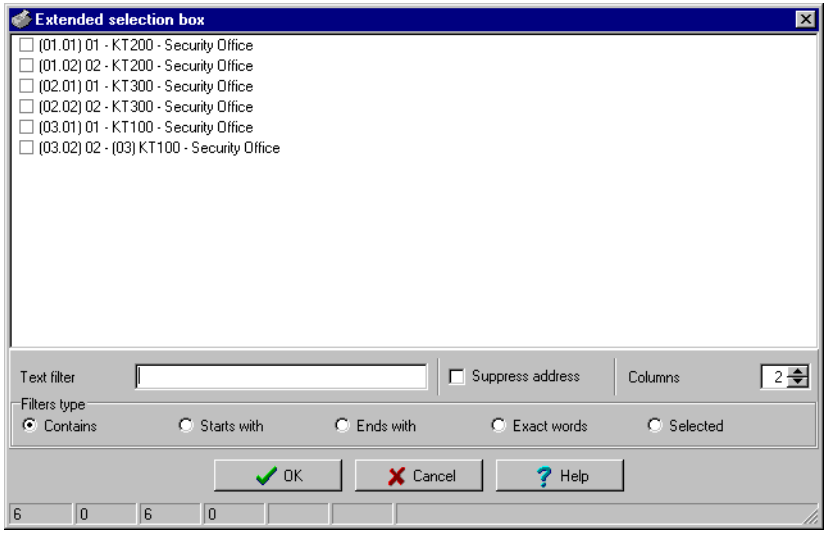
5 You may also check the **Print selected fields** to include specific data. If you select this field, no other fields below, the system will print the cards that match the filters you specified above with the card number and user name only.

6 Click the [Select door for access filter] button if you want to include cards associated to a door.



7 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.*



8 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 screen to preview your report.

Viewing Last Transactions

The **View last transactions** feature lets you view the most recent transactions for the selected cardholder. For example, the screen 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.

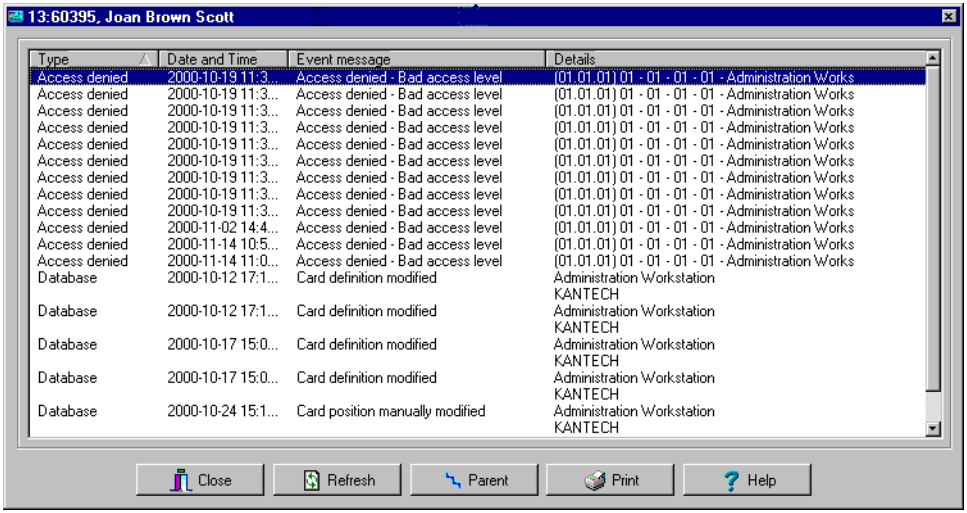
The system displays the 15 most recent transactions for each category:

- 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 screen, select the **View last transaction** icon.



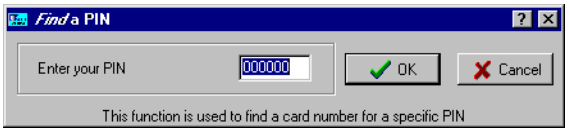
13:60395, Joan Brown Scott

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 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - 01 - Administration Works
Access denied	2000-10-19 11:3...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - 01 - Administration Works
Access denied	2000-11-02 14:4...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - 01 - Administration Works
Access denied	2000-11-14 10:5...	Access denied - Bad access level	(01.01.01) 01 - 01 - 01 - 01 - Administration Works
Access denied	2000-11-14 11:0...	Access denied - Bad access level	(01.01.01) 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 to the server (and to the authorized workstation) 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 list the workstation from which the card was modified as well as the operator name.
- **Refresh**—This button can be used to refresh the screen 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 40.
- **Print**—Use this button to print an exact copy of the screen. For more information, see "Basic Functions" on page 40.

Select your own PIN

If you want to select a specific PIN, you have to use the "find a pin" button.



1. Enter the desired PIN and system displays the card number that is associated to this PIN.
2. Note the card number on a piece of paper.
3. Click on "New".
4. Enter the card number and save.

Defining Card Access Groups

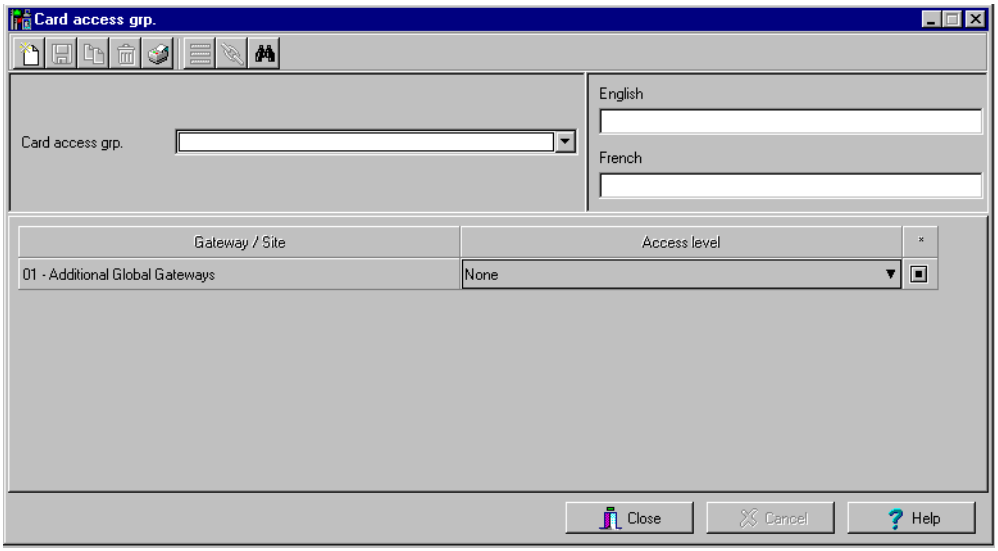
Pre-programmed card access groups allow quick selection of access levels for various sites of the system. This card access group can be recalled during card programming instead of re-entering the access levels for each site.

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.*

To create Card access groups:

1 From the card definition screen, 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 primary access level that will determine the access to the doors of the selected site.

Defining Access Levels

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.

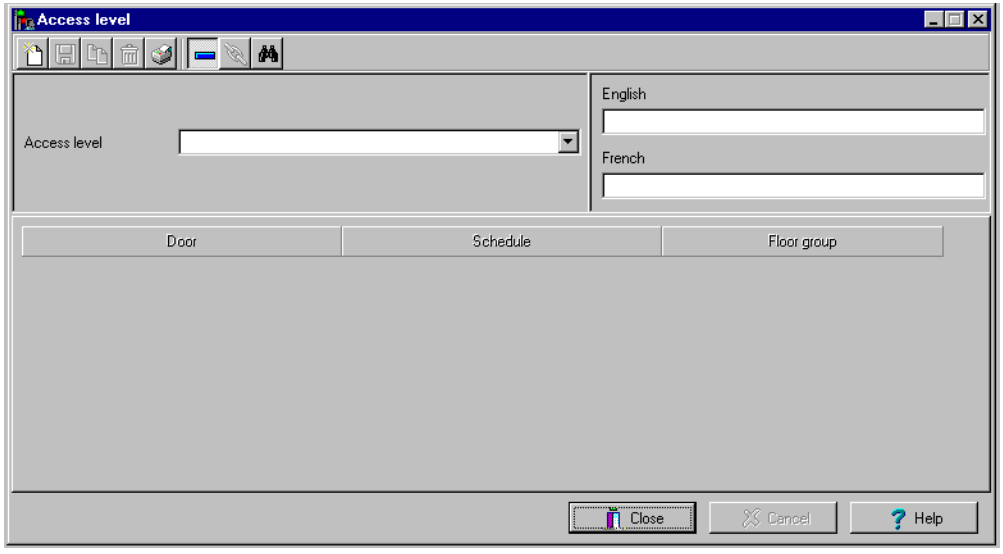
In order to assign an access level to a card, you have to:

- 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.*

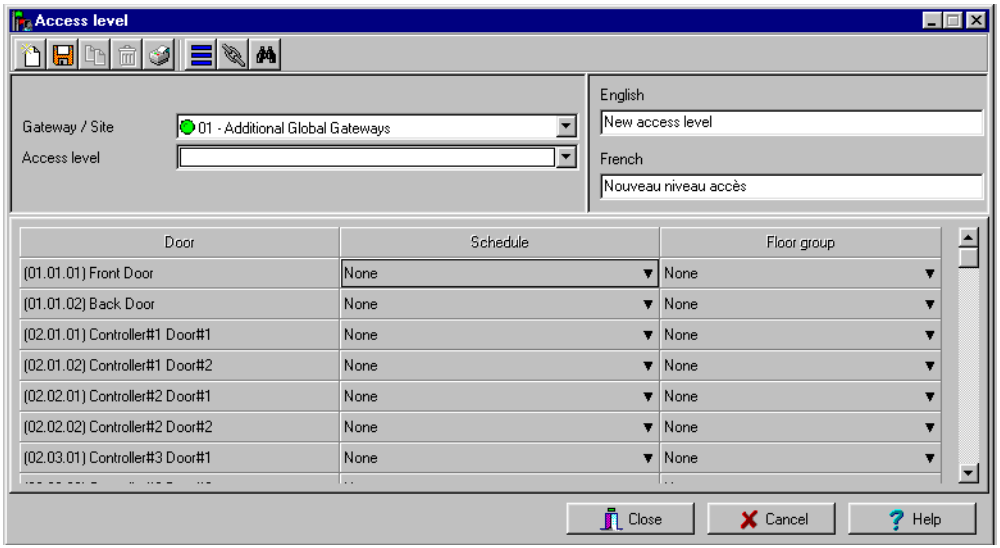
To define access levels:

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



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.

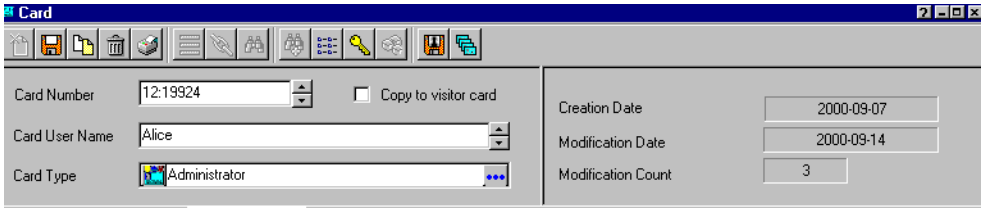
Defining Visitor Cards

A visitor card is issued on a temporary basis. It serves as a template for entering user information. You can create visitor cards in two ways:

- Copying the card information field into the Visitor card database when a new card or a daypass is created in the system,
- Creating a new visitor card.

To create a visitor card when creating a new card:

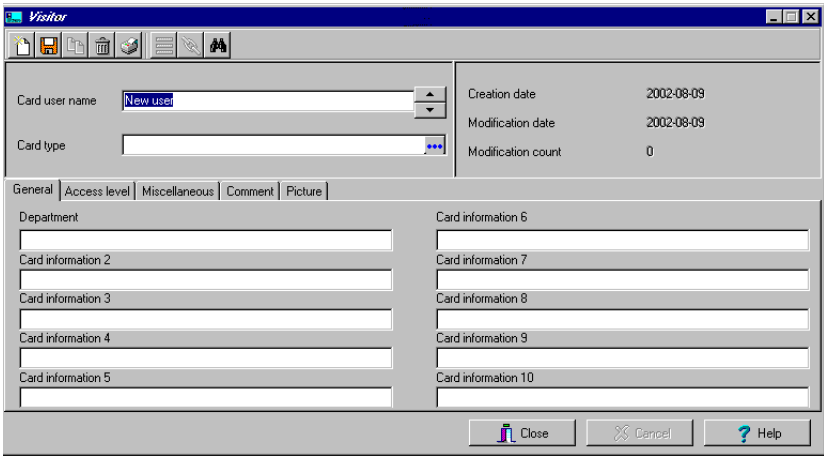
1 Select the **Card** icon from the Users screen. The Card window appears.



2 Check the **Copy to visitor card** option. The card information will be used later for creating new cards and issuing day passes.

To create a visitor card using the card template:

1 Select the **Visitor card** icon from the Card window toolbar.



2 Enter the required information in the **Visitor card** fields.

NOTE: *For more information on Day Passes and Visitor cards, see "Defining Cards" on page 150. The Picture tab allows you to display the cardholders picture and signature as well as to preview and print badges.*

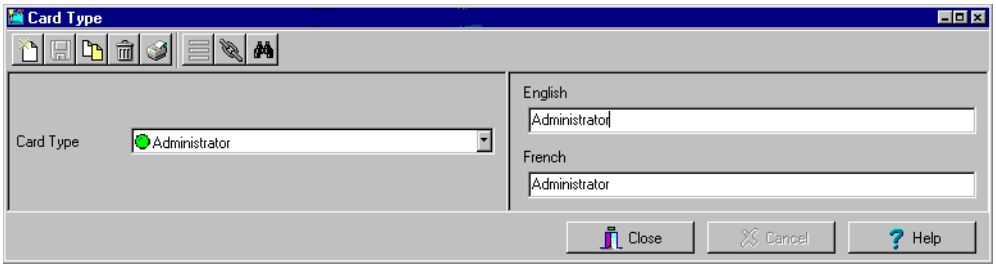
Defining Card Types

A card type is used to group cardholders and can later be used to modify an existing card group or to create reports. It can also be used to restrict access to card information for a particular operator. For example, you can restrict an operator's ability to issue or view a specific card group. For instance, if a card type is defined as "Administrators", an operator who does not have the appropriate security level will not be able to issue, view, modify, delete, or print this type.

NOTE: *The system is preset with five card types: administrator, employee, security, maintenance and visitor.*

To create a new card type:

1 From the Users menu, click the card type icon. The Card type screen appears.



2 In the Card type screen, click the "New" button in the toolbar and enter the necessary information in the language section.

3 To assign a card type to a cardholder, see "Users" on page 149.

Defining Day Passes

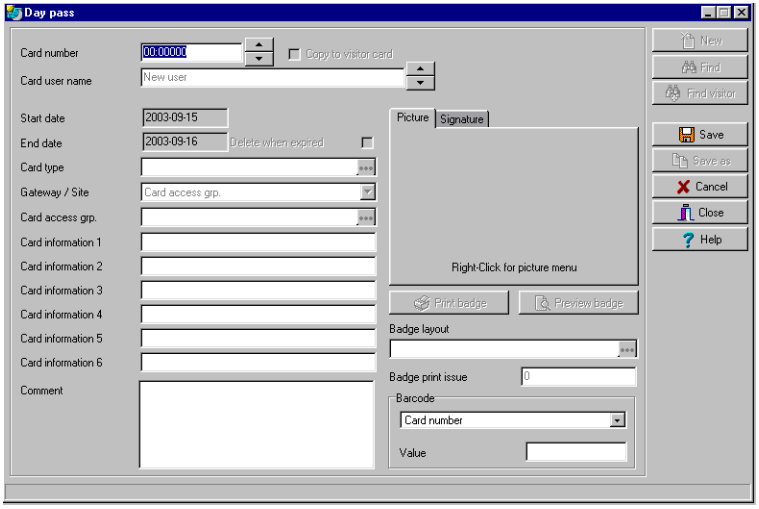
A day pass is issued to visitors such as contractors, employees from different divisions, customers, etc. This menu option offers an easy way to allow access to “visitors” for a single day.

Even if the day pass cardholder does not return the day pass card, the card will expire the same day at 24:00, and will no longer grant access.

You can use profiles that were copied to the “Visitor definition” menu to create day passes (use the “find visitor” button).

To create a day pass:

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



2 You can fill out the displayed fields or browse the card databases to the desired card. For more information, see “Users” on page 149.

3 Check the Copy to visitor card option if you want to save this day pass in the visitor database.

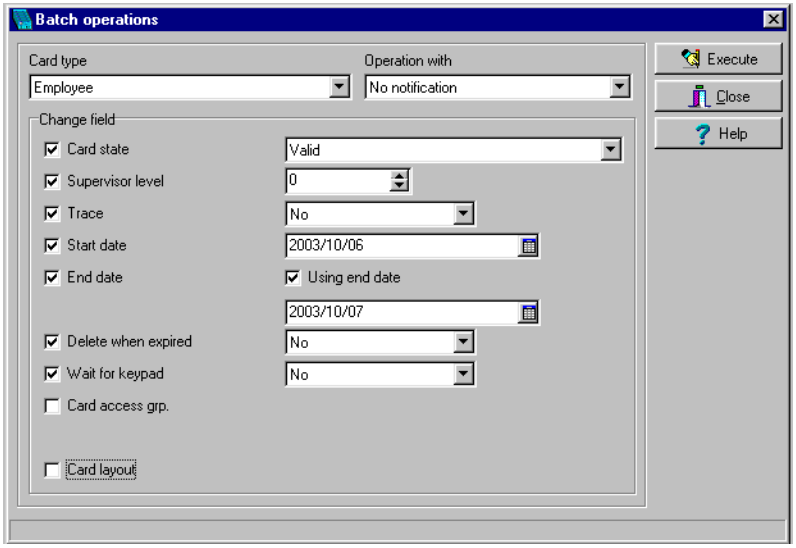
NOTE: *For more information of visitor cards, see “Defining Cards” on page 150. The Picture tab allows you to display the cardholders picture and signature as well as to preview and print badges.*

Batch Operations on Cards

This menu is used to modify a specific card type group. For example, you could modify the “end date” of all the cards assigned the “administrator” card type. Individual fields will appear only when the appropriate check box is checked.

To perform operations on a group of cards:

1 From the Users menu, click the **Batch operations** icon.



2 Select a user group from the **Card type** drop-down list. All cards having this card type will be modified.

3 Select the appropriate option from the **Operation with** drop-down list.

- **No notification**—The system will not notify nor request confirmation from the operator.
- **Notification**—The system will display a screen displaying the process.
- **Notification and confirmation**—The system will display a screen displaying the process and will prompt operators to confirm the operation for each cardholder having the selected card type.

4 Check the option you want to modify for the selected type.

- **Card state**—If a card state is selected, the system will assign this new card state to all the cardholders of the selected card type.
- **Supervisor level**—If supervisor level is selected, the system will set levels according to according to screen values.
- **Trace**—If trace is selected, the system will trace all cardholders of the selected card type.

- **Start date**—If a start date is selected, the cards will be valid only from this start date. This new date will be assigned to all cardholders having the selected card type.
- **End date**—If an end date is selected, the cards will be invalid after this end date. This new date will be assigned to all cardholders having the selected card type.
- **Delete when expired**—If selected, the cards will be deleted when the end date specified in the Card Definition menu is reached.
- **Wait for keypad**—If selected, all the cardholders of the specified card type will have to enter their PIN at the keypad after a valid card read, in order to permit access to the door (if keypads are defined).
- **Card access group**—If checked, four options are provided to modify card access groups.
  - Replace card access group.
  - Update card access group.
  - Add new access level.
  - Update add access level.

5 Click the **Execute** button to start the process. The system will prompt you to accept the operation.

6 Click **Yes** if you want to continue.

Importing/Export CSV Files

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 for the two application 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 user 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).*

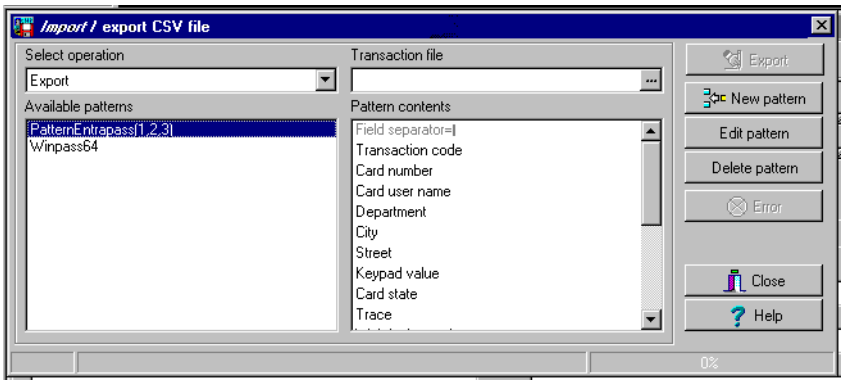
To import/Export card information, you may use Kantech pre-defined patterns or you may create your custom patterns. Two patterns are available: the EntraPass (1,2,3) and the WinPass 64 models. You may use the Kantech template “as is” or you may edit it.

Using 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.

To use a predefined template:

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.

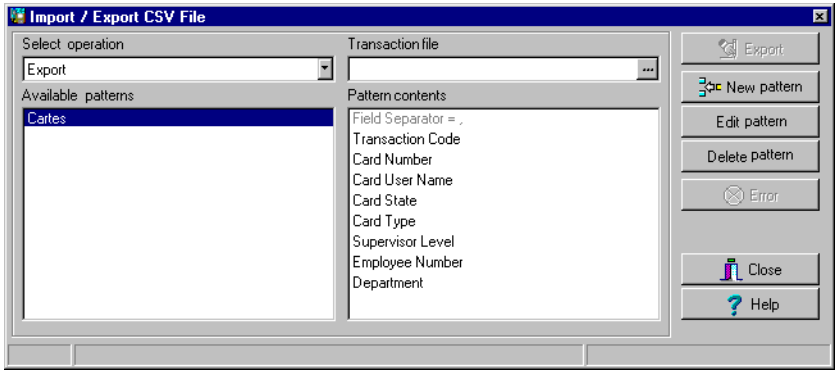
4 Use the **Edit** button if you want to edit the pattern.

Creating a New Pattern

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

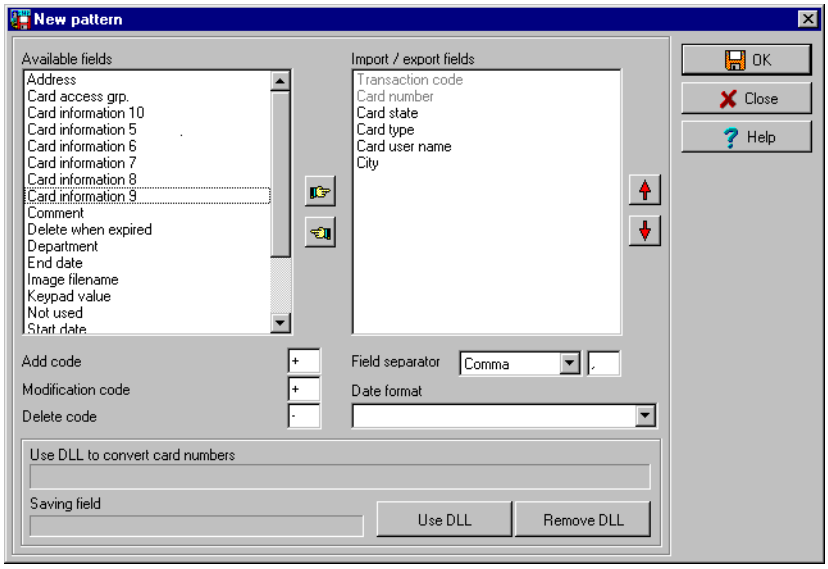
To create an import/export pattern:

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



2 From the Import/Export CSV file screen, click the **New pattern** button. The New pattern screen 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 “+”.

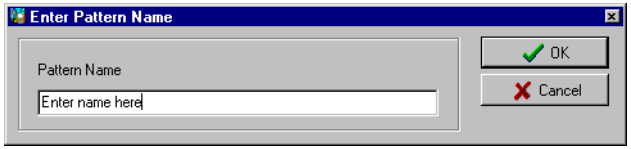
5 Select the **Delete code**. This code is used by the system to identify, when importing a file, which card has to be removed from the card database. Default delete code is “-”.

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 screen 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 screen. The pattern you have just created is displayed in the **Available patterns** list.

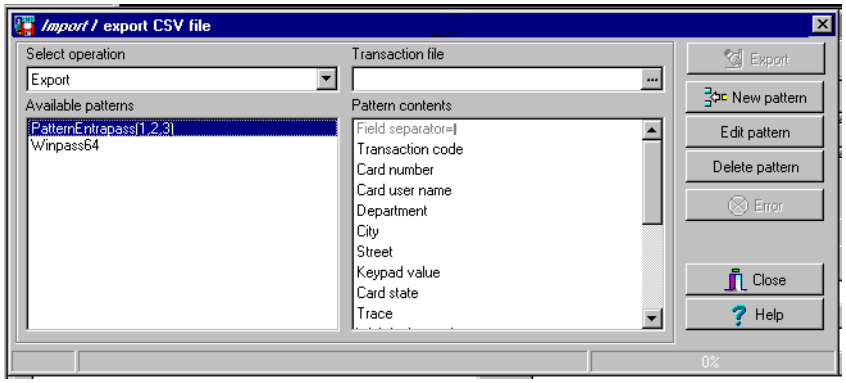
10 If you want to add or remove fields from your pattern, double-click the new pattern to edit and make the necessary modifications. Now you can import or export your information using the new pattern you have just created.

Exporting 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.

To export data:

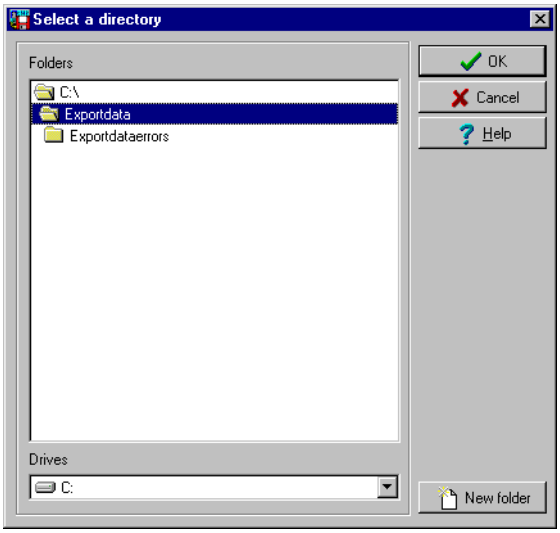
1 From the Users menu, select the **Import/Export CSV File** button. The system displays the Import / Export CSV file screen.



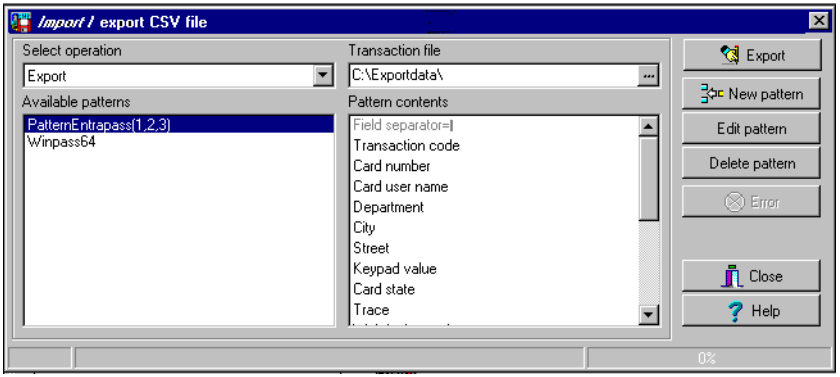
2 From the **Select operation** drop-down list, select **Export**.

3 From the **Available patterns** list (left 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 “Creating a New Pattern” on page 214).

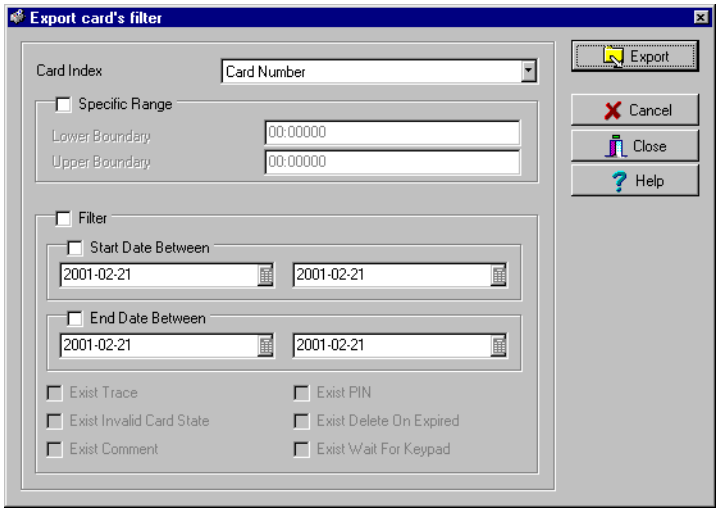
4 From the **Transaction file**, select the folder in which EntraPass will save the card database content. You can open the CSV file in Excel, Notepad, etc.



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

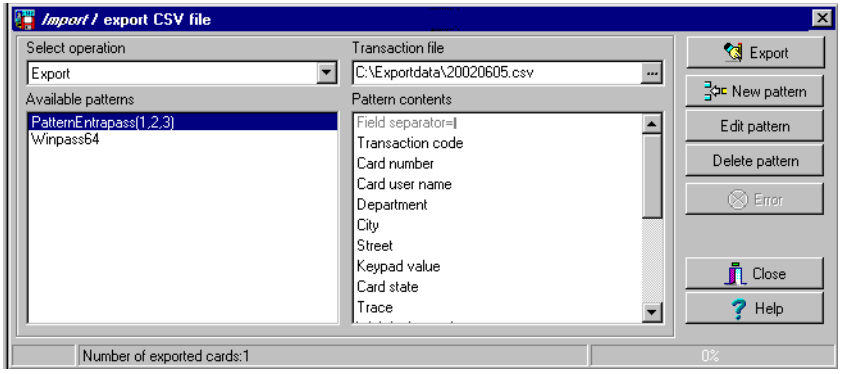


6 Click the **Export** button; it is enabled once the transaction file is selected. The system displays a screen allowing you to filter the cards you want to export.



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.*

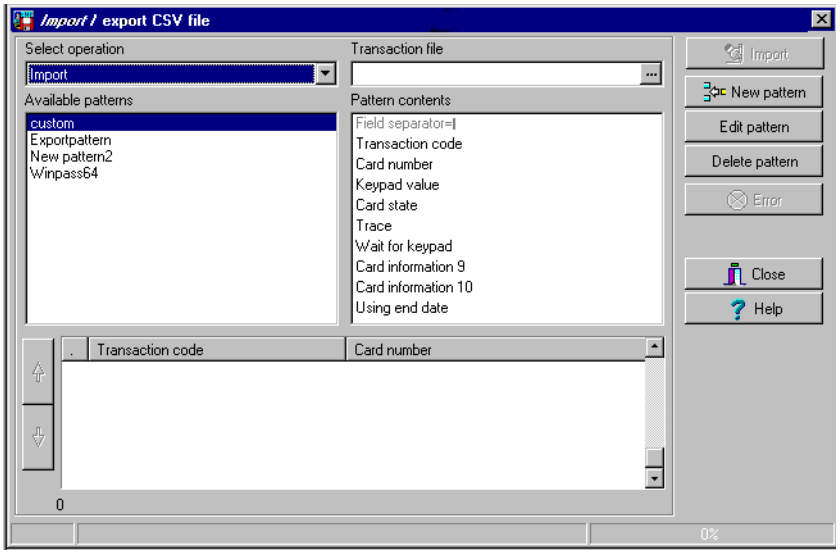
7 In the Export Card's filter screen, specify the cards you want to export. Once you have made all your selections, click the **Export** button. The Import / Export CSV file screen appears.



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 screen), 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.*

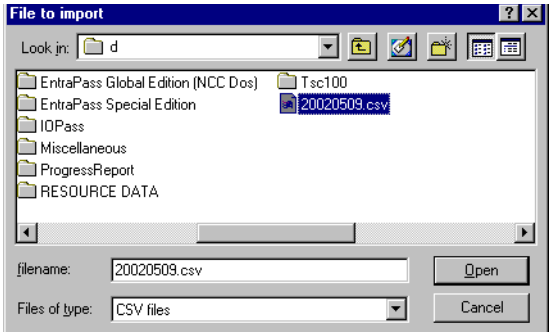
Importing Cards

1 From the **Users** menu, select the **Import/Export CSV File** icon. Then select Import from the **Select operation** drop-down list.

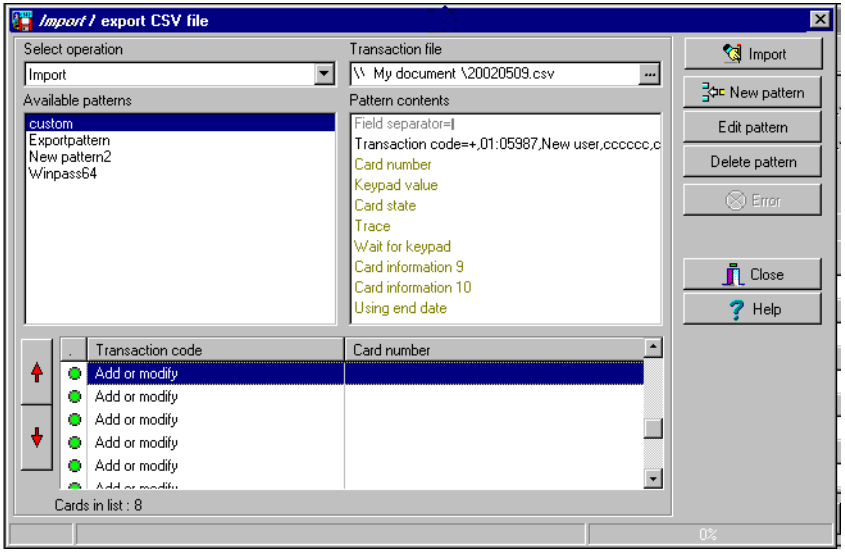


2 From the **Available patterns** list, select the pattern that will be used to import the cards information (for more information on how to create a pattern, see “Creating a New Pattern” on page 214).

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 screen 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 the **Import** button to complete the operation.

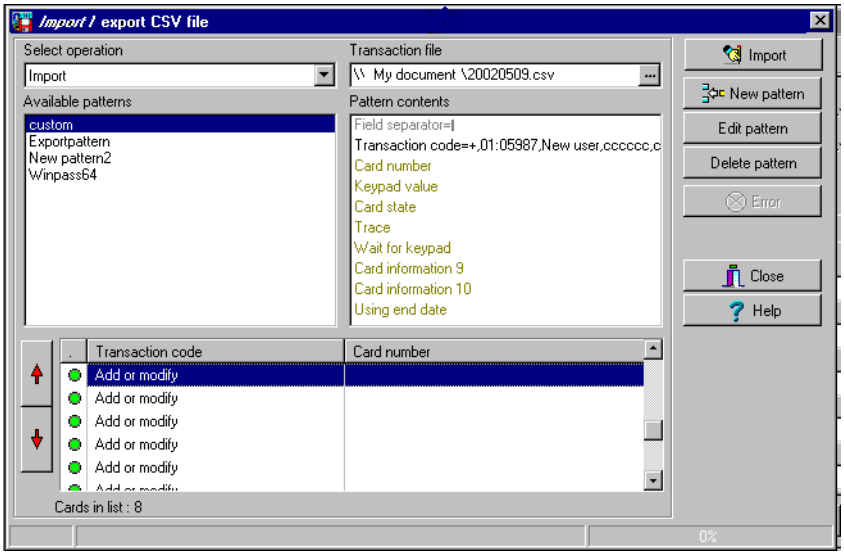
Correcting Import/Export Errors

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.

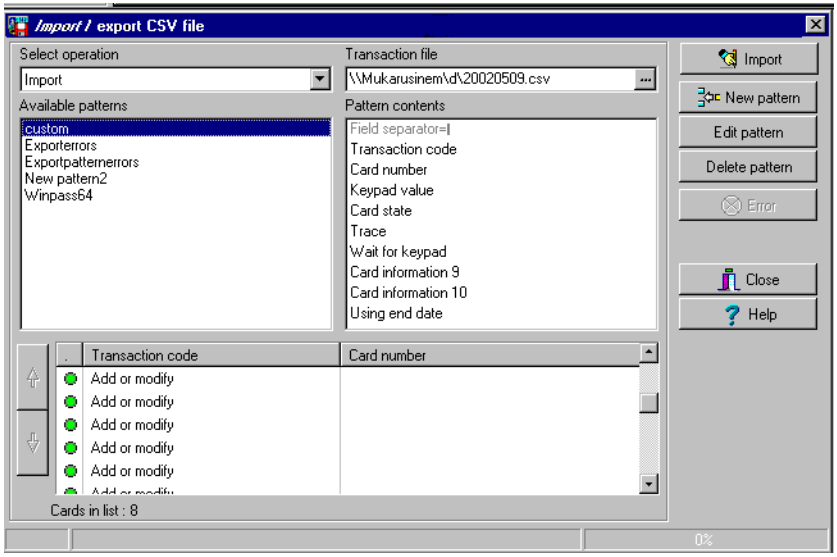
To correct import/export errors:

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 screen displays the number of cards in the list.



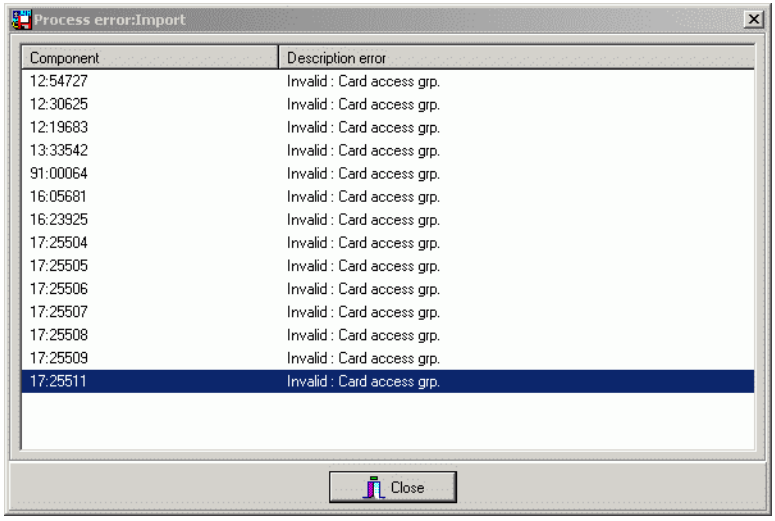
NOTE: *Although entries in the* ***Transaction code*** *column are identified with a green flag, the* ***Card number*** *column is empty. This indicates problems in the pattern conversion.*

2 Click the **Import** button.



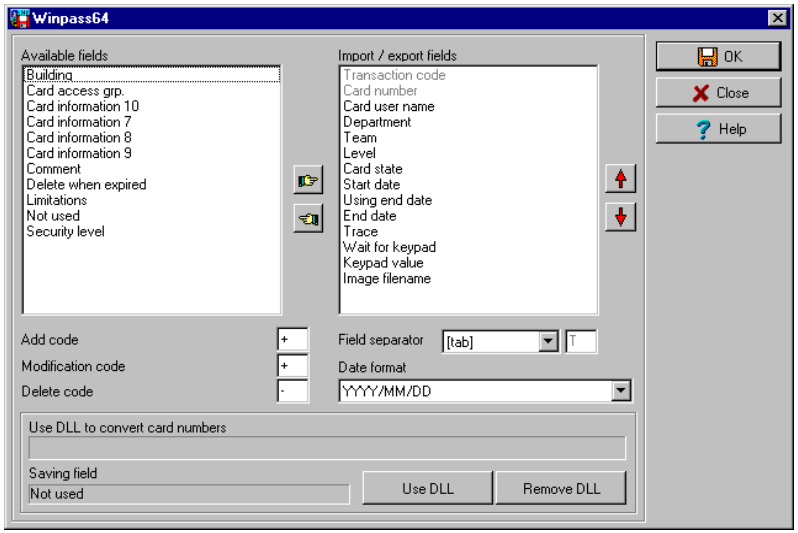
NOTE: *The **Error** button is enabled because the system encountered problems during the import transaction.*

3 You may click the **Error** button to display information about the error. The Process error screen shows that the pattern used is invalid.

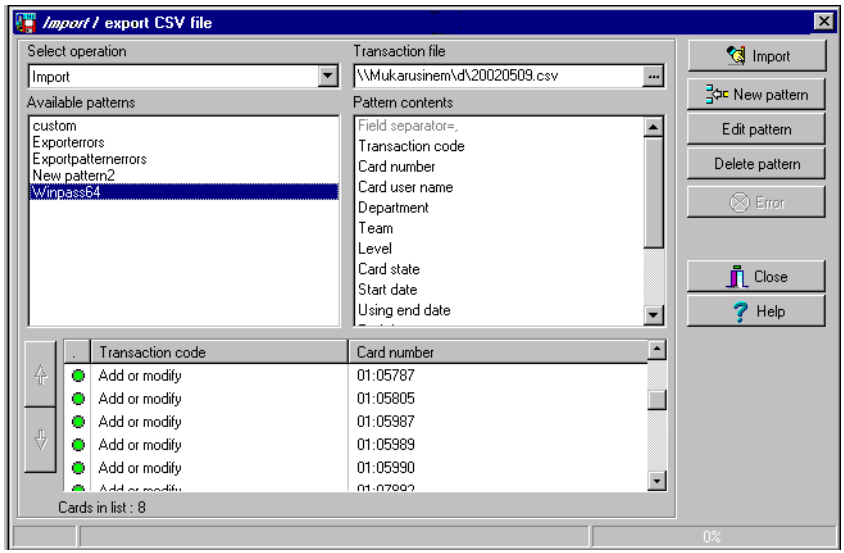


4 Click the **Close** button to go back to the Import Export screen.

5 In the Import/Export CSV screen, 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 9 • Creating 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:

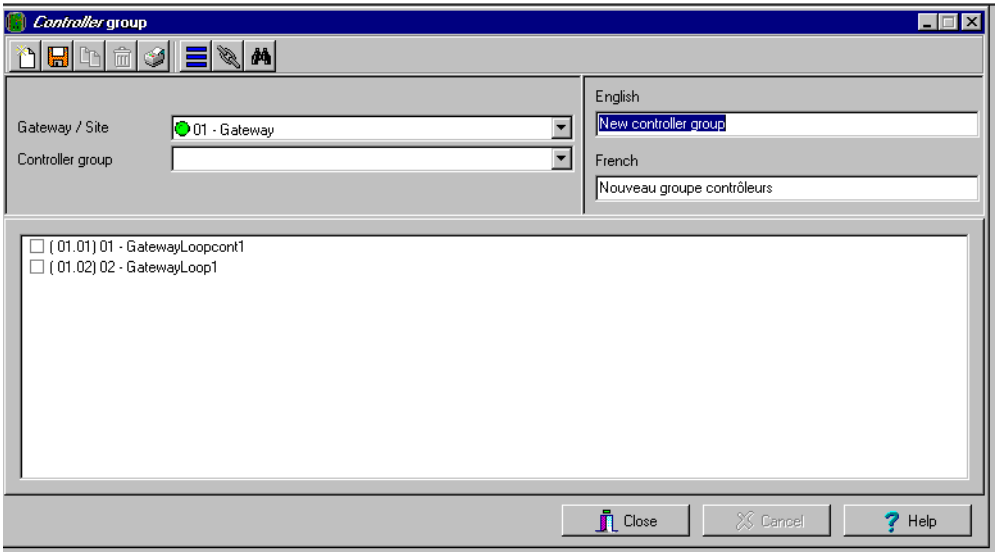
- Controller groups,
- Door groups,
- Relay groups,
- Input groups,
- Access level groups,
- Floor groups.

Creating a Controller Group

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).

To create a controller group:

1 From the Groups screen, 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.

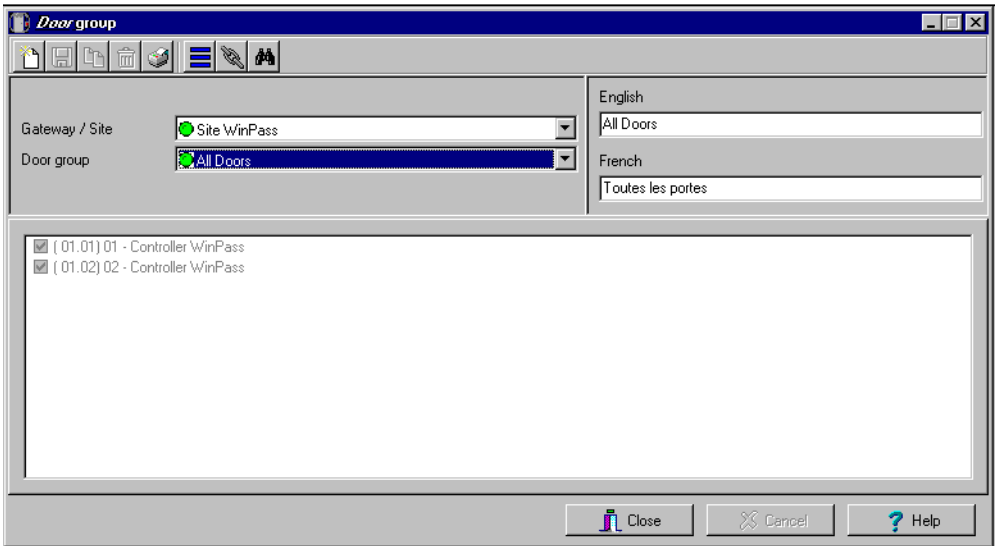
NOTE: *For more information on controllers, see “Configuring Controllers” on page 74*

Creating a Door Group

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.

To group doors:

1 From the Groups screen, 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.

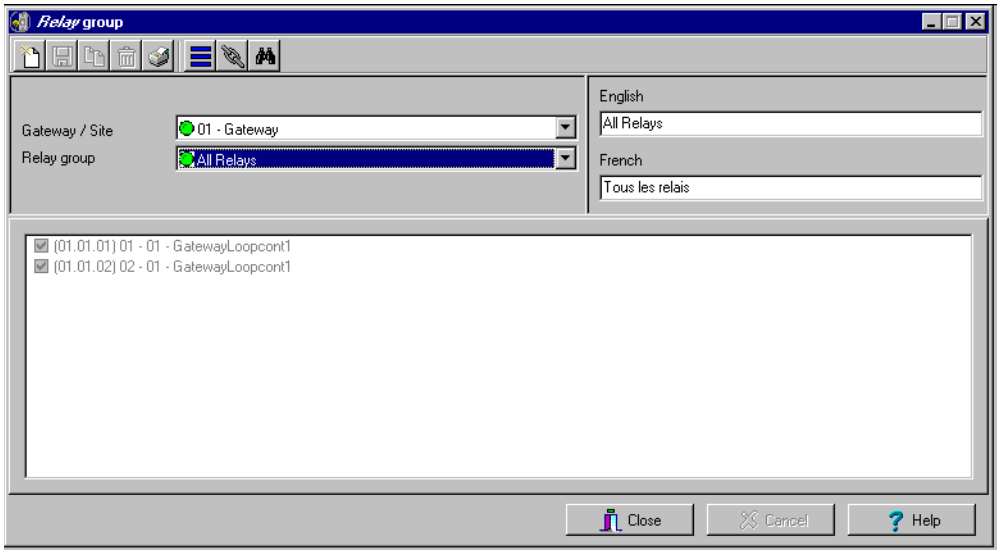
NOTE: *For more information on doors, see “Configuring Doors” on page 88.*

Creating a Relay Group

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.

To create a relay group:

1 From the Groups screen, 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 “Configuring Relays” on page 102.*

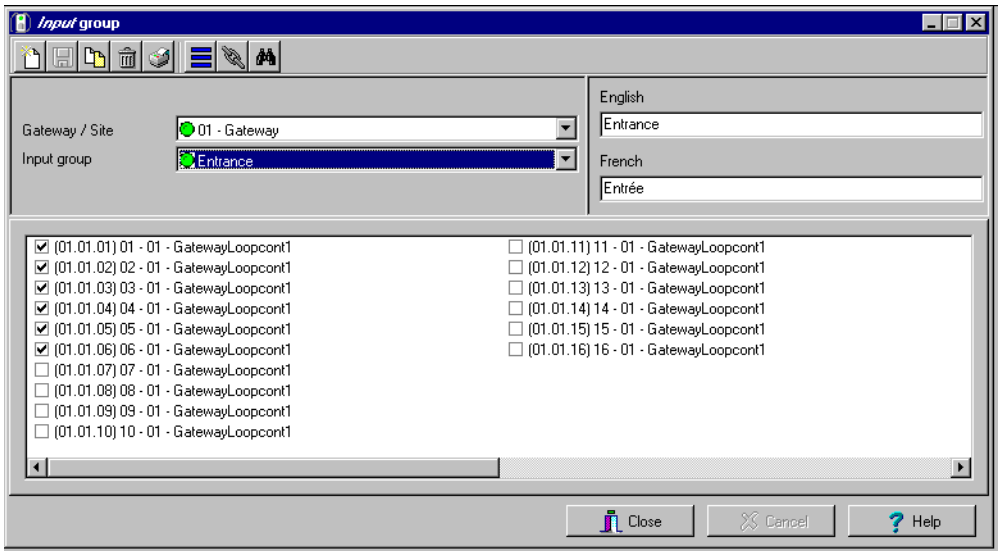
Creating an Input Group

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.

To group inputs:

1 From the Groups screen, 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.

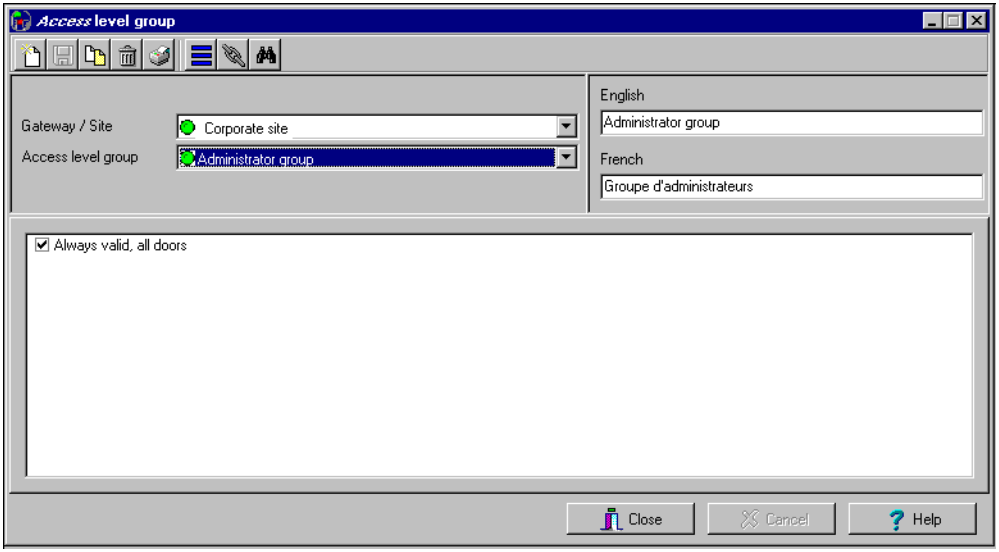
NOTE: *For more information on inputs, see “Configuring Inputs” on page 104.*

Grouping Access Groups

The Access level group menu is used to group access levels of the same site.

To group Access groups:

1 From the Group screen, select the **Access level group** icon.



2 Select the **View hierarchy** button to display all the sites defined in the system.

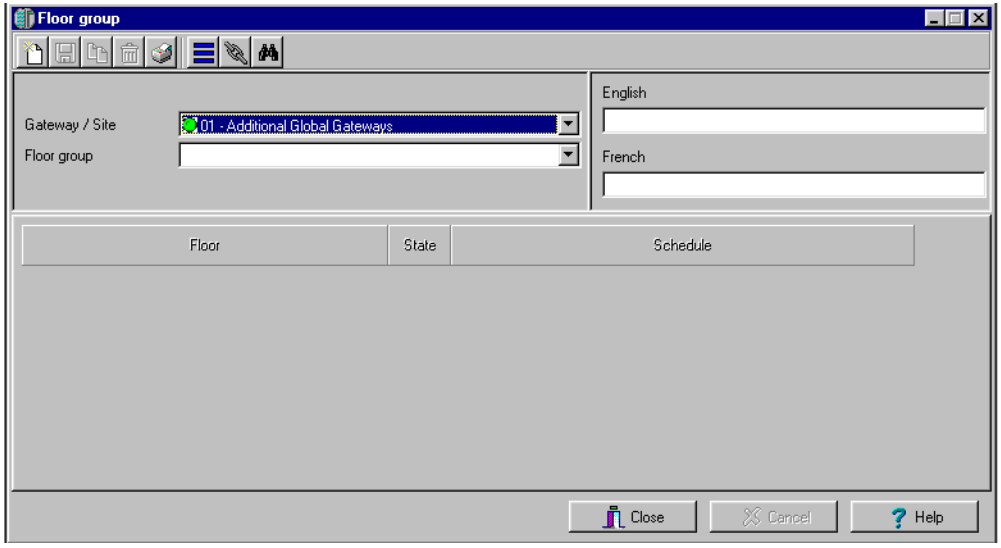
3 From the **Gateway/Site** drop-down list, select the site or gateway from which you want to group access levels.

Creating a Floor Group

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.

To group floors:

1 From the Groups screen, select the **Floor/Elevator door** icon.



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
- A schedule for each floor is assigned in the Schedule column.

Chapter 10 • System Status

The **Status** menu allows system operators to view the status of various devices and components of the access system:

- The **Text status** button allows operators to view, in text, the status of workstations, gateways, sites, controllers (KT-100, KT-200, or KT-300), doors, relays, inputs. The status displayed depends on the controller installed.
- The **Numeric status** 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 status** button allows operators to display the graphic status of a controller.
- The **Workstation status** button provides information regarding workstations connected to the server (operator name, local identification, etc.).
- The **Database status** button provides information on the database structure. In addition, an operator can perform configuration operations or manual commands from the database screen.

Text Status

The Text status features 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: workstations, gateways, sites, controllers, doors, relays and inputs. The text screen contains additional buttons/icons that assist operators in their tasks:

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 text status:

1. From the Status window, select the **Text Status** button. The **Text status** window appears.

NOTE: *When a component is selected, the button background turns yellow.*

2. In the Text screen, select the icon of the component for which you want to view the text status. If the **Workstation** icon is selected, the system displays the list of the EntraPass workstations.
3. Enter a few characters of the component to be searched in the database in the field at the top of the screen), i.e. “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 components; or select specific components by clicking in the checkboxes beside a component name. The **Clear all** button removes the check marks from the selected components. Click **Cancel** to return to the previous screen without any selections or changes.
4. You may check the **View sub-components** option 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 screen if this option was checked. For more focus in one screen, filter doors, relays or inputs by site.
5. Click **OK** to return to the previous screen 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.
2. From the **Gateway** drop-down list, select the gateway for which you want to display the status. The system displays the number of cards for that gateway, the number of inputs in alarm, the number of relays manually activated, the number of doors forced open, etc. This can be very useful if you need to find out how many cards are defined.

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 relays,
- 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 (in the list) identifies the component.
4. Select a controller from the **Controller list** drop-down list (right side of the screen), 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).

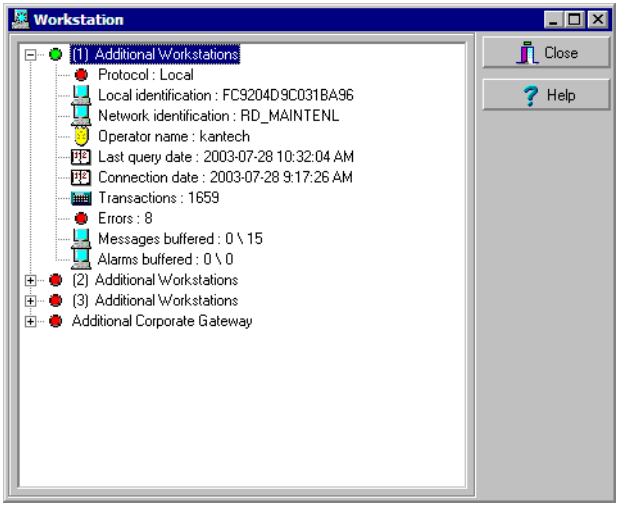
NOTE: *If there is more than one controller site per gateway, the numbers between brackets (xx) indicates the controller number and the following numbers (xx) indicate the component number.*

Workstation Status

The Workstation status feature displays details about a selected workstation, such as: operator name, last query date, local identification number, etc. It is also used to verify if workstations are connected to the server.

To view a workstation system status:

1. In the Status window, select the **Workstation** icon. The **Workstation status** screen appears.
   - The **Red** circle indicates that the workstation is not connected to the server
   - The **Green** circle indicates that the workstation is connected to the server.
2. Select a specific workstation for which you want to display the status. Click the "+" sign to see detailed information about a workstation; to see if an operator is logged into the workstation, for example.



- **Protocol**—Identifies the protocol (language) used to communicate with the server. The protocol is used to inform the system on how the information is shared between computers.
- **Local identification**—Identifies the label of the workstation on the network. This name is used by the server to identify your workstation.
- **Network identification**—Provides the IP address of the workstation on the network or NetbEUI name.
- **Operator name**—Displays the name of the operator currently logged on this workstation. The operator name is used for many purposes, such as to identify who performed a modification to a card, who acknowledged an alarm, etc. For information on modifying the operator name, see "Operator Definition" on page 242.

- **Last query date**—Displays the time the workstation last polled the server. The server and workstation exchange information on a regular basis.
- **Connected date**—Displays the date and time at which this workstation started its connection with the server. This date will be used to generate an event and kept in archives.
- **Transactions**—Displays the number of requests performed by the workstation (number of exchanges with the server), i.e. report queries, for example.
- **Errors**—Displays the amount of errors encountered by the workstation. This field will reset when the workstation is shutdown.
- **Messages/Alarms buffered** (0/1)
  - 0: the number of messages/alarms buffered for this workstation on the server when the workstation is off-line (not in communication). This number will reset to “0” when the workstation connects to the server and messages are sent.
  - 1: the number of messages/alarms that were sent to this workstation since the Server is operational. If the Server is shutdown, this number will reset.

NOTE: *The server holds a maximum of 60,000 messages and 60,000 alarms per workstation (default: 5,000) in the buffer. You can modify these settings through the Workstation Definition menu. You can also specify if newer or older events should be buffered. Events will be buffered only when the workstation is off-line (not connected to the server); and when the fields “Apply operator parameters for messages” and “Apply operator parameters for alarms” are not selected (for more information, see “Configuring EntraPass Workstations” on page 48).*

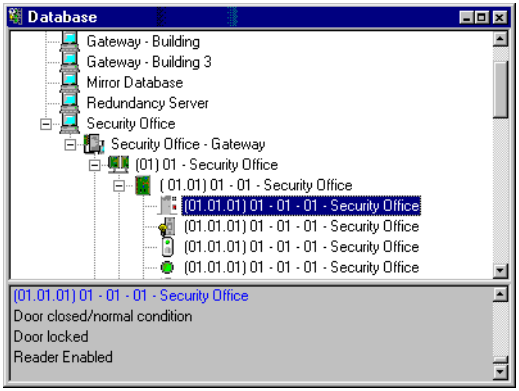
Database Status

This screen displays the status of the components within the database while browsing the database structure. The system displays all workstations (connected or not), the Gateway, controller sites, etc.

You can also perform manual operations directly from the screen 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 screen, select the workstation you want to view the database. The lower part of the screen 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 screen. 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 screen. 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 workstations 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 screen so you can modify its definition and when finished, return to the screen you edited the component from.

- **Limited display / No limited display—**When you click on a physical component, the bottom part of the screen 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.*

Chapter 11 • System

Use the **System** menu to define parameters for systems operators, security levels, events, instructions and message filters, and to view the database structure.

You will define system parameters as follows:

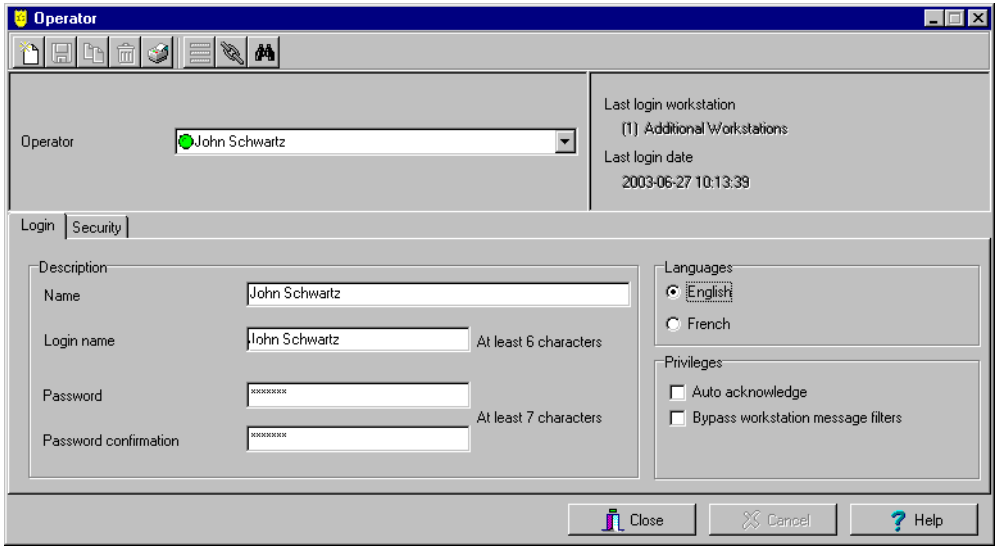
- **Operators**: username, login name, password, etc.,
- **Security levels**: authorized menus in read-only or full access modes, login restrictions, etc.,
- **Event parameters**: priority, color, display schedule, printing schedule, acknowledge schedule, etc.,
- **Instructions**: instructions for alarm messages and SmartLink applications,
- **Message filters**: select events to be included in a filter, etc.,
- **Database structure**: display physical and logical components, edit and sort components etc.

Operator Definition

This menu is used 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. To increase security, each person using the system and accessing the database should have his/her own operator defined to insure that each action performed in the system will be traceable.

To create a new operator:

1 From the **System** tab, select the **Operator** icon to open the Operator screen.



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.*

There are three levels created for operators on login. Each login has a separate name, password and security level.

- Operator Name: Installer
  - Login Name: kantech
  - Password: kantech
  - Security Level: Installer
- Operator Name: Administrator

- Login Name: kantech1
- Password: kantech1
- Security Level: Administrator

- Operator Name: Guard
  - Login Name: kantech2
  - Password: kantech2
  - Security Level: Guard

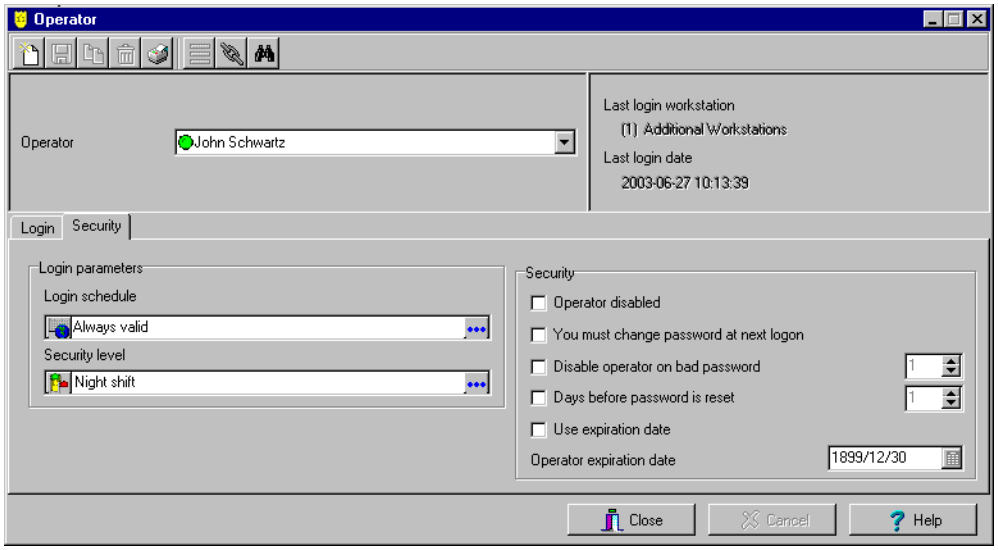
4. In the **Password** field, enter the password that will be used to login with the login name. The password is alphanumeric and consists of a maximum of 20 characters (minimum 7 characters). The password is not displayed nor printed, the system displays the password as asterisks.

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 closes the workstation, the next operator who starts the workstation will see the startup screen in the language of the last operator.
7. Select the **Auto acknowledge** option. If this option is selected, the **Manual** button is added to the Alarms desktop (see Chapter 12 ‘Working with Desktops’ on page 263). The operator can decide to manually or automatically acknowledge events. This is an operator privilege.
8. Select the **Bypass workstation message filter** option, if applicable. When this field is selected, the basic workstation configuration will be ignored and the operator will receive events from all workstations and gateways.

NOTE: *The* ***Bypass workstation message filter*** *option is a privilege granted to operators. It allows them to receive all events regardless of which workstation they are logged into at the time. If this option is selected and the “Apply operator parameters for messages” and “Apply operator parameters for alarms” options of the Workstation definition are also selected, then the basic configuration will be ignored and events will be filtered according to the security level of the operator who is currently logged into the workstation.*

9 Click on the **Security** tab to set operator access parameters.



10 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.

NOTE: *To allow an operator to logon to different EntraPass workstations or to the EntraPass Server select the field Allow login on workstation and/or Allow login on server (System > Security Level >* ***Miscellaneous*** *tab).*

11 From the **Security Level** pull-down menu, select a security level that will determine which menus an operator has access to.

NOTE: *It is possible to define up to 250 custom security levels; the system offers 3 built-in security levels (Installer, Administrator and Restricted) 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.*

12 Access the **Security** section to edit the security features of the currently displayed operator profile. Use these features to suspend (**Operator disabled**) or control the EntraPass logon process (**You must change password at next logon**, **Disable operator on bad password**, **Days before password is reset**).

NOTE: *Changes to the currently displayed profile will take effect at the next logon 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.

By default, an operator has unlimited access. However, it is possible to customize an operator security level; the system allows you to create up to 250 security levels.

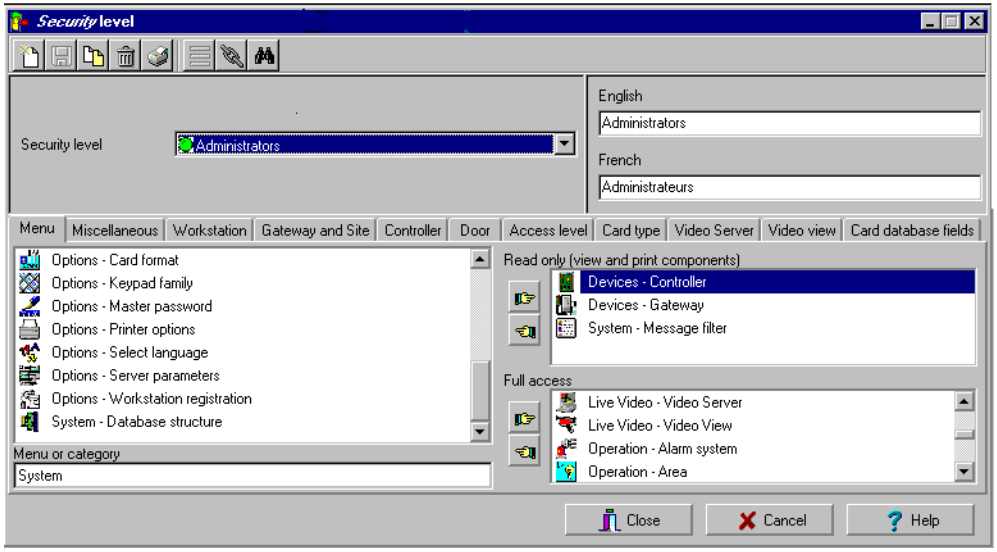
You have to program the other levels if you want to limit operator access to commands and/or options of the system menu.

There are three types of access rights:

- Installer: Full access to view, modify, delete, print components.
- Administrator: Medium access with limits to some sections.
- Restricted: Low access with limits to most sections.

To create/modify an operator security level:

1 From the **System** main screen, select the **Security level** icon. The Security level window appears.



NOTE: If the Live Video feature is enabled in EntraPass, the Video Server and the Video View tabs are added in the Security level window.

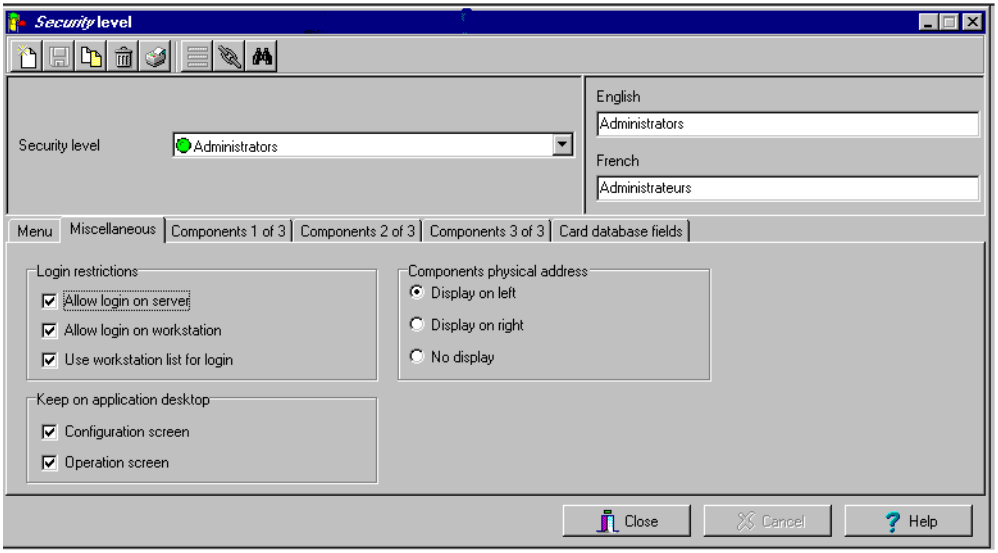
2 To modify a security level, select one from the **Security level** drop-down list. To create a new security level, click the **New** button and enter the necessary information in the language section.

3 In the **Menu** screen, select an access item you want to transfer either to the **Read-only** pane (upper pane so that the operator can view the item) or to the **Full access** pane. To do so, use the

Hand icons. You may also transfer an item back to the **Menu** pane. The **Menu or Category** display field shows the category of the selected item. For example, if you select “time report” the system displays “report”.

NOTE: *Assigning security levels is critical to the system. In fact, if a Security level is given full access to a system menu, it means that operators who are assigned this level can modify the system parameters. Make sure that each operator is given the security level corresponding to his/her tasks. Moreover, operators will not be able to see items that were not transferred to the Read-only pane or to Full-access. For example, if you want to restrict access to the Users-Card menu, do not transfer this item to the Read only or Full access pane (or transfer it back, if it were already transferred). This way, Operators who do not have the security level to access the Card menu will not view the Card menu in their windows.*

4 Select the **Miscellaneous** tab to define other parameters for the Security level being defined.



5 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 (Primary or Redundancy).
- Select **Allow login on workstation** to allow the operator to log onto any workstation in the system.
- Select the **Use workstation list for login** option to restrict the number of authorized workstations If selected, the operator will only be allowed to log onto the workstations that are selected in the **Components 1 of 3** tab. The **Allow login on workstation** option must be selected.

6 The **Keep on application desktop** section allows you to define the display option during the System definition:

- Check the **Configuration screen** option if you want the screen to be on top in the main screen.
- **Check the Operation screen** option if you want the screen to be on top in the main window, when you are, for instance, viewing the system Database structure.

NOTE: *These two options allow operators to keep more than one active screen on the desktop. They can bring to front or send to back the screen they want to display, simply by pressing ALT-F6. An operator may need to logout and then login in back for these changes to take effect.*

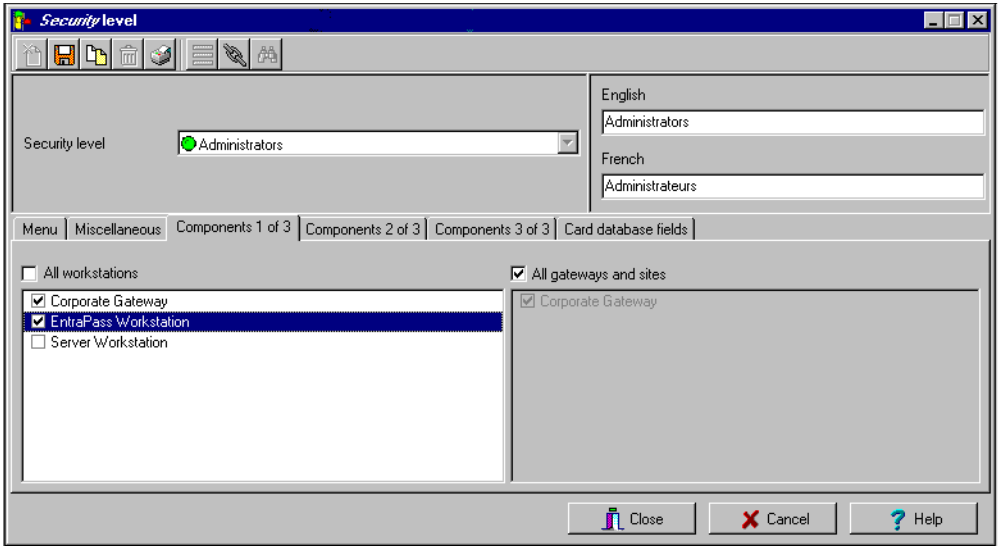
7 In the **Components physical address** section, specify how the component's physical address will be displayed in the windows, for the security level being defined. This will also affect how components will be sorted.

- **Display on left**—If selected, components will be sorted by address (i.e. 01.01.01 Controller xyz).
- **Display on right**—If selected, components will be sorted by 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 define available workstations and gateways:

1 Select the **Components 1 of 3** tab to define workstations and gateways that will be available for this Security level, when viewing or modifying components. You may check the **All workstations** and **All gateways and site**s options, or you may select the items one by one.

NOTE: *Operators will see only workstations that are selected here. Operator assigned a given security level will not see a specific workstation (Devices >Workstation) because it is not selected here in their security level definition.*



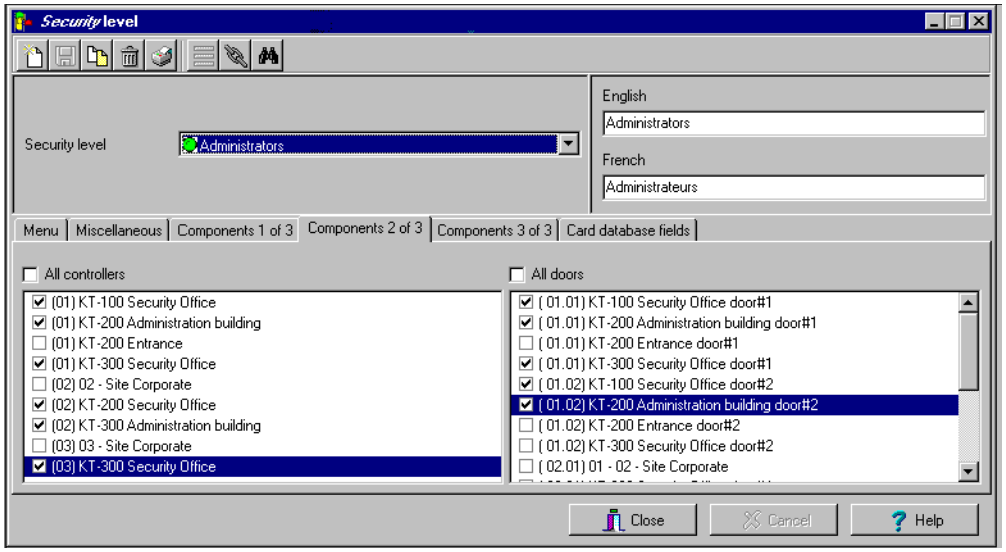
NOTE: *When an operator is allowed to use the "Network alarms message screen" (Desktop definition menu), only alarm events originating from the workstations and components of the gateways selected in this screen will be displayed. The security level definition acts as a filter for the "Network alarms message screen".*

2 Check the **All gateways** option if you want the operators assigned this Security level to see all the gateways.

NOTE: *When you select a gateway, you* ***also select all the components*** *defined "under" or attached to the gateway (i.e. sites, controllers, doors, relays, inputs, outputs, etc.).*

To filter the list of components:

1 Select the **Components 2 of 3** tab to narrow down the list of components (controllers and doors) that will be available to the operator who is assigned this security level for modifications or normal operations.



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). Make sure that you have also selected the gateway (Components 1 of 3) for which the selected controller is defined. If the gateway is not selected, the controller will not be available even if it is selected in the list.*

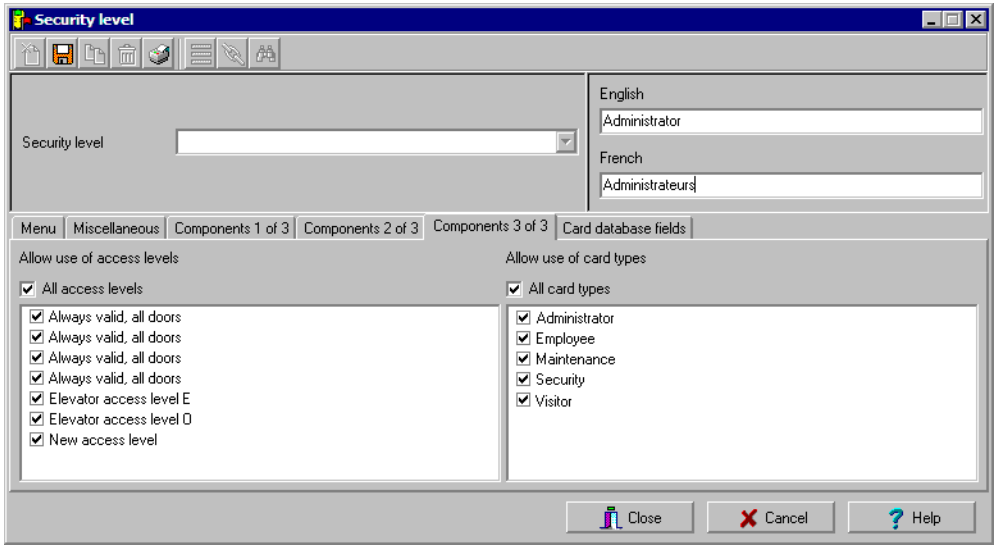
2 Select **All controllers** if you want all the displayed controllers to be available to the operator assigned this security level when modifying doors, relays, inputs, etc. or performing modifications/operations related to controllers. You can also selectspecific controllers from the displayed list.

3 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 logical components

1 Select the **Components 3 of 3** tab to restrict the number of logical components (access levels and card types) that will be available to the operator who is assigned this security level.



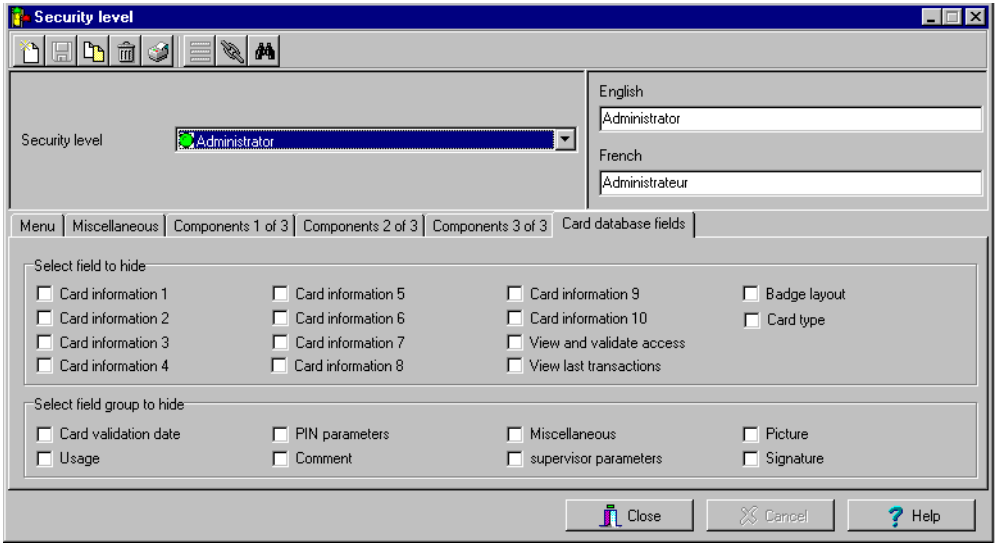
2 Select **All access levels** if you want all the displayed access levels to be available to the operator assigned this security level when creating cards or performing modifications related to access levels. You can also select only the access levels you want from the displayed list. Selecting specific access levels allows you to control the access levels that an operator can define. For example, a security guard may have the right to issue cards that are valid for a given door or access level only.

NOTE: *Make sure that you have also selected the gateway for which the selected access level is defined. If the gateway is not selected, the access level will not be available even if it is selected in the list.*

3 Select **All card types** if you want all the displayed card types to be available to the operator assigned this security level when creating cards or performing modifications related to card types. You can also select only the card types you want from the displayed list. This feature restricts the operator action. For example, if the Security level is not selected, an operator will not be able to view, modify, delete, or print cards defined with the Security level option.

To restrict access to user card details

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) whose access will be denied to the selected security level.

Event Parameters

Defining event parameters is one of the most powerful features of the system. For each event, it is possible to determine the actions process, to direct events to output devices (such as workstation screen (Messages desktop), printer (print to log printer)). It is also possible to define schedules that will allow, for example, sending alarms to a workstation only at night.

There are more than 400 different system events such as: “Access granted”, “Input in alarm”, “Card modified by operator”, etc. Events are associated with system components, such as doors, controllers, alarm systems, gateways, workstations, etc.

For every event message, there has to be an association with system components and output devices or group of devices. For example, the “Access granted” event can be defined for each individual door of the system or by default, it can be defined for all doors. This allows different actions or responses on a door-by-door basis.

Defining Events Parameters

The first step consists in defining what actions will be carried out when an event is generated. By default, all events are defined to display on all workstations in the system (the Messages list desktop) and have an “always valid” schedule in the display settings.

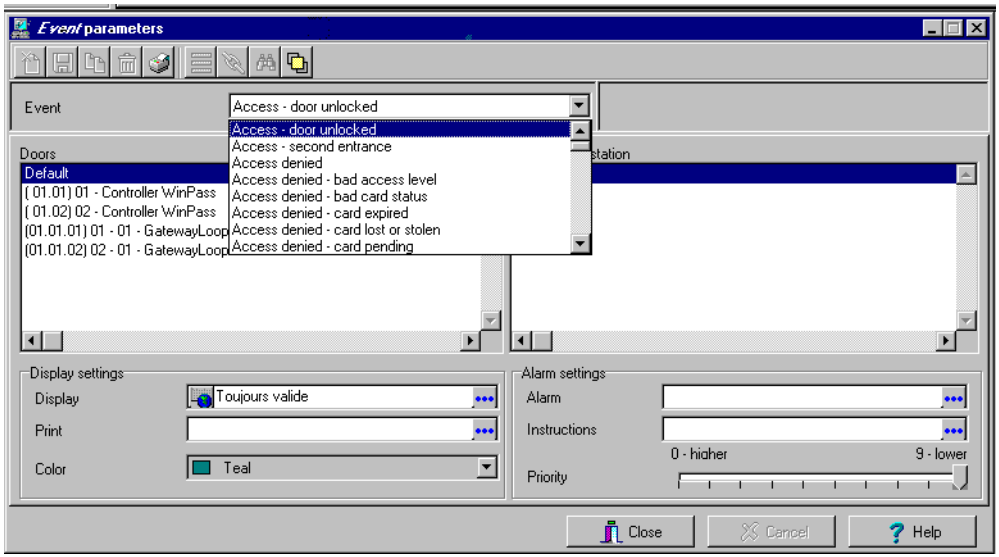
The **Event parameters** menu allows you to customize your system event. In fact, you can specify certain events to be printed automatically, or to be acknowledged during a specific schedule. You can also send instructions to inform an operator of the alarm on screen or through other media (i.e. e-mail, pager, etc.) when alarms are generated.

There are two types of associations: manual and default. But, there are three types or configurations of manual associations. In the first manual configuration, a specific component is associated with a specific workstation (example, events generated by Door 1 will be sent to only Worksation 1). In the second manual configuration, a specific component is associated with unspecified or default workstations (example, events generated by Door 1 will be sent to all Workstations). In the third manual configuration, unspecified or default components are associated with a specific workstation (example, events generated by any of the Doors will be sent to only Workstation 1).

NOTE: *Manual associations are privileged; therefore all default associations will be ignored. Manual associations should be used cautiously. The most common use for this feature is the SmartLink application.*

To define parameters for a system event:

1 From the System main screen, select the **Event** parameters icon.



2 From the **Event** drop-down list, select an event for which you want to define associations. If you selected default settings for this events, the system will send the event to all workstations. You may also select a specific workstation to which you want to send the selected event.

NOTE: *By default, all events are defined to be sent to all workstations of the system (in the Messages List Desktop) and have an "always valid" schedule in the display settings. Default settings allow to assign system parameters to events. It is useful to keep default settings, especially when these settings apply to all components/events.*

NOTE: *If you chose Default in the* **Component** *section and Default in the* **Send to workstation** *section, (which includes all components to all workstations) for display and alarm settings, this is called a "default" association.*

3 In the **Display settings** section, specify the display options: by default, all events are programmed to be displayed in the Messages desktop screen of all the workstations of the system. An "always valid" schedule is already inserted in the field "Display".

NOTE: *For the SmartLink application, this schedule must remain to "all valid" or otherwise messages/commands will* ***not*** *be forwarded to the application.*

4 From the **Print** pop up-down menu, select a schedule. When this schedule is valid, the selected event will be printed on the printer defined on the workstation 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 40.*

5 From the **Color** drop-down list, select the color that will be used to display the event on the workstation terminal. The default colors are set according to the following conventions:
- **Red** for alarm events;
- **Green** for elements returning to a normal condition;
- **Yellow** for warnings and errors;
- **Blue** for other events.

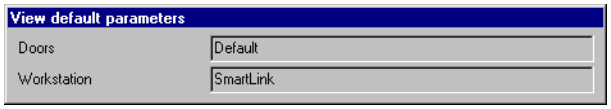
6 In the **Alarm Settings** section, specify:
- Alarm (schedule)—When this schedule is valid, the event will be sent to the "Alarms Desktop Screen" of the selected workstations and will require an acknowledgement from the operator.
- Instructions—Select the instruction that will be sent to the "Instruction Screen" in the Alarms Desktop with the event to be acknowledged. Instructions will only be sent when the "alarm schedule" is valid.

NOTE: *For the SmartLink application, the instruction does not require that the "alarm schedule" be valid. You can leave the "alarm schedule" blank, and the instruction will be sent anyway.*

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).

Viewing Associations

1 To view the display and alarm settings for a specific component, select a component and a workstation and click on . The following screen will be displayed:



2 In this case, the system will apply the display and alarm settings for the "Default" (component) and "SmartLink" (workstation) association. To view the settings, select "Default" in the component section and "SmartLink" in the "Send to Workstation" section.

Deleting and Restoring Associations

1 To delete the alarm and display settings for a specific association, select a component and a workstation and click on .

2 From the Delete event parameters screen, make your choice:
- **Restore defaults**—This option will apply the default alarm and display settings.

- **Suppress message**—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.

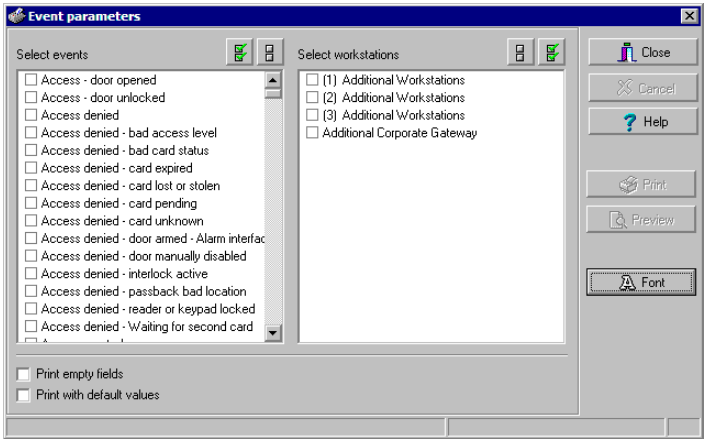
Printing Event Parameters

This menu is used to print parameters (alarm and display settings) for the selected events for the selected workstations.

When you are done selecting the fields, you can preview your report before you actually print it. When you preview the report, you can print from the displayed screen or click **Close**, then modify the settings (fields) if necessary and print your report.

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

1 From the Event parameters screen, select the **Printer** icon.



2 In the **Select events** display 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 workstations** section select the workstations to be included in your printout or click on the **Select all** button to select all the workstations from the displayed list.

4 You may check the **Print empty fields** option in the bottom of the screen. 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** options. If selected, the system will print the "Default" associations as well as "Manual associations".

***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 workstation xx), the report will be empty.*

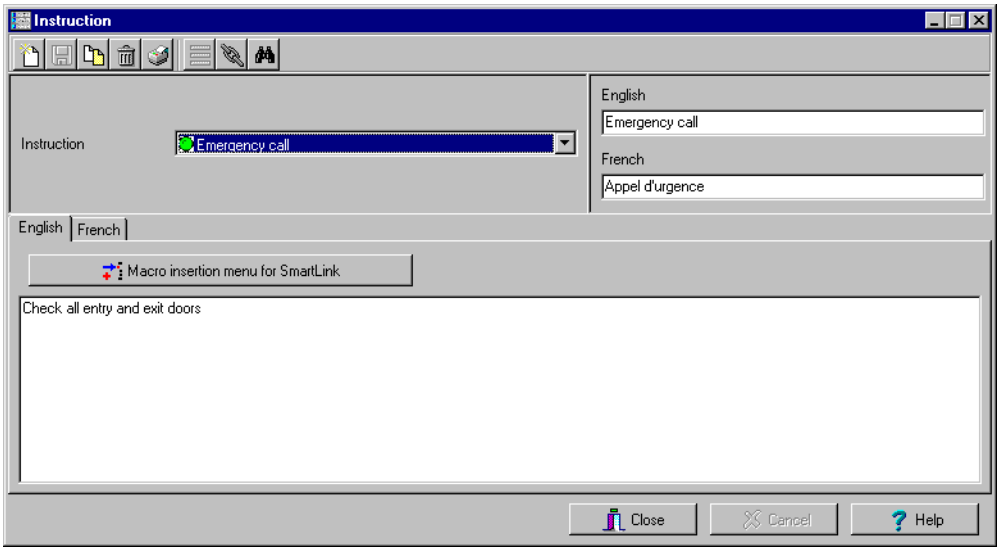
6 Select the **Preview** button before printing, if desired.

Instruction Definition

This menu is used to define instructions that will be sent to the Instruction screen (Desktop menu) when an alarm is generated and sent 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.

1 From the **System** main screen, 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.*

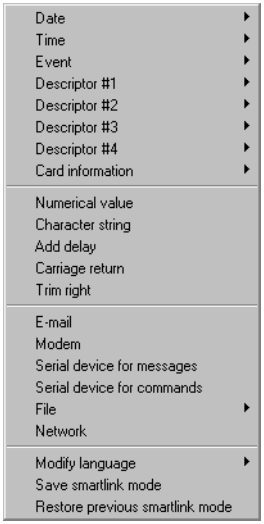
5 To assign instructions to events, see "Event Parameters" on page 252.

Creating a SmartLink Application Instruction

The Instruction definition menu allows you to create SmartLink instructions. If you have a SmartLink application installed, the Macro-insertion menu button is enabled. It allows operators to send built-in macro-commands to the SmartLink application.

To enter a Smart Link instruction:

In the Instruction screen, select the Macro insertion menu for SmartLink button or right-click and a menu will be displayed.



NOTE: *When creating SmartLink instructions, only commands that are written in the primary language are considered as valid commands. For more information on macro-commands, refer to your SmartLink Specifications Manual.*

Message Filters Definition

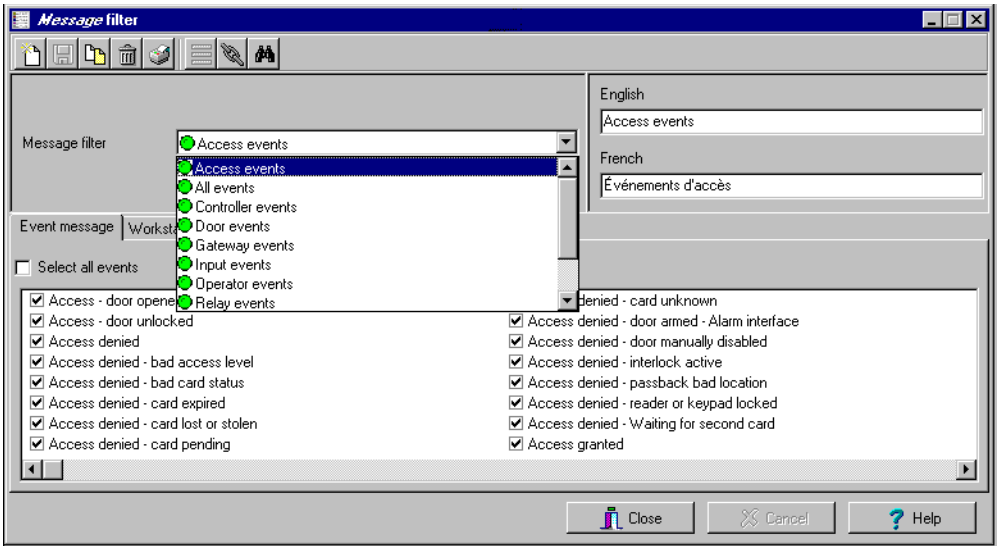
This menu is used to create filters for the “Filtered Message” desktop. These filters are used to view a specific selection of events.

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 Message List” desktop or from the Message Filters definition menu.

NOTE: *For more information, see “Filtered Messages Desktop” on page 269.*

To define message filters for events:

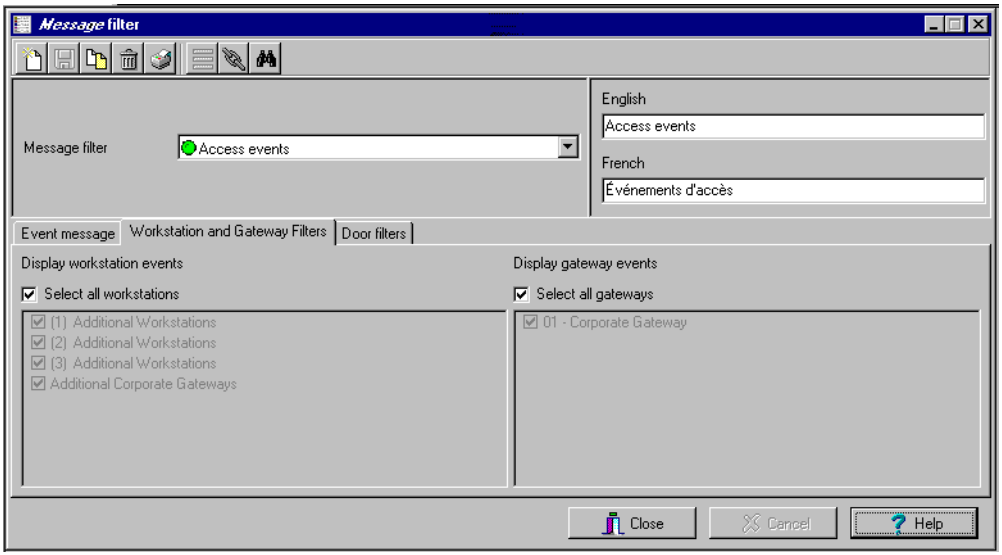
1 In the System main screen, select the **Message Filter** icon.The Message filter screen appears.



2 From the **Message filter** drop-down list, select the event message 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, you may select the Access-denied type of events.

4 Select the **Workstation and Gateway filters** tab to filter workstation and gateway.

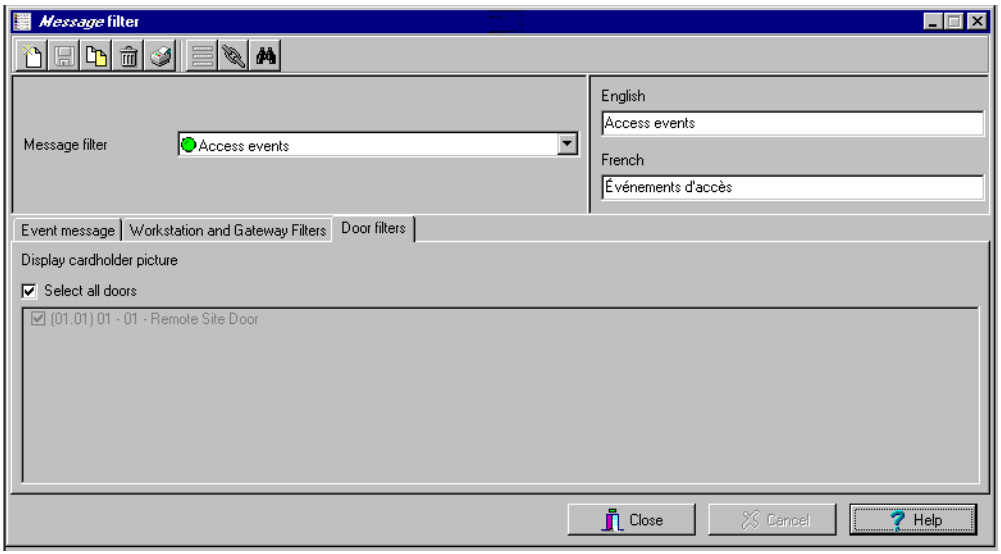


5 Check the **Select all workstations** option in order to receive events originating from all workstations of the system. This option must be selected in order to receive all events originating from all system workstations. You may also choose to display events from specific workstations. To do this, select the workstation from which you want to receive events.

6 Check the **Select all gateways** option to receive events originating from the components of the gateways. You may select the Gateway 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 filters these events according to the settings of the selected filter. If some events originating from a specific gateway are displayed in your messages desktop and this gateway is not selected in the filter definition, then these events will not be displayed when you select this filter.*

1 Select the **Door filters** tab to display the cardholder's information.



2 Check the **Selected all doors** options or choose specific doors for which the cardholders's picture will be displayed an door event. When "Access events" are filtered, a picture of the cardholder 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.

Database Structure

Use the Database structure menu to browse the system database. It will display the entire structure of the database including:

- The system *physical components* (workstations, gateways, sites, controllers, doors, relays, inputs and auxiliary outputs), and
- *Logical components* (cards, schedules, reports, instructions, areas, alarm systems, groups, etc.).

Operators can edit or sort the system components from the Database structure screen.

To view the data base components:

1. From the System menu, select the **Database structure** icon.

NOTE: *If the Live Video feature is enabled in EntraPass, its components will appear in the Database explorer.*

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 side of the screen.
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 screen 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 pane of the screen 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 245.*

Chapter 12 • Working with Desktops

EntraPass offers the ability to customize up to eight work areas or desktops. These desktops are used to receive or acknowledge system events. There are five main desktops and three additional windows:

- Alarms screen,
- Messages screen,
- Filtered messages screen,
- Graphic screen (or Live Video desktop),
- Network alarms screen.

Additional windows allow operators to display:

- Instructions,
- Pictures,
- Graphics.

NOTE: *If the Live Video option is enabled in EntraPass, you can define a desktop for to call up the Video View component for viewing.*

It is possible to have a combination of all the display options in one Desktop. Depending on their Security level, operators can modify the settings of each of these windows (background color, size, toolbar, etc.). 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). However, it is possible to temporarily allow a Read-only operator the ability to modify his/her desktop settings. In this case, the changes apply only to the current session.*

Customizing desktop properties

To change the desktop properties, an operator must have the appropriate Security level. To define an operator's security level: **System** menu > **Security Level**.

However, it is possible to allow an operator the ability to change his/her desktop settings for a limited time (during one login session **Desktop** (right-click) > **Properties** > **Permit**).

To change your desktop properties:

1. From the Desktop window, right-click anywhere in the screen.
2. From the Properties screen that appears, select the display options: you may change the default size of buttons, the default background color, etc. The changes you make apply to all system windows.
3. To customize a specific desktop, right-click the desktop you want to customize to open the Desktop properties screen.

NOTE: *The **Assign desktop** option allows an operator who has the permission to modify the desktop settings the ability to transfer one or more customized desktop(s) to users who do not have the right to customize their desktops.*

4. From the shortcut menu, select **Properties**.

NOTE: *If the Live Video option is enabled in EntraPass, the lower part of the Desktop properties window will display the Live Video Screen option.*

5. From the **Desktop name** field, assign a meaningful name to the desktop you are configuring.
6. Select the window type:
   - **Floating window**—a floating window can be resized and positioned anywhere in the Desktop screen, or even outside the desktop screen. For example, you can choose to send it back or to bring it back to front. When a floating window was sent to back, you may bring it to front by right-clicking the desktop button, then selecting the **Bring to front** menu item.
   - **Desktop window**—a desktop window is trapped within the main screen; it is impossible to position it wherever you want; you can just position it within the main Desktop window area.
7. 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 screen you have just configured.

NOTE: *When your windows are displayed for the first time, you may need to re-size them in order to view the information correctly. To do so, point to the frame border you want to change; when the pointer becomes a double-headed arrow, drag the border to exact size. You may then position the screen in the desktop to the desired position.*

Changing desktop properties temporarily

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.

To change desktop properties:

1. Log on, using the operator with the limited security level user name and password (restricted access security level).

NOTE: *The operator who is currently logged in does not have the permission to view all the eight workstations.*

2. Right-click a desktop, then select **Properties.** The desktop properties screen appears.
3. Click the **Permit** button. The operator login screen appears. The operator with the full-access desktop permission has to enter his/her username and password.

NOTE: *The permission acquired will be valid until the operator logs out.*

Assigning desktop properties

Another possibility available to the Security Manager (or to the operator with the appropriate Security level) is to customize his/her desktop, and then to assign the settings to other operators who may not have the appropriate security level to modify their desktop settings.

To transfer 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 screen, select the operators who will be copied to the desktop properties (you must place a checkmark in the checkbox). You may select operators one by one, or you may use the **Select all** button.

Using Desktops

Messages Desktop

A desktop configured as a **Messages desktop** displays all events. Events are displayed with date and time, event description, details and associated cardholder pictures (if defined). When a new event is displayed, the screen scrolls up. The newest events are added at the bottom of the screen.

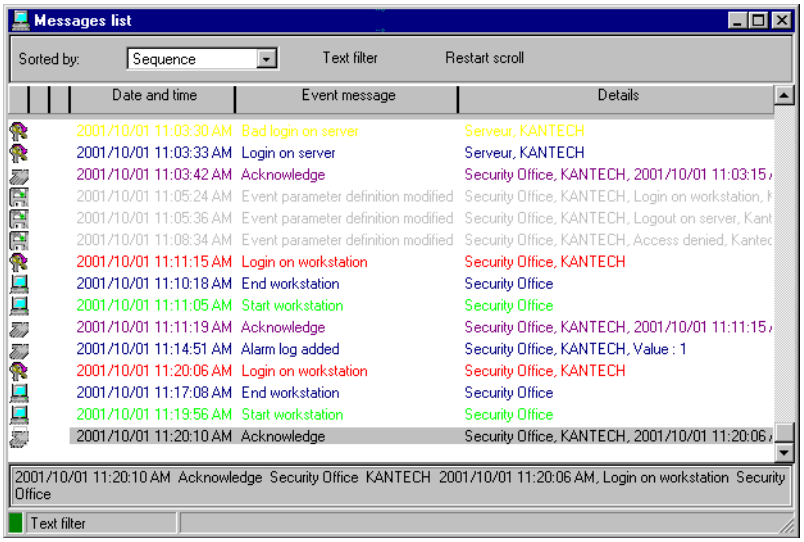
Messages desktops (including Filtered messages screen) may be configured as **Message screens** and **Picture screens** at the same time.

- **Message screen** —Allows you to view events. You may use pre-defined filters to view the displayed messages. You can also define new filters, by right-clicking and enabling a shortcut menu.
- **Picture screen**—When a desktop is selected as a picture screen, the cardholder's picture is displayed on access events, if pictures are defined in the system. For more information on assigning pictures, see Chapter 8 'Users' on page 149.

NOTE: *When you configure a Desktop as a message screen and a picture screen at the same time, two windows are displayed simultaneously when you select the desktop.*

To view system messages:

1 Right-click the Messages desktop. It displays the Messages list screen.



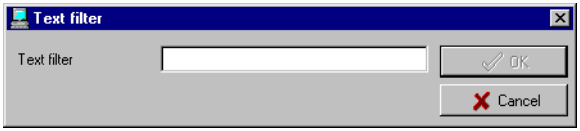
NOTE: *You may change the message color:* ***System*** > ***Events parameters****.*

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 screen.
- **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.
- **Message type**—When selected, the system sorts the **Event message** column in alphabetical order, grouping *similar* events. For example, all **Site** events are grouped.

NOTE: *When you select an event from the list, you interrupt the incoming sequence (the green rectangle located on the bottom left part of the message desktop turns red when scrolling is interrupted). To restore the normal scrolling operation, click on the* **Restart scroll button***, in the top of the screen. Select* **Sequence** *from the* **Sorted by** *drop-down list to go back to the default display.*

3 Click the **Text filter** button **(top of the screen)** 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.



4 To close the **Find** dialog box, click the **Cancel** button or the Windows closing button (X).

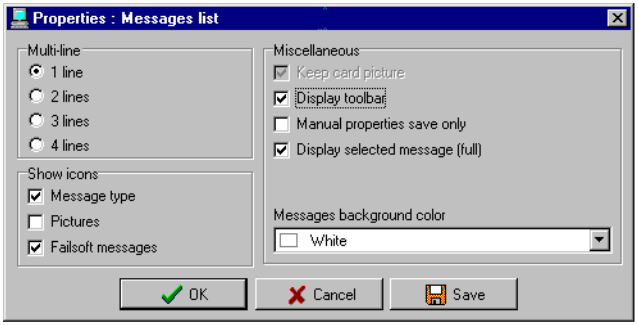
5 To return to normal display in the Messages list screen, click the **Text filter** button.

6 To restore normal scrolling, click the **Restart scroll** button (top of the screen).

7 Right-click an event to enable a shortcut menu:

- **Delete all**—This option allows an operator to delete all the events displayed.
- **View card**—This option allows an operator to view information contained on a card.
- **View card transactions**—When you are positioned on an event related to a card, you can select this menu item and obtain a report on card transactions.
- **View parent**—Displays the parent components of the selected component.
- **Send to back**—This option only works when the window type is set to floating. It sends the active window behind the main application screen. To bring back to front, right click the desktop button, then select **Bring to front**.

- **Properties**—The system displays additional options:



8 From the Properties screen, 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 icons besides 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 screen 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 screen** as well as the position of the screen within the Messages Desktop.
  - **Display selected messages (full)**—When you select this option, a smaller screen is added at the bottom portion of the **Message screen**. It displays the selected event with its full description. This feature is very useful when your Message screen is too small to display the entire description of an event.
- **Message background color**—Allows the operator to modify the background color of the message screen.

NOTE: *To change the font color of system messages: go to System > Event parameters.*

9 If you selected **Picture screen** when defining the Message desktop, the Message desktop always appears with a Picture screen.

10 You can right-click the picture to size the image; however the image will not maintain proportions.When you right-click the picture, a shortcut menu appears:

- **Stretch ratio**—This option stretches the picture to the screen size while maintaining proportions.
- **Send to back**—This option only works when the window type is set to floating. It sends the active window (Picture screen) behind the Message desktop main screen. To bring it back to front, right click the Message desktop button, then select **Bring to front** from the shortcut menu.

Filtered Messages Desktop

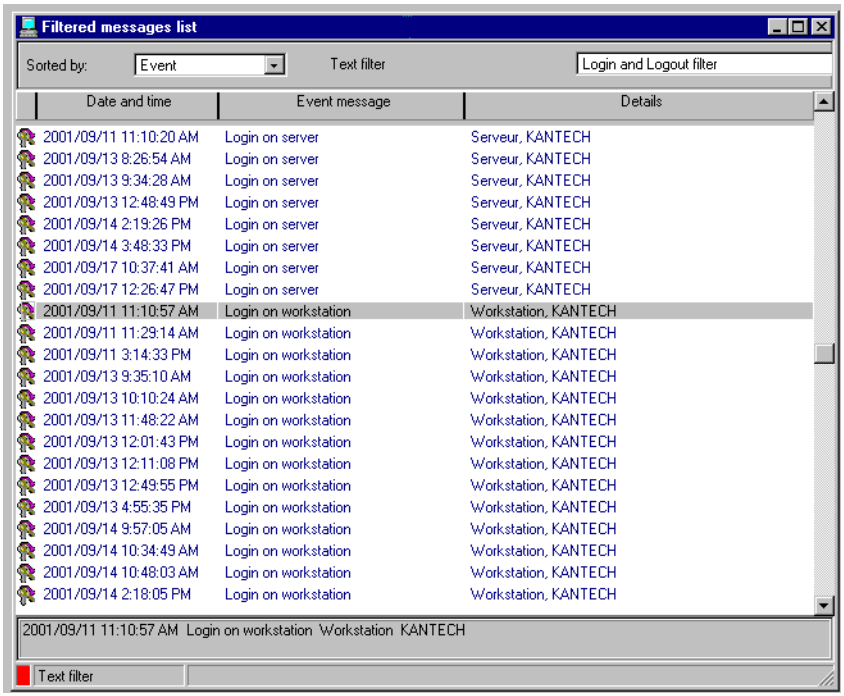
The Filtered Messages desktop is a copy of the Messages desktop. It allows the operator to display events that are part of a selected filter. For example, you can create filters to display events that are related to a specific controller and from a particular gateway of the system.

It is recommended to use a separate Desktop to view filtered events, and to name it according to its content.

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 screen, Picture screen or both).



3. You can change the **Text filter**, to display specific events. For details on the Filtered messages desktop, see “Messages Desktop” on page 266.

Alarms Desktop

The Alarms desktop is used to view and to acknowledge alarms of the system. Only events that require operator acknowledgment and that are programmed in the Event Parameters definition (System > Event Parameters) 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 screen.

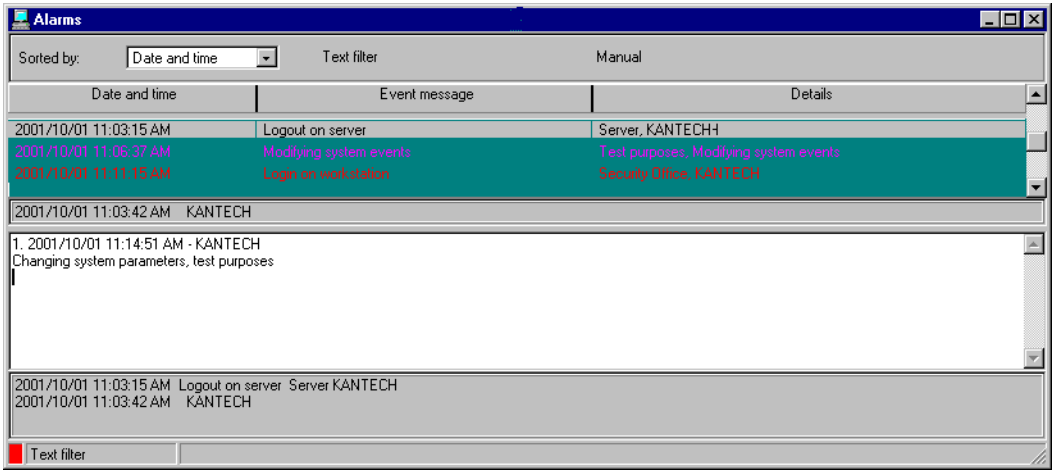
NOTE: *An Alarms desktop may be defined as a Message screen, a graphic screen and an Instruction screen. These features may apply to a single desktop. When you select a desktop defined with these three features, three windows are displayed simultaneously. For a better display, you may need to resize and to position the windows.*

To define an Alarms desktop:

1. From the Desktop main screen, select the desktop in which you want to display alarm messages, then define the window type: **Floating** or **Desktop type**.
2. Specify additional options for the Alarms desktop:
   - **Message screen**—This screen allows the operator 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 screen 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 definition menu > Instructions. Then after, they may be associated with events.
   - **Graphic screen**—This screen will display the location of the alarm being reported (if graphics are defined in the system). For more information on assigning graphic, see Chapter 7 'Defining Graphics' on page 143.

To view system alarm messages:

1. Select the desktop you want to define as an **Alarm messages** desktop.
2. Assign a meaningful name to the **Alarm messages desktop**; then define the desktop type (Message screen, Instruction screen, Graphic screen). You may assign the three features to one screen.



3 You can double-click the log area (middle of the screen) to add a comment.

4 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 screen 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**).

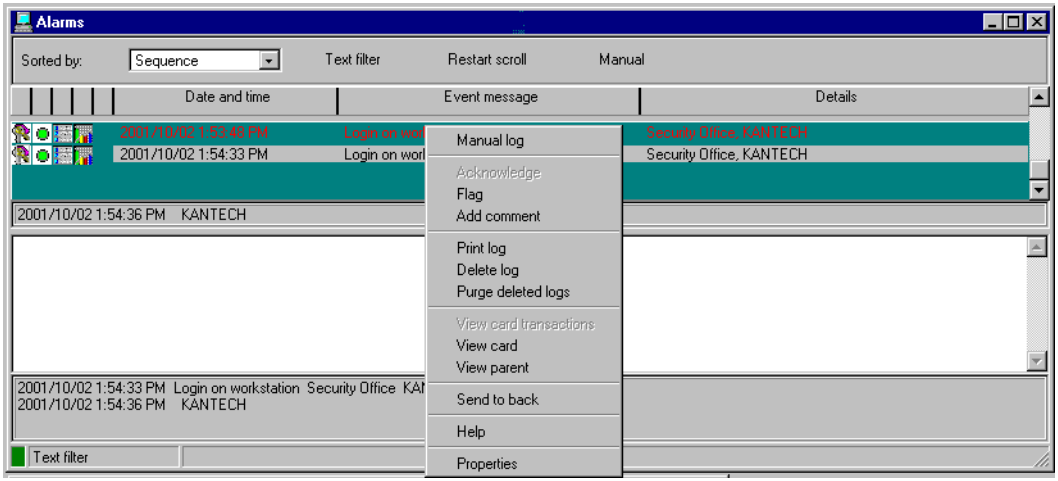
5 You may right-click anywhere in the screen to enable the Properties screen from which you can enable alarm status icons:

- **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.

6 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 "Operator Definition" on page 242.

NOTE: *This option (Manual automatic acknowledgement) is only available through the Alarms Desktop. When the operator logs out, it will return to "manual" by default.*

7 Right click an alarm message for additional options:



- **Manual log**—When selected, the system displays the Manual log screen 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 screen. 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 screen and select **Properties** then select **View deleted logs**.
- **Purge deleted log**—Select this option to permanently remove logs that were marked for deletion.
- **View card**—This option allows an operator to view information contained on a card.
- **View card transactions**—Select a card related event to obtain a report on card transactions.
- **View parent**—Displays the parent components of the selected component.

- **Send to back**—This option only works when the window type is set to floating. It sends the active window behind the main screen (Alarms Desktop). To bring back to front, right click the desktop button, ten select **Bring to front**.
- **Properties**—Display a Properties screen from which you can customize the alarms desktop display, such as adding icons, changing the background color, etc.

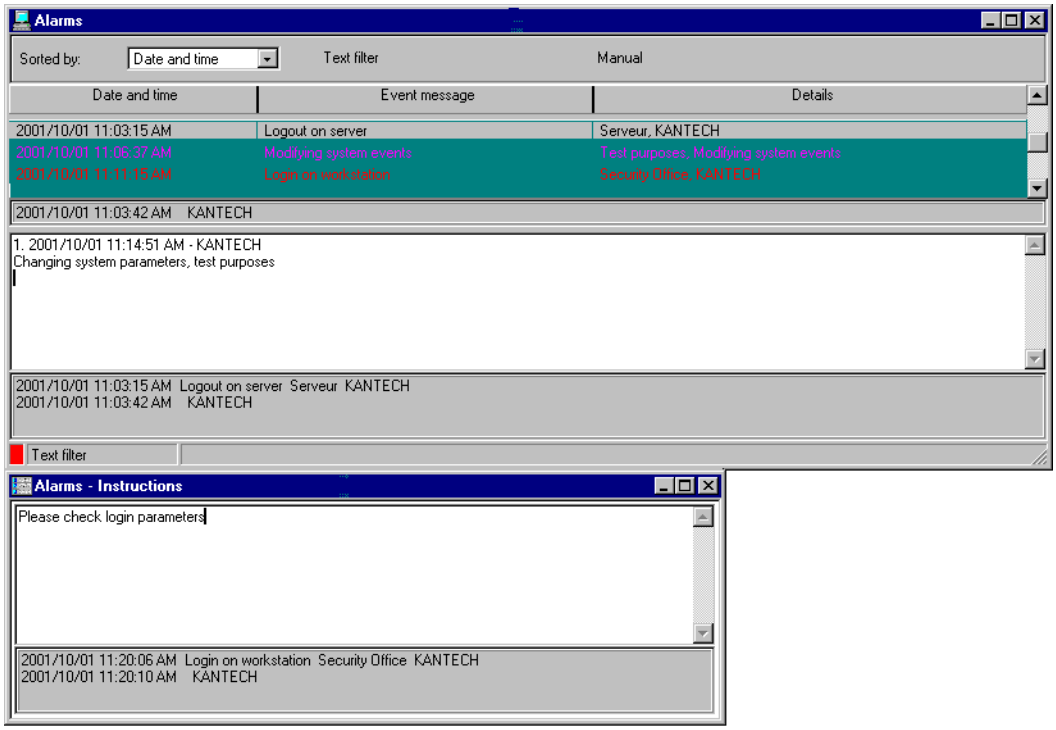
Instruction Screen

The Instruction screen displays the instructions to follow when an alarm is reported.

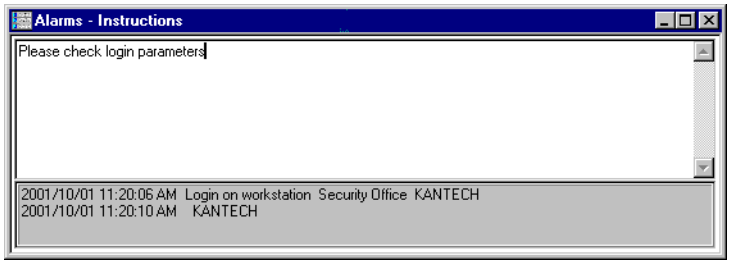
Instructions will only be displayed if this option is enabled during the Event Parameters settings (System > Event parameters, Alarm settings).

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 screen, or defined as an instruction screen. When a desktop is defined as being both a message screen and an instruction screen, 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.*

Acknowledging Alarms/Events

Operators have to acknowledge receipt of an alarm condition (event—such as intrusion, input in alarm, etc.) by responding in some way such as depressing an acknowledgment button.

Events that require operator acknowledgment must be defined in the System definition menu, under Event Parameters.

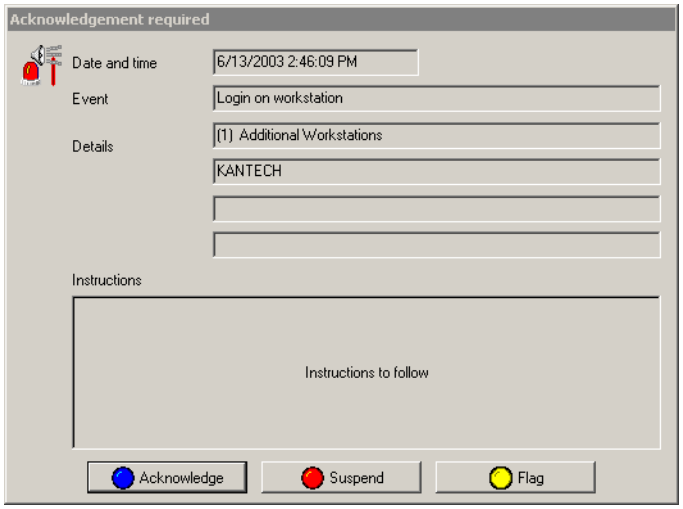
NOTE: *You can use the sound feature that will warn the operator when an event needs to be acknowledged" For more details see "Setting up Multimedia Devices" on page 368.*

You may acknowledge alarm messages from an alarm warning box or from the Alarms desktop screen.

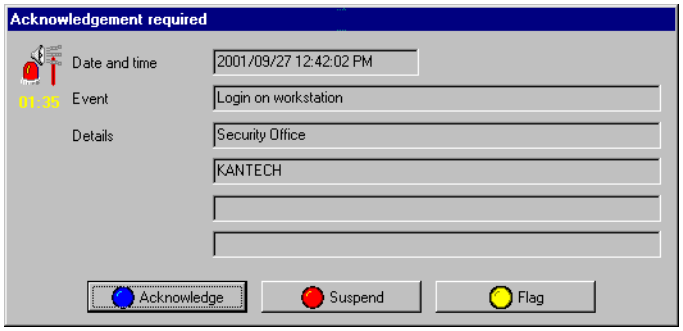
Acknowledgement options are setup in the Workstation definition (Devices > Workstation (selected Workstation) > Message 2 of 2 tab, Acknowledgement parameters).

To acknowledge an alarm message:

1 When the **Acknowledgement required** message box appears, take one of the following actions:



NOTE: *The* ***Acknowledgement required*** *message box will be presented in a format without the Instructions window if no instructions accompany the message box.*



- 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 **Workstation 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.

NOTE: *The alarm message is not displayed if the operator who is logged on has the Automatic acknowledgement feature enabled (**System** > **Operator definition**). Alarms are automatically acknowledged and logged in the system.*

Acknowledging alarms in the Alarms desktop

NOTE: *If this option is enabled, operators **CANNOT** suspend alarms.*

1. Select the alarm event you want to acknowledge.
2. Right-click to enable a shortcut menu.
3. Select **Acknowledge** from the sub-menu. The status indicator becomes green. If you want to identify an alarm message for specific purposes, select the alarm event you want to identify; right-click and select **Flag** from the sub-menu.

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. When this option is enabled in the Operator definition menu, the Manual button is added in the Alarms desktop. This button toggles between Manual and Automatic acknowledgement.*

Graphic Desktop

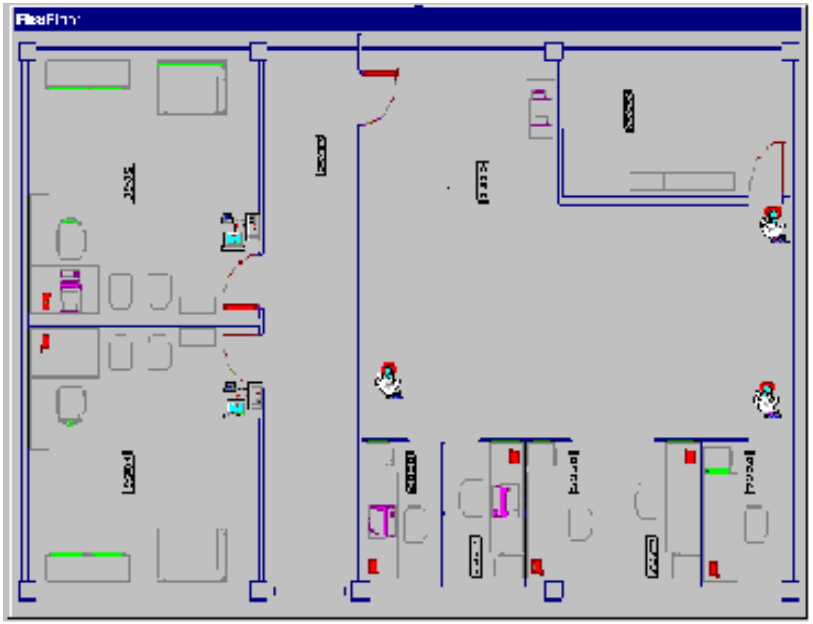
The Graphic screen displays the graphical location of the alarm being reported (if graphics are defined in the system). Graphics are assigned to physical components of the system.

Operators can perform manual operations on components assigned in the graphic. For example, they can manually lock or unlock a door defined in the graphic just by clicking the door in the graphic and selecting the appropriate option. Graphics allow them also to diagnose an abnormal situation and to take appropriate action.

To view graphics in the desktop windows:

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.

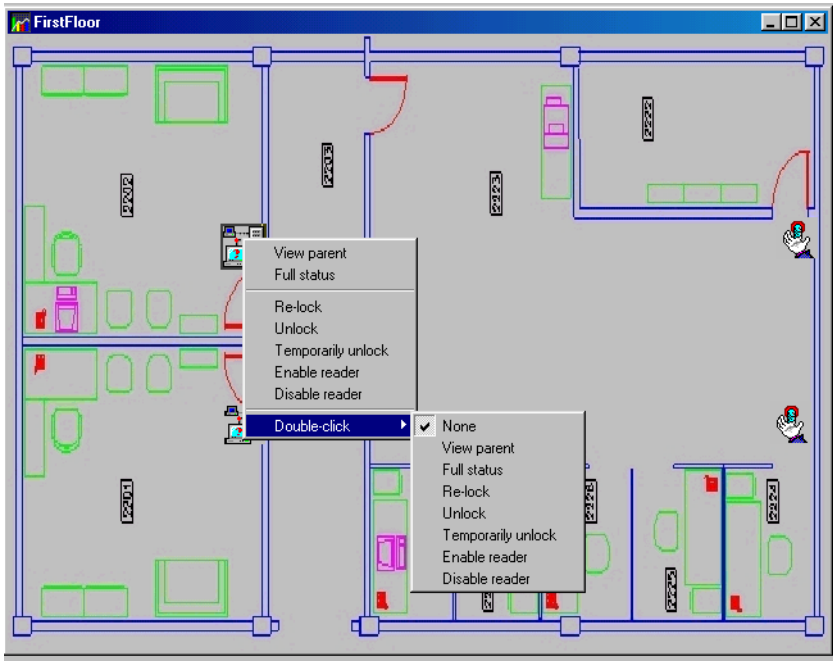


NOTE: If the screen is smaller than the graphic size, you can click-hold-and-drag the graphic to move it around within the Graphic screen.

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 via the Graphic desktop, the system does not save the modifications. You have to modify the default double-click feature via the* ***graphic definition*** *(****Definition*** *>* ***Graphics****, Design screen, right click a component >* ***Default dblclick*** *menu item).*

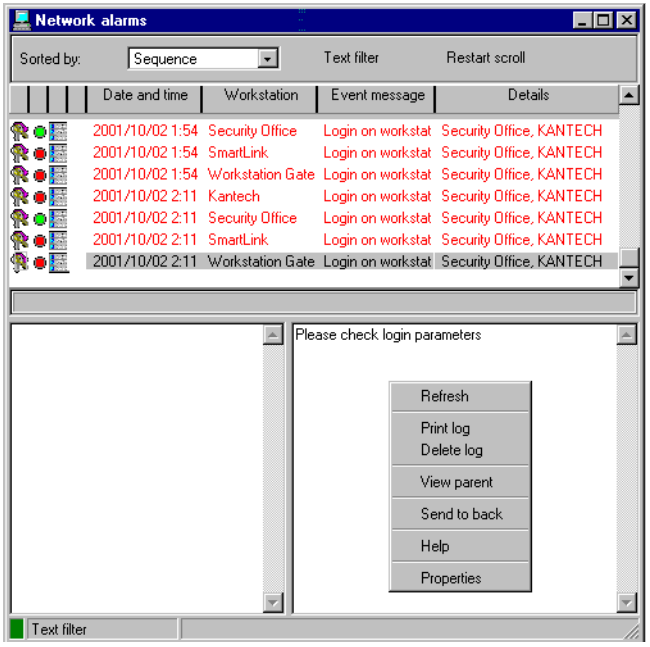
- For more information on how to create graphics and on how to assign components to graphics, see "Defining Graphics" on page 143.

Network Alarms Desktop

The Network Alarms desktop is used to view *all* the alarms in the system. Only events that require operator acknowledgment and that are programmed in the **Event Parameters** menu are displayed in the Network Alarms Desktop.

To view network alarms as well as their status:

1 Select the Network Alarms desktop.



2 Right click anywhere in the screen to enable a shortcut menu:

- **Refresh**: this options allows operators to load new alarm messages in the Network alarms desktop. The **Refresh** menu item is particularly useful when the server does not load automatically network alarm at startup; that is, when the **No reload network alarms on startup** option is checked in the Workstation definition menu (Devices> Workstation > Messages 1 of 2 tab).
- **Print log**—When selected, the system prints the alarm message.
- **Delete log**—Purges alarm records from the system as chosen in the **Delete network alarms** screen.
- **View parent**—Displays the parent components of the component in alarm.
- **Send to back**—This option only works when the window type is set to floating. It sends the active window behind the main screen (Alarms Desktop). To bring back to front, right click the desktop button, then select **Bring to front**.

- **Properties**—Display a Properties screen from which you can customize the alarms desktop display, such as adding icons, changing the background color, etc.

Other information...

- The system administrator cannot carry out any system operation from the Network Alarms desktop; only alarm can be deleted or printed from this menu.
- The network alarms are available on all workstations of the system. By default the server sends network alarms to all workstations at startup.
- If you do not want the system to "automatically" send network alarms, you can use the **No reload of network alarms on startup** option of the Workstation Definition menu. This option is useful when the connection between the workstation and the server is slow.
- To limit the number of records kept in the alarm database, use the **Maximum records on network alarm table** option of the **Server definition** menu. This option is used for the server and workstation alarm message databases.

NOTE: *Operators will only be authorized to view network alarms that were sent to the workstations that are selected in their security level definition menu.*

NOTE: *The **Delete network alarms** screen is called up with the **Delete log** command.*

Live Video Desktop

If the Live Video feature is enabled in EntraPass, you can configure a desktop as a Live Video desktop.

To define a Live Video desktop:

1. From the Desktop menu, right-click a desktop to bring up the Desktop properties window.
2. In the **Desktop name** field, assign a name to the new desktop.
3. Select the window type for this desktop.
4. Check the **Live Video screen** option.

To use the Live Video Desktop:

1. In the Desktop window, select the desktop defined as the Live Video desktop.The Live video display window appears.
2. Select an icon (in the lower part of the window) to determine for instance the size of the views or to display the Panel screen (a small window associated with the video display).

The following table shows the available options:

View Icon	Description
	Large. This view sets the screen to 1024x768 pixels
	Medium. This view sets the screen to 800x600 pixels
	Small. This view sets the screen to 640x480 pixels
	Tiny. This view sets the screen to 400x300 pixels.
	Creates a new video view
	Shows panel screen
	Edits Custom buttons functionality
	Edits the current video view
	Shows the help related to the Live Video desktop
	Closes the Live Video window

3 Click the **Property** button to edit the custom button functionality. This feature allows you to configure five buttons for performing specific tasks in the current view.

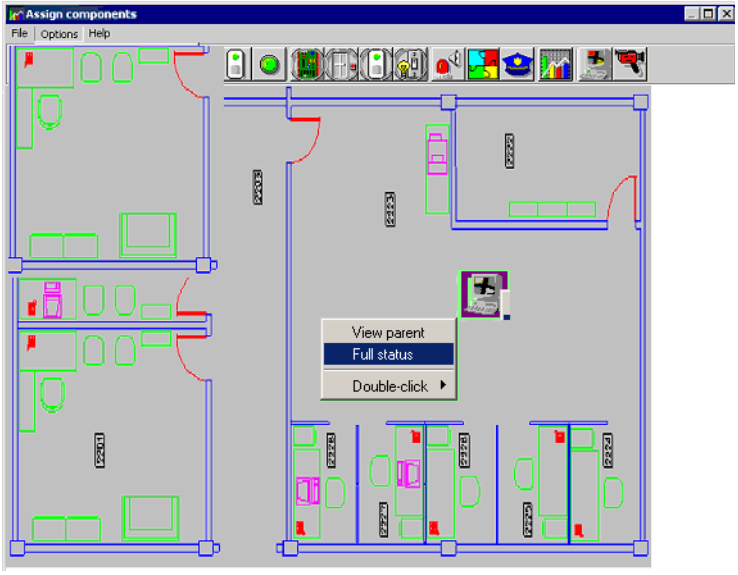
Video Server Status

EntraPass offers the ability to display parameters of the video devices connected to the Video server. Operators can for example view information related to network data transfer (images and digital sounds).

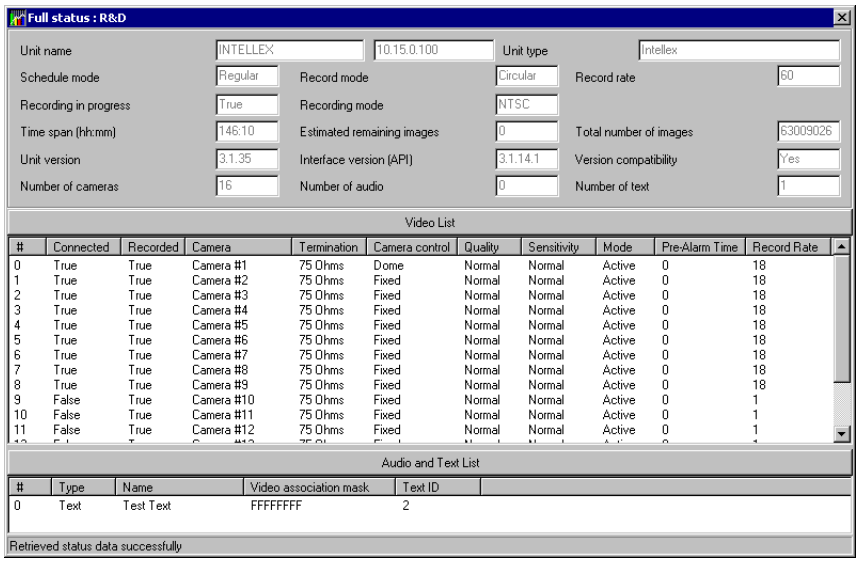
NOTE: *Installing and using the Live Video feature may take a great amount of your company network bandwidth (LAN or WAN). The network administrator may control the use of the network bandwidth for Live Video transfer.*

To view the Video Server full status:

1 From the Graphic desktop window, right-click the Video Server icon to display a shortcut menu.



2 From the shortcut menu, select **Full status** to display information about the video server status.



The content of the Full Status window depends on the video server associated with EntraPass. The following list provides a short description of the displayed fields.

- **Unit name**: the network name of the remote DVMS system (Intellex in this example). The Unit name is followed by the DVMS IP address.
- **Unit type**: indicates the type of the unit. can be Intellex, Iris (network client), etc.
- **Schedule mode**: indicates the current schedule mode of the remote DVMS unit. It indicates how images are recorded by the DVM installation. The values for this field can be:
  - **Regular** (regular schedule)
  - **Single** (only a single camera)
  - **Custom** (a custom schedule has been set by the operator).
- **Recording in progress**: indicates the current recording statue of the remote DVMS unit. Values can be:
  - **True**: is recording
  - **False**: is stopped.
- **Time span** (h:mm): indicates, in seconds, the time interval between the oldest and newest images in the database.
- **Unit version**: indicates the official version of the DVMS unit.
- **Number of cameras**: indicates the number of cameras connected to the Video server. The source of the video data is generally a camera, but it may also be a television station or other video source.The value varies from 0 to 16.
- **Record mode**: the record mode can be linear or circular.

- **Linear**: if you select this option, the recording will continue uninterrupted until the available space is finished.
- **Circular**: if you select this option, the DVMS will notify the operators before the recording space is completely filled. The operator will then choose to continue the recording or to stop it. By default, the recording mode is set to Circular.

- **Recording mode**: indicates the recording standard of the remote unit. The recording standard depends on the area.Values can be:
  - **NTSC**: the NTSC standard is mainly used in America and in many Asian countries such as Japan and South Korea.
  - **PAL**: the PAL standard is mainly used in Germany, Great Britain, China, Australia and Brazil.
- **Estimated remaining images**: indicates the estimated number of frames that may still be recorded in the video database before the DVMS unit space is completely filled. This option is only useful if the recording mode is linear.
- **Interface version (API)**: Indicates the version of the application interface between EntraPass and the selected Video server.
- **Number of audio**: indicates the number of audio streams available of the video server unit. The source of the audio data is generally a microphone, but may be another audio source.
- **Record rate**: indicates the rate code value. This value indicates the aggregate recording rate for the DVMS unit in number of frames per second. The value can be: 1, 2.5, 7.5, 15, 30, 60, 120, other value.
- **Total number of images**: indicates the total number of images in the remote unit's database.
- **Version compatibility**: indicates compatibility between the versions of the DVMS unit and the application interface used.
- **Number of text**: indicates the numbers of text data streams available from the DVMS. The text data source may be a cash register or other device.

Chapter 13 • Defining and Requesting Reports

EntraPass software allows users to define and generate reports. These reports may be generated automatically or requested manually. The Report toolbar displays the icons required to create reports.

There are three types of reports:

- **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.
- **Quick reports**: these are based on selected group of events (i.e.: door, controller, etc.) and event types (normal, abnormal, etc.)

From the Report toolbar, EntraPass users may also:

- View reports— this feature allows an operator to preview and to view report details, or to print pre-defined reports.
- View Report states—this features allows an operator to view the status of all reports in execution.
- Perform Manual operations on Time and attendance reports to add, insert, and delete Time and attendance entries.

Defining Historical Reports

The Historical report definition feature allows users to define customized historical reports and card use reports with their own automatic execution parameters.

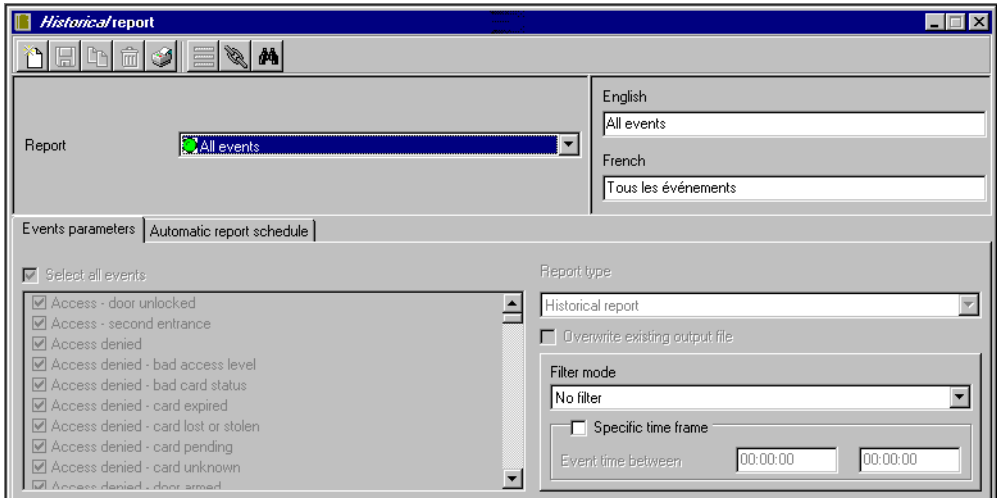
Reports that are defined with automatic settings are automatically generated at the specified time. However, they may be requested manually when needed. The “Historical Report Request” menu enables operators to trigger reports by overriding automatic settings. When requested manually, automatic settings are ignored.

Defining a Default “All events” Report

You may generate a default report that will include all events. The default report is a Historical report type.

To generate a default “all events” report:

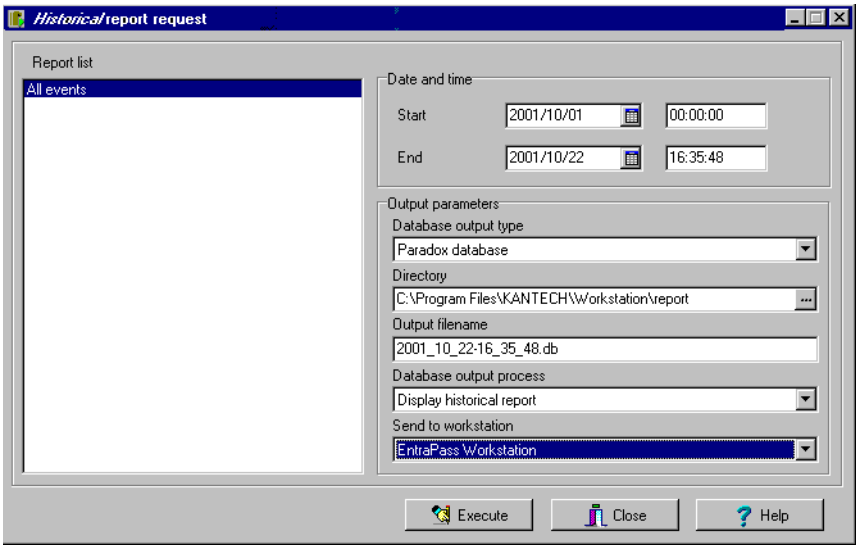
1 Select the **Historical report** icon from the Report toolbar. The Historical report screen appears.



NOTE: *Automatic report schedule features are set to default, you cannot change these features.*

Requesting an “All events” Report

1 Select the **Historical Request** icon from the Report toolbar. The Historical report request screen 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 “Defining a Report Output Format” on page 298.*

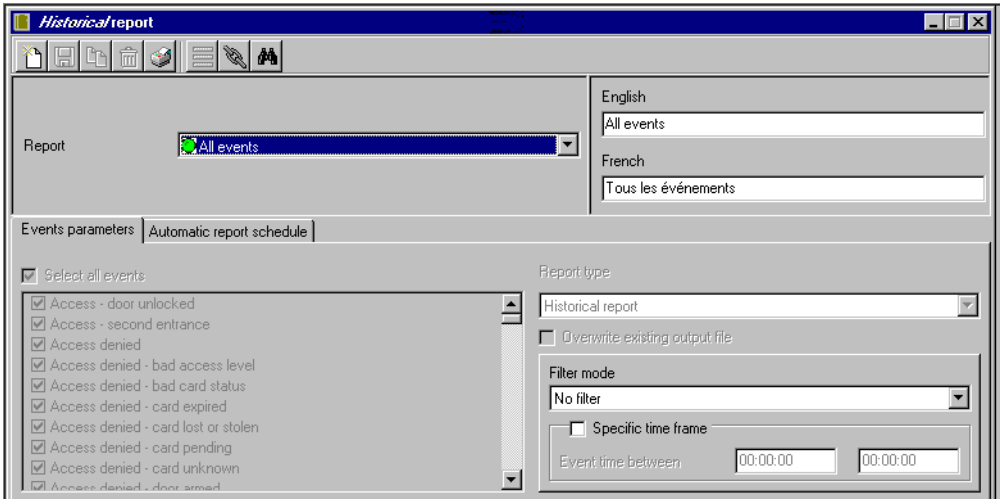
4 Select the **Report state** icon from the toolbar to view the report status.

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.

Defining a Custom Historical Report

To define event parameters for a Historical report:

1. From the Report screen, 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 screen when the selected report is a **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".

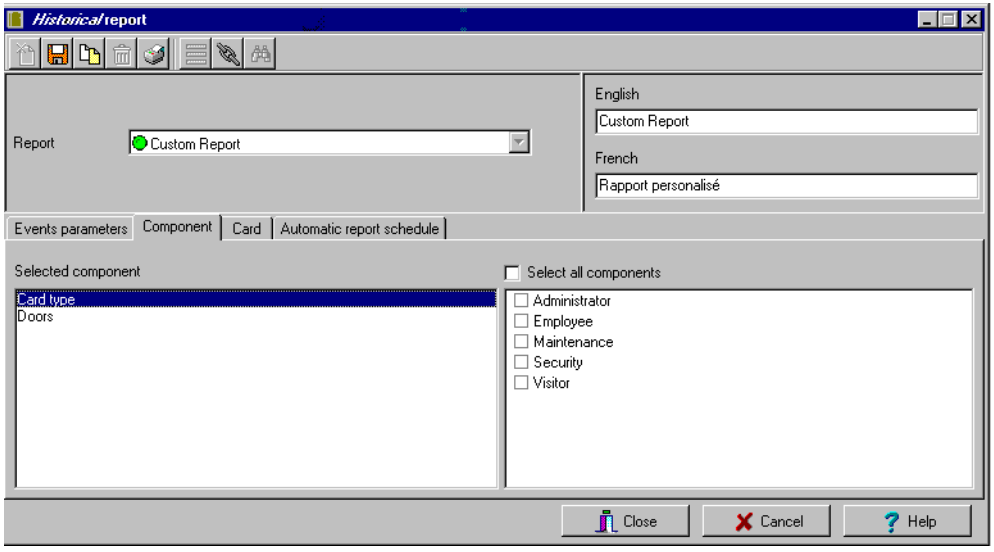
7 *Historical Reports Only.* Select the **Filter mode** if you want a report from specific components. These filters are used to target specific events that were generated from selected components. You can select various filtering methods. When you use this field, you have to specify which component(s) 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.

To define components for a Historical Report

When you have selected the **Historical report** type and when you have selected a **Filter mode**, you have to specify the components and filters that may affect your report. To do this:

1 From the Historical report screen, selected the **Components** tab. The Components screen lists all the component types that have a direct link with the selected events.

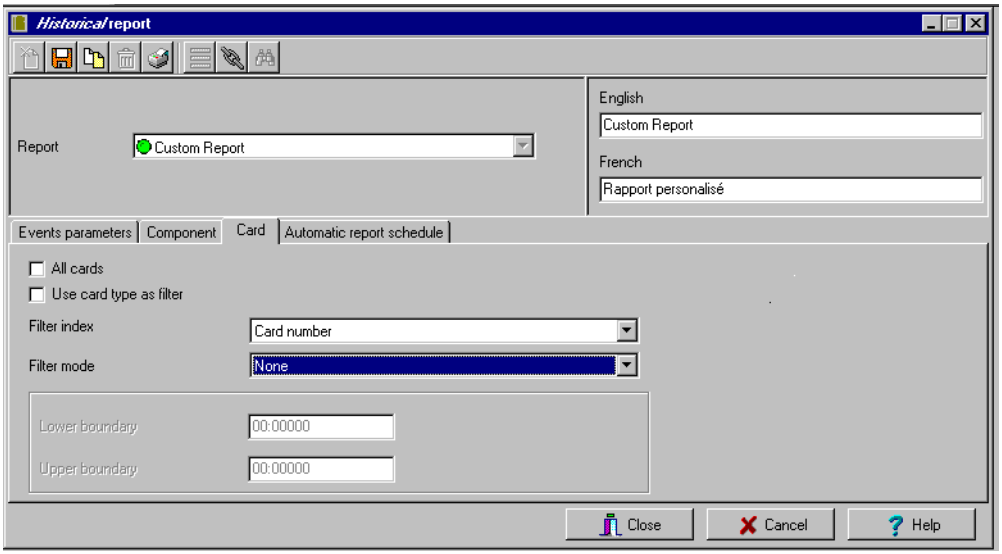


2 Select an event type to display its items in the right pane. If you select **Card type**, the right pane displays all the card types defined in the system. If you select Doors, all the access system doors are displayed in the right pane.

NOTE: *When an item in the left pane (Selected components) is selected, its color changes (turns red). When it is deselected, it resumes to the default color.*

To define card options for a Historical report:

1 From the Historical report definition screen, 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.



2 Select the **All Cards** option to include all cards. The other fields are disabled. When you select the **Use card type as filter** option, you can add filters for your report.

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 what you have selected 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 users 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.*

Defining 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.

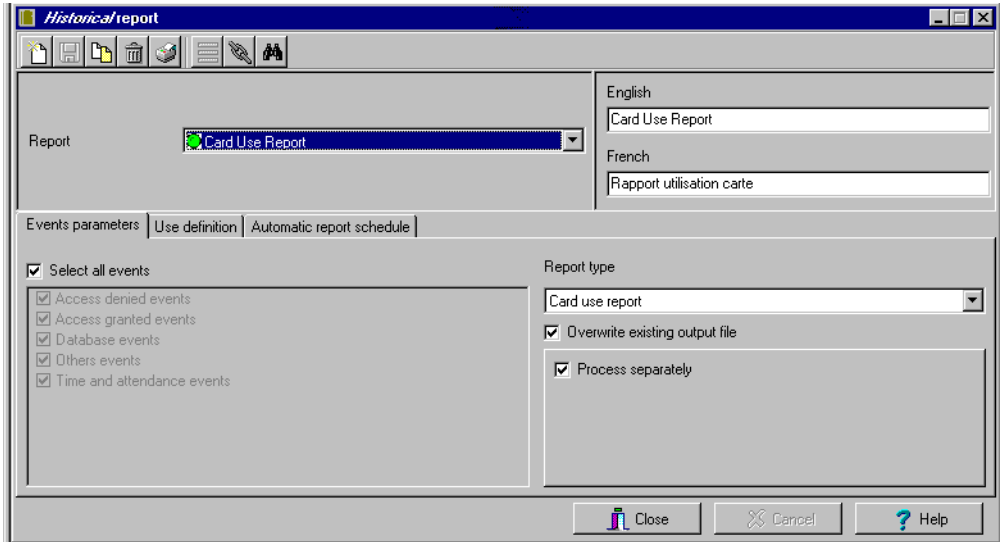
NOTE: *When you select a card use report option, the Use definition tab appears in the Historical report screen. It allows you to define the card use parameters, such as: used since a specific date, not used since 30 days before today, etc.*

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).

To define a card use report:

1. From the Historical report screen, 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. 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 pane.
3. 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.

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**.*

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 calender when you click the **Calender** 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.

Defining Automatic Report Schedules

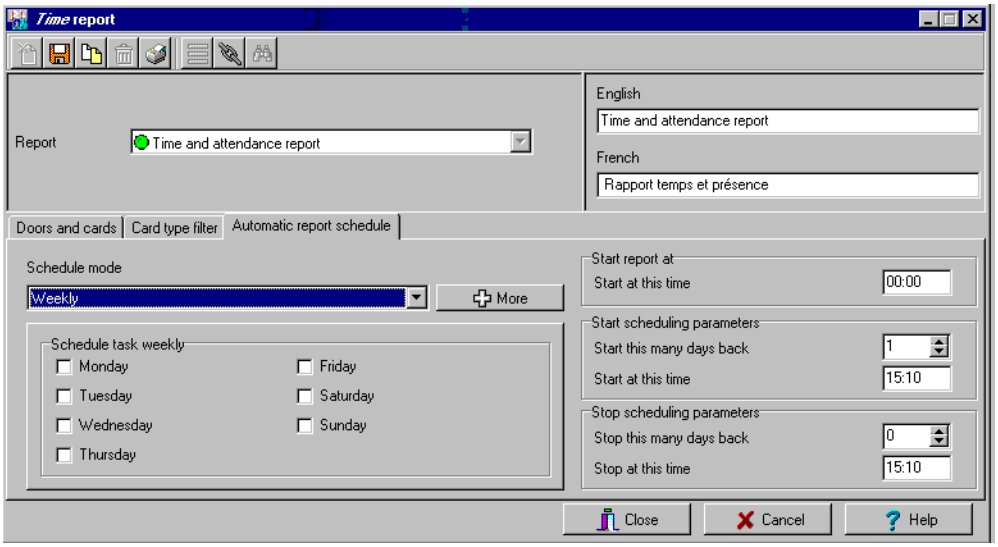
For both Historical and Card use reports.

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 destination (workstation),
- The language and the filename.

To define an automatic report schedule:

1 From the Historical report screen, 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** ***Only for Historical Reports.***

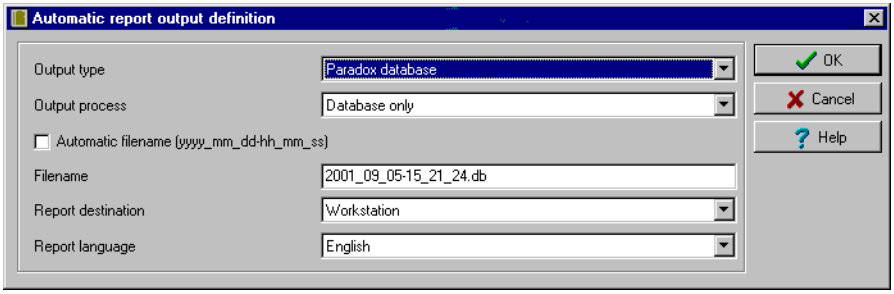
NOTE: *These settings are* ***ignored*** *when the report is requested manually by an operator.*

- **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.

- **End 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.*

5 Select the **More** button to add more settings to the automatic scheduled report. When you click the **More** button, the Automatic report output definition screen appears.



6 From the **Output type** drop-down list, select the output format of the report. You may choose Paradox, Dbase IV, or CSV formats.

7 You may check the **Automatic filename (...)** option. The default file name is YYY_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
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

The following table summarizes 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**

8 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, refer to the next section.

Defining 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 "Previewing Historical Reports" on page 310. 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 of the destination workstation.

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 of the destination workstation. The report is saved in the reports folder in the specified format, but not displayed.

Time and Attendance Reports

NOTE: *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 "Previewing Time and Attendance Reports" on page 311.

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**—Select the workstation to 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.

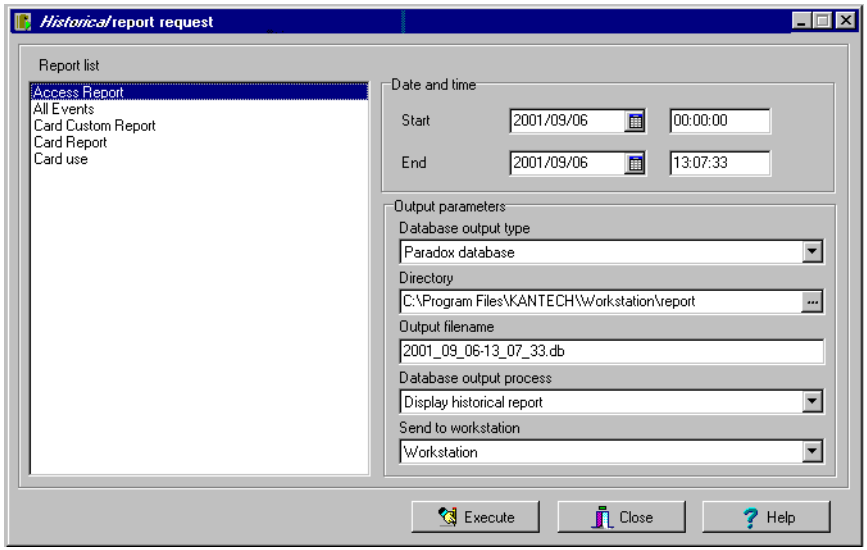
Requesting Historical Reports

With this feature operators can request pre-defined **Historical reports** or **Card use** reports that were created using the Historical Report menu.

NOTE: *If your report contain automatic settings, these will be ignored. You must indicate new settings.*

To request Historical reports manually:

1 From the Report toolbar, select the **Report Request** icon. The Report request screen appears.

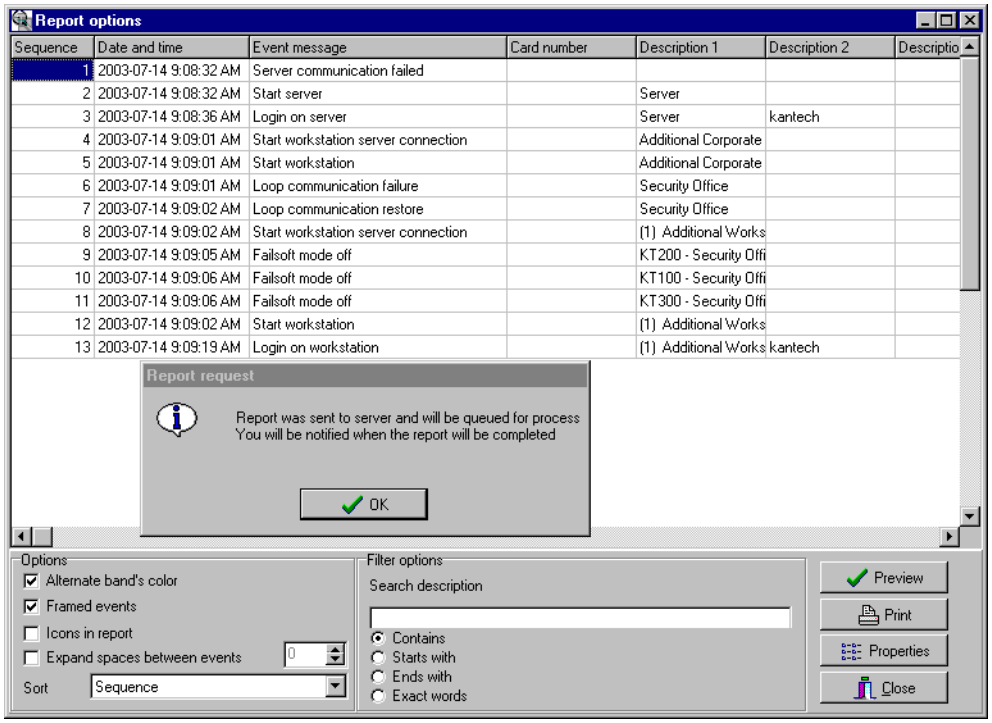


2 In the **Report list** display pane, select the report that you want to execute.

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 “Defining a Report Output Format” on page 298.

NOTE: *Once a Card use report is selected, the “Date and time” section is disabled.*

4 Click the **Execute** button. A system message informs you that the report is being processed. The Report options screen appears and is then minimized to the task bar.



5 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)

6 Enter the **description** in the **Search description** field. The report is updated in real-time when you enter a filter option.

7 You may use the **Preview** button 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 screen, you can save the report (in a.QRP format) or print the report.

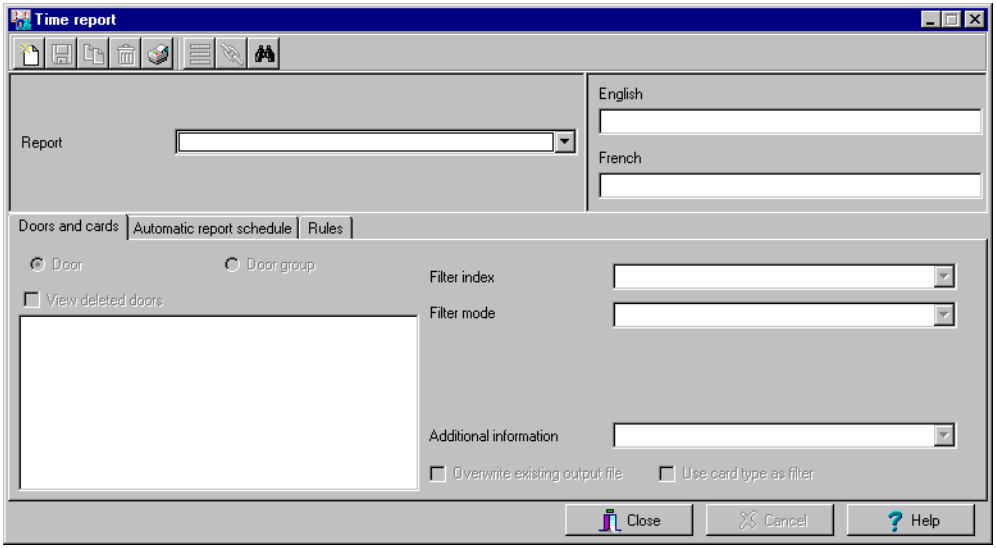
Defining Time and Attendance Reports

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 You may select a **Filter index** from the drop-down list. When you select a Filter index, you have to specify the filter mode and to enter the value range in the **Upper/Lower boundary** fields according to what you have selected in the Filter mode field. You may also select a multi-filter index to narrow down the output report.

4 From the **Filter mode** drop-down list, select a filter mode (None, Include, Exclude). To include all the cards, leave the "filter mode" to **None**. For example, if you select Card number as the Filter index, you have to leave the filter mode to **None** so that only events in which the defined card numbers appear will be selected.

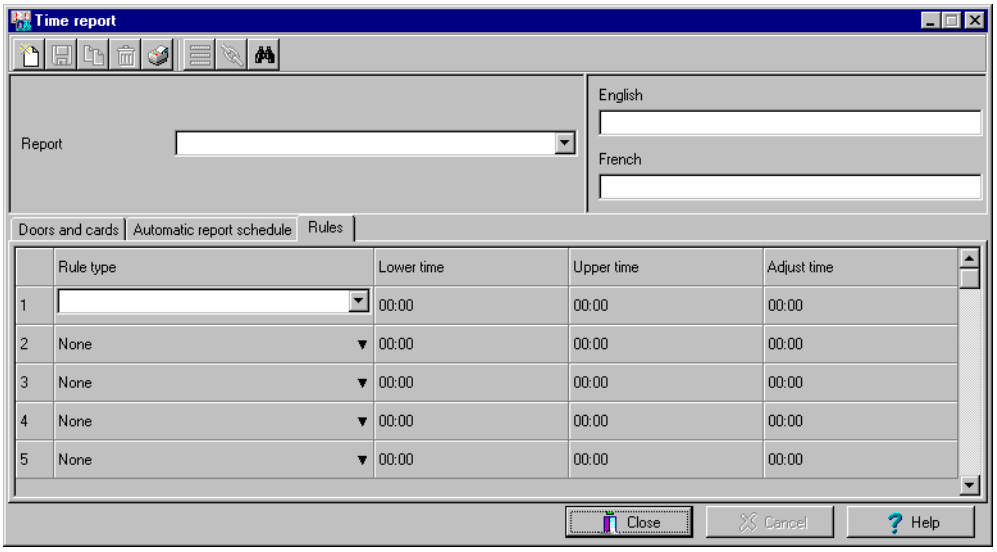
5 To add information in the sort criteria, select an item from the **Additional information** drop-down list. You have to repeat these steps for all the card information fields that are listed in

the filter index field. You could use the card user name and specify A to F in the **Upper/Lower boundary** fields. As a result the system will 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).

6 If you want the system to modify the same file, check the **Overwrite existing output file** option. If you leave this option unchecked, the system will create another output file.

7 Select the **Use card type as filter** option, if applicable. When this option is selected, the Card type filter tab is displayed.

NOTE: *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.*



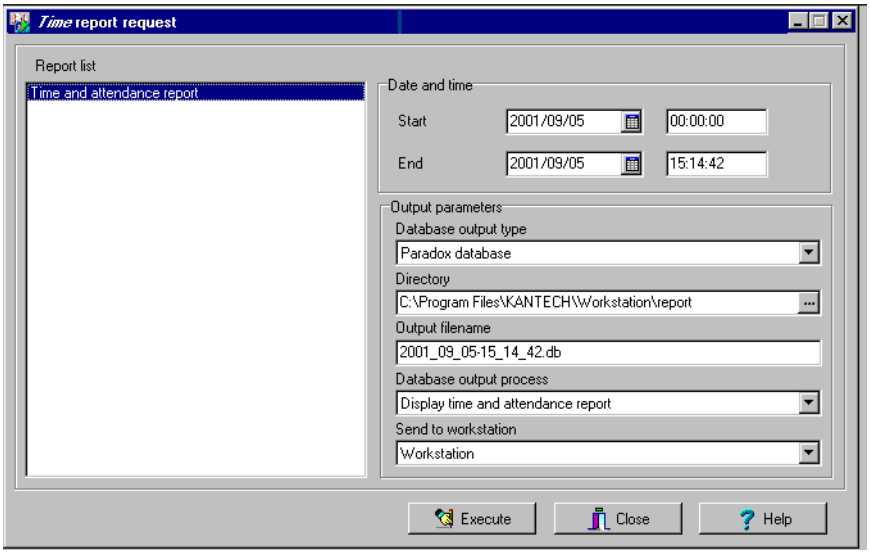
Requesting Time and Attendance Reports (T & A)

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 **Time report request** icon. The Time report request screen 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 the **Execute** button to trigger the report.

NOTE: *The Time and Attendance report is automatically saved in the output folder of the specified workstation. It is not printed nor displayed. You will have to retrieve it manually to view. You can also use the View report icon in the Report toolbar. For the Paradox output type, a report preview screen will appear with the report details section and a report request section. For details on reports output formats, see "Defining a Report Output Format" on page 298.*

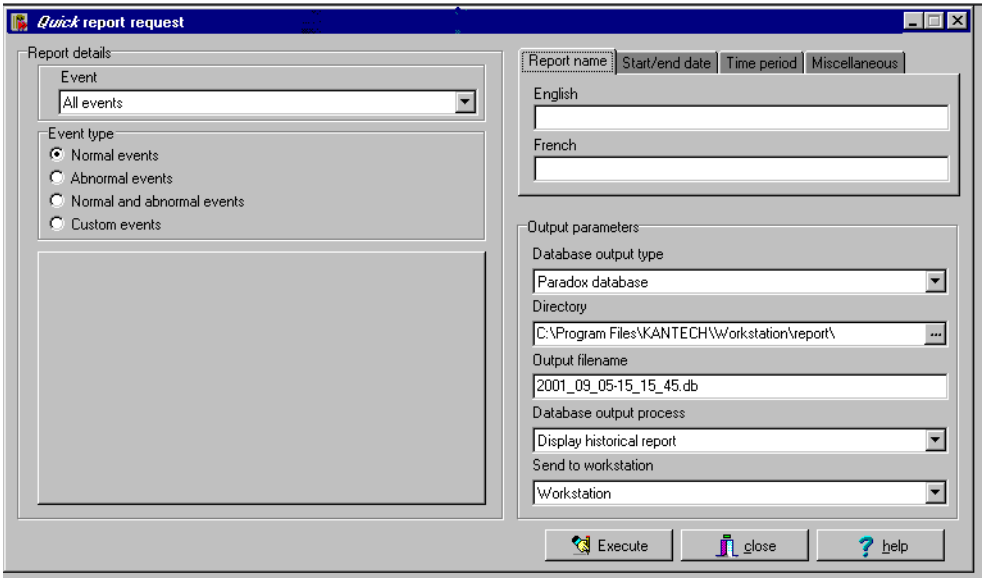
Defining a Quick Report

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 screen.

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 selects 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 indicate if all cards are to be included in the report or to add filters if you want to generate a report for a range of cards.The **Card** tab appears only if a card-related event is selected.
   - In the **Filter 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.
   - In the **Filter mode** drop-down list, specify if the system should exclude or include the range specified in the "Upper/Lower boundary" fields.

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. As a result the system would 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.*

5 Select the **Report name** tab to enter the name of the report (this name will be displayed on your report).

6 **Start/end date** tab allows the operator to indicate 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, then this event will not be included. To target events that occurred during a specific time frame, you can use the **Specific time frame** option.

7 Select the **Time period** tab to include events that match the specified time frame.

8 Select the **Miscellaneous** tab for additional options: select the **Overwrite existing output file** if you want to replace the existing default output file.

9 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_CE \Report\your file.xx
   - **Output filename**—Indicates the output file name. By default, reports are saved on disk in C:\ProgramFiles\Kantech\Workstation_CE \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 report template, which must be used with the requested report.
- **Send to workstation**—Select the workstation to which the quick report should be sent.

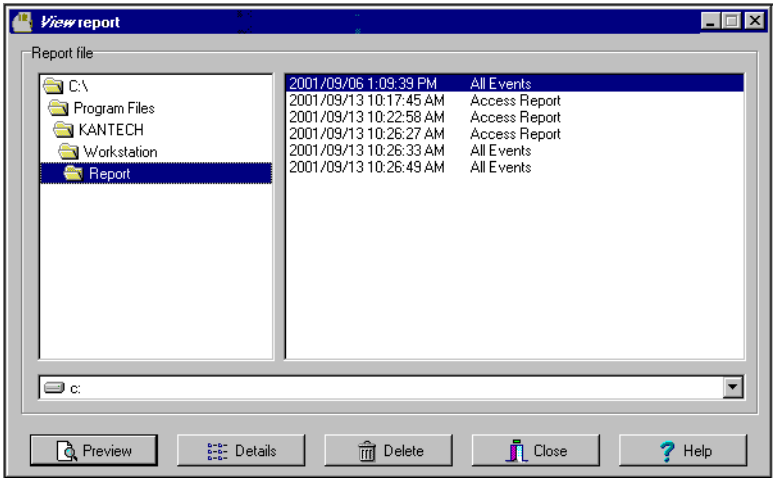
Viewing Reports

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 screen. When you click "Preview", the system automatically launches the appropriate program to view the report.*

To display a report:

1 From the Report screen, 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 screen) to the report you want to display.



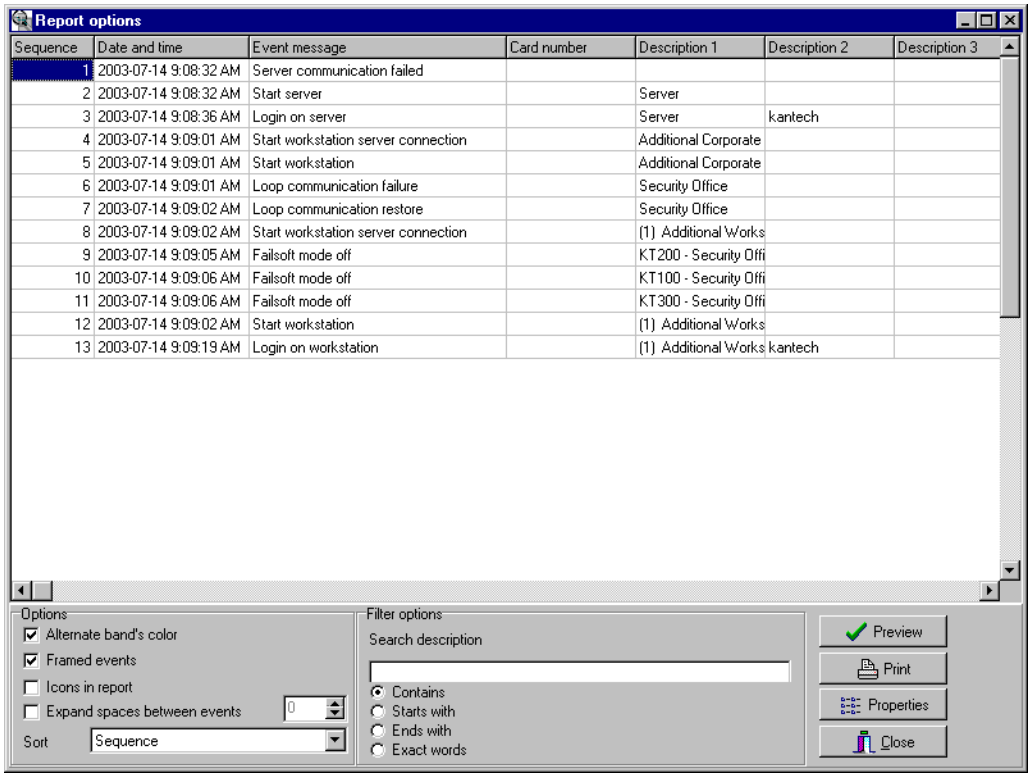
2 Select the report you want to view. If there is a printer installed, the **Preview** button is enabled. It is used to preview the report before printing it.

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 **Preview** button to view the report in the system displays the Report preview screen.

Previewing Historical Reports

1 From the View report screen, select the report you want to view in the right pane. If you select a Historical report, the following screen 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.

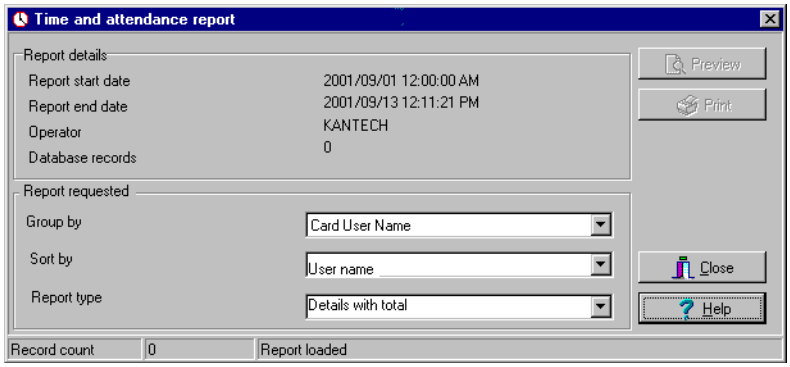
4 Click the **Preview** button. The system displays the result of the report. From that screen, you can save the report (in a.QRP format) or print the report.

5 Use the **Properties** button 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.

Previewing Time and Attendance Reports

1. From the **View report** screen, 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 screen 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 the **Preview** button to display the result of the report. From that screen, you can save the report (in.QRP format) or print the report.

Report State

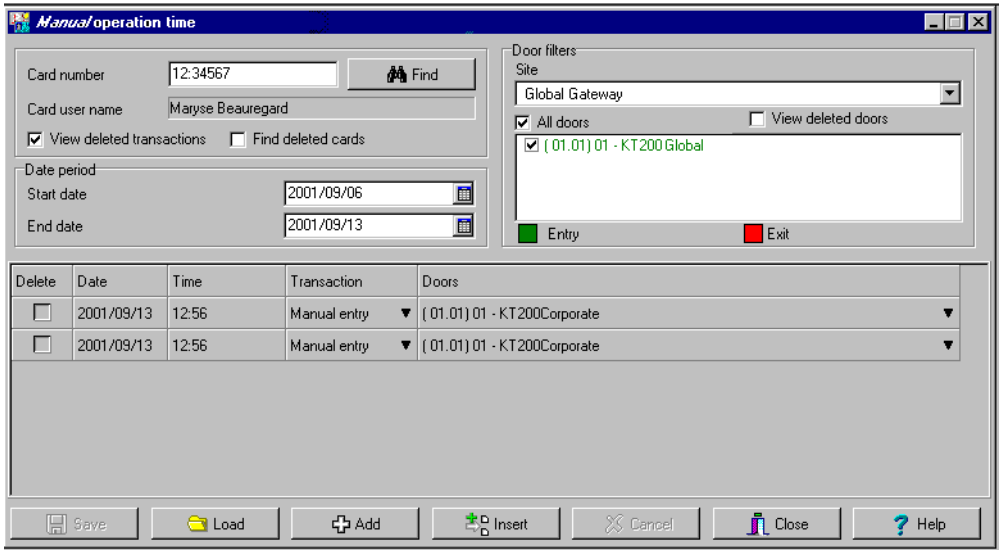
Use the **Report state** feature to display a list as well as the status of all requested reports that are still pending. To delete/stop a pending report, select it, then click **Cancel**.

Manual Operation On Time and Attendance

Use the Manual 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 screen, select the **Manual operation on Time and A**ttendance icon.



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 **Calender** 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.

You may check the View deleted doors option. 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.*

9 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 your are inserting an exit transaction, only doors defined as “Exit doors” will be displayed in the list.*

10 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.

11 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.

12 Use the **Insert** button to insert a transaction between existing transactions or above any transaction.

13 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.*

Chapter 14 • The EntraPass Server

The EntraPass Server is a dedicated computer on a network that manages the access control system database. It is used to receive and dispatch information received from the different gateways and workstations receiving information from connected controller sites.

In some applications, a Redundancy Server and a Mirror Database can be used as an alternative if the Primary server failed.

The EntraPass server can be used for:

- Displaying all the workstations connected to the server, the system event log and system error log
- Registering new connections and system options (workstation, gateway, client applications, etc.)
- Creating and restoring backups (Data, Archives, Time and Attendance databases)
- Restoring data (Data, Archive, Time and Attendance databases)
- Verifying database integrity,
- Changing the database language,
- Cleaning the database by clearing records relating to previously erased data.

Launching the Server

In order to access the EntraPass Server commands, you have to start the Server and login. Operators are identified when they login. This allows them to have access to the security system menu associated with their access level, and to establish communication and initiate interaction with the workstations. However, it is not mandatory to login for the Server to operate.

To launch the Server:

1. From the Windows Start menu, click **Start** > **Programs** > **EntraPass Corporate** > **Server** > **Server**. You may also click to the **Server** icon on the desktop, if applicable.
2. Enter your **User name** and **Password** (case sensitive) and click **OK** to continue. To modify this password, see "Operator Definition" on page 242.

NOTE: *To allow an operator to login to the server, select the "Allow login on server" option, during the Security Level definition of an operator. For more information, see "Security Level Definition" on page 245.*

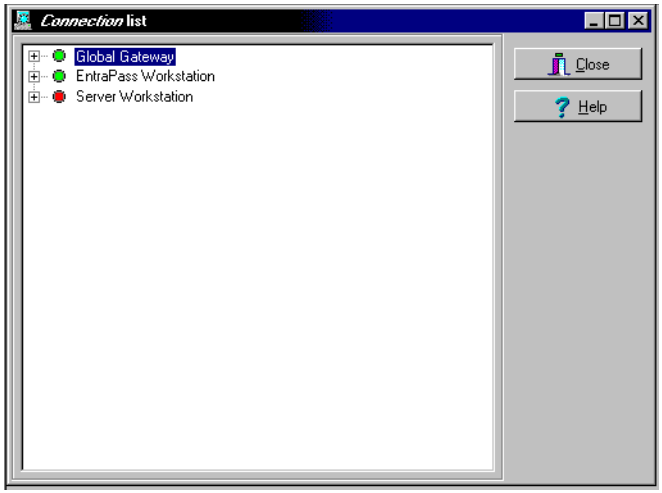
3. To login to the server, click the **Login/Logout button**, the system displays the login screen. The status bar indicates the communication status: Green: Communication is OK, **Red**: Communication problems.

The colored flags represent the status of a system logical or physical component.

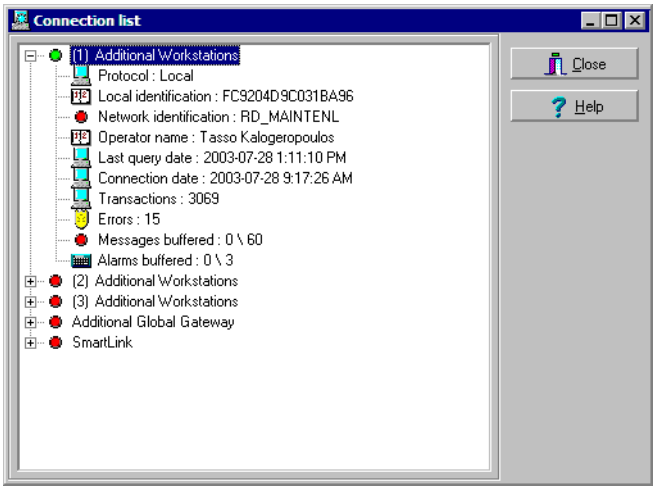
- Database state availability state,
- Database locked state: it turns red when the database is locked,
- System date and time,
- Login name of the operator who is currently logged in the Server,
- Number of client connections, that is, the number of workstations connected to the server,
- Number of system logs (messages and events),
- Number of error logs,
- Computer name (NetbEUI) where the server is installed,
- Server's IP address,
- Secondary IP address, if the Mirror database and Redundancy server communicate with the server through a TCP/IP connection and if they are configured in the system,
- Other IP address, if applicable.

Viewing the Connection list

1 Start the server (from Windows Start menu or the shortcut on the desktop).

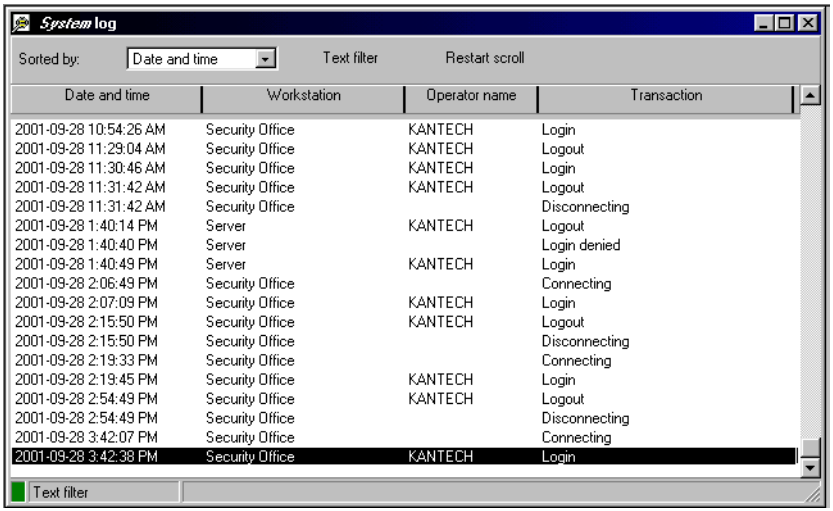


2 Click the + sign beside each workstation to view details about a workstation (such as: registration codes, TCP/IP address, connections, messages buffered, etc.).



3 To view system log, select the **View System Log** icon. The System Log screen contains all the login and logout events for all workstations defined in the system. The logs are displayed with

date and time, the workstation name, the operator name using the workstation as well as they type of log.



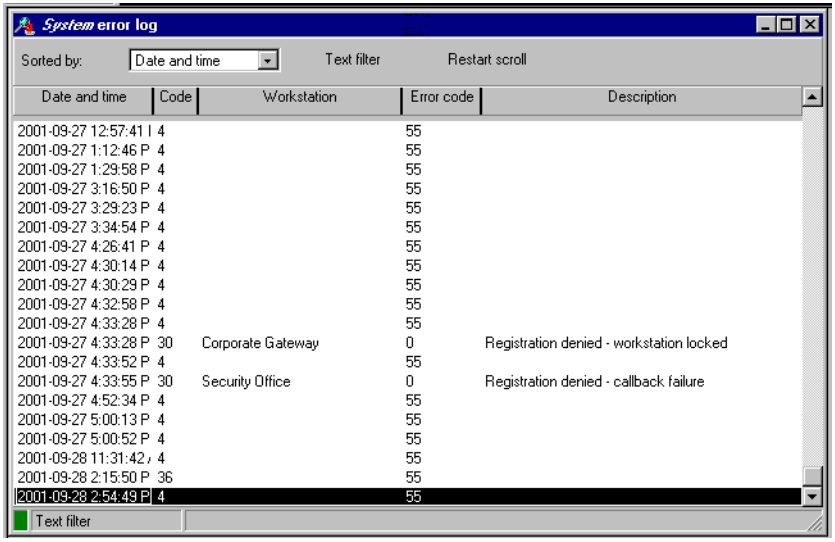
4 From the Sorted by drop-down list, select the sorting criterion: the system events will be displayed according to your specifications.

- **Date and time**— This is the normal incoming sequence, if you select another sorting mode, you interrupt the normal sequence. Select date and time to restore the normal sequence. To do this, you have also to use the “restart scroll” button.
- **Operator**—When selected, all columns will be sorted according to the **Operator** column in alphabetical order.
- **Workstation**—When selected, all columns will be sorted according to the **Workstation** column in alphabetical order.
- **Text filter**—When selected, a new screen will be displayed. From that screen, enter the text string (i.e.: kantech), and the system will only display logs containing the specified string text. To return to normal display, click on text filter.

5 You may change the **background color**. To do this, right click on the screen and select a color from the displayed short-cut list.

6 You may also clear the screen. To do this, right click in the window, then select **Clear** from the shortcut menu.

7 Select the **View system errors** icon to view all the errors that occurred in the system. The system errors are displayed with the date and time, the workstation name where the error originated from, the code number and its description.



8 You may also use the right-click menu to change the window background or to clear all the data displayed.

NOTE: *For information on system registration, see “Installing the System” on page 11.*

Creating/Restoring 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 manually 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
  - The EntraPass Backup Scheduler to apply automatic schedules parameter, 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.

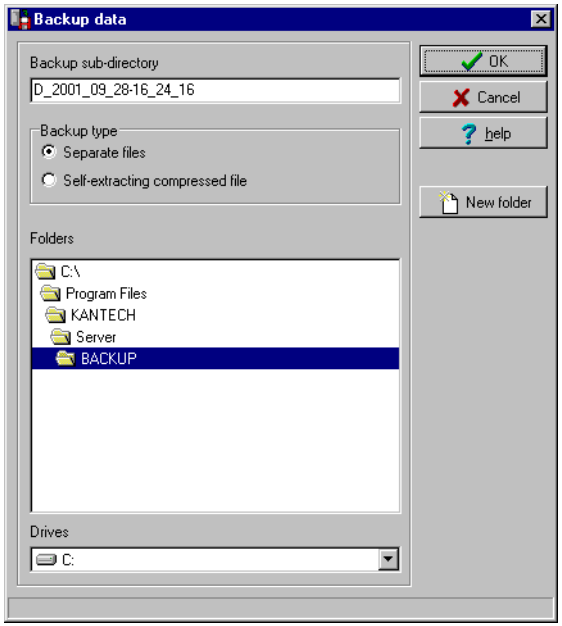
Each time a backup is done (even if it is done automatically), a new sub-folder containing the data or the self-extracting file is created. If you are using the “incremental” backup type and you want to restore information, you will have to restore all the sub-folders one-by-one (starting with the oldest).

To create a backup:

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).

NOTE: *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.



2 Select the Backup type:
- **Separate file**: the system will back up the databases one by one (standard)
- **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.

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 screen.

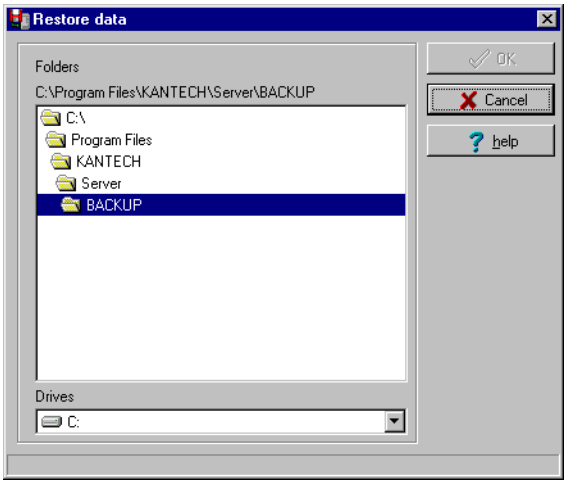
NOTE: *You can use the "Backup Scheduler" to schedule or plan automatic backups. To schedule automatic backups see "EntraPass Utilities (Options)" on page 359.When you backup or restore files, the Server databases are temporarily disabled. You cannot modify the databases when a backup is in process.*

To restore archived data:

If you are restoring information, it is strongly recommended to perform a backup before restoring the data.

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 screen. It displays the path of the backup folder.



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**).*

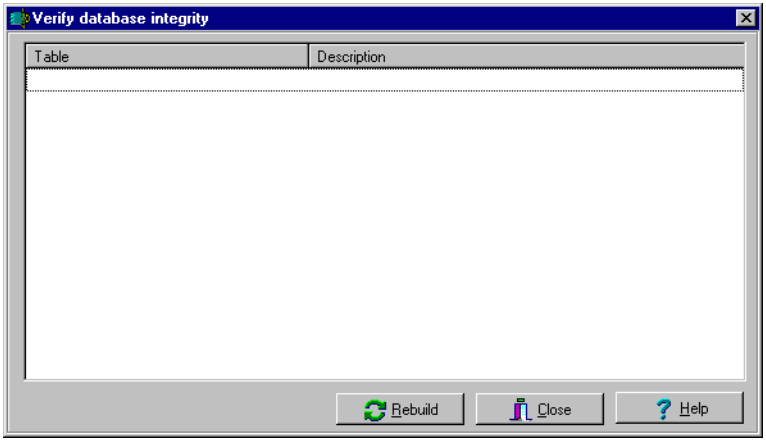
Using the Server Utilities

This menu allows users to verity the system database integrity and to restore the system data bases. This menu is also accessible from workstations. For more information on the system utilities, see Chapter 15 ‘System Utilities’ on page 327.

To use the system utilities:

1 Select the **Utility** tab to use the server utilities.

2 Select an icon in the toolbar.



3 Click the **Rebuild** button. The system automatically starts the operation and displays a progression bar indicating that the process is on-going.

NOTE: *Certain windows may provide only a Yes or No button rather than a Rebuild button to start the operation.*

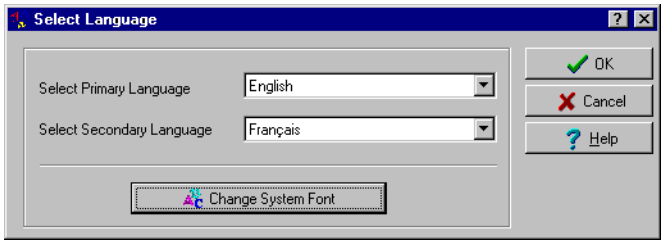
NOTE: *The Clean database utility also provides a Yes or No button to clear records from the database relating to previously erased data.*

Swapping the System Language

In order to have the system run in the language of your choice, first change the system language (Option > Select a language) and then run the **Swap description** utility.

To change the system language:

1 From the Server main window, select the **Options** tab.



***NOTE:* Important!** *When you modify the primary language of the database, the database operation will be suspended during the operation (not available for users) and the changes will be effective only when the server is shutdown and restarted.*

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 Shutdown the server.

4 Restart the server and login.

5 Select the **Utility** tab, then select the **Swap descriptions** button.

6 Once completed, restart the server.

NOTE: *You may also click the* ***Change system font*** *button to modify the font: this option is used to select the font for the database.*

Chapter 15 • System Utilities

This section groups the utility programs of the EntraPass Software. These programs are accessible from the Windows **Start** menu. The following programs are launched from the server or the workstation.

- **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.
- **PING Diagnostic** —Program used to diagnose network intermittent related problems.
- **Quick Viewer —**Program used by the operator to view reports without having to start a workstation.
- **Vocabulary Editor**—Program used to translate, in the language of your choice, the display text of the software.
- **Workstation—Configuration Program**—Program, similar to a standard workstation, used by the system administrator to configure the system logical and physical components.
- **Migration Utility**—Program used to transfer database information for the upgrade from Special to Corporate Edition or Corporate Edition to Global Edition.

Database Utility, Workstation & Server

Since the information from the system databases is sent back and forth between the server and the workstation, some data might end up in the wrong table. 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.

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.

Some operations such as verifying the database integrity, index, links and hierarchy can be performed while the Server/workstation are up and running.

From a workstation, 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 workstation tables and correct errors (if they are found).

You may want to start this utility when your systems hangs up frequently.

NOTE: *You may also verify the system databases from the Server (Server > Utility). However, this will only allow you to perform "surface" verification. If you are experiencing problems (when the system hangs frequently, for instance), use the Database Utility program. To do so, you have to shutdown the server.*

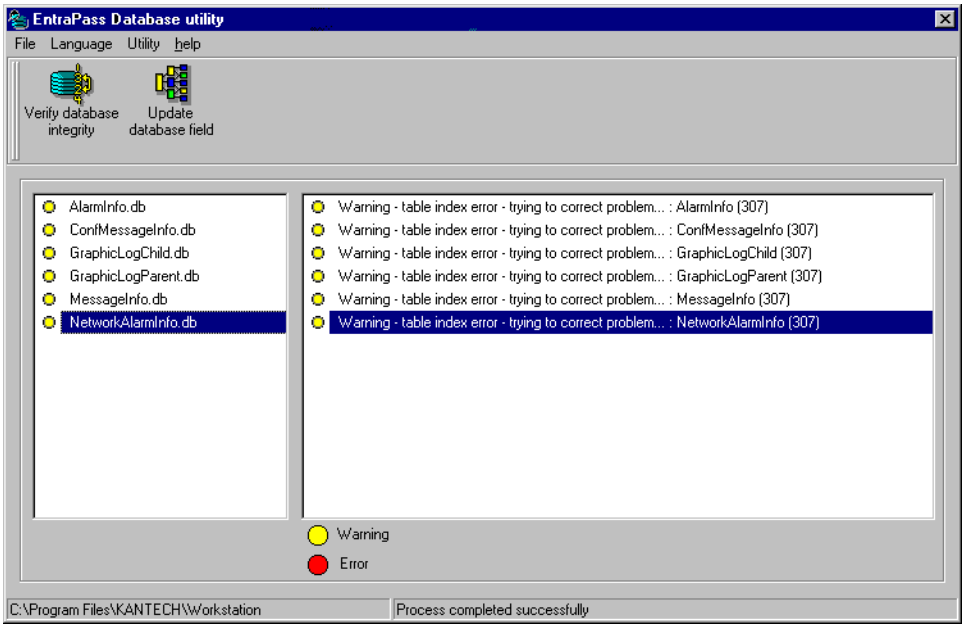
To verify the database integrity:

1. To verify the database integrity, click the **Verify database integrity** icon in the toolbar (you may enable this feature through the **Utility** menu also). You have the choice to perform a **quick** or **complete** check.

NOTE: *When you launch the Verify database integrity utility from the workstation Options menu, this is only a surface operation. When your system experiences problems, you have to run the Database Utility program.*

2. 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.

3 If you select a **Complete check of the database**, a detailed report is displayed.



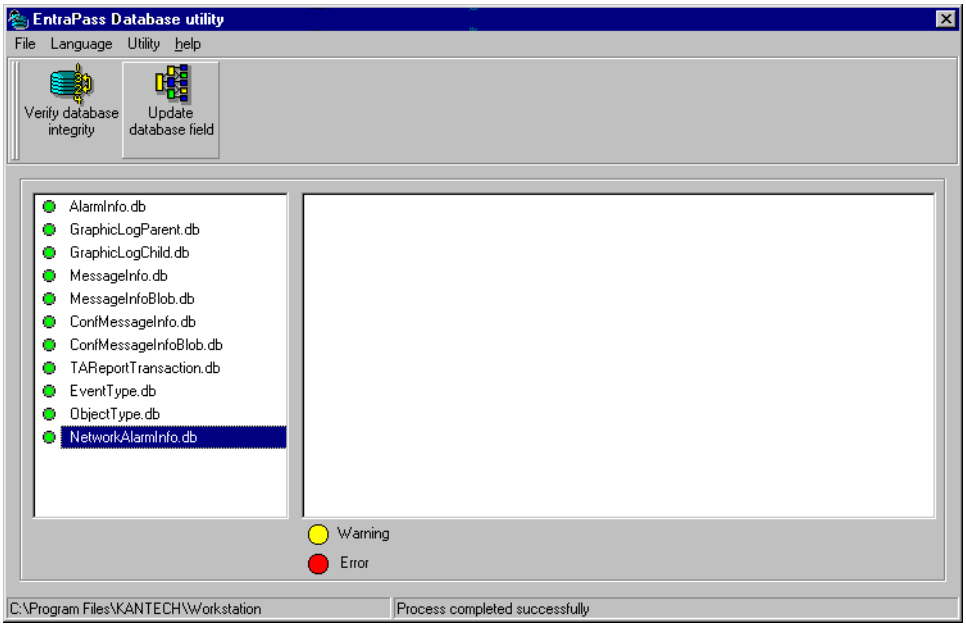
Update Database Fields

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.

To update the database fields:

1 From the EntraPass Database utility window, select the **Update database field** icon.



NOTE: *Use this function when for instance you experience problems when starting the server or workstation. 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.*

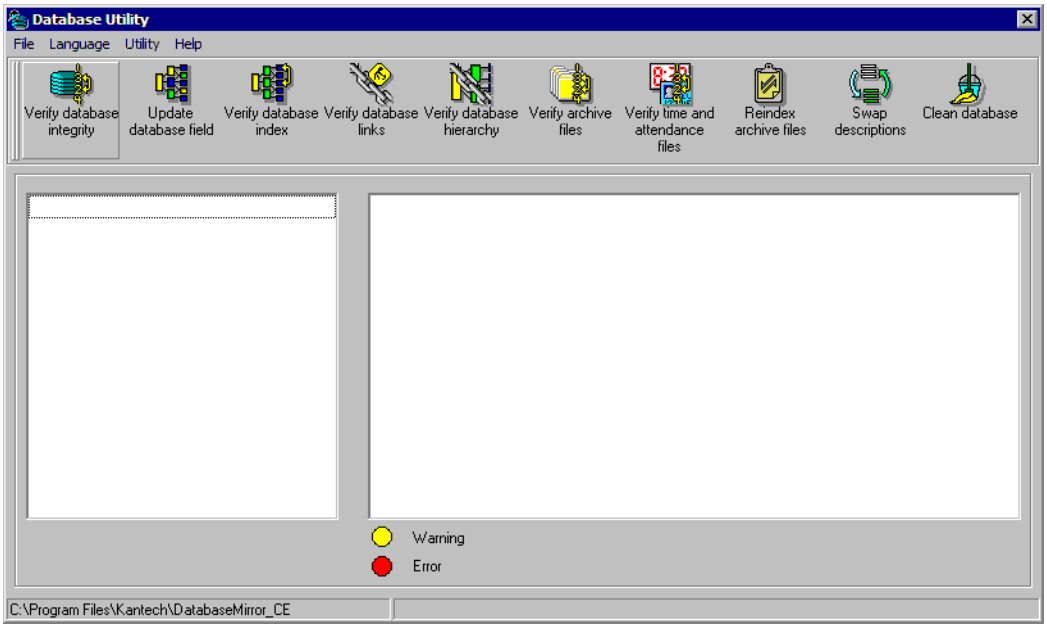
Database Utility, Server

Usually, the system verifies the database integrity automatically at start-up (a system message is displayed). If an operator decides not to perform a database check at startup, he/she may trigger the operation later, using the Database Utility program.

It may also be necessary to launch the database utility program when for instance the system experiences problems frequently. This operation should be executed when the system is not much used since the system databases are not available during operations on the databases.

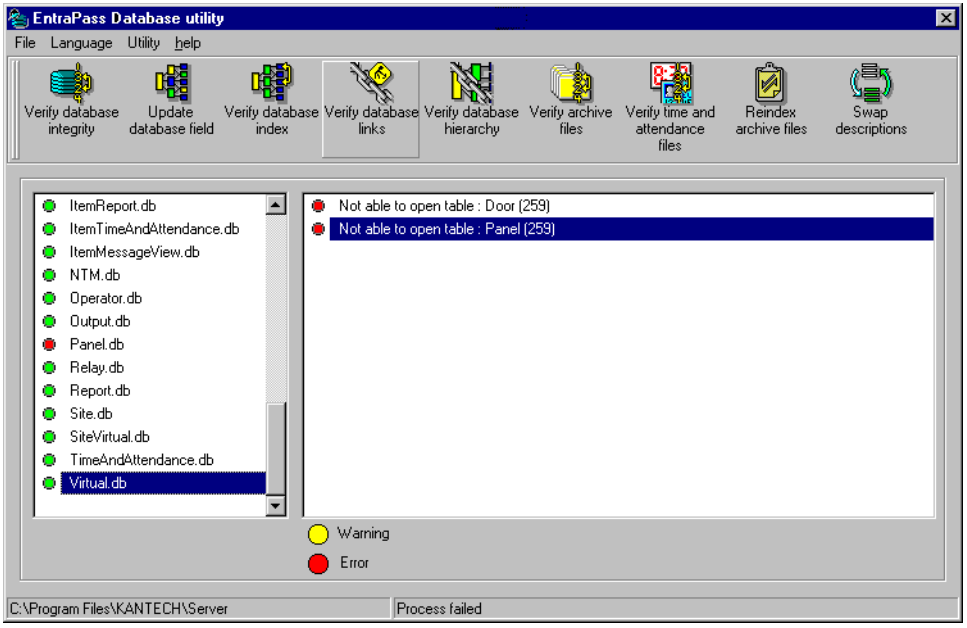
NOTE: *It is recommended to exit the Server before you run the Database utility.*

1. Exit the server program. During this operation, the system databases are suspended. A red square button in the status bar to indicates that the databases are unavailable
2. From Windows start menu, select **Start > Program > EntraPass Corporate Edition** > **Server** > **Database Utility**.



NOTE: *When you select* ***File*** > ***Workstation****, the system displays only two icons, the* ***Verify database integrity*** *and the* ***Update database fields*** *icons. The Server toolbar offers more choices.*

3 Select the icon or menu item corresponding to the program you want to execute. The system displays the result of the analysis.



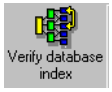
Update Database Fields

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 (copy the databases from a third party backup program), this function is automatically be carried out when the Server is started up again.

NOTE: *Use this function when for instance you experience problems when starting the server or workstation. 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.*

Verify Database Index



This program allows to entirely rebuild the index by using the information that was copied in the primary databases and grouping it to rebuild the Registry.DB database. The latter is used to increase the system performance.

NOTE: *This program can be used when a database is corrupted because it has not been backed up.*

Verify Database Links

The Verify Database Links utility is used to rebuild all the links of the database. Moreover, this program cleans the databases by deleting links that are no longer valid. For example, if a schedule was assigned to a functionality and this schedule was deleted, the system will initialize the field where it was assigned in the primary database. It will also remove the records that point to deleted components. For example, if an access level is assigned to a gateway and this access level was deleted, it will delete the record in the database.

The Verify Database Links utility enables complete management of the links between each component and ensures that the correct information is displayed when:

- Viewing the structure of a component's links to all other components of the system,
- Removing all the traces of a component within the database when this component has been deleted. For example, if a schedule is deleted, the system will use the link list to initialize all the database fields that contains this schedule.

NOTE: *It may be necessary to use this function when it is obvious that the database links are incorrect. This features is useful when for example the system experiences abnormal terminations.*

Verify Database Archive Files

This function is used to verify archive files. It assigns a new unique sequential value to all primary indexes of archive files.

Verify Time & Attendance Files

This function is used to verify time and attendance database files. It assigns a new unique sequential value to all primary indexes of time and attendances database files.

Verify Database Hierarchy

In EntraPass, the database is set up in a hierarchical way, which means that all components have a parent and can have child components.

The **Verify database hierarchy** utility is used to rebuild the parent-child links within the database. The results of this program are limited if the damages of the database are severe.

NOTE: *When a user tries to access a controller by selecting a gateway and a site and when the result does not correspond to the reality, this means that the database hierarchy is probably corrupted. In this case, the Verify database hierarchy feature can be used to correct the problem. If the problem could not be fixed, this could mean that the database is too damaged to be fixed. It will be necessary to restore the database.*

Swap Description

This function is used to interchange description #1 (primary language) with description #2 (Secondary language) in all the database of the system.

NOTE: *When this function is executed, the current primary language becomes the secondary language, and the secondary language becomes primary. This function must be executed with caution to avoid system language problems.*

Follow this procedure to modify the database language, otherwise the database operation will be suspended during the operation and the changes will be effective only when the server is shutdown and restarted.

To interchange the system languages:

It is strongly recommended that you to follow this procedure:

1. Modify the system language (**Server** > **Options**> **Select language** icon).
2. Shutdown the server.

NOTE: *If the server is not shut down, the Database Utility program will not operate.*

3. In the Database Utility main screen, click on the **Swap descriptions** button.
4. Start the server.

Clean Database

This option is used to physically remove database records which have been identified by the system as erased. Most of these records relate to cards and are kept in the Deleted Components section of the database. Using this option will considerably reduce the space required by your database. It will also improve system performance relating to searches for card information. It will not affect the table Registry, nor will it have an impact on historical reports.

To clean the database:

1. Start the **Clean database** utility (**Server>Utility> Clean database** icon).
2. Click on the **Yes** button.

NOTE: *It is strongly suggested to back-up the database before performing this operation.* ***Clean database*** *will suspend operation of the database while cleaning is in effect.*

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 display 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 screen (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.*

Installing the Vocabulary Editor

EntraPass Vocabulary Editor is a stand-alone program. You can install it and run it independently.

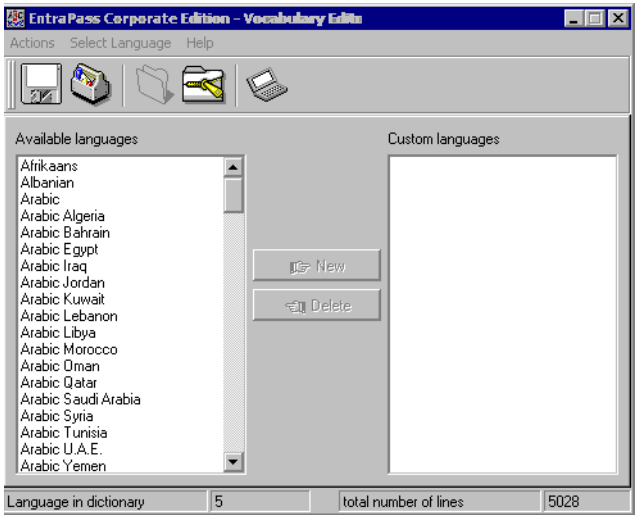
If you want to translate the system language, you just have to install the Vocabulary editor and then to translate the vocabulary database.

NOTE: *You do not need an additional license to install the Vocabulary Editor. You have just to select it in the Setup screen. For details on installing additional options, see* *"Installing Additional Workstations and Gateways" on page 19.*

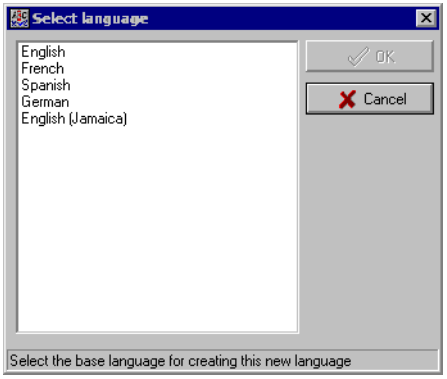
Translating the System Language

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.

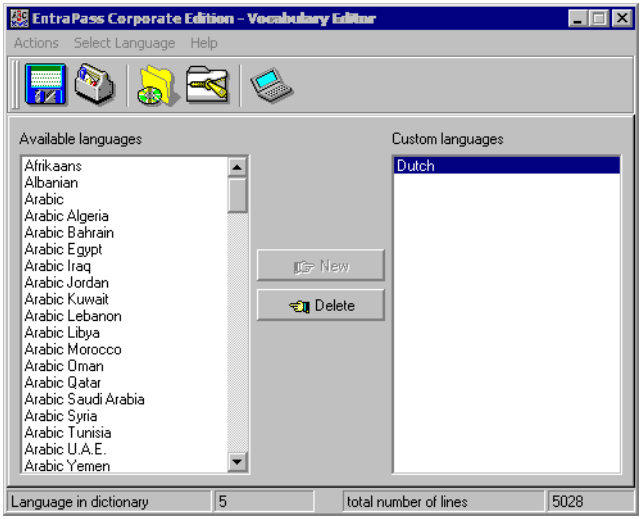
To translate the software language:



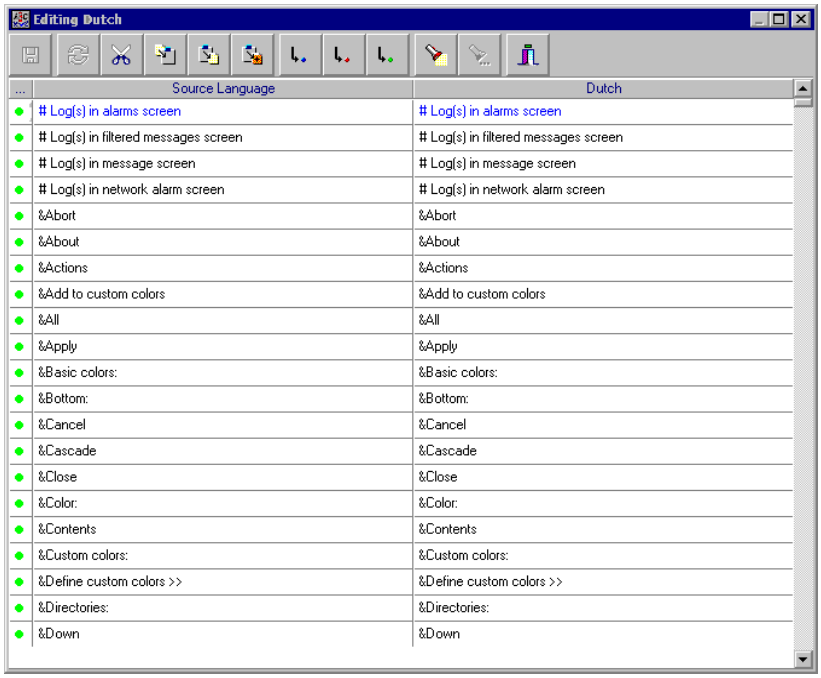
3 From the available **Language list**, select the new language, then click the **New** button. The system displays again the **Select language** screen. Select the source language for the translation, then click **OK**. The newly selected language is transferred to the right in the **Custom Languages** display list. The **Edit** and **Delete** buttons are enabled.



4 Select **Edit** to view the vocabulary database table.



5 In the Vocabulary Editor screen, click the **Edit** button to start translating the software vocabulary. The system displays the dictionary database.



NOTE: *You must make sure that the Customdictionnary directories are regularly backed up (C:\ProgramFiles\Kantech\Vocabulary Editor\CustomDictionary\files.xxx.ath) or C:\ProgramFiles\Kantech\"Workstation 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.**

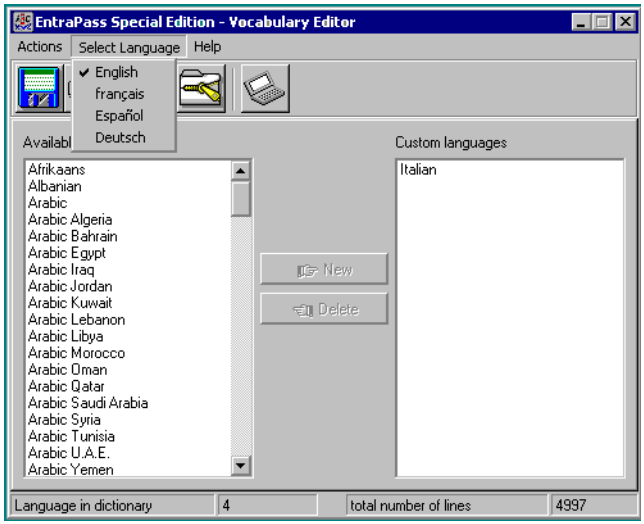
6 The “Source language” column contains text based on the basic language that was selected during the creation of the vocabulary. This column will serve as a “source” for the translation. Software language columns cannot be modified by the user.

7 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.

Integrating your Custom Language in Entrapass

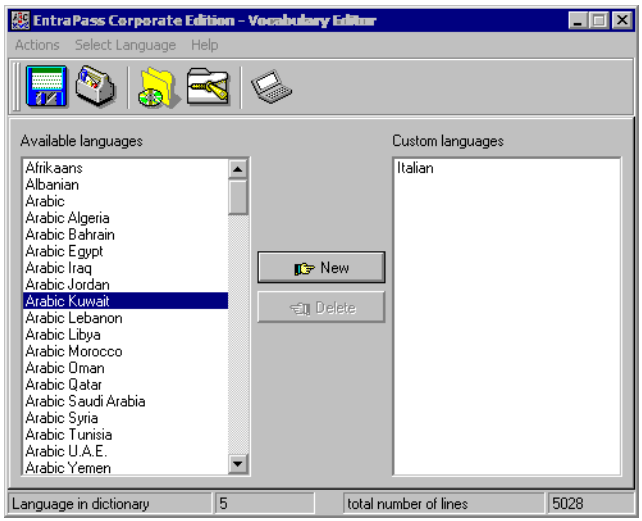
Once the translation is finished, you have to integrate the new dictionary into the system dictionary so that system operators can use it.

1 Start the Vocabulary Editor. The Vocabulary Editor screen 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.

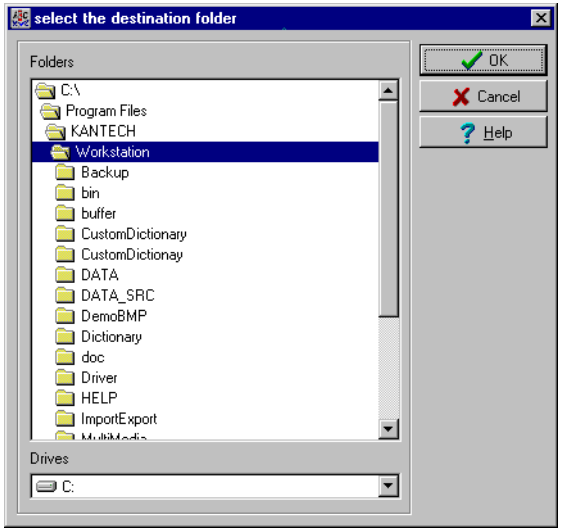


- You may choose to **Apply changes to the Operational dictionary**: this option is useful when you want to test your changes before you update other workstations.

- **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.*

Distributing the New System Vocabulary

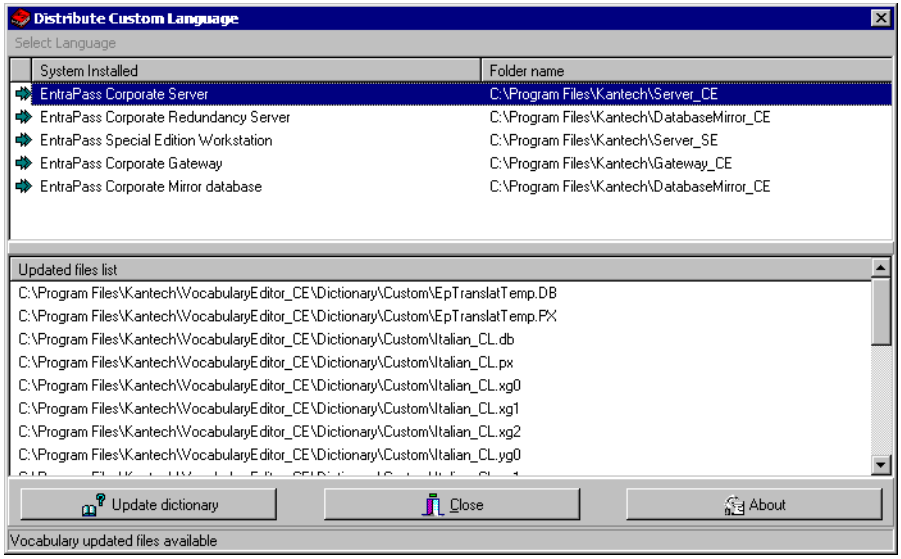
Before you run the file, make sure to exit the EntraPass software; otherwise the operation will not work. To update the system vocabulary, you have to update the EntraPass server first. If you have a Mirror database application, close it before you shutdown the server (so it does not start the Redundancy Server when you close the EntraPass server). Once the Mirror database application is shutdown, shutdown the Primary server, update it and re-start the server. Update the Mirror database and the Redundancy server, then start the Mirror database.

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.

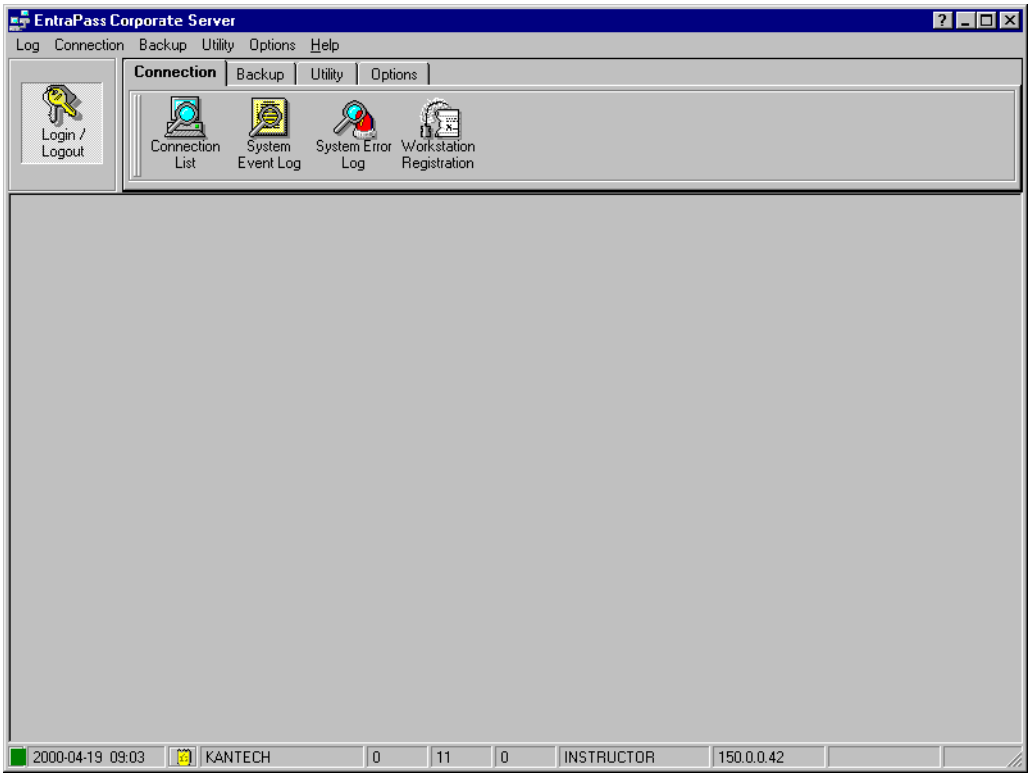
5 You have to copy **Updatedictionary.exe** on every computer where EntraPass is installed, and then double-click it in order to launch the language update. To do so, you have first to exit all EntraPass applications before you run the self-extracting file.

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.

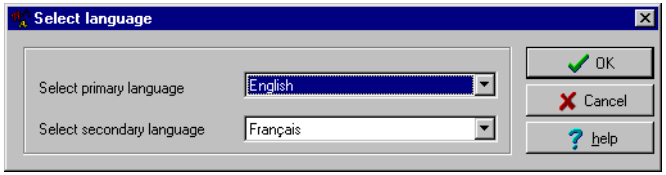
NOTE: *You MUST update all the workstations in the system.*

NOTE: *To restore the dictionary back to original default values, follow the same procedures as for updating the dictionary.*

7 Once you have finished updating the dictionary database for the Primary Server, the Mirror Database and the Redundancy Server, start the Primary server.



8 Select the **Options** tab, then select the **Select language** icon.



9 In the **Select the language** screen, 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.*

10 Before you update the workstations, login on the server and verify the display language. If everything seems to be normal, then you can proceed with the system update. Remember, the computers must support the language (display and keyboard).

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.*

Upgrading 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.*

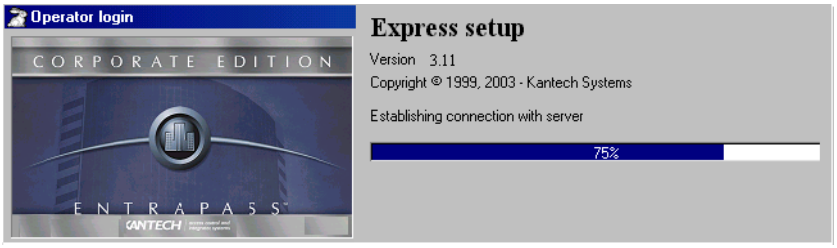
Express Setup Program

The Express Setup program is 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, modify the door names and will automatically apply default settings to all the relays and inputs of the controllers, if selected.

Configuring a Site Using Express Setup

To configure a Site under a Corporate Gateway using Express Setup:

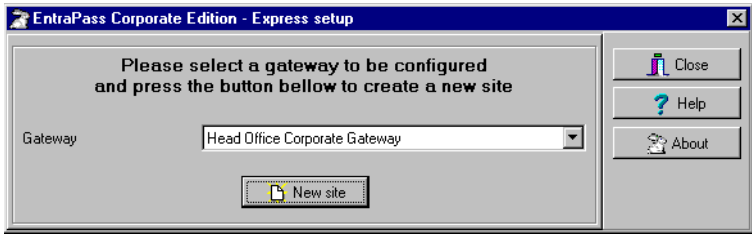
1 From Windows Start menu: **Start** > **Programs** > **EntraPass Corporate** > **Workstation/Server** > **Express Setup**. You may also launch Express Setup by clicking the Express Setup icon from a workstation registration or gateway definition screen.



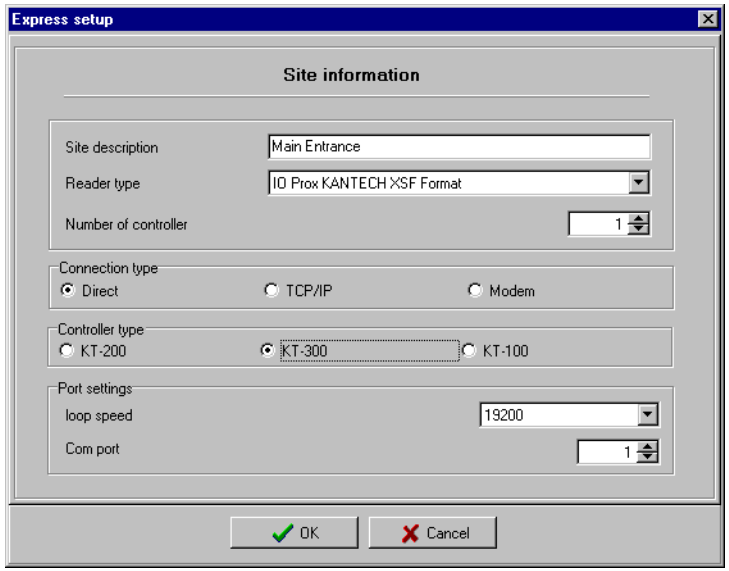
2 Click the **Login** icon. You have to log into the server before you modify the system configuration. Only authorized operators can modify the system parameters.

NOTE: *The Operator login screen appears only when starting Express setup in stand alone mode.*

3 Enter your Operator user name and password, then click **OK**. The **OK** button is enabled when the **Password** field contains data.



4 Select the gateway for which you want to configure a site, then click the **New site** icon.



5 Enter the Site name in the **Site description** field, then select the reader type.

6 Set the number of controllers.

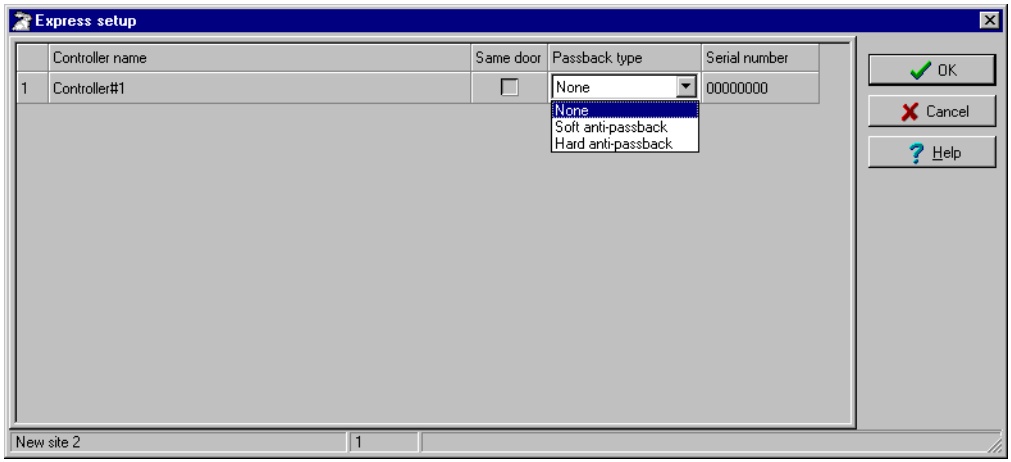
7 Specify the connection type. This indicates how the site communicates with the gateway computer.

- 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 (maximum allowed is 99). 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.

8 Select the controller type for this site.

9 Click **OK**. You have to specify minimum configuration for the controllers defined in the site. This include assigning a name to the controller, specifying the passback option, and entering the serial number (the serial number column appears only when it is a KT-100 or KT-300 controllers).



NOTE: *The passback feature will not allow any card to re-enter unless it has been used to exit. This requires that readers be used for both entry and exit.*

10 Check the **Same door** box if a reader is installed on each side of the door.

11 Select the appropriate passback type (none, soft or hard). If a door is defined as an access door, there is no passback defined for this door. An entry or an exit door can be assigned a passback option.

12 Enter the serial number cell, if this column is displayed. Usually the information is found on the controller label.

13 Once you click **OK**, components associated with the controller and to the site are created in the server database. By default, each controller is assigned two doors, if the **Same door** option is not checked. The following table summarizes default values that are assigned to controllers.

NOTE: *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:

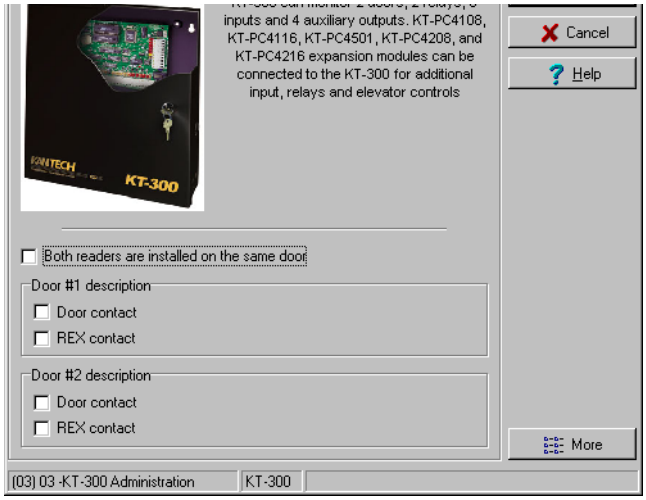
- The reader is Ioprox Kantech 26 bits Wiegand,
- The power supervision schedule is always valid,
- The failsoft delay is enabled for 45 seconds,
- The resistor type is single (KT-100 and KT-300),
- The wait for second card delay is 30 seconds.

Configuring 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 screen toolbar.

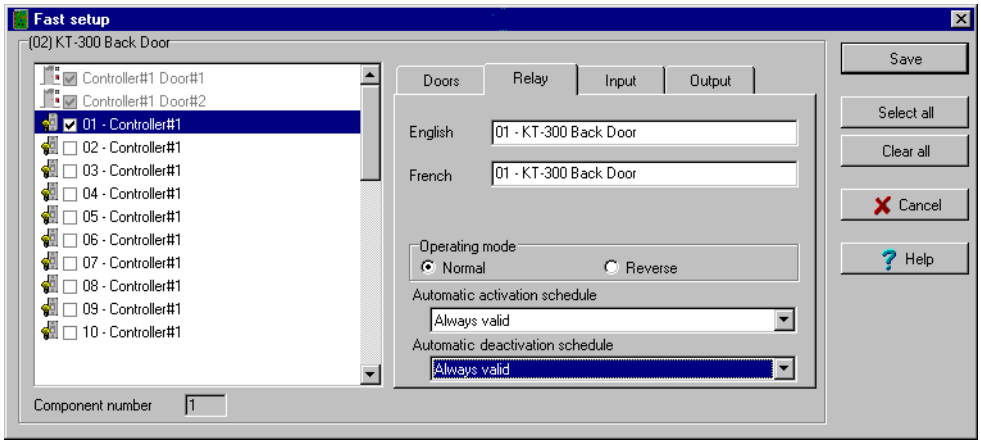
To configure a controller using Express Setup:

1 From a controller definition screen, 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.

3 Click the **More** button to define the other devices, such as doors, inputs, relays and outputs.

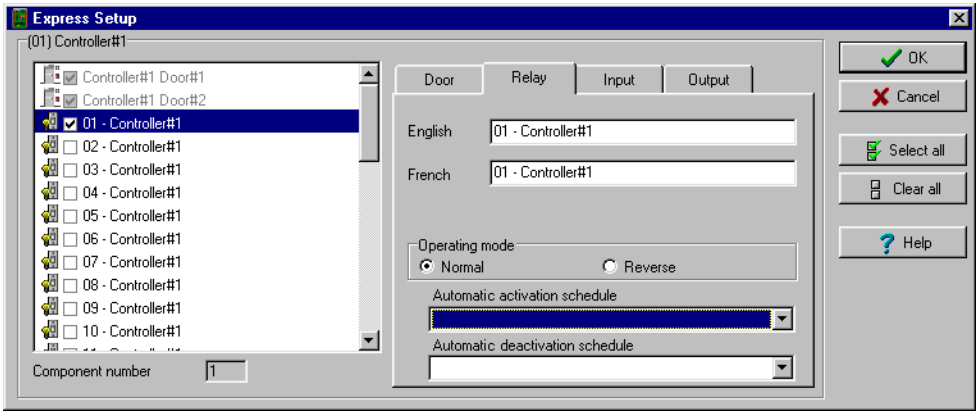


NOTE: *Components are listed in the left pane. The related tabs are displayed in the middle of the screen. When you select a component, its default name, number and default settings are displayed in the language section. Select a component to enable its tab. Components that are assigned are gray. You 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.).*

To define 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.

1 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.



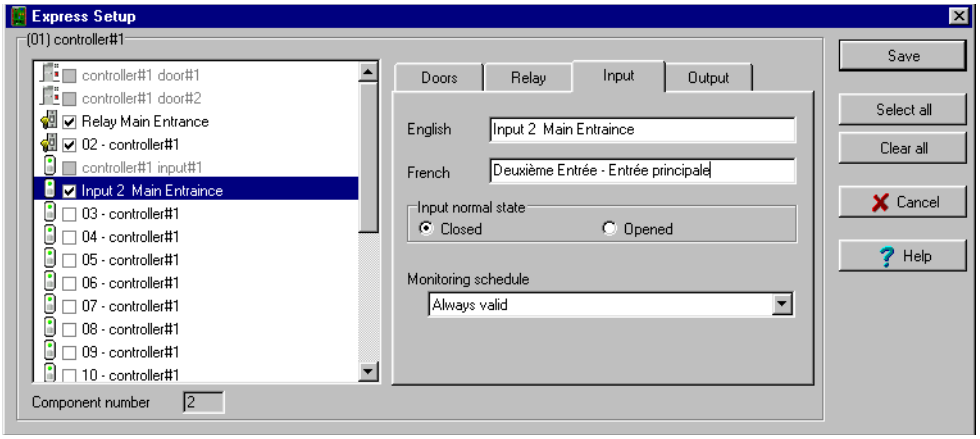
2 Check the appropriate options for the **Operating mode** and for the **Activation mode**.

3 In the **Automatic activation schedule** drop-down list, choose the appropriate activation Schedule.

To define 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).

To define 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**)

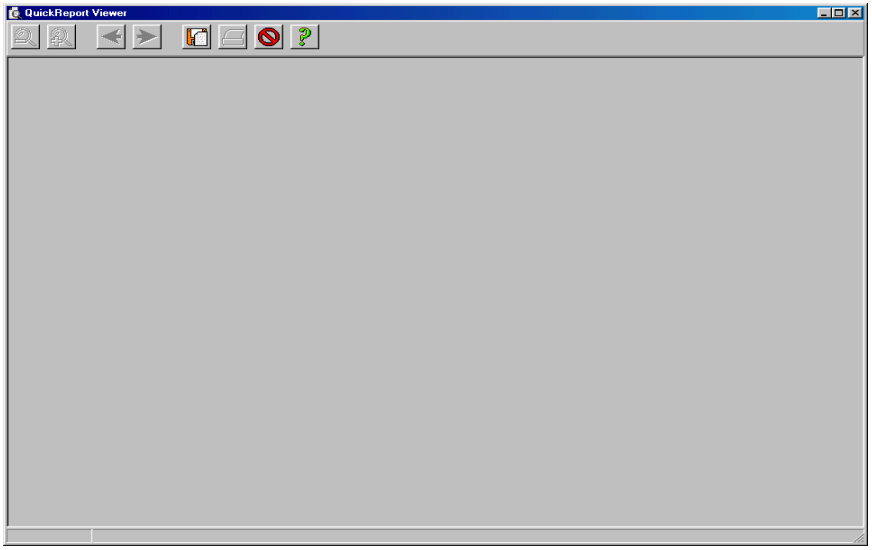
Quick Viewer

The **Quick Viewer** program allows operators to view previously saved reports without having to start a workstation. 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 Chapter 13 'Defining and Requesting Reports' on page 287.

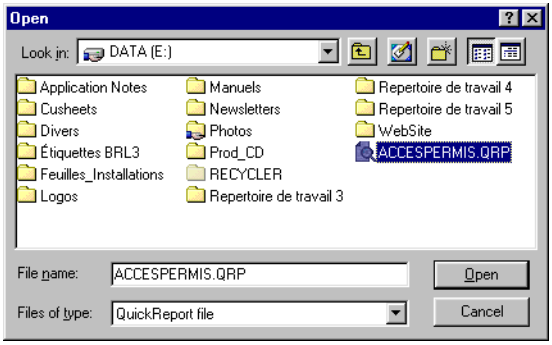
This program is useful when a workstation is off-line and when a report must be displayed for specific purposes.

To start the Quick Viewer:

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** screen:



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:

- —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.

PING Diagnostic

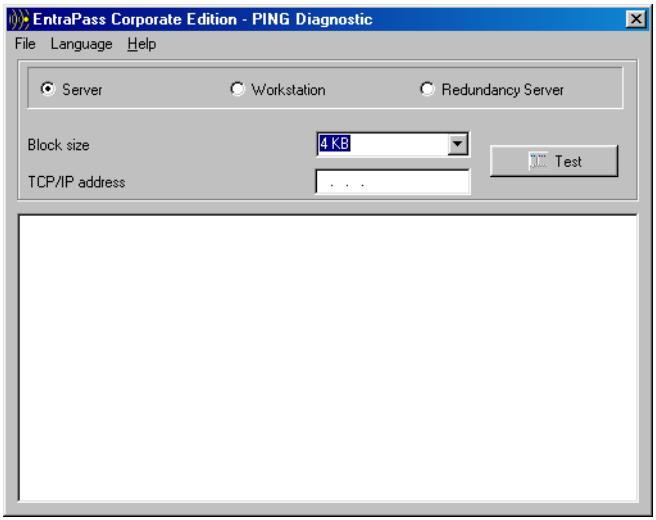
This stand-alone program is used to diagnose network intermittent related problems and/or to determine whether a specific IP address is accessible.

It works by sending a packet (block) to the specified address and waiting for a reply. The PING diagnostic program is used primarily to troubleshoot Internet connections.

NOTE: *If you want this option to be available, you have to select the "Allow diagnostic on network" field when defining the server parameters. For more information, see "The EntraPass Server" on page 317.*

To use the PING diagnostic program:

1 From the Windows Start menu, click **Start** > **Programs** > **EntraPass Corporate** > **Workstation/ Server PING Diagnostic**.



2 Select **Server, Workstation or Redundancy Server** depending on which station you want to operate.

3 Select the **Block size** from the drop-down list. This field is used to select the amount of data that will be sent. Selections vary from 1KB to 1024KB (1MB).

4 In the **TCP/IP address** field, enter IP address of the computer you want to test the communication link.

NOTE: *See Network Administrator for the required TCP-IP address.*

5 When you have entered the TCP/IP address, click the **Test** button to execute the command. The information will be sent 16 times.The system displays the number of bytes sent and the number of bytes received and the delay (in milliseconds).

NOTE: *The delay between attempts should be similar, except for the first attempt which could be longer than the others. If you do not have a response, the message will be displayed in the following format: Sent(block) Bytes, No Answer (1717)*

Workstation—Configuration Program

This utility program is useful when a workstation or gateway needs to be configured. It contains all the menus and features necessary to configure a system with event display, desktops, manual operations or reports.

The system installer can configure all workstations directly from this program without having to go from workstation to workstation.

Start the Workstation config system utility from Windows start menu **Start** > **Programs** > **EntraPass Corporate** > **Server**> **Workstation for Configuration**. This program can also be launched from a shortcut on the desktop.

When using this option, you must first create the operators and security levels (**System** menu), then define the gateway, sites, controllers (**Devices** menu).

NOTE: *For more information see “Software Installation” on page 7*

Chapter 16 • EntraPass Utilities (Options)

The **Options** toolbar offers users the ability to change a number of system parameters. These include changing the card format, the master password, the date and time, or changing server parameters. Some of the system utilities are accessed from the Server or the Workstation windows.

The following menu options are available from both the Workstation and the Server windows:

- Change card format,
- Change the master password,
- Select a language,
- Keypad family,
- Change the system date and time,
- Modify the server parameters,
- Backup Scheduler,

The following utilities are available from the Workstation Option menu, only:

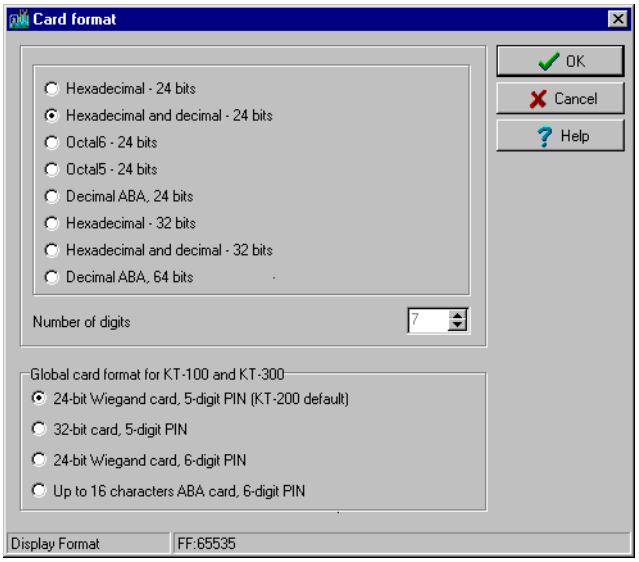
- Printer option (select a log printer and a badge printer),
- Multimedia devices (alarm, video and signature capture settings),
- Verify database integrity.

Changing the Card Format

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 screen.

- **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.*

Changing the Master Password

The master password is used to authenticate EntraPass Workstations to the EntraPass Server.

The Master password screen is automatically displayed when the system has not yet been registered.

NOTE: *If you are not using a specific password for authentication, then the user will have to use the master default password for workstation authentication. The default master password is kantech, in lower case. Passwords are case sensitive.*

To change the master password:

1. From the **Options** main screen, select the **Master password** icon.
2. Enter the current master password (case sensitive) in the **Old master password** field. The default master password is kantech, in lower case.
3. Enter the new master password in **New master password** field (case sensitive).
4. Enter the new master password in the **Verify master password** for confirmation. This field will verify that the new master password was typed properly (case sensitive).
5. Click **OK** to exist. When you receive an error message, make sure that the data you have just entered in the **New master password** and in the **Verify master password** fields are identical (case sensitive).

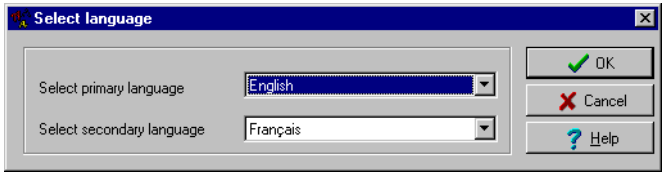
NOTE: *The master password is different from the operator password. The master password is used to authenticate workstations, whereas the operator password is used to open a session.*

Selecting a Language

In order to have the system run in the language of your choice, you have to change the system language.

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.*

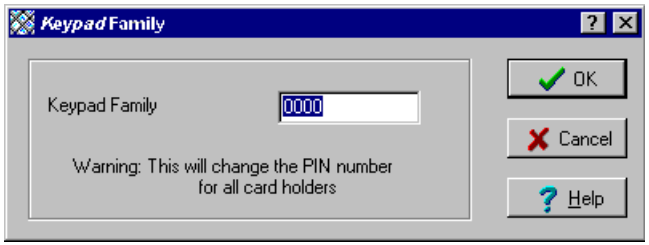
NOTE: *When you modify the primary language, the database language will be modified according the ascii values of the characters in the primary language. Accents and special characters of different languages will have an impact on your database.*

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.

Keypad Family

The PIN numbers are generated by the system using an algorithm. For additional security, a keypad family number can be used to modify the keypad numbers.



NOTE: *Modifying the keypad family will change the keypad code (PIN) on all existing cards.*

Keypad Family—Enter the number on which the system's keypad code generation algorithm is based on.

Selecting and Configuring Printers

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.

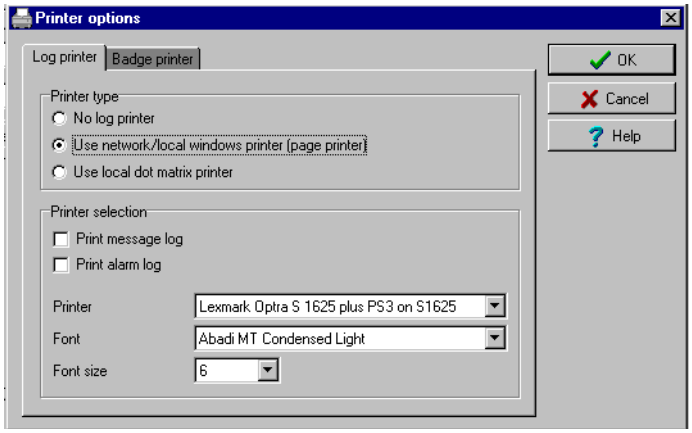
Selecting and Setting up a Log Printer

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 a workstation, 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 (for details, see "Printing Event Parameters" on page 255).*

To select and set up a log printer:

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.

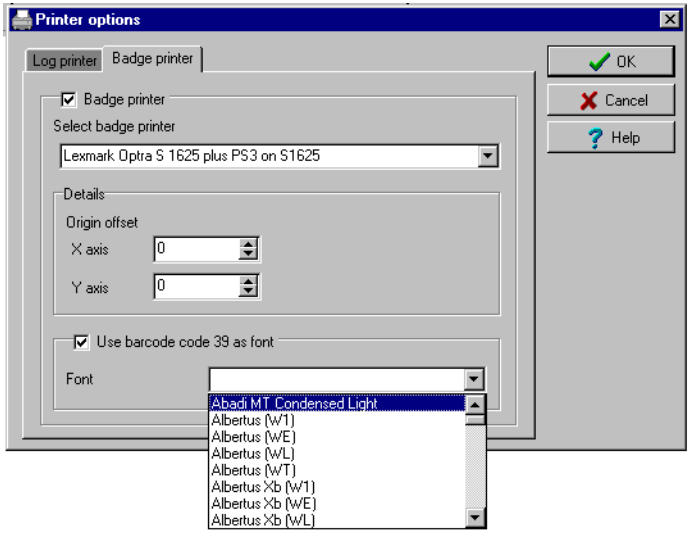
3 In the **Printer selection** section, specify whether you wont to print message or alarms.

- **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.

Selecting and Setting up a Badge Printer

1 From the Printer option screen, 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, Visitor, and Day pass windows.

3 From the **Select badge printer** drop-down list, select the appropriate badge printer.

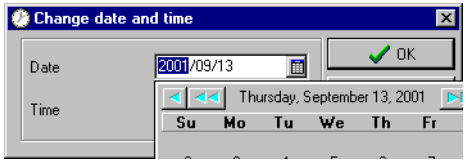
Changing System Date & Time

The **Change system date and time** option should be used with caution and only when necessary; this functions may affect logical components of the access system (i.e. schedules, etc.).

If, for any reason, you want to adjust the system time and date, it is better to do so using the Server parameters settings (**Options** > **Server Parameters** > **Time adjustment**).For details on network time adjustment, see "Configuring Server Parameters" on page 371.

To change the system date and time:

1 From the Option main screen, select the **Change System date and time** icon.



2 Enter the date in the **Date** field, or select a date from the calender. Connected components of this workstation will also receive the date change notification.

3 Enter the time in the **Time** field. Connected components of this workstation will also receive the time change notification.

4 Click **OK** to exit.

NOTE: *If you want the system to automatically change the time when necessary, use the Time adjustment tab of the Server Parameters definition menu. For details, see "Configuring Server Parameters" on page 371.*

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.

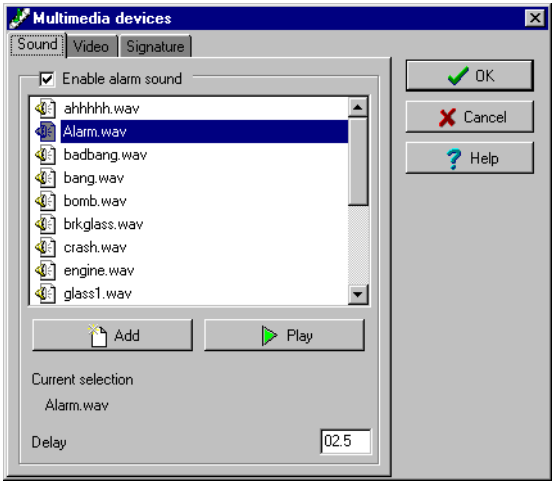
Setting up Multimedia Devices

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 screen, 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.

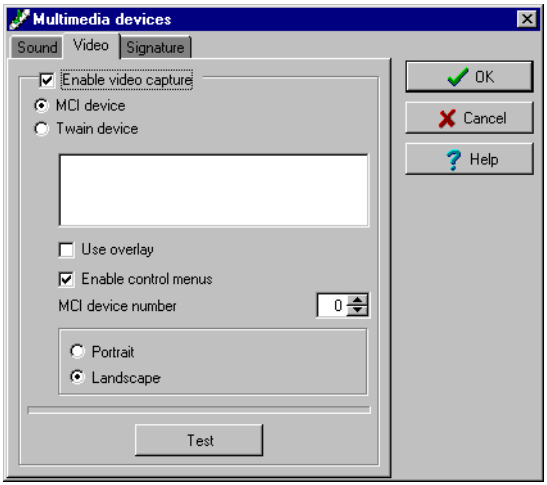
4 Click the **Play** button to listen to the selected sound.

5 Click the **Add** button to add a new sound from your personal files. Clicking on this button displays a new screen 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 screen, select the **Video** tab.



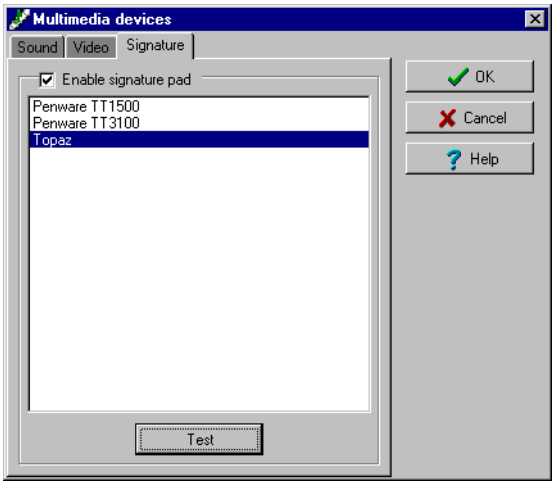
2 Check the **Enable video capture** box to enable the video capture options in your system.

- **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 screen, 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 screen appears. This screen appears whenever you choose the **Signature pad** option (Card, Visitor and Daypass definition windows).*

Configuring Server Parameters

The server parameters configuration menu allows the system administrator to modify server parameters.

This menu may be accessed from a workstation or a server.

To modify the Server parameters:

From **the Option main window, select the Server parameters icon.**

4 In the Server parameters screen, select the **Logout and idle** tab to specify the server application behavior on idle (when there is no action on the keyboard from the operator). You may select:

- **Automatic logout on idle**: the operator will have to re-inter his/her user name and password to enable the server application again. The maximum allowed delay is (mm:ss): 59 minutes and 59 seconds.
- **Send to tray on idle**: the server application will be minimized and sent to the task bar when the specified delay expires, if the operator who is currently logged in is inactive. The maximum allowed delay is (mm:ss): 59 minutes and 59 seconds.

NOTE: *For increased security, select the option* ***Must login to close a Server application*** *so that operators have to enter their user name and password to close the Server application.*

5 Select the **Time adjustment** tab in order to specify which Gateway will be used to automatically adjust the time of all the computers connected to the EntraPass server.

NOTE: *The gateway polls the first controller on the first site at 1:47 pm or 13:47, 7:47 pm or 19:47 and 5:47 am or 05:47 to get the controller time. Kantech controllers are very precise. For instance, they (KT-100, KT-200 & KT-300) will only lose one to two minutes per year.*

6 Select the **Time adjustment** tab to set time adjustment options:

- **No time adjustment**. If you select this option, no adjustments will be made.
- **By Gateway**. If you select this option, you must select the appropriate gateway from the **Gateway** drop-down list.
- **By Server**. If you select this option, time will be refreshed at a regular intervals by the server. You must select the number of hours between refreshes in the adjacent selection box.

7 To modify the Server parameters, select the **Server** tab.

- Specify the **Maximum record in system logs.**
- Specify the **Maximum record in system error logs**.

NOTE: *The maximum record in* ***system logs*** *and in* ***system error logs*** *include transactions such as: login to server, logout from server, disconnection, connection, stop server, start server, registration requested, etc. These records are kept with the date/time, the workstation (where the event or error came from), the operator and the description of the transactions.*

8 Select the **Diagnostic** tab, if you want to allow diagnostic on network.

9 Check the **Allow diagnostic on network** option in order to use the PING (Packet INternet Groper) utility program. This stand-alone program is used to diagnose network intermittent

related problems and/or to determine whether a specific IP address is accessible. For details on the PING program, see “System Utilities” on page 327.

10 Select the **Network alarm** tab to define maximum records to be kept in the network alarm table.

11 Enter the maximum number of records (100,000 maximum allowed) that will be kept in the network alarms table. You may use up/down controls to set this number. When you define this setting, the server will automatically apply the same setting for the workstations of the system. This is to ensure that the file size does not take too much disk space on the workstation and the server's hard disk.

NOTE: *When the table reaches the maximum records, events are removed from the table on a first in first out basis. For approximately 100,000 (max) events, the file is about 100 MB. For more information on network alarms, see “Working with Desktops” on page 263.*

12 Select the **CSV report** tab to 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; the TAB for instance.

13 Check the **Date and time on separate fields** option. It is recommended to check this option**.** When you select “CSV” 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.

14 Select the **KT-100** tab to specify the folder containing the program for KT-100 controllers.

15 Select the **KT-300 Firmware** tab to specify the folder containing the firmware for KT-300 controllers. The system will use this data to update data for the installed controllers.

16 Select the **JPEG quality** tab to adjust the image and signature quality for the Badging feature.

NOTE: *The Jpeg quality value indicates the Jpeg save quality. 0 is poor and 100 is excellent. If you are not using the Badging feature, you may reduce the jpeg quality of your images so that they will not occupy much space in the database. However, if you are using the Badging feature, it is recommended to leave the jpeg quality to default. Reducing it may affect the quality of the photos imported into badges. If you are not an advanced user, leave these values to default.*

17 Select the **User name format** tab to choose how name will display and method of parsing data.

Backup Scheduler

A backup is a copy of the systems database which serves as a substitute or alternative in case the computer fails. If your system computer fails, you may restore a backup copy onto another computer (on which the EntraPass software has been installed).

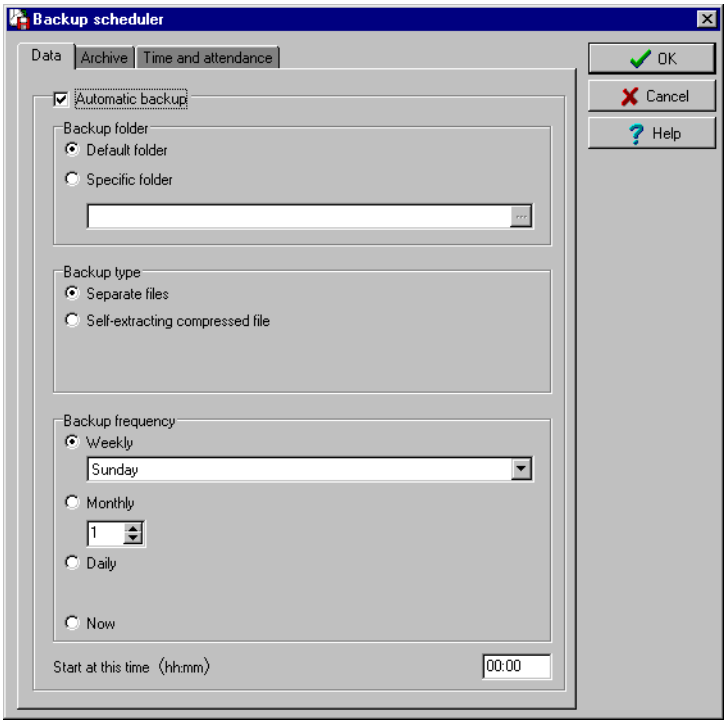
- Back up your files regularly, at least once a week or more if many modifications were made to the database.
- We recommend that you make two backups of all your database files. To be especially safe, keep them in separate locations.
- To backup your files, you can use:
  - the menus of the Server/Backup Tab, or
  - the Backup Scheduler to apply automatic schedules, or
  - other third party software and hardware.

NOTE: *By default, when you backup or restore files, the Server databases will temporarily be disabled (not available). The Workstations will not be able to modify the databases.*

The Backup Scheduler program is used to schedule automatic backups of your data, archives, and Time and attendance databases. Define the default settings and the system will do the rest!

To schedule automatic backups of the system database:

1 From the Options main screen, select the **Backup Scheduler** icon.



2 Select the tab corresponding to the information you want to backup: **Data, Archive,** or **Time & Attendance**.

3 Select the **Automatic backup** option to enable the options displayed in the screen. The options displayed depend on the tab that is enabled.

4 Select the backup folder:

- **Default folder**—will backup your files in a system default backup folder. By default, the name of the backup sub-directory is generated automatically according to the following convention: X_YYYY_MM_DD_HH_MM_SS (Where 'X' = Data or Archives or Time and Attendance (D, A or T), year, month, day, hour, minutes, and seconds.

NOTE: *By default, the system backs up all the information originating from the following directories: C:\PROGRAMFILES\ KANTECH\SERVER\DATA or ARCHIVE or TIME. The information is sent to:C:\PROGRAM FILES\ KANTECH\SERVER\BACKUP\X_YYYY_MM_DD_HH_MM_SS*

- **Specific folder**—will backup your files in a sub-folder labeled according to the default convention in the XXX folder.

5 Select the **Backup type**. The options that are displayed depend on the type of the data to be saved.

- **Separate files**: will backup the databases one by one (standard) (*Data only*).
- **Separate files (full backup)**: will backup all databases (*Archive, Time and Attendance)*.
- **Separate files (incremental)**: will backup all databases. Only the information that was modified since the last backup will be saved (*Archive, Time and Attendance)*.
- **Self-extracting compressed file**: will create an executable file (*.exe) that will compress the information so as to reduce the amount of disk space taken by the backup. (*Data only*)
- **Self-extracting compressed file** (full backup): will create an executable file (*.exe) that will compress the information so as to reduce the amount of disk space taken by the backup (Archive, Time & Attendance).
- **Self-extracting compressed file (incremental)**: will create an executable file (*.exe) that will compress the information so as to reduce the amount of disk space taken by the backup. Only the information that was modified since the last backup will be saved (*Archive, Time & Attendance*).

NOTE: *When you have selected "full backup", each time a backup is done a new sub-folder containing the data or the self-extracting file will be created. If you are using the incremental backup type, only the information that was modified since the last backup will be saved. If you want to restore information, you will have to restore all the sub-folders one-by-one (starting from the oldest).*

6 Select the frequency of the backup,

- **Weekly**: the backup will be carried out once a week. Specify which day (example, the backup will be executed every Thursday).
- **Monthly:** the backup will be carried out monthly, specify the day of the month (example, the backup will be carried out every first day of the month).
- **Daily**: the backup will be carried out every day.
- **Now**: this option allows you to request a backup when you need it.

7 Enter the time at which the backup will start (24:00 format), then click on **OK** to save.

8 Repeat steps 1 to 8 for all the tabs.

Workstation Registration

This menu is used register new system applications such as workstation, gateway, SmartLink, etc. in order to register and use the system's database and to establish communication with the Server.

NOTE: *For more information on how to install and register new applications, see Chapter 2 'Software Installation' on page 7. Before you install new applications, make sure that you have the proper serial numbers for the installation.*

Chapter 17 • Animated Icons

Animated icons indicate the status of physical or logical components in the screens 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

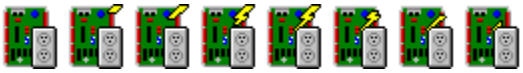
Controller animated icons indicate the status of a door controller in the graphic screen (Desktop > Graphic desktop) or in the “Operation” screen.

Status unknown

This animated icon appears when the workstation has not received the component' status after four (4) attempts. It is displayed in:

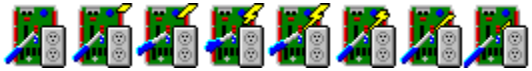
- the Operation screen (alarms, door, elevator door, relay, input, reload data) or the “Graphic” screen (Desktop—graphic).

Controller AC failure



This animated icon appears when the controller is in AC failure. It is displayed in:

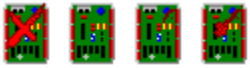
- the Graphic desktop (Desktop > Graphic desktop screen)
- the “Operation” — “Controller Reset” Controller AC failure and Tamper Switch in “alarm”



This animated icon 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 screen)
- the Operation > Controller Reset

Controller is not communicating



This animated icon appears when the controller is not communicating. It is displayed in:

- the “Operation” — “Controller Reset” screens.
- the “Graphic” screen (Desktop—Graphic desktop).

Controller communication is regular (no problem)

This animated icon appears when the controller is communicating and the communication is regular. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop screen)
- the Operation > Controller Reset.

Controller status is not yet known

This animated icon appears when the status of the controller is not yet known. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop screen)

Controller is in “Reset” and AC failure

This animated icon appears when the controller is in “reset mode” and in “AC failure”. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop screen)
- the Operation > Controller Reset.

Controller is in “Reset”, “AC failure” and “Tamper in alarm”

This animated icon 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 screen)
- the Operation > Controller Reset

Controller is in reset and tamper in alarm

This animated icon appears when the controller is in “reset mode” and the tamper is in alarm. It is displayed in:

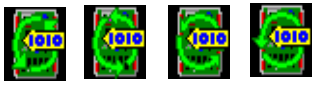
- the Graphic desktop (Desktop > Graphic desktop screen)
- the Operation” > Controller Reset.

Controller tamper in alarm

This animated icon appears when the controller tamper is in alarm. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop screen)
- the “Operation” “Controller Reset” when the controller tamper is in alarm.

Controller reloading firmware



This animated icon appears when the controller is reloading firmware. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop screen)
- the “Operation” “Controller Reset”.

Doors

Icons representing a door state indicate the status of door within the graphic screen (from the desktop) or within the “Operation” screen.

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 screen)
- 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” screen (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 screen)
- 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:

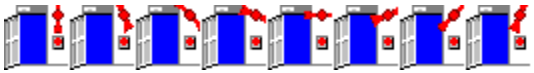
- the Graphic desktop (Desktop > Graphic desktop screen)
- the “Operation > Door.

Door status unknown

This animated icon appears in:

- the “Graphic” screen (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 screen)
- 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 screen)
- 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 screen)
- 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 screen)
- 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 screen)

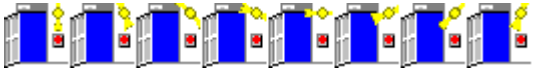
- the Operation >Door > Elevator door”.

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 disable. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop screen)
- 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 screen)
- 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 screen)
- 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 screen)
- 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 screen)

- 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 screen)
- 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 screen)
- 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:

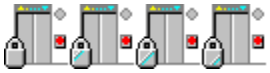
- the Graphic desktop (Desktop > Graphic desktop screen)
- the Operation > Door/Elevator door”.

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 screen)
- 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 screen)
- the Operation > Door/Elevator door”.

Relays

Relays icons indicate the status of a relay within the graphic screen (from the desktop) or within the “Operation” screen.

Relay activated by an event

This animated icon appears in:

- the “Graphic” screen (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” screen (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” screen (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” screen (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” screen (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” screen (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” screen (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” screen (desktop—graphic) when the relay is not activated.
- the “Operation” “Relay” when the relay is not activated.

Relay status unknown

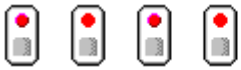
This animated icon appears in:

- the “Graphic” screen (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 screen (from the desktop) or within the “Operation” screen.

Input in alarm—Not supervised



This animated icon appears in:

- the “Graphic” screen (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” screen (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” screen (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” screen (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” screen (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” screen (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” screen (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” screen (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

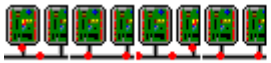
This animated icon appears in the “Graphic” desktop when the status of the input is not yet known.

Sites and Gateways

These icons indicate the status of a site, or gateway within the graphic screen (from the desktop) or within the “Operation” screen.

Controller Site:

Site status is not yet known



This animated icon appears in:

- the “Graphic” screen (desktop—graphic) when the status of the controller site is not yet known.

Controller site connected

This animated icon appears in:

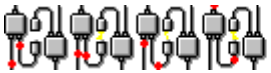
- the “Graphic” screen (desktop—graphic) when the site is connected and communication is OK.
- the “Operation” “reload data” when the site is connected and communication is OK.

Controller site connected and in “Reload Data”

This animated icon appears in:

- the “Graphic” screen (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” screen (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) screen when the gateway is in communication failure.
- the “Graphic” screen (desktop—graphic) when the gateway is in communication failure.

Gateway in “Reload Data”

This animated icon appears in:

- the “Graphic” screen (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:

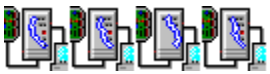
- the “Operation” (reload data gateway) screen when the gateway loses communication during a reload data operation.
- the “Graphic” screen (desktop—graphic) when the gateway loses communication during a reload data operation.

Gateway communication is regular (no problem)

This animated icon appears in:

- the “Graphic” screen (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” screen (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” screen (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:

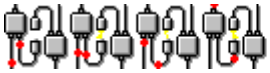
- the “Graphic” screen (desktop—graphic) when the gateway is communicating.
- the “Operation” “reload data” when the gateway is communicating.

Gateway in “Reload Data”

This animated icon appears in:

- the “Graphic” screen (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” screen (desktop—graphic) when gateway is not communicating.
- the “Operation” “reload data” when the when gateway is not communicating.

Workstation

Workstation status is not yet known

This animated icon appears in:

- the “Graphic” screen (desktop—graphic) when the status of the workstation is not yet known.

Workstation attempts communication

This animated icon appears in:

- the startup screen when the workstation attempts to communicate with the server.

Workstation—Communication Failure

This animated icon appears in:

- the “Graphic” screen (desktop—graphic) when the workstation is in communication failure.
- the “Operation” screen (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 screen 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” screen (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) screen when the workstation has not received the component' status after four (4) attempts.
- the “Graphic” screen (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) screen when a specific error is detected.
- the “Graphic” screen (desktop—graphic) when a specific error is detected.

Undefined Component

This animated icon appears in:

- the “Operation” screen (alarm, door, elevator door, relay, input, reload data gateway) when the component does not exist.
- the “Graphic” screen (desktop—graphic) when the component does not exist.

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

KANTECH | access control and integrated systems

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

DN1415-0401