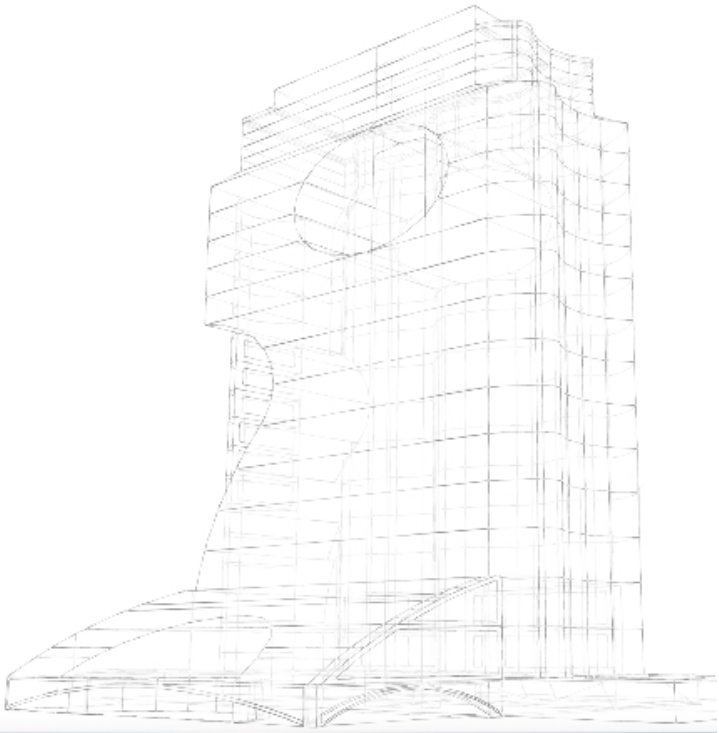
ENTRAPASS

Security Management Software



CORPORATE EDITION

KANTECH

A Tyco International Company

CONTENTS

EULA I

PRIVACY NOTICE VII

ENTRAPASS HELP 1

Release Notes 8.10 1

HOW TO 5

How to Create a Backup 5

How to Create a Badge 6

How to Create a Card 7

How to Create a Schedule 8

How to Create a Simple Report 9

How to Create an Access Level 10

How to Print a Card List 11

How to Print a List of Access Levels 12

How to Print a List of Doors 13

How to Setup the Desktops 14

How to use shortcut keys 15

How to personalize the Web login screen 16

How to enable GO Pass for a user 17

How to use HID Mobile Access 18

How to migrate from Event Parameter to Event Operator mode 20

How to manually set the database to read-only mode 21

How to enable EntraPass maintenance mode 22

How to setup the ioSmart 23

FAQ 25

CONTENTS

Can I use an Input to unlock an elevator floor or a group, and how long will it remain unlocked? 25

Is it possible to import access levels? 25

What are the communication ports for EntraPass, such as server, workstation, SmartLink, gateway, mirror database, video vault and EntraPass Web? 25

What are the various options available in batch operation? 25

What happens when card pictures are saved on a hard drive instead of the server database? 26

What is the difference between “One time access and Temporary unlock door option on KT-100 200 300 and 400? 26

What is the purpose of Custom messages? 26

Why do we use card access groups? 27

Where can I synchronize operators with Active directory? 27

INTRODUCTION 28

What is EntraPass? 28

EntraPass Main Features 29

Technical Support 35

INSTALLATION 38

Minimum System Requirements 38

Security Hardening Guide 39

System Installation 40

System Registration 43

Adding System Components 47

System Components Edition 49

GETTING STARTED 52

Basic Functions 52

Delete details 61

CONTENTS

Displaying Components Links 61
EntraPass Toolbars 62
Express Setup 64
Finding Components 65
Session Start and End 67
System Tree View 73
Using the Extended Selection Box 75

DESKTOPS 76

Alarms Desktop 76
Changing the Display Properties 83
Custom Report Desktop 83
Customizing Event Display in the Message Desktops 86
Graphic Desktop 87
Message List Desktop 90
Picture Desktop 96
Specific Desktop Customizing 97
Transferring a Customized Desktop 99

STATUS 101

Application Status 101
Text Status 102
Numerical Status 103
Graphic Status 104
Database Status 106
Video Server Status 107
Server State 110

CONTENTS

Logins 111

OPERATION 113

Manual Operations on Gateway 113

Manual Operations on Sites 114

Manual Operations on Controllers 116

Manual Operations on Doors 120

Manual Operations on Elevator Doors 123

Manual Operations on Relays 126

Manual Operations on Inputs 128

Manual Operations on View Roll Call 130

Manual Operations on Integrated Panels 130

Manual Operations on Action Scheduler 131

USERS 135

Access Exception 135

Access Levels Definition 135

Badges Designing 136

Batch Operations on Cards 146

Card Access Groups Definition 148

Card Options Definition 149

Card Printing 151

Card Type Definition 153

Cardholder Access Levels Assignation 154

Cards Definition 162

Creating a New Import/Export Pattern 181

Creating a Visitor Card When Creating a New Card 183

CONTENTS

CSV Files Import and Export 183

Customizing Card Information Fields 188

Day Passes Definition 189

Issuing a New Card in Enhanced User Management Environment 190

Issuing Cards Using the Batch Load Feature 192

Last Transactions Display 193

Quick Access to Door List per Card 194

Tenants List 195

To Add Objects to a Badge Layout 200

To Modify Picture Properties 201

Validating Card Access 202

Visitor Cards Definition 202

DEFINITION 203

Schedules Definition 203

Floors Definition 206

Graphics Definition 206

Holiday Definition 210

Trigger and Alarm (previously Event Trigger) 211

Task Builder Definition 214

GROUPS 227

Controller Group Creation 227

Door Group Creation 227

Relay Group Creation 228

Input Group Creation 228

Access Level Groups Grouping 229

CONTENTS

Floor Group Creation 229

Trigger Group Creation 230

DEVICES 231

Application Configuration 231

EntraPass Gateways Configuration 260

Site Configuration 263

Change Site Labels 266

Connection Configuration 266

Setting up Communication Timing 278

Controllers Configuration 278

KT-300 Combus Modules 315

Expansion Modules Setup 317

Kantech Telephone Entry System (KTES) Configuration 318

Doors Configuration 329

Relay Configuration 344

Input Configuration 346

Output Device Configuration 350

Reader Templates 353

Integrated Panel Configuration 353

Integrated Component Configuration 363

Trigger and Alarm tab 366

Comment Field 367

VIDEO 370

Camera Definition 370

Current Recording 374

CONTENTS

EntraPass Video Vault Browsing 375
Exported Video Viewing 375
Exporting Video Files 376
Finding Video Events 377
Recording Parameters 379
Video Desktop 381
Video Event List 382
Video Playback 389
Video Server Configuration 390
Video Triggers 398
Video Views Creation and Modification 399
Video Views Definition 401

SYSTEM 405

Active Directory 405
Associations 429
Commissioning 430
Creating/Modifying an Operator Security Level 432
Creating or Editing an Operator 433
Database Structure Definition 438
Event Parameters Definition 439
Instructions Definition 445
Message Filters Definition 445
Operators Definition 447
Security Level Definition 454
Workspace Definition 458

CONTENTS

Audit 468

REPORT 471

Archive Viewing 471

Card Use Report 474

Custom Reports Definition 475

Defining a Report Output Format 480

Defining Automatic Report Schedules 482

In/Out Reports Definition 484

In/Out Reports Request 486

Operations on In/Out 487

Previewing In/Out Reports 489

Previewing Reports 490

Quick Report Definition 491

Report Log 493

Report State 494

Requesting Reports 495

Roll Call Reports 497

Specifying Additional Options for an Automatic Report 498

OPTIONS 500

Backup Scheduler 500

Connection Password Modification 503

Credentials Parameters 503

Custom Messages 504

Dealer Information 505

Defining a Card Display Format 507

CONTENTS

Event Color and Priority 509
Integration 510
Login Messages 510
Multimedia Devices Configuration 512
Printers Selection and Configuration 514
Registration 516
Selecting and Setting Up a Badge Printer 516
Service Login Information 517
System Date & Time Modification 517
System Language Selection 518
System Parameters Configuration 519
Time Parameters 536
User Name Format 537

THE ENTRAPASS SERVER 538

General 538
Application 538
Error Log 538
Log 539
Registration 540
Report Log 540
Backup 541
Backups 541
Restores 543
Options 544
Defining a Card Display Format 544

CONTENTS

Connection Password Modification 547

System Language Selection 547

System Date & Time Modification 548

System Parameters Configuration 549

Dealer Information 566

Backup Scheduler 568

Custom Messages 571

Login Messages 572

UTILITIES 574

Configuring a KTES Using Express Setup 574

Database Utility 576

EntraPass Video Vault 580

Express Setup Program 583

PING Diagnostic 591

Quick Report Viewer 592

The SmartLink Interface 593

Vocabulary Editor 595

ENTRAPASS ICONS 600

EULA

TYCO INTERNATIONAL LTD

END-USER LICENSE AGREEMENT

IMPORTANT - READ THIS END-USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE OPENING THE DISK PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE.

THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU AND SENSORMATIC ELECTRONICS, LLC ("TYCO"), AND GOVERNS YOUR USE OF THE SOFTWARE ACCOMPANYING THIS EULA WHICH SOFTWARE INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE MEDIA, PRINTED MATERIALS, AND "ON-LINE" OR ELECTRONIC DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE"). BY BREAKING THE SEAL ON THIS PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS EULA, DO NOT OPEN, DOWNLOAD, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.

1 - SCOPE OF LICENSE. The Software may include computer code, program files and any associated media, hardware or software keys, printed material and electronic documentation. The Software may be provided to you pre-installed on a storage device (the media) as part of a computer system or other hardware or device ("System"). The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, and text incorporated into the Software), the accompanying printed materials, and any copies of the Software, are owned by Tyco and/or its suppliers. The Software is licensed, not sold. All rights not expressly granted under this EULA are reserved by Tyco and its suppliers.

2 - GRANT OF LICENSE. This EULA grants you the following rights on a non-exclusive basis:

a - General. This EULA permits you to use the Software for which you have purchased this EULA. Once you have purchased licenses for the number of copies of the Software that you require, you may use the Software and accompanying material provided that you install and use no more than the licensed number of copies at one time. The Software is only licensed for use with specified Licensor-supplied Systems. If the Software is protected by a software or hardware key or other device, the Software may be used on any computer on which the key is installed. If the key locks the Software to a particular System, the Software may only be used on that System.

b - Locally Stored Components. The Software may include a software code component that may be stored and operated locally on one or more devices. Once you have paid the required license fees for these devices (as determined by Tyco in its sole discretion), you may install and/or use one copy of such component of the Software on each of the devices as licensed by Tyco. You may then use, access, display, run or otherwise interact with ("use") such component of the Software in connection with operating the device on which it is installed solely in the manner set forth in any accompanying

documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software.

c - Remotely Stored Components. The Software may also include a software code component for operating one or more devices remotely. You may install and/or use one copy of such component of the Software on a remote storage device on an internal network with all of the devices and may operate such component with each device over the internal network solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software; provided however, you must still acquire the required number of licenses for each of the devices with which such component is to be operated.

d - Embedded Software/Firmware. The Software may also include a software code component that is resident in a device as provided by Tyco for operating that device. You may use such component of the Software solely in connection with the use of that device, but may not retrieve, copy or otherwise transfer that software component to any other media or device without Tyco's express prior written authorization.

e - Backup Copy. You may make a back-up copy of the Software (other than embedded software) solely for archival purposes, which copy may only be used to replace a component of the Software for which you have current valid license. Except as expressly provided in this EULA, you may not otherwise make copies of the Software, including the printed materials.

3 - OTHER RIGHTS AND LIMITATIONS. Your use of the Software is subject to the following additional limitations. Failure to comply with any of these restrictions will result in automatic termination of this EULA and will make available to Tyco other legal remedies.

a - Limitations on Reverse Engineering and Derivative Works. You may not reverse engineer, decompile, or disassemble the Software, and any attempt to do so shall immediately terminate this EULA - except and only to the extent that such activity may be expressly permitted by applicable law notwithstanding this limitation. You may not make any changes or modifications to any portion of the Software, or create any derivative works, without the written permission of an officer of Tyco (except as provided in Section 3(f) of this EULA with respect to "open source" software). You may not remove any proprietary notices, marks or labels from the Software. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA by your personnel and agents.

b - Copyright Notices. You must maintain all copyright notices on all copies of the Software.

c - Transfer. You may only transfer your rights under this EULA (i) as part of a permanent sale or transfer of all of the devices for which the Software is licensed as applicable; (ii) if you transfer all of the Software (including all component parts, the media and printed materials, any upgrades and this EULA); (iii) if you do not retain any copies of any portion of the Software; (iv) if the recipient agrees to the terms of this EULA; and (v) if the Software is an upgrade, such transfer must also include all prior versions of the Software. You agree that failure to meet all of these conditions renders such transfer null and void.

d - Termination. Without prejudice to any other rights, Tyco may terminate this EULA if you fail to comply with the terms and conditions herein. In such event, you must immediately destroy all copies of the Software and all of its component parts. To the extent the Software is embedded in hardware or firmware, you will provide prompt access to Tyco or its representative to remove or lock Software features or functionality as Tyco determines.

e - Subsequent EULA. Tyco may also supersede this EULA with a subsequent EULA pursuant to providing you with any future component, release, upgrade or other modification or addition to the Software. Similarly, to the extent that the terms of this EULA conflict with any prior EULA or other agreement between you and Tyco regarding the Software, the terms of this EULA shall prevail.

f - Incorporation of "Open Source" and other Third Party Software. Portions of the Software may be subject to certain thirty party license agreements governing the use, copying, modification, redistribution and warranty of those portions of the Software, including what is commonly known as "open source" software. No warranty is provided for open source software. By using the Software you are also agreeing to be bound to the terms of such third party licenses. If provided for in the applicable third party license, you may have a right to receive source code for such software for use and distribution in any program that you create, so long as you in turn agree to be bound to the terms of the applicable third party license, and your programs are distributed under the terms of that license. If applicable, a copy of such source code may be obtained free of charge by contacting your Tyco representative.

g - Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of Tyco, its affiliates or its suppliers.

h - Rental. You may not sub-license, rent, lease or lend the Software. You may not make it available to others or post it on a server or web site or otherwise distribute it.

i - Software Keys. The hardware/software key, where applicable, is your proof of license to exercise the rights granted herein and must be retained by you. Lost or stolen keys will not be replaced.

j - Demonstration and Evaluation Copies. A demonstration or evaluation copy of the Software is covered by this EULA; provided that the licenses contained herein shall expire at the end of the demonstration or evaluation period.

k - Registration of Software. The Software may require registration with Tyco prior to use. If you do not register the Software, this EULA is automatically terminated and you may not use the Software.

l - Additional Restrictions. The Software may be subject to additional restrictions and conditions on use as specified in the documentation accompanying such Software, which additional restrictions and conditions are hereby incorporated into and made a part of this EULA.

m - Upgrades and Updates. To the extent Tyco makes them available, Software upgrades and updates may only be used to replace all or part of the original Software that you are licensed to use. Software upgrades and updates do not increase the number of copies licensed to you. If the Software is an upgrade of a component of a package of Software programs that you licensed as a single product, the Software may be used and transferred only as part of that single product

package and may not be separated for use on more than one computer or System. Software upgrades and updates downloaded free of charge via a Tyco authorized World Wide Web or FTP site may be used to upgrade multiple Systems provided that you are licensed to use the original Software on those Systems.

n - Tools and Utilities. Software distributed via a Tyco-authorized World Wide Web or FTP site (or similar Tyco-authorized distribution means) as a tool or utility may be copied and installed without limitation provided that the Software is not distributed or sold and the Software is only used for the intended purpose of the tool or utility and in conjunction with Tyco products. All other terms and conditions of this EULA continue to apply.

4 - EXPORT RESTRICTIONS. You agree that you will not export, re-export or transfer any portion of the Software, or any direct product thereof (the foregoing collectively referred to as the "Restricted Components"), to IRAN, NORTH KOREA, SYRIA, CUBA and SUDAN, including any entities or persons in those countries, either directly or indirectly ("Tyco's Position"). You also agree that you will not export, re-export or transfer the Restricted Components to any other countries except in full compliance with all applicable governmental requirements, including but not limited to applicable economic sanctions and constraints administered by the U.S. Treasury Department and applicable export control measures administered by the U.S. Department of Commerce and U.S. Department of State, any other U.S. government agencies, and measures administered by the European Union or the government agencies of any other countries. Any violation by you of the applicable laws or regulations of the U.S. or any other government, or where you breach Tyco's Position notwithstanding whether or not this is contrary to any aforementioned applicable laws or regulations, will result in automatic termination of this EULA.

5 - U.S. GOVERNMENT RESTRICTED RIGHTS. The Software is Commercial Computer Software provided with "restricted rights" under Federal Acquisition Regulations and agency supplements to them. Any use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in sub-paragraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFAR 255.227-7013 et. seq. or 252.211-7015, or sub-paragraphs (a) through (d) of the Commercial Computer Software Restricted Rights at FAR 52.227-19, as applicable, or similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Sensormatic Electronics, LLC, 6 Technology Park Drive, Westford, MA 01886.

6 - LIMITED WARRANTY.

a - Warranty. Tyco warrants that the recording medium on which the Software is recorded, hardware key, and the documentation provided with it, will be free of defects in materials and workmanship under normal use for a period of ninety (90) days from the date of delivery to the first user. Tyco further warrants that for the same period, the Software provided on the recording medium under this license will substantially perform as described in the user documentation provided with the product when used with specified hardware. THE FOREGOING EXPRESS WARRANTY REPLACES AND IS IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED OR OTHER WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OR NON-MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY, CUSTOM, TRADE,

QUIET ENJOYMENT, ACCURACY OF INFORMATIONAL CONTENT, OR SYSTEM INTEGRATION. TYCO MAKES NO WARRANTY THAT ANY PORTION OF THE SOFTWARE WILL OPERATE ERROR-FREE, FREE OF ANY SECURITY DEFECTS OR IN AN UNINTERRUPTED MANNER. TYCO SHALL NOT BE RESPONSIBLE FOR PROBLEMS CAUSED BY CHANGES IN THE OPERATING CHARACTERISTICS OF THE DEVICE(S) UPON WHICH THE SOFTWARE IS OPERATING, OR FOR PROBLEMS IN THE INTERACTION OF THE SOFTWARE WITH NON-TYCO SOFTWARE OR HARDWARE PRODUCTS. TYCO 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. THE WARRANTY MADE BY TYCO MAY BE VOIDED BY ABUSE OR MISUSE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS UNDER MANDATORY LAW THAT VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

b - Exclusive Remedy. Tyco's entire liability and your exclusive remedy under the warranty set forth in this Section 6 will be, at Tyco's option, to (i) attempt to correct Software errors with efforts Tyco believes suitable to the problem, (ii) replace at no cost the recording medium, Software or documentation with functional equivalents as applicable, or (iii) refund a pro-rated portion of the license fee paid for such Software (less depreciation based on a five-year life expectancy) and terminate this EULA, provided, in each case, that Tyco is notified in writing of all warranty problems during the applicable warranty period. Any replacement item will be warranted for the remainder of the original warranty period. No remedy is provided for failure of the Software if such failure is the result of accident, abuse, alteration or misapplication with respect to the Software or any hardware on which it is loaded. Warranty service or assistance is provided at the original point of purchase.

7 - LIMITATION OF LIABILITY & EXCLUSION OF DAMAGES.

a - LIMITATION OF LIABILITY. IN NO EVENT WILL TYCO'S AGGREGATE LIABILITY (INCLUDING, BUT NOT LIMITED TO, LIABILITY FOR NEGLIGENCE, STRICT LIABILITY, BREACH OF CONTRACT, MISREPRESENTATION AND OTHER CONTRACT OR TORT CLAIMS) ARISING FROM OR RELATED TO THIS EULA, OR THE USE OF THE SOFTWARE, EXCEED THE GREATER OF USD$5.00 OR THE AMOUNT OF FEES YOU PAID TO TYCO OR ITS RESELLER FOR THE SOFTWARE THAT GIVES RISE TO SUCH LIABILITY. BECAUSE AND TO THE EXTENT THAT SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSIONS OR LIMITATIONS OF LIABILITY ABOVE, THESE MAY NOT APPLY TO YOU.

b - EXCLUSION OF OTHER DAMAGES. UNDER NO CIRCUMSTANCES SHALL TYCO OR ANY OF ITS RESELLERS OR LICENSORS BE LIABLE FOR ANY OF THE FOLLOWING: (I) THIRD PARTY CLAIMS; (II) LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA, OR LIABILITIES RELATED TO A VIOLATION OF AN INDIVIDUAL'S PRIVACY RIGHTS; OR (III) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR COVER DAMAGES (INCLUDING LOST PROFITS AND LOST SAVINGS), IN EACH CASE EVEN IF TYCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ARE SOLELY RESPONSIBLE AND LIABLE FOR VERIFYING THE SECURITY, ACCURACY AND ADEQUACY OF ANY OUTPUT FROM THE SOFTWARE, AND FOR ANY RELIANCE THEREON. SOME JURISDICTIONS DO

NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO SOME OF THE ABOVE LIMITATIONS MAY APPLY TO YOU ONLY TO THE EXTENT PERMITTED BY THOSE LAWS.

8 - GENERAL. If any provision of this EULA is found to be unlawful, void, or for any reason unenforceable, then that provision shall be severed from this EULA and shall not affect the validity and enforceability of the remaining provisions. You should retain proof of the license fee paid, including model number, serial number and date of payment, and present such proof of payment when seeking service or assistance covered by the warranty set forth in this EULA. This EULA is governed by the laws of the State of New York, without regards to its conflicts of law principles. The parties hereby irrevocably agree that they submit themselves to the personal jurisdiction of the state and federal courts of New York for purposes of resolving any and all disputes arising under or related to these terms and conditions. The parties specifically exclude the application of the provisions of the United Nations Convention on Contracts for the International Sale of Goods.

Privacy Notice

The personal data processed by this application by Johnson Controls as controller will be processed in accordance with the Johnson Controls Privacy Notice at **https://www.johnsoncontrols.com/legal/privacy**. By installing this software, you acknowledge that you have read and understood the Johnson Controls Privacy Notice. If your consent is required under applicable law for the processing and/or transfer (including international transfer) of such personal data, and strictly to the extent that consent is required under applicable law, your above actions are your consent.

EntraPass Help

Release Notes 8.10

ioModule

The KT-MOD-IO16 is an add-on module for the KT-400, and the KT-1 controllers. The RS-485 board has 16 inputs/outputs that you can configure in banks of four from EntraPass. You can define the module as inputs, relays, or as an elevator. There is an option to use terminals 9 - 12 as SPI relays in addition to the current 32 SPI relay modules defined in the SPI tab.

Furthermore, a full status review of the ioSmart reader and the ioModule is available from the controller they are connected to. For more information see, **Module status**.

A new icon in the controller menu facilitates finding unassigned modules. For more information see, **ioModule.**

We have used the same functionality to find unassigned ioModules as we use for ioSmart readers. For more information, see **Requesting unassigned modules**.

To assist administration requirements, a new ioModule tab is available to view firmware parameters, for more information, see **ioModules**.

For compatibility, you must use the latest firmware on the KT-1 and KT-400 controllers.

Audit trail

For faster auditing and troubleshooting, we have added a new audit feature. Audit reports are available based on cards, components, and operators.

The audit functionality provides a detailed report on who made changes, and when the changes occurred to a card, or to a component. Detailed information includes some of the following: the type of change, the menu that was changed, the number of fields changed, the name of the GUI field, the value before the change, the value after the change, and the data type. The Audit icon is available in any menu where you can edit a card or a component, and the operator based report is under the system menu. For more information, see **Card audit trail**, and **Activity report.**

Additional card information fields

EntraPass Corporate Edition now has 20 information fields available, as ten additional fields have been added. Information fields have editable labels, and are useful for storing information regarding the cardholder, for example, department, address, employee number. For more information, see **Issuing a new card**.

User last accessed door

We have added an additional field to the user card report. Last access is now an option in the print selected fields area of the print card window. If selected, three additional columns appear in the report: last door accessed, last used date and time, and last event message. For more information, see **Card printing**.

Unique ID to import and export cards

To improve the import/export feature for card information, we have added UniqueID to the available fields list. When you create your import pattern, and select UniqueID, you can import without a card number. You can also delete users without a card number. For more information, see **Creating a new import/export pattern**.

Round badge images

We have enhanced the template properties for badge design. Two new options are available, the first is the standard rectangular image with rounded corners, and the second is a round or ellipse shaped image. For more information see, **Badges designing**.

Display user display fields in the access level links

We have added an additional field to primary links in the access level module. Prior to 8.10, the primary links showed a list of all cardholders who have access to the selected access level. To assist recognition, the user can add a column for the card information fields, with the ability to select any one of the card information fields of the users. EntraPass maintains your selection to ensure it is available for subsequent logins.

Remove compressed backup options

Due to admin settings restricting correct execution of the self-extracting compressed backup file, we removed this option from the data, archive, in/out, and video backups, and the backup scheduler. Use the separate files backup instead. For more information see, **Backups**.

Prevent conflict of versions in backup data

To avoid restoring the incorrect data version and creating database conflicts, when an operator is restoring a data backup, EntraPass validates the first two digits of the version and if the version the operator is restoring is different to the current version of the software, it displays a message instructing the operator to ensure that the versions match. This is available for all backup types. For more information, see **Restores**.

Hide thumbnail images from information fields

To facilitate different security levels requirements, EntraPass offers the ability to hide card information fields from view. Thumbnail images for operators and users now have this functionality and you can choose to see pictures only when needed. If the setting is set to none, the image thumbnail displays in the top right corner of the user and operator page. For more information see, **Hiding card information**.

Personalize the welcome message

To personalize the user's experience you can customize the welcome e-mail that EntraPass sends for new users and operators. For situations when you need to disable an operator, you can also write a message to explain why.

Close acknowledgement screen when alarm is acknowledged

To eliminate multiple responses in a multiple workstation setup, the notification windows automatically close on the other workstations, when someone acknowledges the alarm. For more information, see **Application status**.

8 Assa-Abloy wireless locks per KT-1

Due to the continued success of the KT-1, the one-door controller can now support eight Assa-Abloy wireless locks. The addition of six wireless locks reduces the installation costs by minimizing the amount of controllers required for large volumes of wireless locks, and the labour required to fit them.

Run activity report from user screen

A new icon in cards generates a new report for a card's last transactions. This quick report is in addition to the existing list found in the message desktop but provides more report options with unlimited results. For more information, see **Activity report**.

Added the Simplex 4007ES to our integration range and simplified integration names and descriptions in the GUI

The simplex 4007ES fire panel has been added to the list of fire panels that EntraPass integrates with. Additionally, to make installation easier when integrating with intrusion or fire panels, we have rewritten the drop-down text and the description for all DLL types. For more information, see **Integrated panel configuration**.

Sybase update

To enable all EntraPass applications to run on Windows Server 2016, and Windows Server 2019, we have updated to the latest Sybase database.

Database cleanup

We have improved the efficiency of the Sybase database by adding functions to automatically perform a clean-up, and pack files that reach a certain size. Additionally EntraPass will automatically delete large card records that have not been modified in five years.

Windows server 2019 compatibility

EntraPass is now compatible with Windows Server 2019 Standard. For more information, see **Minimum system requirements**.

Print access levels directly in PDF format

When you want to print access levels, you now have the option to save the access level to a PDF format and a CSV file format, this is in addition to the existing print functionality. The option to save an electronic copy of the definition supports a paperless office.

Small workstation enhancements

When you update to the latest version of EntraPass, you will notice a couple of improvements when launching the system. The product version appears on the upper-right section of the screen and eliminates the need to click into the about section for the information. Additionally, to reduce clicks, after you login, the credential window automatically displays, with the focus on the user name.

Enhanced EntraPass web service

To accommodate circumstances when EntraPass web is installed in a different Internet Information Services (IIS) folder, the operator now controls the link for the welcome e-mails for EntraPass web, EntraPass go, and EntraPass go Install. The operator can make the modifications directly in the GUI. This update also facilitates multiple SmartLink connections, where you can select, which mobile applications to connect to, which SmartLink connection. For more information, see **Configuring the SmartLink application**.

How to Create a Backup

1 - Click the **Options** tab.

2 - Click the **Backup Scheduler** button.

3 - Select the data type from the tabs on the top (**Data, Archive, In/Out** or **Video Event**).

4 - Click the **Automatic Backup** check-box to enable the function and enter the **Start time**.

5 - If you choose **Automatic Backup**, select a frequency.

6 - Click the **Now** check-box to start the backup immediately.

For more details about the configuration of backups, please refer to ***Backups***

How to Create a Badge

1 - Click the **Users** tab.

2 - Click the **Badge** button.

3 - Click the **New** button ( ) in the toolbar.

4 - Set the badge properties and click ***OK***.

5 - Enter the badge name for both languages.

6 - Click on ***Click here to modify the badge layout*** at the bottom of the window.

7 - In the ***Badge design*** window, select the elements to be included in the badge.

8 - Once finished, click the ***Layout*** menu and select ***Exit***.

9 - Click the **Save** button.

*For more details about the configuration of a badge in EntraPass, please refer to **Badge Designing**.*

How to Create a Card

*A Gateway or a Connection must exist prior to creating a new card in EntraPass. Please refer to **EntraPass Gateways Configuration** for more details.*

*An Access Level must exist prior to creating a new card in EntraPass. Please refer to **How to Create an Access Level?** for more details.*

1 - Click the **Users** tab.

2 - Click the **Card** button.

3 - Click the **New** button ( ) in the toolbar. The **Card number** field is enabled.

4 - Enter the **Card number** and press the **Enter** key.

5 - Enter the **Card user name**.

6 - Click the **Access level** tab.

7 - Select an **Access level** from the drop-down list.

8 - Click the **Save** button.

*For more details about the creation of a card, please refer to **Cards Definition.***

***NOTE:** If you enabled the Enhanced User Management, see **Issuing a New Card in Enhanced User Management Environment**.*

How to Create a Schedule

1 - Click the **Definition** tab.
2 - Click the **Schedule** button.
3 - Click the **New** button ( ) in the toolbar.
4 - Enter a name for the new schedule in both languages.
5 - Click the **Save** button.
6 - Enter a **Start time**and **End time**.
7 - Select the days of the week for which the schedule applies.
8 - Select the **Holidays** that applies (up to 4)

For more details about the definition of a holiday in EntraPass, please refer to ***Holiday Definition***

How to Create a Simple Report

*For more details about the creation of a report in EntraPass, please refer to **Quick Report Definition**.*

1 - Click the **Report** tab.

2 - Click the **Quick Report** button.

3 - Select the event type from the **Event** drop-down list.

4 - On the right side of the window, enter a name under **Report name** in both languages.

5 - Click the **Execute** button.

How to Create an Access Level

*A **Gateway** or a **Connection** must exist prior to creating a new access level in EntraPass. Please refer to **EntraPass Gateways Configuration** for more details.*

*For more details about the creation of a card, please refer to **Access Level Definition**.*

1 - Click the **Users** tab.

2 - Click the **Access level** button.

3 - Select a **Gateway / Connection** from the drop-down list.

4 - Click the **New** button ( ) in the toolbar. The **Card number** field is enabled.

5 - Enter a name for the access level in both languages.

6 - Click the **Save** button.

How to Print a Card List

1 - Click the **Users** tab
2 - Click the **Card** button
3 - Click the **Print** button.
4 - Select the **Card index** from the drop-down list.
5 - Optionally, you can specify a card number range, filters and select the card fields to be printed (see **Card Printing** for more details).
6 - Click the **Print** button.
7 - Select a printer from the drop-down list then click **OK**.

How to Print a List of Access Levels

1 - Click the **Users** tab.
2 - Click the **Access level** button.
3 - Click the **Print** button.
4 - Select a **Site/Gateway/Connection** from the drop-down list.
5 - Select the access levels to be printed.
6 - Click the **Print** button.
7 - Select a printer from the drop-down list then click **OK**.

How to Print a List of Doors

1 - Click the **Devices** tab.

2 - Click the **Door** button.

3 - Click the **Print** button.

4 - Select a **Site/Gateway/Connection** from the drop-down list.

5 - Select the doors to be printed.

6 - Click the **Print** button.

7 - Select a printer from the drop-down list then click **OK**.

How to Setup the Desktops

*For more details about the configuration of desktops in EntraPass, please refer to the **Desktops** section in the Table of Contents.*

1 - Click the **Desktops** tab.

2 - Right click on any **Desktop** button and select **Properties**.

3 - Enter a name for the new desktop in the **Desktop name** field.

4 - Select the desktops to display.

5 - Click **OK and GO** to save and apply the changes.

How to use shortcut keys

EntraPass supports the use of shortcut keys for faster operation.

EntraPasss shortcut keys

Key	Active from location	Function
F1	Any menu	Help
F2	Any list	Extended selection
F3	Any menu	Display all open windows
F4	Any menu with drop down	Open list
F5	Where available	Refresh
F8	Anywhere	Global Search
F10	Anywhere	Login / Logout
F11	Anywhere	Workspace
F12	Anywhere	Switch Account

How to personalize the Web login screen

You can customize the default welcome message and icon for EntraPass Web login. To customize the login screen, do the following:

1 - Open the web.cfg file located at C:\inetpub\wwwroot\EntrapassWeb using a text editor.

2 - Find the key entry *<add key ="WelcomeMessage" value="EntraPass Web"/>*.

3 - Replace *"EntraPass Web"* with your customized message. Do not use more than 30 characters to ensure the message can be viewed correctly. Special characters are supported through **HTML ascii codes**.

4 - Find the key entry *<add key ="WelcomeImage" value="Resources/Images/chip_bw.png"/>*

5 - Replace *"Resources/Images/chip_bw.png"* with the path of your preferred image. JPG and PNG file formats are supported.

6 - The default image size is 57 x 57 pixels. To change the default image size edit the key entries *"WelcomeImageHeight"* and *"WelcomeImageWidth"*. Do not use an image size greater than 155 x 155 pixels to ensure the entire image is visible.

How to enable GO Pass for a user

A user can open doors with their smartphone using the GO Pass application.

To use GO Pass you must add GO Pass to the **system components** and enable GO Pass for the Smartlink application. To enable GO Pass for the Smartlink application complete the following steps:

1 - Select **Devices**, **Application** and select the Smartlink that will be used in for your GO Pass application.
2 - Select the **Web Service** tab and the **Allow Go Pass** option.
3 - Ensure the **Connection name**, **IP address** / **Domain name**, and **port** numbers, are present for the Smartlink connection.
4 - Select the **SmartLink e-mail** tab.
5 - Ensure the **E-mail Server parameters** are present for the connection.

To enable GO Pass for a user and send credentials do the following:

1 - Under the **Users** tab select **Card**.
2 - Select an existing **Card user name** or create a new one.
3 - Select the **GO Pass** check box.
4 - Enter the user's email address. This will be used to send the GO Pass instructions to the user.
5 - Select the **Notify** check box to enable the instruction email.
6 - Select the language of the user.
7 - Select **Save**.

An email is automatically generated and sent to the user with details on how to download the application to their smartphone. The user's credentials are automatically entered into the application.

The system uses the **Card #1** details in the **Card** tab to grant access. Ensure that this field is complete.

Changing the Smartlink port or address will stop GO Pass access. GO Pass access requires updated credentials. To send the updated credentials to all GO Pass users do the following:

1 - Under the **Options** tab select **System Parameters**.
2 - From the menu select **EntraPass Web** and select **Resend to all GO Pass users**.

Updated credentials are automatically sent to all GO Pass user through an e-mail.

*NOTE: You must have a valid KAP to use the GO Pass feature. For more information click **here**.*

How to use HID Mobile Access

HID Mobile Access gives a user door access with their smartphone. The HID Mobile Access system is configured in EntraPass along with the user's card credentials.

You must register the HID Mobile Access integration in **system components** using the component name **HID Mobile Access**.

To enable HID Mobile Access, complete the following steps:

1 - Select the **Options** tab, and then select **System Parameters** from the menu.
2 - Select the **Integration** button and select the **HID Mobile Access** tab.
3 - Enter a **Client ID** and **Password**. PKI certificate validation is not currently supported. You can get these credentials from your HID system account. The **Portal URL**, **Login URL**, and **Path** are automatically completed but you can edit if you require.
4 - Select the **Configure Part Numbers** button. This opens the **Part Number Configuration** window.
5 - Select **Update from HID Portal** to update the list.
6 - Enter your **Facility Code** and select your **Card Display Format**. The facility code and card display format are specific to the HID cards you have purchased. Select **OK** to save your configuration.
7 - Select **OK** to save your HID Mobile Access parameters.

To add a new HID Mobile Access user in your system, complete the following steps:

1 - From the **Users** tab, select **Card**.
2 - Select an existing **Card user name**. This integration works on existing user accounts.
3 - Select the **HID Mobile Access** button. This opens a **HID Mobile Access** window.
4 - Select a part number from **Part Numbers** list. Each part number represents a box of cards. The **Qty** field displays the number of remaining card numbers.
5 - Select **Send Invitation & Issue Mobile ID** to prompt the user to register their smartphone.
6 - Select **OK**.

To view the status of an existing HID Mobile Access user, complete the following steps:

1 - From the **Users** tab, select **Card**.
2 - Select an existing **Card user name**.
3 - Select the **HID Mobile Access** button. This opens a **HID Mobile Access** window.
4 - Select the **Advanced** check box.

5 - In the **Invitations** section the status of the invitation is displayed. Here you can resend or delete invitations. The **Credential Containers** list displays all devices that have already been associated with the user.

6 - Select **OK**.

To add multiple devices to a single user, complete the following steps:

1 - From the **HID Mobile Access** window, select a part number from the **Part Numbers** list.

1 - Select the **Advanced** check box.

2 - Select the **Send Invitation** button. When the user registers their device, a new container is created in the **Credential Containers** list .

3 - Select the new device from the **Credential Containers** list.

4 - Select the **Issue Mobile ID** button.

5 - Select **OK**.

To add multiple cards to a single user, complete the following steps:

1 - From the **HID Mobile Access** window, select a part number from the **Part Numbers** list.

1 - Select the **Advanced** check box.

2 - Select a container from the **Credential Containers** list.

3 - Select the **Issue Mobile ID** button. This sends another mobile ID to the user's smartphone.

4 - Select **OK**.

NOTE: *Each device can hold 1 mobile ID from each part number. A device can hold up to 5 different mobile IDs if they come from 5 different part numbers.*

How to migrate from Event Parameter to Event Operator mode

Event operator mode replaces the event parameter mode for managing events. New installations will use Event Operator mode by default. Upgraded systems must enable the mode. To enable Event Operator mode and transfer existing event parameters to triggered alarm notifications complete the following steps:

1 - Log into the EntraPass server or workstation application.

2 - Click on **Options**, then **System Parameters**.

3 - Click on the **Server** icon.

4 - Click on the **Alarm Management** tab.

5 - Select **Migrate from Event Parameters to Event Operator**.

6 - Select **OK** to begin the migration.

7 - Select **OK** to confirm the operation. To ensure safety, an automatic backup is performed and the database is set to **locked**.

8 - During migration, events are displayed in the operator's default desktop.

- If the **Override workstation workspace message** option is selected, events are displayed in the workspace defined in the **Security** tab.
- If the **Override workstation workspace message** option is not selected, events are displayed in the default desktop.
  - If the operator has never logged into workstation or the operators last login was not in workstation, the operator will get all events
  - If the operator's last login was in workstation and **Apply Workstation workspace and event parameters** option is selected , the operator will get events in the workspace defined in **When Logged In** option and from the schedule defined in **Event Parameters** from that workstation.
  - If the operator's last login was in workstation and **Apply Workstation workspace and event parameters** option is not selected, the operator will get events with the display schedule defined in **Event Parameters** from that workstation.

9 - Existing Event Parameters are merged into single Triggers and Alarms based on their type (Application, Door, Input, etc), their alarm schedule, and their instruction. Task Builder tasks defined through **Event Parameters** are also migrated.

10 - The alarm management model is transferred to each Trigger and Alarm. **Compatible** and **Event Priority** modes are transferred to **Acknowledge for all connected workstations**.

11 - Following migration, all active workstations must be logged out and logged in to view the changes.

NOTE: The migration from Event Parameter mode to Event Operator mode cannot be reversed.

How to manually set the database to read-only mode

When database read-only mode is enabled, no modifications can be made to the database. Messages, alarms and manual operations will continue to work as normal. To manually set your EntraPass database to read-only mode complete the following steps:

1 - Log into the EntraPass server or workstation application.

2 - Right-click anywhere in the main window to launch the menu.

3 - Click **Database read-only**.

4 - Click **Yes** to confirm the action.

5 - Click **OK** to close the confirmation box. The network database state indicator, located at the bottom left of the screen, will turn from green to black.

6 - To restore your database back to normal mode, right-click anywhere in the main window and click **Database read-only**. The status indicator located at the bottom left of the screen will turn from black to green.

NOTE: *The database will remain in read-only mode until an operator disables it or the server is restarted.*

How to enable EntraPass maintenance mode

When maintenance mode is enabled in EntraPass all alarm notifications are bypassed. This includes all alarm acknowledge popup messages and e-mails sent from an **Event Trigger**. This mode does not affect reports sent by e-mail, and KAP reminder e-mails.

To enable maintenance mode, complete the following steps:

1 - Log into the EntraPass server or workstation application.

2 - Right-click anywhere in the main window to launch the menu.

3 - Click **Maintenance mode**.

4 - Click **Yes** to confirm the action.

5 - Click **OK** to close the confirmation box. While maintenance mode is enabled, a **Maintenance mode** message is displayed at the bottom of the window.

6 - To disable maintenance mode, right-click anywhere in the main window and click **Maintenance mode**.

NOTE: Maintenance mode will remain active until an operator disables it or the server is restarted.

How to setup the ioSmart

The Kantech ioSmart card reader must be connected to a supporting controller (KT-400 or KT-1). The ioSmart supports both wiegand and RS-485 connections to the controller.

When connecting using the wiegand connection, use the Express Setup Program to configure the reader. When connecting using the RS-485 connection, complete the following steps:

1 - Click the **Devices** tab.
2 - Select the **Controller** icon.
3 - Select a controller and click on the **ioSmart** tab.
4 - Select the **+** symbol to add an ioSmart reader to the controller.
5 - Enter your ioSmart reader's **Serial number**.
6 - Select the **Associated door**.
7 - Select the **Keypad** option if your ioSmart reader includes a keypad.
8 - To configure the reader's inputs and outputs, click the terminal button, and select the I1 and I2O terminal function.
   - **Disabled**
   - **Single input**
   - **Dual input**
   - **Lock output**
   - **Relay**

It is possible to configure I1 and I2O for a maximum of 4 inputs (using both I1 and I2O in dual inputs mode) or 2 inputs and 1 output (lock output or relay).

9 - Click the **KT-1/KT-400** tab, an select the appropriate **Baud rate** for your system.
10 - Click the three dot button to assign the **Reader template**. Use the **Devices/Reader template** to configure the reader template.

You can also configure your ioSmart in the **Operation** tab.

1 - Click the **Operation** tab.
2 - Select the appropriate controller icon, and the controller windows appears.
3 - Select the appropriate device, right-click the controller, and select **Request unassigned modules** from the menu.
4 - Right-click a controller and click **Unassigned Module**. This creates a **Controller unassigned module requested by operator** event on the desktop.

5 - Right-click the event to assign the reader. The serial number of the ioSmart reader is automatically populated in the configuration tab.

*NOTE: You will see the error message **Cannot add a module to this controller** when additional readers cannot be added to a controller.*

The configured ioSmart status is displayed in the **Operation**... **Door** menu. Right-click on the appropriate door to view the status. The status of all configured ioSmart readers connected to a controller is displayed in **Operation**.... **Controller** menu.

Can I use an Input to unlock an elevator floor or a group, and how long will it remain unlocked?

Yes, an input can be used to unlock a single floor or group. The floor or the group, will follow the unlocked time for the door. The default is 10 seconds, which can be modified.

Is it possible to import access levels?

Access levels cannot be imported.

What are the communication ports for EntraPass, such as server, work-station, SmartLink, gateway, mirror database, video vault and EntraPass Web?

- Server: TCP 18000
- Workstation: TCP 18101
- Gateway: TCP 18102
- Smartlink: TCP 18103
- Mirror Database: TCP 17999
- Video Vault: TCP18107
- EntraPass WEB: TCP 8801

What are the various options available in batch operation?

The batch operation allows the user to do massive changes to the card database with one single click. The fields that can be changed with a batch operation are: Card State, Supervisor Level (GE), Maximum card usage, Trace, Start Date, End Date, Delete When Expired, Wait for Keypad, Card Access Group, or Badge Layout. The batch operation can also be done via Card Type.

F.A.Q.

What happens when card pictures are saved on a hard drive instead of the server database?

A parameter allows you to save cards and visitor card pictures, signatures and background graphics, to a file instead of directly to the database. We are offering this option for sites that have large banks of pictures and graphics. The picture, signature and graphic database can currently contain up to 2 Gb of data each. The parameter will be used in instances where a connection may need more space to save pictures, signatures and graphics.

What is the difference between “One time access and Temporary unlock door option on KT-100 200 300 and 400?

One time access on the KT-100-200-300-400

This command can be achieve via the operation door menu it will follow the unlock time of the door. If the door stay open longer then unlock time it will generate an event pre alarm door open too long and if not close at the end of the open time it will generate door open too long.

Temporary unlock on KT-100-200-300

This command can be achieve via the operation door menu it will follow the unlock time of the door. If the door stay open longer then unlock time it will generate an event pre alarm door open too long and if not close at the end of the open time it will generate door open too long.

Temporary unlock on KT-400

This command can be achieve via the operation door menu once the door is open if it goes beyond the set time for the temporary unlock it will generate a different event Door alarm on relock.

What is the purpose of Custom messages?

The Custom Messages option allows operators, with proper security rights, to define custom messages that can generate an event based on a schedule. Up to 10 custom messages can be programmed to trigger an event at a preset time. Each custom message can be triggered when the schedule becomes valid, invalid, or both. In other words, you can trigger up to 20 custom events if you take into account the start and/or end of a schedule interval.

Each custom event is displayed in the Messages List on the desktop.

F.A.Q.

Why do we use card access groups?

Pre-programmed card access groups allow quick selection of access levels for various sites of the system. A card access group can be recalled during card programming, instead of re-entering the access levels for each connection. It is only card access group information that is associated with the card; therefore, you can modify the card access group information without modifying card access.

Card access groups can be imported from a CSV file.

Where can I synchronize operators with Active directory?

It is possible to launch synchronization from a number of locations, these include:

- **System / Active directory:** use the **Sync Now** button to manually start synchronization with the selected Active directory server.
- **Status / Application**: right click SmartLink to see two Sync options:
  - **LDAP force synchronize all** will synchronize all Active directory servers.
  - **LDAP force synchronize** will synchronize only one particular Active directory server.
- **LDAP service control:** right click the Active directory icon in the Windows system tray to see the **Sync Now** option:
  - This option synchronizes all Active directory servers on the selected SmartLink.

What is EntraPass?

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

- A new database engine (Sybase)
- Remote communication capability
- SmartLink interface with paging systems, HVAC systems, email and more
- Redundancy server for fail-safe operation (optional)
- Connection to the Kantech IP Link
- KT-100, KT-200, KT-300 and KT-400 compatibility

NOTE: *You can connect a loop of KT-200 controllers on the RS-485 of the KT-400 if not mixed with other controllers (Kantech KT-100, KT-300 and KT-400).*

- Kantech Telephone Entry System (KTES)
- Third party hardware integration
- Express setup
- Local anti-passback, interaction between door controllers, and DayPass for temporary visitors
- Elevator control
- Integrated badging capability
- Interactive floor plans
- Configurable desktops by operator

- CardGateway (optional)
- Multiple reader technology
- External alarm system interfacing
- In/Out reporting, Email reports capability
- Visual diagnostics
- Video Integration with American Dynamics family of Intellex® Digital Video Management System (DVMS)
- Support of 40 TVR II
- Support of 40 NVR
- Live video display, recorded video playback, local event logging and saving
- Video archiving via EntraPass Video Vault
- Vocabulary editor
- Intrusion Integration
- Windows 7 Pro 64-bit supported

What is Access Control?

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

EntraPass Main Features

Kantech Advantage Program (KAP):

KAP provides 12 months of free upgrades and online training for end users. For further details, refer to the Application Note, *New Optional Kantech Advantage Program, DN1874.*

SmartLink

EntraPass enables organizations to interface to most intelligent devices such as CCTV multiplexers, alphanumeric pager systems, automated emails, HVAC systems, LCD panels, video matrix switchers, etc., using an RS-232 or network connection between one of the EntraPass SmartLinkF workstation and remote EntraPass WebStations. Advanced system integration can be accomplished by using the bi-directional SmartLink to communicate with software applications such as In/Out systems, Badging systems, Human Resource Management systems, Student Registration systems, etc., through TCP/IP, an RS-232 port or with DLLs. This allows complete and real-time data exchanges between systems, eliminating redundant data entry.

Mirror Database and Redundant Server

The Mirror Database and Redundant Server component provides an alternative duplication mechanism in case of failures and errors of the Primary Server. The mirror database creates a real-time copy of the system database on the Redundant Server. In the event of a failure from the primary server, the mirror database launches the Redundancy Server which supports all the features and functionality of the primary server, except the Card Gateway program. Once the primary server returns online, all archives are merged and the entire database is copied or merged from the Redundancy Server.

NOTE: *The **Card Gateway** is not compatible with windows server 2008 64 bits. Client 32 bits must be installed.*

Wireless Door License

The wireless door license feature supports the addition of wireless doors to your EntraPass system. EntraPass supports the addition of Assa Abloy wireless doors. Wireless doors can be configured to work with Kantech controllers KT-1 and KT-400.

NOTE: *Purchase door licenses for each wireless door.*

Kantech IP Link

EntraPass is compatible with the Kantech IP Link that provides a secure Ethernet connection that serves as a polling device that will control the excess bandwidth by communicating to the Multi-site Gateways only when necessary. The Kantech IP Link's main function is to relay information between the controllers and the gateway.

KT-100, KT-200, KT-300 and KT-400 Controllers

EntraPass is compatible with Kantech's KT-100, KT-200, KT-300 and KT-400 controllers. 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.

KT-400

The KT-400 controller is a four-door Ethernet encrypted controller that is used as a door controller and as a IP communication device for a remote site loop.

Expansion Modules for the KT-400

The KT-400 controller allows connection of expansion modules in order to add outputs, like relays and open drain outputs, and inputs. *Mixing up input and output expansion modules gives the ability to connect up to 256 inputs and 256 outputs per KT-400 Controller.*

- **KT-MOD-REL8** : This expansion module is an 8-relay expansion module used as general relays or elevator control outputs. The module supports daisy chaining which can add up to 32 KT-MOD-REL8 modules for a total of 256 external relays per KT-400 controller.

- **KT-MOD-INP16** : This expansion module is an input module that adds up to 16 zones to the KT-400 controller. The module supports daisy chaining; you can interconnect up to 15 KT-MOD-INP16 modules for a total of 240 external inputs per KT-400. Adding the 16 onboard inputs of the KT-400 gives a total of 256 inputs per KT-400.

- **KT-MOD-OUT16** : This expansion module is an open drain to 12 VDC 16 output module. It can be used for elevator access control (may require additional hardware). The module supports daisy chaining; you can interconnect up to 16 KT-MOD-OUT16 modules for a total of 256 external outputs per KT-400.

Kantech ioSmart card reader

The Kantech ioSmart card reader enables card access for users through a Kantech door controller (KT-400 and KT-1).The ioSmart supports the transmission of card numbers using the Wiegand protocol. Supported formats include the standard 32-bit format, the standard 26-bit format and other Kantech proprietary formats like eXtended Secure Format(XSF) and Smartcard Secure Format(SSF). To provide an easy upgrade path to customers, some models support both the Smart Card technology and the Kantech proximity technology (ioProx).

HID Mobile Access

The HID Mobile Access system integration for EntraPass enables door access using an authenticated smartphone. Registration and management of credentials is controlled though EntraPass.

Kantech Telephone Entry System

The Kantech Telephone Entry System enables users to grant access to the building, to their visitors, via their own land telephone or cellular telephone. This telephone line can also serve, via an integrated modem, as a programming link or a monitoring link. The KTES is designed to be a stand-alone unit as well as a part of a complete access control system such as EntraPass from Kantech or any access control system. It can communicate with EntraPass through a Multi-site Gateway for programming and monitoring. The KTES installation can also include Kantech controllers (KT-100, KT-300 and KT-400) as well as any controller that supports a Wiegand interface port. Also, in order to ease the process of importing and exporting tenant lists, an automated procedure has been implemented to guide you through the various steps. For details concerning the installation and the local programming of the KTES, refer to the *KTES Installation Manual*, DN1769 and *KTES Programming Manual*, DN1770.

Express Setup

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

Elevator Control Capability

EntraPass allows installers to program up to 64 floors per elevator cab using expansion devices such as KT-PC4216, KT-PC4204 (16 floors maximum) with the KT-300 or such as KT-MOD-OUT16, KT-MOD-INP16 or KT-MOD-REL8 with the KT-400. This indispensable feature in a multi-tenant building allows facility managers to restrict specific floor access to authorized cardholders.

Integrated Badging

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

Interactive Floor Plans

EntraPass can import and display high-resolution graphics created on CAD-type systems (converted to .jpg or .bmp), allowing you to design a graphic-based system that operators can use with minimal training. Interactive buttons can be added to floor plans to display component status and offer full manual operation of the component in real-time.

Configurable Desktops by Operator

With EntraPass, each Operator can be assigned up to 8 configurable desktops. These desktops display selected windows featuring message events, user photos, filtered events, high-resolution graphics and videos, and alarm instructions. Desktops can contain any combination of windows.

Interfacing with External Alarm Panels

KT-100, KT-300 and KT-400 controllers allow users to arm, disarm, and postpone the arming of an external alarm panel . This allows EntraPass to easily integrate with an external alarm system.

In/Out Feature

The In/Out feature is a low-cost alternative to high-priced dedicated In/Out systems. It enables operators to print or download time sheets in a CSV format to a payroll system.

Visual Diagnostics

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

Enhanced Video Integration

EntraPass adds real-time monitoring capability as a response to the growing importance of video in access control systems. Integration with American Dynamics' Intellex® digital video management system through the powerful Intellex Application Programming Interface (API) provides real-time video monitoring as well as video playback. Video can be linked to real-time video monitoring as well as video playback. Video can be linked to access events and recorded from one to sixteen cameras from different Intellex units simultaneously. Presets, sequences, dome control and 1x1, 2x2, 3x3, and 4x4 views are available through the EntraPass software. All cameras can be called up directly from a floor plan simply by double-clicking on the camera or dome button. Operators can configure viewing parameters for digital video applications through an EntraPass user interface.

EntraPass Video Vault

EntraPass Video Vault enables all video clips from an Intellex alarm or an EntraPass video alarm to be automatically stored as Audio Video Interlaced format (.AVI) files or Kantech Video Intellex (.KVI), Kantech Video Archive (.KVA) and American Dynamics' Network Client's video format (.IMG) which can be password protected. Each EntraPass Video Vault may be connected to as many Intellex units as defined within the EntraPass software. Video may be saved to up to 24 pre-programmed hard drive locations. A .bmp image may be associated automatically with each video clip, and a thumbnail image may be created on the first frame of the video clip.

Vocabulary Editor

Simple and easy program used to translate the software in the language of your choice. By default, EntraPass is available in English, French, Spanish, German and Italian. It can also be translated in up to 99 languages, by using this feature.

Intrusion Integration

Addition of a manual operation on the intrusion components. A full access of the Panel Virtual Keypad attached to a KT-400 is now provided. A pass-through mechanism on the KT-400 links the Panel Manager of the Gateway directly with the panel's DLL. An auto-detection function has been added to fetch the data directly from the hardware panel in order to optimize the provisioning process.

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, refer to the following table for the Technical Support Help Desk in your area.

USA and Canada	**GMT - 05:00**		
North America	Toll free	+1 888 222 1560	08:00 to 20:00
	Direct	+1 450 444 2030	http://www.kantech.com/Support/Contact_Technical_Support_Advanced.aspx
Latin America	**GMT - 03:00**		
Argentina, Buenos Aires	Direct	+54 11 5199 3104	08:00 to 20:00
Brazil, Sao Paolo	Direct	+55 11 3181 7377	http://www.kantech.com/Support/Contact_Technical_Support_Advanced.aspx
Chile, Santiago	Direct	+56 2 3210 9662	
Colombia, Bogota	Direct	+57 1 344 1422	
Colombia, Cali	Direct	+57 2 891 2476	
Colombia, Medil-lin	Direct	+57 4 204 0519	
Costa Rica, National	Direct	+506 4 000 1655	
Dominican Repub-lic, Santo Domingo	Direct	+1 829 235 3047	

USA and Canada	GMT - 05:00		
El Salvalor, San Salvador	Direct	+503 2 136 8703	
Guatemala, Guatemala City	Direct	+502 2 268 1206	
Mexico, Mexico City	Direct	+52 55 8526 1801	
Panama, Panama City	Direct	+507 836 6265	
Peru, Lima	Direct	+51 1 642 9707	
Venezuela, Caracas	Direct	+58 212 720 2340	
Asia	**GMT + 08:00**		
	Toll free	+800 CALL TYCO	09:00 to 17:00
		+800 2255 8926	http://www.kantech.com/Support/Contact_Technical_Support_Advanced.aspx
	Direct	+86 21 6023 0650	
China	Direct	+400 671 1528	
India	Direct	+1 800 1082 008	
Australia	Direct	+02 9684 3980	
EMEA	**GMT + 01:00**		

USA and Canada	GMT - 05:00		
United Kingdom	Direct	+44 330 777 1300	08:00 to 18:00
Israel	Direct	+972 772 201 350	http://www.kantech.com/Support/Contact_Technical_Support_Advanced.aspx
Spain	Direct	+900 99 31 61	
France	Direct	+0800 90 79 72	
Germany	Direct	+0800 1806 757	
Italy	Direct	+39 0230 510 112	
Belgium	Direct	+0800 76 452	
Ireland	Direct	+180 094 3570	
Bahrain	Direct	+800 04127	
Nordic Countries	Direct	+45 4494 9001	
Greece	Direct	+00800 3122 9453	
Russia	Direct	+81 0800 2052 1031	
Turkey	Direct	+00800 319 23007	
United Arab Emirates	Direct	+80 03107 123	
South Africa	Direct	+27 21100 3882	

Minimum System Requirements

Operating System Compatibility

- Windows Server 2008 R2 Standard/Enterprise
- Windows Server 2012 Datacenter x64
- Windows Server 2016 Standard and Windows Server 2016 Datacenter

> ***NOTE:*** *Database access application is not supported in Windows Server 2016, the fix is scheduled for the next version of EntraPass.*

- Windows Server 2019 Datacenter x64
- Windows 7 Pro/Enterprise/Ultimate (all in 32 and 64-bit version)
- Windows 8.1 Enterprise x86/Windows 8.1 Enterprise x64
- Windows 10 Enterprise x86/Windows 10 Enterprise x64

> ***NOTE:*** *Ensure a ll operating systems have their latest service packs and updates.*
> *Perform software installations with administrator rights.*

Make sure the computer that requires the software installation meets the following minimum requirements:

- Dual Core processor
- 4GB RAM
- AGP or PCI Express 8X graphics card with 64 MB memory and DirectX 9.0 support
- 10/100 Base-T network adaptor EntraPass

Web Server

- Processor: Pentium IV at 1.8GHz
- Minimum hard disk space: 10 GB
- 1 GB RAM
- Microsoft Internet Information Services (IIS) version 5.1 or higher with the latest security updates
- Adobe Flash Player 9.0 must be installed on the client's PC when accessing the web pages.

Virtual Environment Supported

- VMware Workstation Version 7 & higher

Additional Requirements

For several applications, you can use the following devices:

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

Security Hardening Guide

Kantech recommends the following setup, configuration, and installation measures to ensure the highest level of security for EntraPass. Failure to comply with the following security configuration may result in a weakened operational state with related security vulnerabilities. For further information, see your product installation guide for specific instructions. To comply with recommended security standards, complete the following steps:

1 - Deploy EntraPass on a Virtual Local Area Network (VLAN).

2 - For an encrypted layer of security during data transit, use Hypertext Transfer Protocol Secure (HTTPS) instead of HTTP. You must obtain a Secure Socket Layer (SSL) certificate from a certificate authority (CA), and generate it for the EntraPass Web website. Refer to how to implement SSL in IIS (Internet Information Services) on Microsoft's website. **https://support.microsoft.com/en-nz/help/299875/how-to-implement-ssl-in-iis**

NOTE: This link is for reference only, contact Microsoft for support on how to implement SSL.

3 - Change default passwords during installation.

System Installation

Once the EntraPass installation is complete, a regular user cannot start the software without modifying folder permissions. To resolve the issue, provide full administrator rights to the user for the following folders:

- For 64-bit OS:
  - the C:\Program files(x86)\Advantage 10.10 and C:\Program files(x86)\Kantech folders.
  - the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Kantech and HKEY_LOCAL_ MACHINE\SOFTWARE\Wow6432Node\Advantage Data Architect registry entries.
- For 32-bit OS:
  - the C:\Program files(x86)\Advantage 10.10 and C:\Program files(x86)\Kantech folders.
  - the HKEY_LOCAL_MACHINE\SOFTWARE\Kantech and HKEY_LOCAL_ MACHINE\SOFTWARE\Advantage Data Architect registry entries.

1 - Before you begin the installation, make sure that no EntraPass application is running.

2 - Insert the software CD-ROM into the CD-ROM drive (or the USB flash drive in a USB port). 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.

3 - Before you go any further, you will be prompted to **Choose setup language** . English is selected by default.

NOTE: The setup (InstallShield) language cannot be changed later on if you need to perform an EntraPass update or install system components with a different language. If you must change the setup language, you have to remove and re-install the software.

NOTE: The system and database language depends on the language you select when installing the software. For example, if you select "English", it will be the system default language at start up. The system and database language can be changed from the EntraPass Server and EntraPass Workstation.

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

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

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

6 - Select the operation (s) you wish to perform. The first set of options are for new installs and the last option is for updates. During the first installation, you will only be able to select one of the install options. We suggest that you install the first option in the list.

- **Install Server, Database and Workstation :** This option will install the EntraPass Corporate Edition system. It will be greyed out if the application is already installed on the machine.
- **Install Additional Workstation** : This option is selected when you are installing an additional workstation. It will be greyed out if a server or a workstation is already installed on the machine.
- **Install EntraPass System Components** : This option allows installing EntraPass optional or additional system components such as Gateways, , WebStations, SmartLink, Video Vault, Oracle/MS-SQL Interface and Mirror Database and Redundant Server, etc. *The option will be greyed out if the component has already been installed on the computer.*

NOTE: *The redundant gateway is installed using the Gateway option. The serial used for registration will distinguish it as a redundant gateway.*

- **Install EntraPass System Tools :** This option allows installing EntraPass System Utilities (Vocabulary Editor, Report Viewer, Video Viewer, etc.). An option is greyed out if the utility has already been installed on the machine.

- **Update Installed Applications**: This option will be greyed out if the system has not been installed previously. To update your EntraPass system, see Updating EntraPass.

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

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

9 - Click **Next** . The system displays the software End-User License Agreement.

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

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

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

12 - Enter the User Name and the Company Name.

13 - Select the user type: Anyone who will use this computer or **Only** the person currently logged in and registered in the system.

14 - Click Next. The **Choose Destination Location** window will be displayed.

15 - You can keep the selected directory and click **Next** , or select another one.

- If you want to change the directory where to install the application, click **Change** . The **Choose Folder** dialog will pop up where you can select the new installation directory.

- Type in the destination directory where you want to install EntraPass or double-click the directory structure all the way down to the destination directory. Then, click **Ok** . The path will be indicated in the **Choose Destination Location** window.

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

17 - If you need to review the parameters you've setup, click Back. If everything is ready for the installation, click Next. The installation will begin.

18 - During the installation process, you will be prompted to Select the primary and secondary languages. This will define the language used to build the database and the languages used to run EntraPass.

19 - Click OK. The installation will continue.

20 - During the installation process, you will be prompted to **in** stall the Intellex API:

- If the Intellex API is required, click **Yes** and follow the instructions.

21 - You can also select to install the applications as Windows services. Applications that run as Windows services will automatically restart after a system shut down even if accidental.

22 - You can select to restart your computer at this time or do it later.

23 - Remove the CD-ROM from the CD-ROM drive (or the USB flash drive).

24 - Click **Finish** to complete the installation.

NOTE: You must restart the computerafter the installation.

25 - Your next step will be to contact Kantech Technical Support desk to get your registration key number for additional systems components. Follow instructions in the next section of this manual.

System Registration

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.

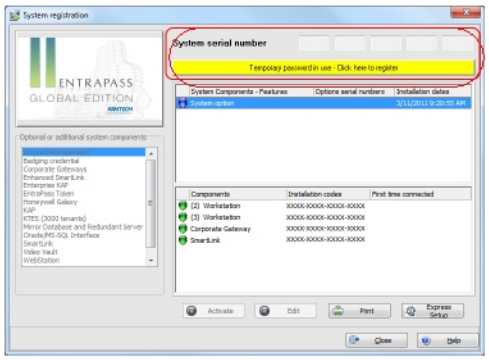
Registering the System

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

2 - Click Login / Logout button. The Operator Login window 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 window (the temporary password appears on new installations only and is highlighted in yellow). The System registration window appears.

NOTE: When you have registered the system, you must change all default passwords and usernames.



4 - Click the Temporary password in use (...) yellow button to register the system. This button is visible on new installations only. The System Registration window appears.

*NOTE: There are two ways of registering a new system; register online at **www.kantech.com** or contact your local technical support to get the registration confirmation code.*

5 - Go to **www.kantech.com** and click on the **Member Center**.

NOTE: *If you are not a member yet, submit your request and your membership confirmation should be received by email within 1-2 business days.*

6 - C lick on **Kantech Registration** .

7 - Enter the **System Serial Number** and follow the instructions online.

8 - Return to the **EntraPass System Registration** screen and enter the **Registration Confirmation Code** , then click **OK** . The **OK** button is only enabled when the registration code is valid.

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

Adding System Components

Once the Server has been registered, you may install additional system components. These include EntraPass applications and other utilities such as the EntraPass Video Vault application. Before you install system components, make sure that the designated computer meets the minimum requirements. You do not need to call Kantech Technical Support to install the first two workstation applications and the first gateway application. These are part of the installation package.

1 - In the **Server** main window, click on the **Connection** toolbar (or Workstation application > **Options** toolbar), then click on **System Registration** . The System registration window appears.

NOTE: *The EntraPass server is supplied with three workstation applications and one Multi-site Gateway application. One workstation application 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-ROM and the Installation codes to install the two additional workstation applications. Make sure that the computer on which they will be 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 workstation or gateway applications. To avoid errors, do not copy the codes on a piece of paper.

NOTE: *When you install an advanced option (for example an additional gateway, you can configure its sites using the Express Setup program.*

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

4 - Enter the **Option Serial Number** (located on the Option Certificate).

*NOTE: There are two ways of registered a new component; register online at **www.kantech.com** or contact your local Kantech technical support to get the registration confirmation code.*

5 - Go to **www.kantech.com** and click on the **Member Center**.

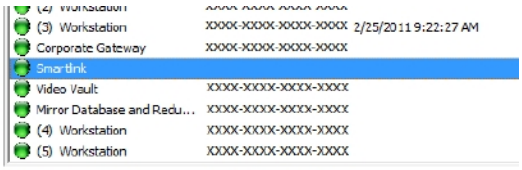
NOTE: If you are not a member yet, submit your request and your membership confirmation should be received by email within 1-2 business days.

6 - C lick on **Kantech Registration** .

7 - Enter the **System Serial Number** and follow the instructions online.

8 - Return to the **EntraPass Component Registration** screen and enter the **Registration Confirmation Code** , then click **OK** . The **OK** button is only enabled when both codes are valid.

*NOTE: After entering the Registration Confirmation Code, the system generates an **Installation Code** in the **System registration** screen. Blue flags identify components that have been created, but not yet activated. Green flags indicate components that have been activated. The installation code is required when you are ready to install the component with the EntraPass CD-ROM.*



9 - Repeat steps 3 to 8 for each system component.

NOTE: *You need to establish communication between the EntraPass Server and the computer where the new component/option is installed (if applicable). Perform this step only if you have installed the component/option on a computer other than where the EntraPass Workstation application has been installed.*

Adding System Components

Once the Server has been registered, you may install additional system components. These include EntraPass applications and other utilities such as the EntraPass Video Vault application. Before you install system components, make sure that the designated computer meets the minimum requirements. You do not need to call Kantech Technical Support to install the first two workstation applications and the first gateway application. These are part of the installation package..

1 - In the Server main window, click on the Connection toolbar (or Workstation application > Options toolbar), then click on System Registration. The System registration window appears.

NOTE: *The EntraPass server is supplied with three workstation applications and one Multi-site Gateway application. One workstation application 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-ROM and the Installation codes to install the two additional workstation applications. Make sure that the computer on which they will be 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 workstation or gateway applications. To avoid errors, do not copy the codes on a piece of paper.

NOTE: *When you install an advanced option (for example an additional gateway), you can configure its sites using the Express Setup program.*

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

4 - Enter the **Option Serial Number** (located on the Option Certificate).

*NOTE: There are two ways of registered a new component; register online at **www.kantech.com** or contact your local Kantech technical support to get the registration confirmation code.*

5 - Go to **www.kantech.com** and click on the Member Center.

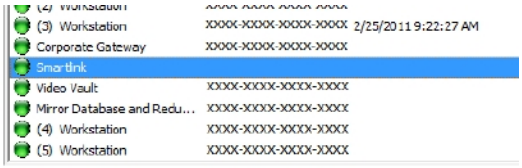
NOTE: If you are not a member yet, submit your request and your membership confirmation should be received by email within 1-2 business days.

6 - C lick on **Kantech Registration** .

7 - Enter the **System Serial Number** and follow the instructions online.

8 - Return to the **EntraPass Component Registration** screen and enter the **Registration Confirmation Code** , then click **OK** . The **OK** button is only enabled when both codes are valid.

*NOTE: After entering the Registration Confirmation Code, the system generates an **Installation Code** in the **System registration** screen. Blue flags identify components that have been created, but not yet activated. Green flags indicate components that have been activated. The installation code is required when you are ready to install the component with the EntraPass CD-ROM.*



9 - Repeat steps 3 to 8 for each system component.

NOTE: You need to establish communication between the EntraPass Server and the computer where the new component/option is installed (if applicable). Perform this step only if you have installed the component/option on a computer other than where the EntraPass Workstation application has been installed.

Windows Services

The Active directory component is automatically installed as a windows service when it is activated. Subsequently, you will see the following icons in the Windows system tray.

Icon	Status
	Service has not started
	Service has started but an error has occurred
	Service is running
	Synchronization is in progress

If you right click the Active directory icon, the following options are available on the menu:

- **Start:** to start the service.
- **Stop:** to stop the service.
- **Restart:** this will first stop the service then restart it.
- **Sync NOW:** requests that the AD changes are pushed to EntraPass immediately.
- **View LOG:** opens the folder where the log.txt file is located.

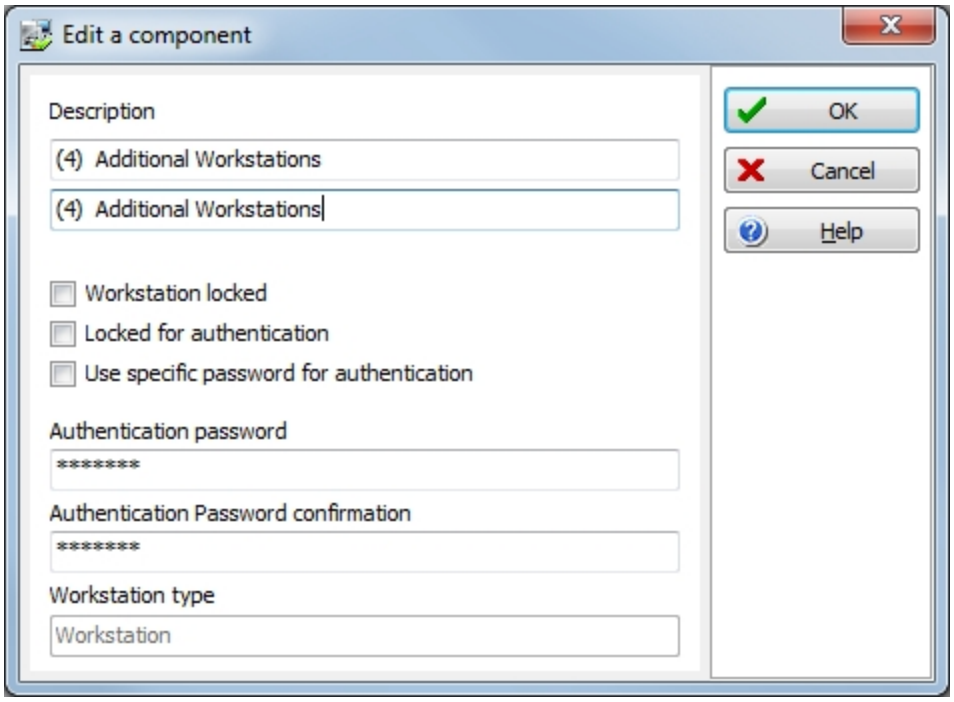
The About sub menu displays general information about the application such as the version installed, technical support contact details and copyright.

System Components Edition

EntraPass enable users to assign custom names to applications for easy identification in system events. You can also modify components names in their definition menu (**Devices** > **EntraPass Applications**).

Assigning a Descriptive Name to an Application

1 - From the Registration window, select an application, then click the Edit button. The Edit a component window appears.



2 - Enter a descriptive name for the selected EntraPass application in the **Description** fields. It is recommended to enter two names, one in the primary language and the second in the secondary language if EntraPass runs in two languages.

3 - Check one or more appropriate option(s):

- **Workstation locked** : check this option if this application will be installed on a computer and be used only for receiving system events.

- **Locked for authentication** : check this option if you want the computer where you have installed the EntraPass application not to send its authentication data to the server.

- **Use specific password for authentication** : check this option if you want to assign a specific password to this workstation. If you select this option, enter the password in the Authentication password field.

NOTE: *The Application type field displays the type of the selected EntraPass application. For instance, it will display "Multi-site Gateway" if the selected application is a Multi-site Gateway application. This identification is also displayed in the EntraPass application definition window (Devices > Defining an EntraPass application).*

Basic Functions

Following are the basic system operations:

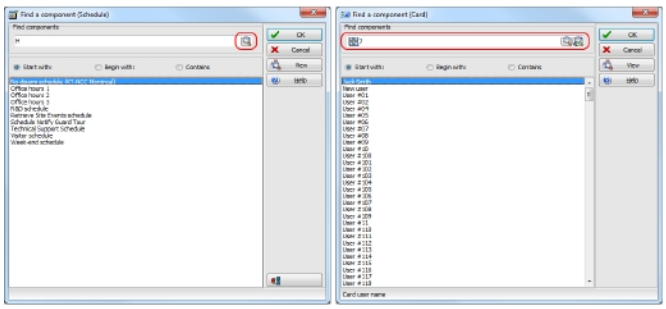
- Find components
- Use the extended selection box
- Select components, a specific folder, a connection or a gateway
- Print lists or reports
- View links between components
- Calling the system tree view

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.

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

1 - In both cases, you must click the binoculars button in the toolbar to open the Find component dialog.

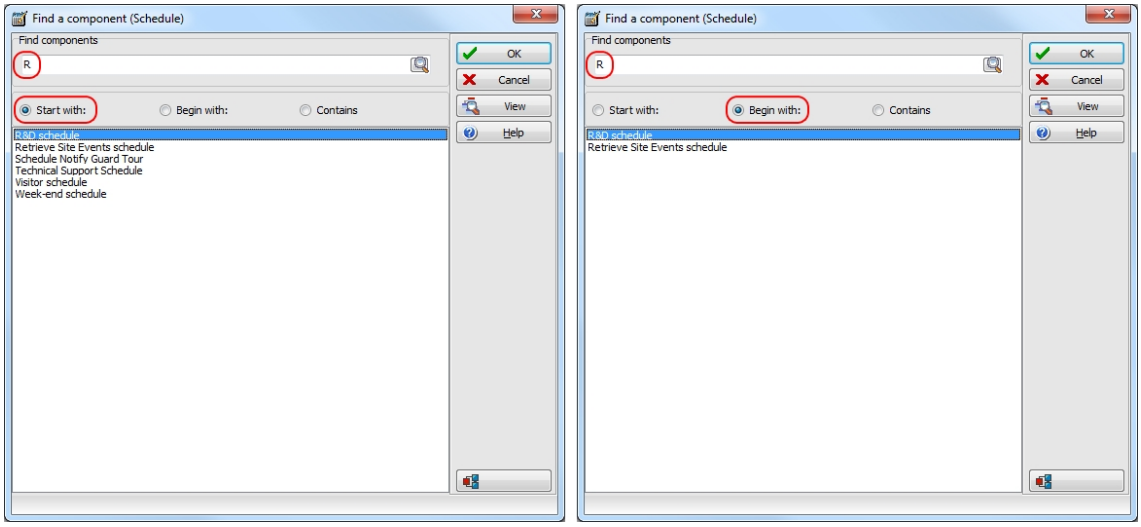


- The window on the left is used to find components and the window on the right is used to find cards.

Icons	Description
	Will search the database for components or cards.
	Will search the database for the picture that corresponds to the card you selected in the list.
	Will open a menu where you can select which card index you want to search on (card number, card-holder name, card information fields, etc.).

2 - To start a search, enter a keyword and click the binoculars on the right. To reduce the search results, check one of the boxes:

- **Start with:** Results will list all components that start with the one you have just entered, in alphabetical order, and will include the rest of the list of components available in the database.
- **Begins with:** Results will list only components with name that start with the text you specified.
- **Contains:** Results will list all components that contain the text you specify.



3 - If you want to view the picture that corresponds to the card selected in the list, click the binocular with a plus sign button.

4 - To cancel a search in progress, click the **Cancel** button.

5 - Click **OK** . The selected component in the list will be displayed in the dialog where you initiated the search.

Using the Extended Selection Box

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

- Available **Filters types** in the extended selection box are:
  - Contains
  - Starts with
  - Ends with
  - Exact words
  - Selected
- You can also enter specific words in the **Text filter** field to locate a specific item.
- You can choose to **Suppress the address** in the search results.
- You can also set the number of **Columns** for search result display.

Selecting Components

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

1 - From the active window, click the **Select Components** button. It opens a secondary window from which you may select appropriate options.

2 - You may need to check options that are displayed or use the **Select All** button (left) to select all the displayed options. You may also select **Single** to view components that are not grouped or select **Group** to view the existing groups.

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

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

5 - 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.

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

Selecting a Specific Folder

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

1 - From the active window, click the **Select** button (it is identified by "..."). It opens a secondary window from which you may select a specific folder.

2 - To change the destination folder, browse the Drives drop-down list (lower part of the window). You may click the **Refresh drive** list to make sure that the displayed list is up-to-date.

3 - Once you locate the folder you are searching, click **OK** to go back to the active window.

Selecting a Specific connection or Gateway

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

1 - From an active window, click the **New** button. The system displays the Select Gateway/ connection window.

2 - Double-click a connection /Gateway from the displayed list, then click **OK** .

3 - Assign a meaningful name to the component being defined.

4 - Follow the steps to complete the task.

Printing a List or a Report

Operators may need the Print function to:

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

1 - From any EntraPass window, click the **Print** button.

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 the **Print empty fields** and/or the **Print component reference** 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 Report Viewer**.

5 - If you want to modify the settings, close, modify and print your list.

6 - You can use the **Font** button to select a specific font and font size for your list.

7 - To select or modify a font selection:

- Select the font type from the Font menu. A preview of your selection will be displayed in the Sample box.

- Choose the formatting attribute from the **Font Style** menu (regular, italic, bold or bold italic).

- Enter the font size from the Size menu (10 or 11 is a default). The smaller the font, the more items appear on your list.

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

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

Displaying 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.

1 - From any menu window, select a component and click the **Link** button. All the components that are associated with the selected component are displayed.

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

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

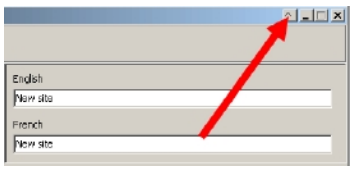
3 - To view the links of the selected door with other components of the system, select the door, then click the **Link** button again:

4 - All system components that are associated with the selected door appear. In this example, the "door" is used in the Administrator access level; users granted this access level are allowed access to the selected door.

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

Floating Windows

The floating window button can be used to move the window outside the workstation screen. This button is located at the left of the Minimize button for windows that support the floating window function.



It is not possible to go back when the window is floating. It should be closed and then reopened. No information on the window's position is kept by the system.

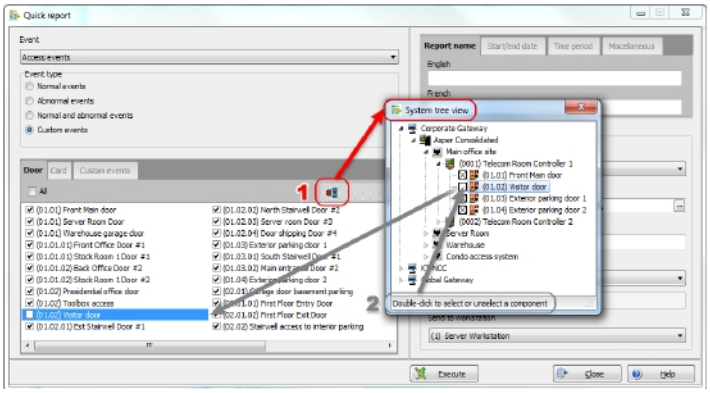
System Tree View

The **System Tree View** button displays the components list in a hierarchy format. The components displayed in this window can be selected or deselected. You can access the **System Tree View** in various ways:

Calling the System Tree View from a Dialog

When applicable, the **System Tree View** button is available like in the **Quick Report Request** dialog.

1 - From the **Reports toolbar > Quick Report Request** dialog. Click on the **System Tree View** button.

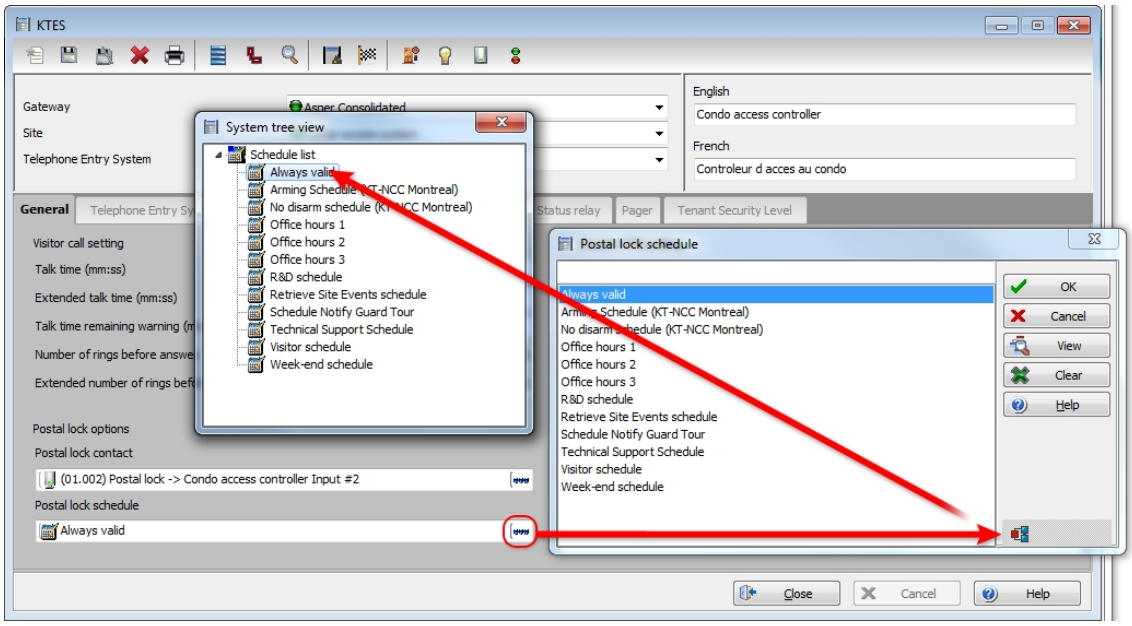


2 - From the **System Tree View** , you can double-click to select or deselect a component. The changes are automatically updated on the corresponding tab.

3 - Click back on the **System Tree View** button to close it.

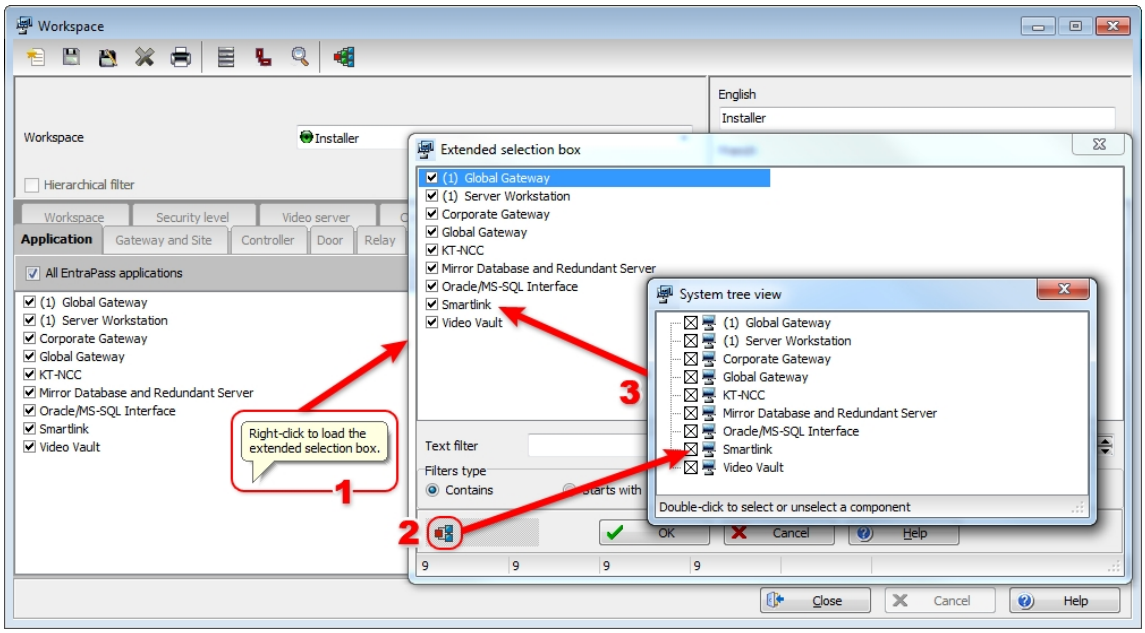
Using the Three-Dot Button

On a given data field, select the **three-dot (•••)** button:



Using the Extended Selection Box

1 - From the **System toolbar > Workspace > EntraPass Application** tab, right-click to load the **Extended Selection Box** :



2 - Click on the **System Tree View** button, you can double-click to select or deselect a component. The changes are automatically updated in the **Extended Selection Box** .

3 - Click back on the **System Tree View** button to close it.

Using the Comment Field as Notepad

The **Comment** field, that you can find in the **Card** and the **Devices** menu windows, can be edited directly but also as a Notepad window.

For example, in the **Card** window double-click anywhere in the blank as shown above. Edit the text in the Notepad window and close it. The text is then displayed in the **Comment** field. Click the **Save** button.

Delete details

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.

When the **Delete details** window is displayed, you will see the number of:

- Deleted components.
- Component links deleted.
- Child component links deleted.

You will also have the **Estimated server processing time** for the deleting operation.

Displaying 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.

1 - From any menu window, select a component and click the **Link** button. All the components that are associated with the selected component are displayed.

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

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

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

4 - All system components that are associated with the selected door appear. In this example, the "door" is used in the Administrator access level; users granted this access level are allowed access to the selected door.

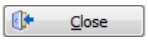
5 - Click the **Print** button to print the information displayed on the screen.

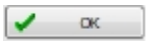
EntraPass Toolbars

EntraPass dialogs display most of the following buttons. They are an easy way to access the system functions. Generally, a "hint" is displayed when you move the cursor over an button.

You may access the toolbar from any EntraPass dialog window. Icons vary according to the window that is open. Most of the buttons are similar to buttons you are familiar with and that are used in the computer industry.

Icon	Description
	The **New** button is used to insert new information in the system database. This may be adding a connection, 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.

Icon	Description
	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, etc.
	The **Parent** button allows operators to display their search in a hierarchy or to divide searches by gateways, connection 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 **Displaying Components Links**.
	The **Find** button allows operators to find a specific item or component in the system database by using a specific character string. .
	The **Express Setup** button allows installers and system administrators to configure system devices by assigning default settings.
	The **System Tree View** button displays the components list in a hierarchy format. The components displayed in this window can be selected or deselected.
	The **Close** button is used to close a menu or a sub-menu. If you forget to save your information before closing a menu, the system displays a window prompting you to confirm the “save” operation before closing the menu.
	The **Cancel** button is used to cancel all modifications that were made since the last time a valid save was performed. The system will prompt you to confirm the operation.
	Use the **Help** button to view the help content on a specific subject.

Icon	Description
	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 deselect all the items or components that were previously selected in a list of choices.
	In several system windows, operators have access to graphic and animation buttons. These buttons are particularly useful when you want to display the status of a component before performing an operation on that component. 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** button: 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.
	The **Audit trail** button: click to open the **Audit trail** window, and view who made changes, and when the changes occurred on a component or a card. This feature is available in any menu where you can edit a card or a component. For more information see,**Card audit trail**.
Right-click	**Right-click** allows operators to enable a shortcut menu from which they can choose a specific command depending on the active menu.

NOTE: Note: toolbar icons for features which are not activated are automatically hidden from view.

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

NOTE: *You may launch Express Setup from Windows® menu:* ***Start*** *>* ***All Programs*** *>* ***EntraPass Corporate Edition*** *>* ***Server*** *>* ***Express Setup*** *or by clicking the* ***Express Setup*** *button from a number of EntraPass workstations' windows.*

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 from a system message box or from a controller definition menu.

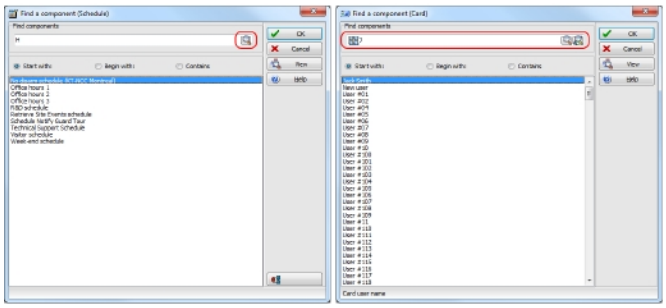
NOTE: *You have to log in to the server when you launch Express Setup. In fact, as the program allows you to modify the system devices configuration, it is essential to authenticate yourself before proceeding with any modification.*

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.

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

1 - In both cases, you must click the binoculars button in the toolbar to open the Find component dialog.



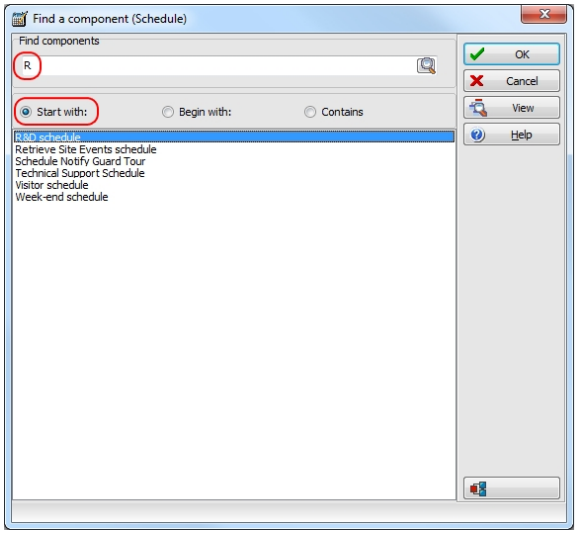
- The window on the left is used to find components and the window on the right is used to find cards.

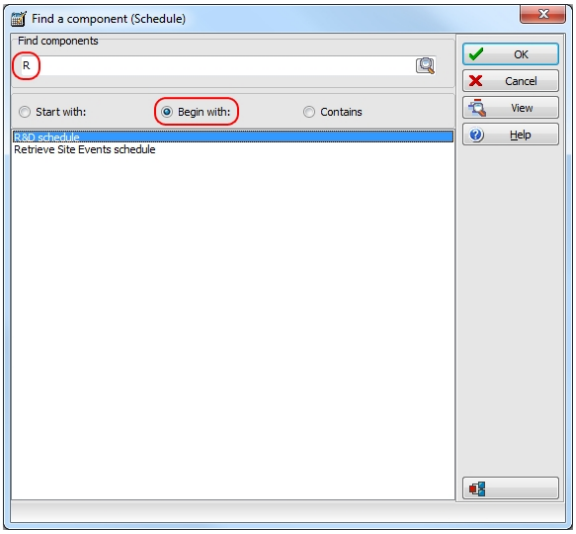
Icons	Description
	Will search the database for components or cards.
	Will search the database for the picture that corresponds to the card you selected in the list.
	Will open a menu where you can select which card index you want to search on (card number, card-holder name, card information fields, etc.).

2 - Title

3 - To start a search, enter a keyword and click the binoculars on the right. To reduce the search results, check one of the boxes:

- **Start with:** Results will list all components that start with the one you have just entered, in alphabetical order, and will include the rest of the list of components available in the database.
- **Begins with:** Results will list only components with name that start with the text you specified.
- **Contains:** Results will list all components that contain the text you specify.





4 - If you want to view the picture that corresponds to the card selected in the list, click the binocular with a plus sign button.

5 - To cancel a search in progress, click the **Cancel** button.

6 - Click **OK** . The selected component in the list will be displayed in the dialog where you initiated the search.

Session Start and End

1 - From the Windows® Start menu, click Start > **All Programs** > **EntraPass Corporate Edition** > **Server** / **Workstation**, 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 button on your desktop.

2 - From the Windows® Start menu, click Start > **All Programs** > **EntraPass Global Edition** > **Server** / **Workstation**, 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 button on your desktop.

3 - On start up, the application attempts communication with the Server. The display language depends on the settings of the operator who was previously logged on the EntraPass. English is the software default language.

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

Starting the EntraPass Server

The EntraPass Server is used for:

- Displaying all the applications connected to the server, the system event and system error logs
- Registering new connections (workstation applications, gateway applications, client applications such as SmartLink, Video Vault, Report Viewer, etc.)
- Performing backups (Data, Archives, In/Out databases)
- Restoring data (data, archive, In/Out databases)

- Verifying database integrity
- Changing the database language

1 - Start the Server (from Windows® **Start** menu or from the desktop).

2 - The server start up window displays a progress bar as well as the information related to the server start up process. When the process is completed, the login screen will display on screen.

3 - Click the **Login/Logout** button to open the Operator login screen.

4 - From the EntraPass Operator login, enter your **User name** and **Password** . The default User name is kantech. It is not case sensitive. The default Password is kantech, in lower case; it is case sensitive.

NOTE: To allow an operator to log in to the server, the System Administrator must select the option "Allow login on server", during the "Operator security level" definition (System > Security Level). For more information, see ***Security Level Definition***.

NOTE: The system keeps the last five user names, allowing operators to select their user name from the drop-down list.To delete a user name from the list, simply select it, then press Delete on the keyboard. By default, the Display Login List parameter is disabled. You must enable it in the EntraPass Application dialog.

5 - Once you have entered the correct login information, the EntraPass Server main window appears with the toolbars activated. Select the desired toolbar to perform an operation or to display system information.

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

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

- 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 it is purple, this indicates that the database is locked because a backup is being restored or the Mirror database is copying data.

- 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.

- A green rectangle indicates that the database is available.

Starting the Gateway Program

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

1 - Start the gateway (from Windows® **Start** menu or from the desktop). You do not need to enter a password or a user name. The EntraPass Corporate Edition main window appears.

2 - Start the gateway (from Windows® **Start** menu or from the desktop). You do not need to enter a password or a user name. The EntraPass Global Edition main window appears.

3 - You may right click anywhere in the Gateway window to display a submenu:

- **Minimize** minimizes the Gateway window

- **Send to tray** sends the window to the status (tray) bar

4 - Pay attention to the progress bars; they 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.

5 - You may select the **System** menu item to log in, to log out, or to perform a gateway **reload** .

6 - 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 window.

NOTE: The status flags show the communication status. The first status flag indicates the status of the communication with the server. If 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 system date and time, the number of gateways and the server IP address appear also on the status bar.

NOTE: The progress bars are not status bars. You do not need to wait until they fill up.

Starting the EntraPass Workstation

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

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

On start up, the workstation application attempts communication with the Server. The display language depends on the settings of the operator who was previously logged on the system. English is the software default language.

NOTE: Start the EntraPass server first. If you start an application before starting the server, you are prompted to register your application to the server even when the application has already been registered. If the application has been registered, you just start the server.

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

2 - The EntraPass Workstation main window will display on screen.

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

3 - Click the **Login** / **logout** button on the toolbar to access the Operator login dialog.

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

NOTE: If you cannot login properly, check if the Caps Lock key on your keyboard is activated. When proper login data have been entered, the system menu, toolbar and status bar are enabled. Also, the server must be running if you want to be able to log in the system.

NOTE: By default, operators are not allowed to log in on more than one EntraPass workstation at a time. If required, an operator can have concurrent logins, see ***Creating or Editing an Operator****. However, an operator may login on the EntraPass Server and EntraPass workstation at the same time.*

Accessing Information on the Server Workstation Connection Status

1 - Click any tab to access the system toolbar or select a menu item to access the system menu. In the lower part of the window, colour-coded flags indicate the communication status: Green, communication is OK; Red: communication problems; Blue: a report is pending.

2 - Move the cursor over the coloured rectangles to show details about the network status, the network database status and the workstation application report status.

3 - Move the cursor over the displayed numeric values to show details. It will indicate, in order, the system date and time, the operator's name, items in the Alarms desktop, alarms to be acknowledged, etc.

4 - Double-click (or single click, depending on your system settings) any number in the status bar to display the Status information window.

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

Modifying your Work Area Properties

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

2 - To modify the size of the toolbar buttons, select one of the following:

- **Small buttons** : small buttons are displayed below menu items
- **Large buttons with images** : components buttons are displayed on large buttons
- **Large buttons without images** : no buttons are displayed

3 - In the Miscellaneous section, make the appropriate choice:

- **Display menu** : only the menu bar appears. No buttons are displayed. Right-click the work area to modify the properties.
- **Display toolbar** : the menu bar and the toolbar are displayed.

4 - Select a background colour for the work space.

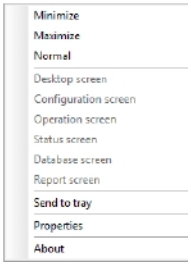
Retrieving Hidden Windows on the Desktop

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

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

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

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



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

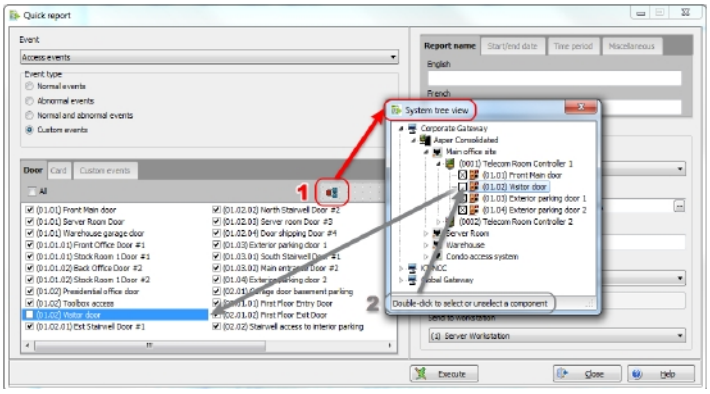
System Tree View

The **System Tree View** button displays the components list in a hierarchy format. The components displayed in this window can be selected or deselected. You can access the **System Tree View** in various ways:

Calling the System Tree View from a Dialog

When applicable, the **System Tree View** button is available like in the **Quick Report Request** dialog.

1 - From the **Reports toolbar > Quick Report Request** dialog. Click on the **System Tree View** button.

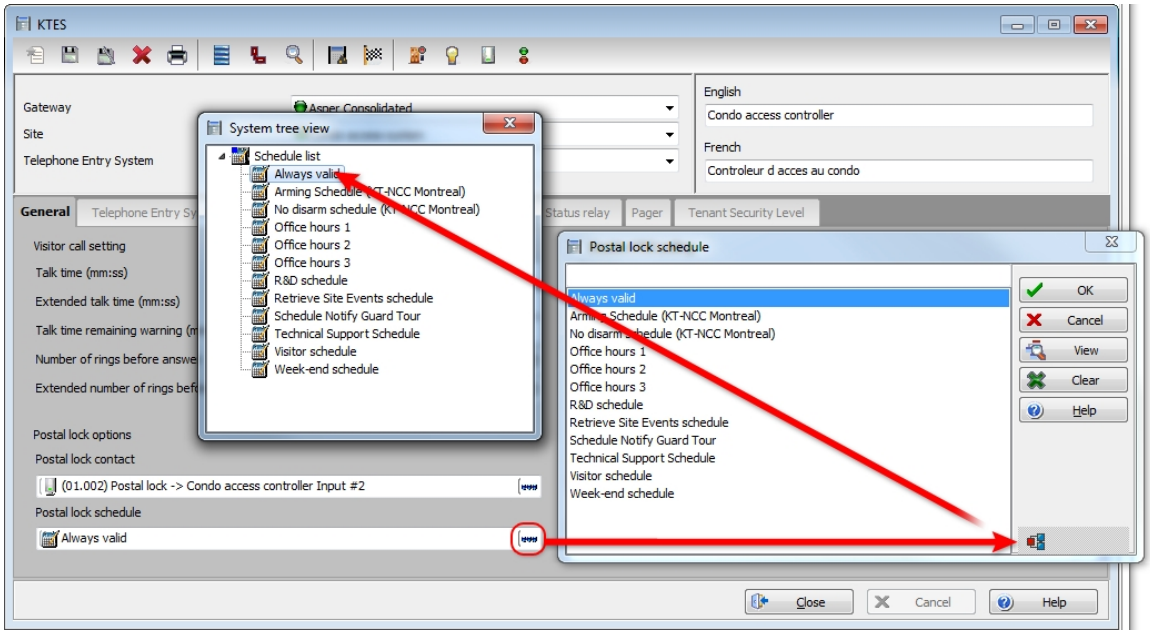


2 - From the **System Tree View** , you can double-click to select or deselect a component. The changes are automatically updated on the corresponding tab.

3 - Click back on the **System Tree View** button to close it.

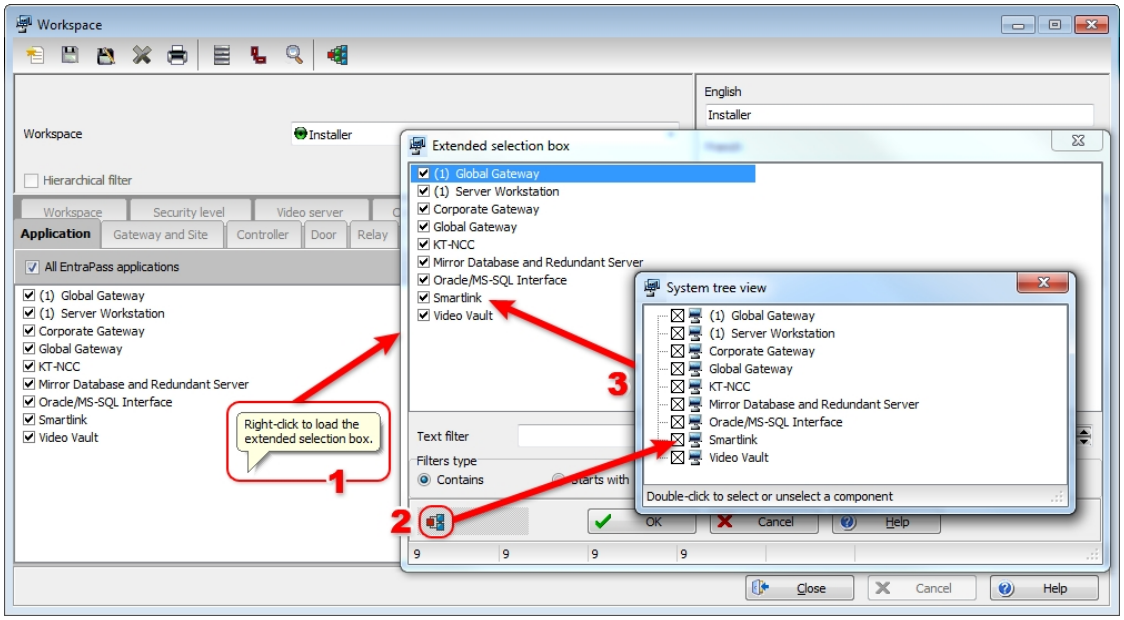
Using the Three-Dot Button

On a given data field, select the **three-dot (•••)** button:



Using the Extended Selection Box

1 - From the **System toolbar > Workspace > EntraPass Application** tab, right-click to load the **Extended Selection Box** :

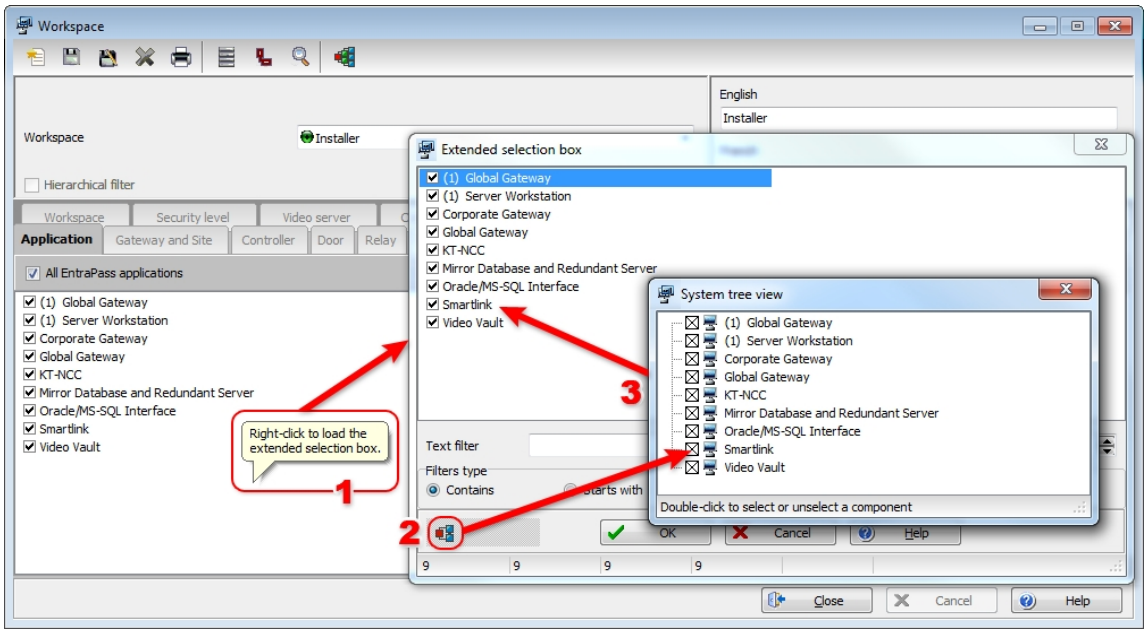


2 - Click on the **System Tree View** button, you can double-click to select or deselect a component. The changes are automatically updated in the **Extended Selection Box** .

3 - Click back on the **System Tree View** button to close it.

Using the Extended Selection Box

1 - From the **System toolbar > Workspace > EntraPass Application** tab, right-click to load the **Extended Selection Box** :



2 - Click on the **System Tree View** button, you can double-click to select or deselect a component. The changes are automatically updated in the **Extended Selection Box** .

3 - Click back on the **System Tree View** button to close it.

Alarms Desktop

The Alarms desktop is used to view and to acknowledge alarm events. Alarm events are defined in the Trigger and Alarm menu **(Definition > Trigger and Alarm)**. Any event can be defined as an alarm event. Alarm events require operator acknowledgement and are displayed in the Alarms desktop. A schedule must be defined for all alarms (**Definition > Trigger and Alarm, Alarm notification**). 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 or video clip. New events are added at the bottom of the Alarm desktop unless you have setup the list to display in descending order (in the Alarm Desktop Properties dialog).

Defining an Alarms Desktop

1 - From the **Desktop** main window, select the desktop in which you want to display alarm messages, then define the window type. Floating or Desktop.

2 - Specify the secondary windows that will be associated with the **Alarms** desktop:

- **Display on new alarm:** When you select this check box, the following actions can occur:
  - The **Alarms** desktop opens automatically when an alarm occurs.
  - An area alarm window opens automatically, when a muster report alarm occurs and you select Area Screen.

- **Message screen:** This window allows operators to view and acknowledge alarms that have an "acknowledgement schedule" selected in the **Trigger and Alarm definition** menu (**Definition** > **Trigger and Alarm** > **Alarm notification**) or to display the auto-acknowledge button configured in the **Operator** dialog (**System** > **Operator** > **Privileges**).

- **Instructions screen:** This window displays the instruction that is linked to the event to be acknowledged (i.e. call the police, send a message to a client application, etc.). Instructions are defined in the **System** > **Instructions** . Then after, they may be associated with events.

- **Graphic screen**: This window will display the location of the alarm being reported (if graphics are defined in the system). For more information on assigning graphic, see **Graphics Definition**.
- **Area Screen:** Select this check box to populate an area alarm window when a muster report alarm occurs. All the cards in the area of the muster report populate the alarm card list.

NOTE: An Alarm desktop may be defined as a Message window, a graphic window and an Instruction window. These features may apply to a single desktop. When you select a desktop defined with these three features, three windows are displayed simultaneously. For a better display, you may need to re-size and to position the windows.

Viewing System Alarm Messages

1 - Select the **Alarm** desktop. Alarm events are displayed according to the criteria selected in the **Sorted by** field.

NOTE: Alarm messages are archived and can be retrieved at all times.

2 - You can double-click the log area (middle of the window) to add a comment. The **Add a comment** window opens and enables you to enter text data. Once you have finished and clicked the OK button to close the window, the alarm event will be preceded by a + sign, indicating that an annotation has been added to the alarm event.

NOTE: Acknowledgements and flags will not be identified by a " + " sign.

3 - You may change/define the sorting order (**Sorted by** drop-down list):

- **Trigger destination** : Alarms are sorted by their order of arrival. This the default sequence. The window scrolls to the end each time a new alarm is displayed.
- **State** : Alarms are sorted according to their status (acknowledged, to be acknowledged or flagged). When you use this option, you interrupt the normal scrolling of events. Select "sequence" to go back to the default display.
- **Date and time** : Alarms are sorted according to the date and time of their arrival.
- **Event** : The **Event messages** column is sorted in alphabetical order, grouping identical events. For example, all **Input in alarm events** are grouped.
- **Priority** : Events are sorted by priority (as defined in **Options** > **Event color and Priority**).

4 - You may right-click anywhere in the window to enable the **Properties** window from which you can enable alarm status buttons:

- **Red** : To be acknowledged or suspended. If suspended, the suspension delay is displayed. When the delay expires, the operator is required to acknowledge again. If the delay is not expired but the operator wishes to acknowledge a suspended alarm, he/she has to click on the delay. The delay will be reset to zero.

- **Green** : Acknowledged.

- **Yellow** : Flagged.

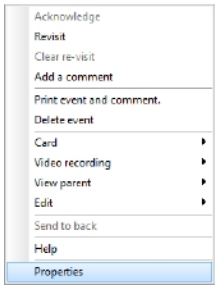
- **Black** : Deleted. To view alarms that have been manually deleted, select the **View deleted logs** from the **Properties** .

- **Blue** : Manual log.

5 - Select the Manual / Automatic buttons to toggle the acknowledgement method (automatic or manual). Only operators who are assigned this feature in the **Operator Definition** menu can use this option. For more information, see **Operators Definition**.

NOTE: The Manual / Automatic acknowledgement option is only available through the Alarms Desktop. When the operator logs out, it will return to "manual" by default.

6 - Right click an alarm message to perform additional tasks on alarm events:



- **Acknowledge** : When selected, a green point is inserted beside an alarm event to indicate that the event was acknowledged.

- **Re-visit** : When selected, the system flags the selected event. A yellow indicator is inserted beside flagged events.

- **Clear re-visit** : Remove the flag for the selected event.

- **Add comment** : Allows operators to enter comments concerning the selected event. The added comments are displayed in the bottom part of the alarm window. A blue + sign beside an alarm event indicates that a comment was added to the alarm event (visible when buttons are enabled: right-click an alarm event > **Properties** > **Show buttons**).

- **Print event and comment** : When selected, the system prints the alarm event and the associated comment.

- **Delete event** : When selected, the selected alarm event is marked for deletion (the indicator becomes "black" to indicate that the event has been marked for deletion). To view the events marked for deletion, before you actually purge them, right click anywhere in the window and select **Properties** then select **View deleted logs** .

Displaying Alarm Desktops Automatically

EntraPass enables users to display graphics automatically - from any desktop - as soon as an alarm occurs. This feature enables operators on duty to automatically view new alarms without having to open the alarm desktop and secondary windows associated with it. If **Display on new alarm** is checked the alarm desktop (and its secondary windows) will be displayed as soon as an alarm occurs regardless of the active window.

1 - **Define a desktop and customize it as an alarm desktop**: For this, you have to check the items of the **Alarms** desktop section.

2 - Check the **Display on new alarm** option so that operators can automatically view new alarms without having to open the alarm desktop and secondary windows associated with it.

*NOTE: If this option is selected when defining a **Filtered message** desktop for instance and if the desktop button is selected, the filtered message desktop will be displayed (the background colour of its button turns blue), but the windows below the **Display on new alarm** section will not be displayed; they are only displayed when a new alarm occurs. If those windows are displayed (on new alarm), clicking the "X" in the top right hand corner of one of them will close all the open windows. If **Display on new alarm** is not checked, the alarm desktop and all its secondary windows will be displayed on call (that is, when the alarm desktop is selected).*

3 - Click OK and Go for your configuration to take effect immediately.

NOTE: *When you define a desktop as an alarm desktop to be displayed on new alarm, it is recommended to reopen the* ***Automatic Alarm Display*** *desktop, to position its windows the way you want them to appear, then to click OK and GO again. This way, it will appear exactly as you have defined it.*

Acknowledging Alarms/Events

Usually, operators have to acknowledge receipt of an alarm condition (event—such as intrusion, input in alarm, etc.) by responding in ways such as clicking the acknowledgement button. In EntraPass, operators acknowledge alarm messages from an alarm warning box or from the **Alarms desktop** window.

NOTE: *When an alarm message is acknowledged by an operator, the notification is acknowledged or removed at all workstations.*

NOTE: *A sound can be added to alarm events. For more details about setting options for an alarm sound, see* ***Multimedia Devices Configuration****.*

Acknowledgement options are setup in the EntraPass application definition (**Devices** > **EntraPass application** > **Alarm** tab, Acknowledgement parameters). Events that require operator acknowledgement are defined in the**Options** > **Event color and priority**.

NOTE: *If the component that is in alarm is assigned to a video view, the video view or video recording is automatically displayed when an alarm occurs.*

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: *In order for the Manual button to display on the* ***Alarm Desktop*** *window, it is important to close the EntraPass session and reopen it after you have selected the Auto acknowledge option.*

*NOTE: Only operators granted the appropriate access privilege should be using this option. If the **Automatic acknowledge** feature is used, the alarm message box is not displayed; therefore, it will not be possible to suspend alarms. If this option is enabled in the Operator definition menu, the Manual button is added to the Alarms desktop. This button toggles between **Manual** and **Automatic** acknowledgement.*

To Acknowledge an Alarm Message

1 - When the **Acknowledgement required** message box appears, take one of the following actions:

- Click the **Acknowledge** button to acknowledge the displayed alarm event. The red status button turns green once an alarm is acknowledged.
- Click the **Suspend** button to suspend alarms while doing other operations in the system. The alarm will be suspended for the delay time specified in the **EntraPass application** definition menu. Once the suspended alarm delay time expires, the system prompts the operator to acknowledge the alarm.
- Click the **Re-visit** button if you want to acknowledge an alarm message, and if you want to identify it for future reference. A flagged alarm is identified by a yellow button.
- Click the **Mute** button (speaker button) if you want to stop the alarm sound.

*NOTE: The **Acknowledgement required** message box will be presented in a format without the Instructions window if there are no instructions associated with the alarm message.*

NOTE: If the component that is in alarm is assigned to a video view, the video view or video recording is automatically displayed when an alarm occurs.

To Acknowledge Alarms from the Alarms Desktop

Each workstation has its own alarm desktop which displays alarm events received from the server. When a workstation starts up, alarms displayed on the desktop will have a “to be updated” status (a blue button in the second column). Once communication is established with the server, all events will be updated on the alarm desktop. The blue button will then be replaced by a red button (alarm), a yellow button (flag) or a green button (acknowledged).

NOTE: This process will occur each time a workstation have a communication failure with the server.

1 - Select the alarm event you want to acknowledge (one that has been flagged, for instance), right-click to enable a shortcut menu.

2 - Select **Acknowledge** from the sub-menu. The status indicator becomes green.

*NOTE: To tag an alarm message for specific purposes, select the alarm event you want to identify; right-click and select **Flag** from the sub-menu. You can also click an alarm message until the colour of its status indicator changes to the desired colour.*

Mandatory Alarm Comment

If an instruction with the **Mandatory alarm comment** checkbox selected in System / Instruction is assigned to an alarm, the operator will have to add a comment in order to mark the alarm as "acknowledged" (see **Instructions Definition** for more details).

NOTE: The alarm sound will stop while a comment is entered by the user.

If the alarm event has already been acknowledged, a warning message will be displayed for you to confirm that the comment should be added.

Changing Desktop Events

To change which events are displayed in the alarm message list, right-click on the alarm message list and select **Desktop Events**. Select the an event group to display the events from that group. For more information about event groups see **here**. Select none to block all messages.

Other options available in this menu are as follows:

- Select **Use message desktop selection** to display the same events defined for the selected desktop.
- Select **View Operator** to view the desktop event selection for the logged on operator read-only mode.
- Select **Edit Operator** to modify the desktop event selection for the logged on operator.
- Select **Assign Operator** to assign one or more desktop events to another operator.

NOTE: *Changes made to desktop events only affect new events. Existing events on the list will remain unchanged.*

Changing the Display Properties

1 - From the **Desktop** window, right-click anywhere in the window.

2 - Select **Properties** from the shortcut menu.

3 - From the **Properties** window that appears, select the display options: you may change the default size of buttons, the default background colour, etc.

- **Small buttons** : If this option is selected, small components' buttons are displayed with no descriptive text. This option can be appropriate for operators who are familiar with EntraPass buttons and do not need an additional description.
- **Large buttons with images** : Icons are displayed with their description.
- **Large buttons without images** : Large buttons are displayed with no description.
- **Display menu** : check this option to view the system menu.
- **Display toolbar** : check this option to view the toolbar for system menus.
- **Change system font** : click this button to change the font for all the user interface.

Custom Report Desktop

The **Custom Report** desktop allows operators to display events that come from pre-defined reports, view the report generation state and, when available, to play video recordings from the EntraPass Video Vault . Security levels will determine which custom reports are available to each operator. The **Custom Report message list** operates the same way as all message lists in EntraPass except that it has an extra combo box that allows operators to select a pre-defined custom report.

NOTE: *Custom reports are defined under* ***Report > Custom Report.***

*NOTE: Security levels for reports are defined under **System > Security Level >** under the **Report** tab.*

Configuring a Custom Reports Desktop

1 - From the **Desktop** main window, click the desktop button you want to configure as a **Custom Reports Desktop**.

2 - Assign a meaningful name to the Custom Reports Desktop, then define the desktop type (Message window, Picture window or both).

3 - Select the sort criteria you want to use to display historical data from the drop-down list (**Date and Time** , **Event** , or **Message Type**).

NOTE: The sequential sort option is not available for archived messages.

4 - You can enter a text string that will be used for searching specific archived messages (when applicable).

5 - In the combo-box, select the custom **report** you want to generate. The list of available reports corresponds to your security level.

6 - After selecting the report, a **Date and Time** window will pop up requesting a reporting date and time period.

7 - Enter **Start and End date and time** or click the calendar button to open the calendar and select the start and end dates, and then type in the start and end times.

8 - Check the **Clear Screen Before Process Request** box in order to clear the **Custom Report message list** of the previous search results.

9 - Click **OK** . The status indicator light located at the bottom left of the screen will change from green to blue to indicate a custom report is being generated. It will turn green again when the data transfer will be completed and the data will be displayed according to the criteria you have selected.

To Create and Edit Custom Reports from a Desktop

- When your security level allows you to create new reports, you can access the **Custom Report** dialog from the **New Report** command in the Custom Report Desktop pop up menu. For more information on Custom Reports, see **Custom Reports Definition**.

- When your security level allows you to edit existing reports, you can access the **Custom Report** dialog from the **Edit Report** command in the Custom Report Desktop pop up menu. For more information on Custom Reports, see **Custom Reports Definition**.

To Display Custom Report State in Real-time

This feature allows you to view the progress of report generation for a specific report in the **Custom Report Desktop List**.

1 - Right-click an entry in the **Custom Report Desktop** window. A contextual menu will pop up.

2 - Select **Report State** . The **Report State** dialog will open displaying report generation information.

3 - When the report is finally generated in the **Desktop** window, the information in the **Report State** dialog will disappear. Click **Close** .

Comment Entry and Display

Also, a comment can be added to any type of event. In the fifth column from the left, a '-' sign will indicate that a comment has been added by the system while a '+' sign will indicate a manually added comment. From the **Custom Report Desktop**, you can display the comments associated to each event.

To view associated comments, select the event and use a right-click to display the contextual menu, then select **View Comment**. A comment can also be added using **Add a New Comment**.

Playing archived video recordings from a Desktop Message list

1 - Select the video you would like to play and right-click to access the contextual menu.

2 - If the video has been stored into the EntraPass Video Vault, the **Play from Vault** option will be enabled. Once you click on it, the **Video Playback** window will open and start playing the selected recording.

Customizing Event Display in the Message Desktops

1 - From the displayed shortcut menu (**Message desktop** > Right-click a message), select **Properties** .

2 - From the **Properties** window, select the appropriate display options.

- **Multi-line:** Usually, events are displayed on a single line. You can increase the line spacing between events by checking the appropriate option (1, 2, 3 or 4 lines).

- **Show columns:** You can choose to display different types of buttons beside each event.

  - **Message type** : When you select this option, the system inserts an button next to events indicating the type of event. For example, if the event is a “door forced open” an button 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 buttons.

  - **Picture** : When you select this option, the system inserts a card button 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.

  - **Video** : Check this option if you want the selected desktop to display video data from the video server connected to your system.

  - **Display account**: On the bottom left, check **Display account**. The desktops window now displays the **Account** column with the corresponding event for each account.

- The **Miscellaneous** section allows you to enable additional options:

  - **Keep card picture** : When selected, the system keeps the latest card picture (if the Picture window option is selected) until another event containing a card occurs.

  - **Display toolbar** : Displays / hides the toolbar on the top of the **Message** desktop.

  - **Manual properties save only** : When you select this option, you have to click the **Save** button (once selected, the button is disabled). The system saves all the settings defined in the **Properties window** as well as the position of the window within the Messages Desktop.

- **Display selected messages (full)** : When you select this option, a smaller window is added at the bottom portion of the **Message window** . It displays the selected event with its full description. This feature is very useful when your **Message** window is too small to display the entire description of an event.

- **Display events in bold** : Select this option to increase the legibility of text event messages displayed in EntraPass desktops (Message list, Filtered messages and Alarm desktops). Moreover, if the colour selected for an event message is the same colour as the background colour, the event message will be displayed in black bold so that it can always stand out (this option is not available for **Archived Messages** list).

- **Last Message on Top :** By default, event messages are displayed in ascending order of occurrence, with the area at the bottom of the screen reserved for the highlighted event. You can select to display the events in descending order, with the highlighted event showing above the list of event messages.

- **Auto-scroll delay (mm:ss):** Will automatically start scrolling the message list after a pre-set delay when the operator selects an item in the list. By default, this option is turned on with a preset delay. You can select to turn this option off which means that the operator will have to click the **Restart Scroll** button in the **Messages** list (this option is not available for **Archived Messages** list) .

- **Message background colour :** Allows the operator to modify the background colour of the message window.

- **Display event colour in separate column** : Event colours can now be displayed in a separate column. Text and message background colours can also be selected.

*NOTE: To change the font colour of system messages:**Options > Event color and priority.***

Graphic Desktop

Use the graphic desktop to display the graphical location of an alarm occurrence, to enable this you must define the graphic in the system, see **Graphics Definition** for more information. A graphic corresponds to a secured area on the system where the following components are located on a connection: EntraPass application, controllers, inputs, and relays. With a graphic, operators can view the exact location of a component installed on a connection, or the status of components and devices. For example, area groups,

areas, doors, contacts, motion detectors, and controllers, assigned to the graphic. If you have defined muster reporting, and an emergency occurs, graphic icons indicate when all employees have vacated the area. Operators can perform manual operations directly from the displayed component, for example, to lock or unlock a door. To define interactive floor plans, see **Graphics Definition.**

Viewing Graphics in the Graphic Desktop

1 - Select the desktop button you want to assign to graphic, right-click for the shortcut menu, and name the desktop (Graphics, for example), then define the window type (**Floating** or **Desktop**).

2 - Click **OK and Go** to display the **Graphics** desktop.

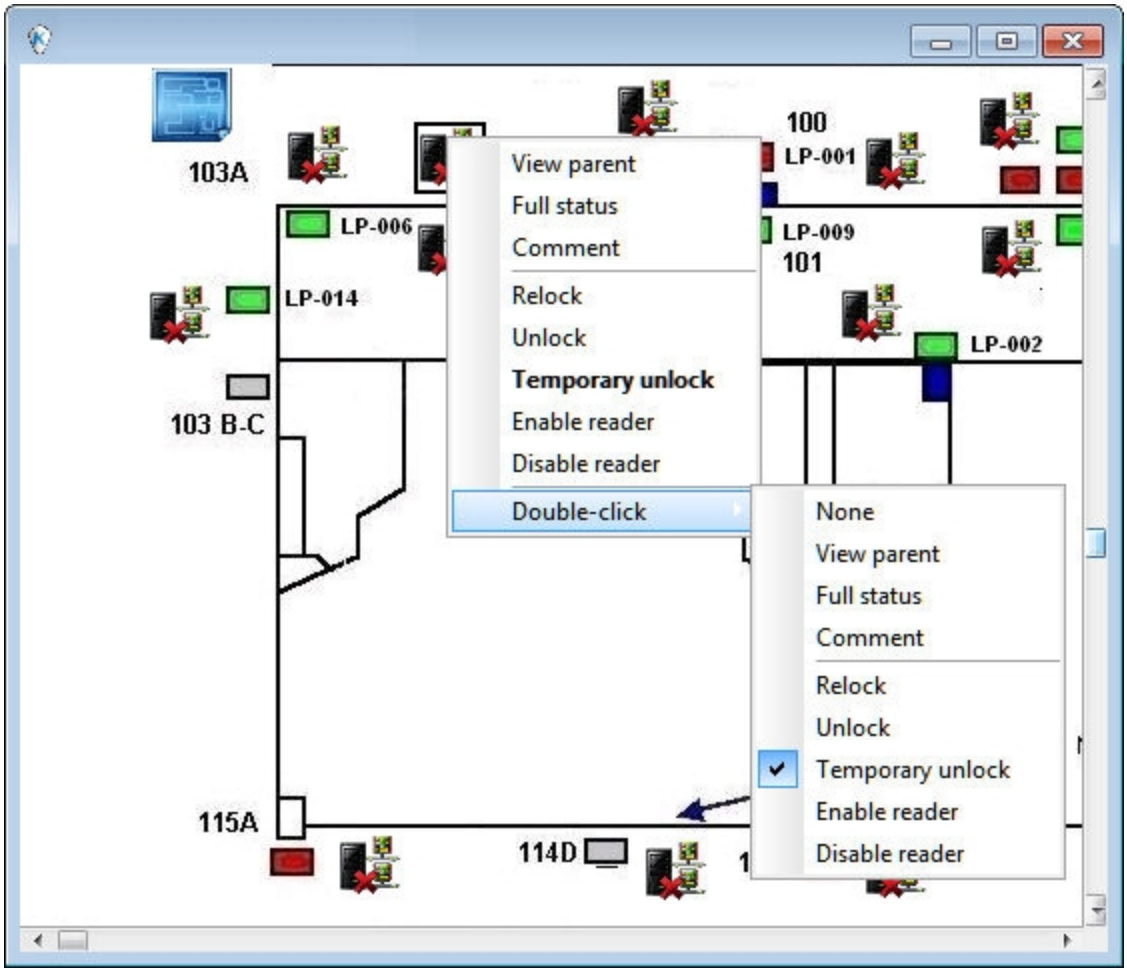
3 - Right- click anywhere in the **Graphic** desktop for the shortcut menu, select the graphic you want to display.

NOTE: If the window is smaller than the graphic size, you can click-hold-and-drag the graphic to move it around within the Graphic window.

4 - To use additional functions, right-click anywhere in the graphic for the shortcut menu:

- To adjust the display size of the selected graphic, click **Fit to screen, Design size or Picture size**. .
- For the system to display a message indicating the cause of the communication loss in case of communication failure, select **Auto result.** . If **Auto result** is not selected, operators have to manually request the results for the component by using **Show result** .

5 - Right-click a component in abnormal condition to enable a shortcut menu.



NOTE: Components in alarms are represented by their animated buttons. If you select an animated button and view its parent components you can 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 **Comment** to display comments already assigned to the device (please refer to see **Comment Field** for more information).

8 - Select the **Double click** menu item to allow operators to modify the status of a component in alarm from the Graphic desktop. For example, if the displayed component is a door, and if the Double click menu item was set to **Unlock** , an operator can manually open the door from the **Graphic** desktop.

*NOTE: When you modify the Double-click feature using the Graphic desktop, the system does not save the modifications. Modify the default **Double-click** feature using the graphic definition (Definition > Graphics, Design window, right click a component > Default double click menu item). For more information on how to create graphics and on how to assign components to graphics, see **Graphics Definition**.*

Message List Desktop

By default, the first desktop is defined as the **Messages List desktop**. It displays all system events. Events are displayed with their button, date and time, description, system components involved in the event such as controllers, cardholder pictures (if defined), etc. When a new event is displayed, the window scrolls up. The newest events are added at the bottom of the window.

Viewing and Sorting System Events

By default, the first desktop is dedicated to displaying system events. When you select an event from the list, you interrupt the incoming sequence (the green status indicator located at the bottom left part of the desktop turns red when scrolling is interrupted). By default, the scrolling will restart automatically after a pre-set period of time, unless the auto-scroll parameter was disabled, In that case, to restore the normal scrolling, click the **Restart Scroll** button.

NOTE: If you configure a desktop as a message screen and a picture screen, two windows are displayed simultaneously when you select the desktop.

1 - Select the first desktop. By default, all system events are displayed in ascending order with an area at the bottom of the screen that displays the selected event in the list.

*NOTE: You may change the message colour: System > Events parameters. You may also change the events display order; see **Customizing Event Display in the Message Desktops**.*

2 - From the **Message list** screen, you may change the sorting criterion by clicking on the **Sequence** drop-down list. You may choose to sort by:

- **Sequence** : Events are sorted according to the normal sequence (default). New events are added at the bottom of the window (This option is not available for **Archived Messages** list).

- **Date and time** : This sort order interrupts the normal scrolling of events. This feature is useful when you want to know when an event was generated. This time may be different from the "normal sequence" for dial-up sites for instance or after a power failure.

- **Event** : When selected, the system sorts the **Event message** column in alphabetical order, grouping identical events. For example, all **Input in alarm** events are grouped together in alphabetical order.

- **Message type** : When selected, the system sorts the **Event message** column in alphabetical order, grouping similar events. For example, all **Connections events** are grouped together in alphabetical order.

*NOTE: To go back to the default display, select **Sequence** from the **Sequence** drop-down list.*

3 - Clicking the **Text filter** button (top left of the **window**) will open the **Text filter** dialog that allows to enter a key word to display all the events that contain that keyword in the **Message** list. In order to avoid delays, select the **Suspend Refresh** checkbox. This way, the Desktop **Message List** will not use the **Text Filter** field while events are displayed live. To close the **Text filter** dialog box, click **Cancel** or the Windows closing button (X).

4 - To return to the normal display of events in the **Messages list** screen, click the **Text filter** button.

Customizing Event Display in the Message Desktops

1 - From the displayed shortcut menu (**Message desktop** > Right-click a message), select **Properties** .

2 - From the **Properties** window, select the appropriate display options.

- **Multi-line** : Usually, events are displayed on a single line. You can increase the line spacing between events by checking the appropriate option (1, 2, 3 or 4 lines).

- **Show buttons:** You can choose to display different types of buttons beside each event.

  - **Message type** : When you select this option, the system inserts an button next to events indicating the type of event. For example, if the event is a "door forced open" an button 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 buttons.

- **Picture** : When you select this option, the system inserts a card button 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.

- **Video** : Check this option if you want the selected desktop to display video data from the video server connected to your system.

- The **Miscellaneous** section allows you to enable additional options:

  - **Keep card picture** : When selected, the system keeps the latest card picture (if the **Picture** window option is selected) until another event containing a card occurs.

  - **Display toolbar** : Displays / hides the toolbar on the top of the **Message** desktop.

  - **Manual properties save only** : When you select this option, you have to click the **Save** button (once selected, the button is disabled). The system saves all the settings defined in the **Properties window** as well as the position of the window within the **Messages** desktop.

  - **Display selected messages (full)** : When you select this option, a smaller window is added at the bottom portion of the **Message window** . It displays the selected event with its full description. This feature is very useful when your **Message** window is too small to display the entire description of an event.

  - **Display events in bold** : Select this option to increase the legibility of text event messages displayed in EntraPass desktops (Message list, Filtered messages and Alarm desktops). Moreover, if the colour selected for an event message is the same colour as the background colour, the event message will be displayed in black bold so that it can always stand out (this option is not available for **Archived Messages** list).

  - **Last Message on Top:** By default, event messages are displayed in ascending order of occurrence, with the area at the bottom of the screen reserved for the highlighted event. You can select to display the events in descending order, with the highlighted event showing above the list of event messages.

  - **Auto-scroll delay (mm:ss):** Will automatically start scrolling the message list after a pre-set delay when the operator selects an item in the list. By default, this option is turned on with a preset delay.

You can select to turn this option off which means that the operator will have to click the **Restart Scroll** button in the **Messages** list (this option is not available for **Archived Messages** list).

- **Message background colour** : Allows the operator to modify the background colour of the message window.

*NOTE: To change the font colour of system messages: **Options > Event color and priority.***

Performing Tasks on System Messages

EntraPass enables you to perform various tasks on system events. These include:

- Deleting messages
- Viewing card information
- Validating card status and card transaction
- Modifying the desktop properties (such as display options), etc.
- Play, edit and export video recordings
- Play archived videos from the EntraPass Video Vault

*NOTE: Some tasks are related to the selected desktop. For example, if you right-click an alarm event, the shortcut menu displays tasks that are related to alarm events. For details, see **Alarms Desktop**.*

1 - From the **Message** desktop, right-click an event to enable a shortcut menu.

2 - Do one of the following:

- **New message filter**: This option displays the **Message filter** dialog to define new message filters (see **Message Filters Definition** for more information).
- **Edit message filter**: **This option displays the Message filter dialog to edit an existing message filter (**see **Message Filters Definition** **for more information).**
- **Delete all** : This option allows an operator to delete all the events displayed.

- **Card** : This menu items offers two choices: **View card transactions** and **Search card**. Select **View card transactions** to display all access information related to the cardholder who has triggered the access event. The **Search card** shortcut allows you to browse the card database and to display information about all the card numbers associated with this specific card user name from the **View card information** window. From this window, operators can perform a variety of tasks including viewing and validating information contained on a card, such as the card number, cardholder name, card state (valid or invalid), card type, etc. They can also select a card and view its transactions or view and validate a card access. For details about validating card holders' access and last transactions, see **Validating Card Access**.

Also, in order to reduce the quantity of data retrieved, a filter can be added to the user name or to the card information fields (1 to 10) when searching for a card. Enter a name for the filter and click the button on the left side of the field to display the contextual menu.

- **Video recording** : This menu items offers three options: **Play** , **Play/Edit/Export** and **Play from Vault** . Selecting **Play** allows users to play the video event in the **Playback** window, offering options to snap (copy) it and save it for future use. Selecting **Play/Edit/Export** offers users features similar to the ones in the **Video Event** list. Operators can then display details about the event (camera, server, comment field) and camera information, etc. The video event can also be played and exported. Selecting **Play from Vault** allows operators to view a video that is already stored in the EntraPass Video Vault.

*NOTE: If camera buttons are not displayed, simply right-click a video event message, select properties from the shortcut menu, and check Video in the **Show buttons** section of the **Properties**.*

- **View parent** : Displays the parent of each component related to the selected event.

- **Edit** : This feature offers you the ability to edit each component associated with the selected event. If **Edit** is selected, a shortcut menu displays components associated with the selected event. In this example, the connection definition modified event involves the EntraPass application, the operator who was on duty when the event was generated and the connection related to the event. It is now possible to edit any of the three components by selecting it from the shortcut menu. If the selected event is an access event and if the card that triggered the event has already been registered in the system, it will be possible to edit the card. However, if the card is associated with an **Access denied - card unknown** event, the card will be created and registered in the system.

- **Audit**, select one of the following options:
  - **Application**: select this to open the **Audit** window to view who made changes, and when the changes occurred on the component.

- **Operator**: select this to open an audit window to view the operator component that generated the message event. For example, any change under the function system for operator, name, security level, and workspace. In the absence of any modification to the selected component, the option is not available.
- **Card**: select this to open the **Audit** window to view who made changes, and when the changes occurred on the card.

- **Send to back** : This option only works when the window type is set to floating. It sends the active window behind the main application window. To bring back to front, right click the desktop button, then select **Bring to front** .

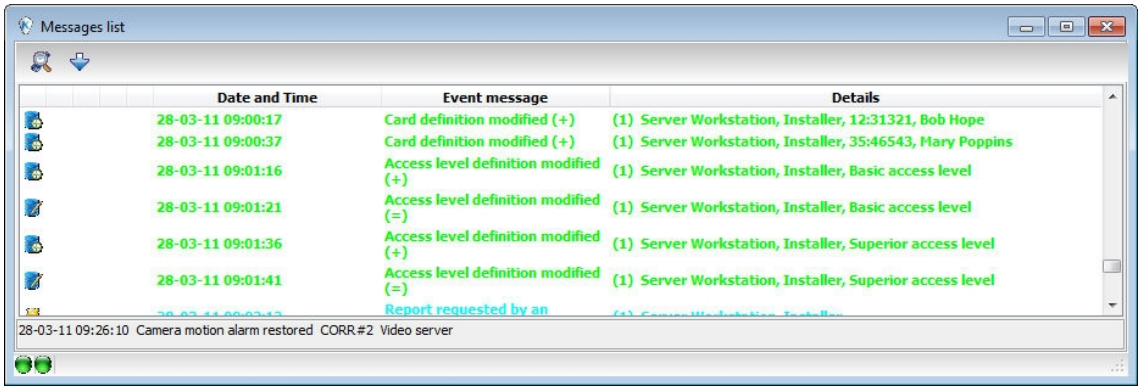
- **Help** : Displays the **EntraPass Online Help** .

- **Properties** : This menu item enables users to modify the display properties for the selected desktop.

Add, Modify or Delete Tagged Events

You can see, in the desktop message list, if a component was newly created, modified or deleted. Database events are precessed by the following signs:

- **+** (New)
- **=** (Modified)
- **-** (Deleted)



Changing Desktop Events

To change which events are displayed in the alarm message list, right-click on the message list and select **Desktop Events**. Select the an event group to display the events from that group. For more information about event groups see **here**. Select none to block all messages.

Other options available in this menu are as follows:

- Select **View Operator** to view the desktop event selection for the logged on operator in read-only mode.
- Select **Edit Operator** to modify the desktop event selection for the logged on operator.
- Select **Assign Operator** to assign one or more desktop events to another operator.

NOTE: Changes made to desktop events only affect new events. Existing events on the list will remain unchanged.

Picture Desktop

If you selected **Picture screen** when defining the **Message** desktop, it will be displayed with the Picture window. Access events are displayed with the card holder's picture if you have set the appropriate display option in the Message filter definition (System > Message filters). For details, see **Message Filters Definition**.

Modifying Pictures Display Options

1 - From the **Message list and Picture** , select an access event, then right-click the card holder's picture.

*NOTE: The **Send to back** option only works when the window type is set to floating. It sends the active window (Picture window) behind the Message desktop main window. To bring it back to front, right click the **Message** desktop button, then select **Bring to front** from the shortcut menu. From the shortcut menu, select **Properties.***

2 - From the Aspect drop-down list, select the display size for the picture:

- **Design size** : The card holder's picture will be displayed with its original size.
- **Stretch** : This option stretches the picture to the window size without maintaining proportions. The picture may appear distorted.
- **Stretch ratio** : This option stretches the picture to the window size while maintaining proportions.

3 - The **Display multiple pictures** option allows you to show up to four photos, depending on your needs. When selected, you can keep the default value " *Message* " or choose a specific door for each of the four photos.

4 - Check **Apply all the following items for all cells** to assign the parameters to all cells.

5 - Select the information you want to see displayed with the card holder's picture:

- **Door** : The door where the card was presented will be displayed above of the card holder's picture .
- **Event** : The event message will be displayed .
- **User information** : The **User information** field will be displayed above the picture.
- **Comment** : If this option is selected, a comment field appears below the card holder's picture. The comment entered when defining the card appears in this field.

*NOTE: If a door is associated to a cell (photo) and the **Door** option is selected (**Display selected fields**), the name of that door will be displayed in blue instead of the usual black colour.*

Specific Desktop Customizing

EntraPass enables operators with appropriate permission to customize their desktop. Moreover, operators with full access permissions can permit operators with read-only permission to customize their desktop. They can also customize a specific desktop and transfer this customized desktop to other operators using the **Assign desktop** feature. The following sections explain how to customize a desktop:

- Customizing a desktop by a full access operator
- Customizing a desktop for a read-only operator
- Transferring a customized desktop

Customizing a Desktop for a "Full Access" Operator

Operators with full access permission have the ability to customize their desktops. To grant full access to an operator (**System > Security Level**):

1 - Select the desktop you want to customize, right-click and select **Properties** in the menu to open the **Desktop** properties dialog.

2 - From the **Desktop name** field, assign a meaningful name to the desktop you are configuring.

3 - Select the window type:

- **Floating window** : A floating window can be re-sized and positioned anywhere in the work area screen. For example, you can choose to send it to the back or to bring it to the front. If a floating window was sent to the back, you may bring it to the front by right-clicking the desktop button, then selecting the **Bring to front** menu item.

- **Desktop window** : A desktop window is trapped within the work area. It is not possible to send the window in the background. It always remains within the main work area.

4 - To save your changes:

- **Click OK** : If selected, you just save your the changes, the window is not displayed.

- **Click OK & GO** : If selected, this function saves your changes and displays the window you have just configured.

NOTE: *When opening a desktop window for the first time, you may need to re-size it in order to view the information correctly. To do so, point to the frame border you want to change; when the pointer turns into a double-headed arrow, drag the border to exact size. You may then position the window in the work area to the desired position.*

Customizing a Desktop for a "Read-Only" Operator

The security manager or an operator with the appropriate security level can give permission to operators who do not have the appropriate permission to customize their desktop during a session.

1 - Log in, using the user name and password of the operator with 'full access' security level.

2 - Select the desktop you want to customize, right-click and select **Properties** in the menu to open the **Desktop properties** dialog.

*NOTE: A **Permit button** appears when the operator who is logged on has 'read-only' access permission. The permission acquired during this session will be valid until the operator logs out. Click the **Permit** button. The operator login window appears. Enter your user name and password, and click, **OK**. The temporary permission will be granted.*

Transferring a Customized Desktop

Another possibility available to the Security Manager (or to the operator with the appropriate security level) is to customize a desktop, and then to assign the settings to other operators who may not have the appropriate security level to modify their desktop settings.

1 - Right-click the desktop you want to assign the settings.

2 - Select the **Assign (desktop)** option from the shortcut menu.

3 - From the displayed window, select the operators to whom you wish to assign the desktop properties (you must check the appropriate checkbox). You may select operators one by one, or you may use the **Select all** button.

Desktops Colors

Event colors can now be displayed in a separate column. Text and message background colors can also be selected.

1 - From any message desktop, right-click on a message and select **Properties** .

2 - Click on the drop down list and choose a color for the background.

3 - Select **Display event color in separate column** if needed.

4 - Click on the second drop down and choose a colour for the message text.

Transferring a Customized Desktop

Another possibility available to the Security Manager (or to the operator with the appropriate security level) is to customize a desktop, and then to assign the settings to other operators who may not have the appropriate security level to modify their desktop settings.

1 - Right-click the desktop you want to assign the settings.

2 - Select the **Assign (desktop)** option from the shortcut menu.

3 - From the displayed window, select the operators to whom you wish to assign the desktop properties (you must check the appropriate checkbox). You may select operators one by one, or you may use the **Select all** button.

4 - Right-click the desktop you want to assign the settings.

5 - Select the **Assign (desktop)** option from the shortcut menu.

6 - From the displayed window, select the operators to whom you wish to assign the desktop properties (you must check the appropriate checkbox). You may select operators one by one, or you may use the **Select all** button.

Application Status

The **Application Status** displays details about a selected application, such as: operator name, last query date, local identification number, etc. It is also used to verify if EntraPass applications are connected to the server.

1 - In the **Status** window, select the **Application** button. The **Application status** window appears.

- A scrolling list contains all applications listed together or individually. You can select **All connections,** or a specific gateway and view the details of the connection for the selected application(s).

2 - Click the **"+"** sign to see detailed information about an application.

- A **Red** circle indicates that the EntraPass application is not connected to the server
- A **Green** circle indicates that the EntraPass application is connected to the server.
- **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 application on the network. This name is used by the server to identify your application.
- **Network identification** —Provides the IP address of the application on the network or NetBEUI name.
- **Operator name**—Displays the name of the operator currently logged on this application. 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 **Operators Definition**.
- **Last query date** —Displays the time the application last polled the server. The server and application exchange information on a regular basis.
- **Connected date** —Displays the date and time at which this application 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 application (number of exchanges with the server), i.e. report queries, for example.

- **Errors** —Displays the amount of errors encountered by the application. This field will reset when the application is shutdown.

- **Messages/Alarms buffered** (0/1)

  - **0:** the number of messages/alarms buffered for this application on the server when the application is off-line (not in communication). This number will reset to "0" when the application connects to the server and messages are sent.

  - **1:** the number of messages/alarms that were sent to this application since the Server is operational. If the Server is shutdown, this number will reset.

*NOTE: The server holds a maximum of 100,000 messages and 100,000 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 **Application Configuration**).*

*NOTE: When EntraPass sends an alarm to multiple workstations, the **Acknowledgement required** windows appear on all workstations. When someone acknowledges the alarm, the **Acknowledgement required** windows close on the other workstations.*

Text Status

The **Text status** allows an operator to display the status of a selected component (and sub-components) as well as all the characteristics associated with this component in a text form. This menu option applies to all the system devices: applications, gateways, sites, controllers, doors, relays and inputs. The text window contains additional buttons that assist operators in their tasks:

- The first seven buttons represent system devices (Workstation, Gateway, connection, Controller, Door, Input and Output).
- Summary/Detailed list —The magnifying glass button 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.

Displaying a Component Status

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

2 - In the Text window, select the button of the component for which you want to view the status. If you select the **Workstation** button, the system displays the list of the EntraPass Applications defined in the system

3 - You can check the EntraPass application you want to display the status or enter a few characters of the component name (field at the top) for the system to search in the database. For example, you can enter "Sec" for Security Office. The system will highlight the first name containing the entered characters. You may also click the **Select all** button to select all the EntraPass applications; or select specific components by clicking in the checkboxes next to each component name. The **Clear all** button removes the check marks from the selected components. Click **Cancel** to return to the previous window without any selections or changes.

4 - You may check the **View sub-components** option (lower part of the window) to display detailed information on the sub-components linked to the selected component. For example, if you selected a controller, all its components (doors, relays, inputs) with appropriate status will be displayed on the window if this option was checked. For more focus in one window, filter doors, relays or inputs by connection.

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

NOTE: The Magnifying glass button is used to display components that are not in normal condition. When it is in a "summary" position, only components that are not in normal condition will be displayed; the "detailed" position, displays a full status of all components.

Numerical Status

This menu allows an operator to view the number of components in a "not normal" state for a selected gateway.

1 - In the **Status** tab, 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 window 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 coloured shapes (circle, square, etc.).

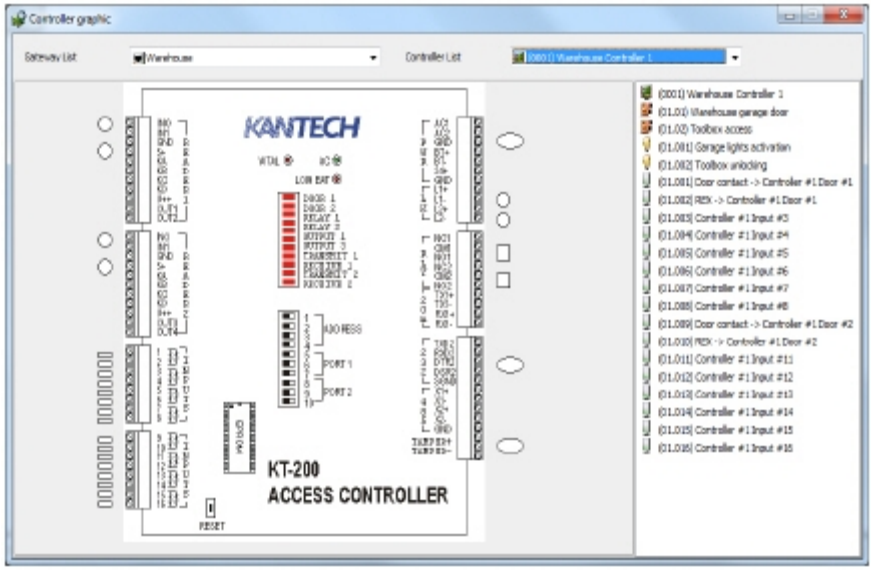
- An ellipse shape represents the controller
- A circle represents a door
- A square represents a relay
- A rectangle represents an input. Rectangles may be horizontal (KT-200 and KT-300) or vertical (KT-100).

Viewing a Controller Status

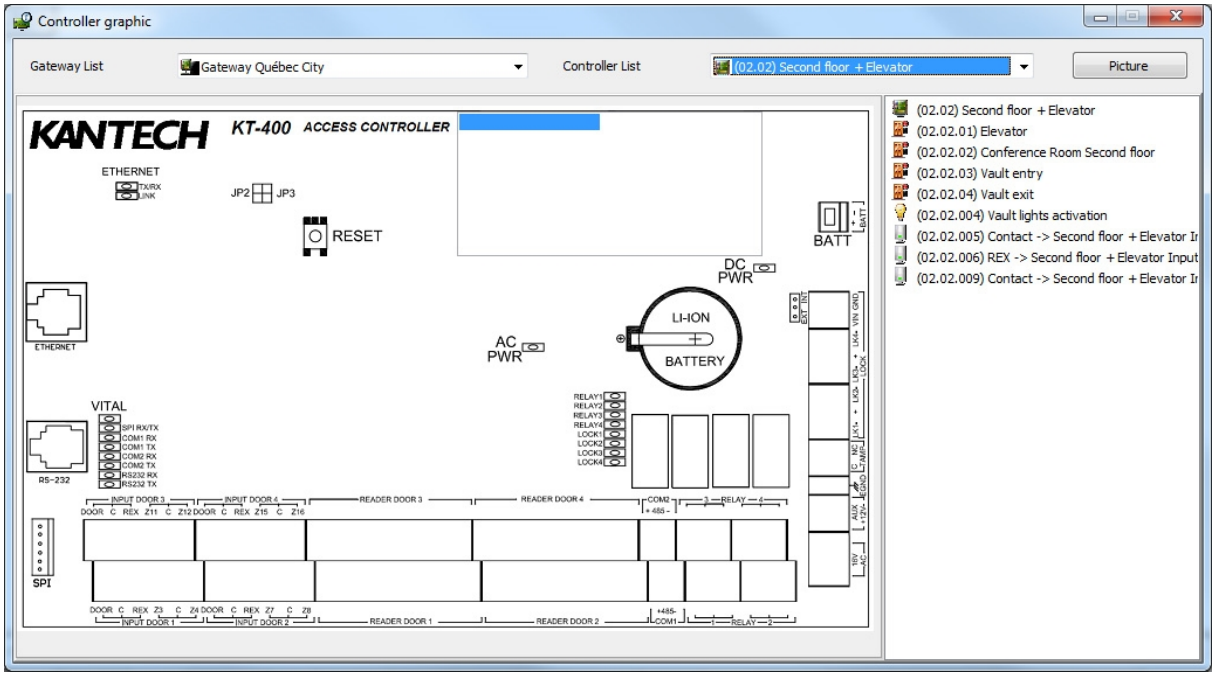
1 - From the **Gateway** drop-down list, select the gateway on which the controller to display is located. You may select “All gateways” to display all the controllers in the list.

2 - From the **Controller** drop-down list, select the controller for which you want to display the status.

Example with a KT-200 Controller



Example with a KT-400 Controller



***NOTE:** The displayed graphic depends on the type of the controller selected.*

3 - To find out which items are represented by a coloured shape, move the mouse over a coloured shape. The item highlighted on the right-hand (in the list) identifies the component.

4 - Select a controller from the **Controller list** drop-down list (right side of the window), double-click the item on which status is required.

- Red —The component is “Supervised” and “in a trouble state”.
- Green —The component is “Supervised” and “in normal condition”.
- Yellow —The component is “Not Supervised” and “in a trouble state”.
- Gray —The component is “Not Supervised” and “in normal condition”.
- Blue —The relay is activated (by an event or an operator).

NOTE: If there’s more than one controller connection per gateway, the numbers between parentheses (xx) indicates the controller number and the following numbers (xx) indicate the component number.

Database Status

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

You can also perform manual operations directly from the window and edit components in order to modify their configuration.

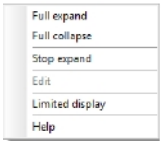
1 - From the Status window, select the **Database** button. The Database window appears.

NOTE: The button identifies the type of component.

2 - In the Database window, select the application you want to view the database. The lower part of the window displays the actual status of the selected component as well as its full name.

3 - Select a component to modify its definition directly from the Database window. For example, if you have selected a door, right-click the door to display a shortcut menu.

4 - Select a command in the cascading sub-menu; select a menu option.



NOTE: The command list varies according to the selected component.

5 - Make your modifications to return to the Database status window. The **Right-click** shortcut menu offers the following options:

- **Full expand** — This feature allows you to fully expand the tree status and view all components. Only applications that are connected to the server will display a **"+"** sign.
- **Full collapse** — This feature allows you to fully collapse the tree status and hide all components of the root component.
- **Edit** — When you select an assigned component (i.e.: input) and click edit, the system will edit the definition window so you can modify its definition and when finished, return to the window you edited the component from.
- **Limited display / No limited display** — When you click on a physical component, the bottom part of the window displays its status.
- By selecting **Limited display** , the system will erase the previous status and display the status of the next selected component.

NOTE: The buttons on the left side components indicate the component type.

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 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 Video transfer.

Viewing the video server full status

1 - From the Graphic desktop window, right-click the Video Server button to display a shortcut menu.

2 - From the shortcut menu, select **Full status** to display information about the video server status.

NOTE: 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.

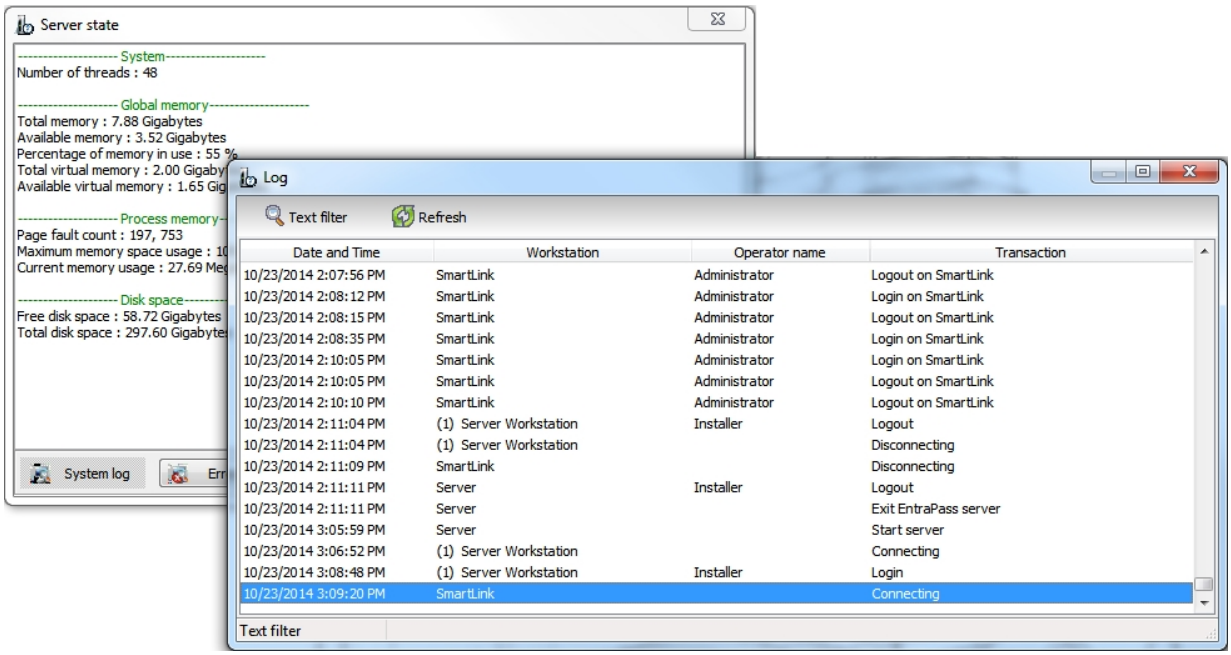
Item	Description
Unit name	The network name of the remote DVMS system (Intellex in this example). The Unit name is followed by the DVR IP address.
Unit type	The type of the unit. can be Intellex, Iris (network client), etc.
Schedule mode	The current schedule mode of the remote DVMS unit. It indicates how images are recorded by the DVR 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	The active record statue of the remote DVMS unit. Values can be: **True** : is recording **False** : is stopped.
Time span (h:mm)	The time interval (in second) between the oldest and newest images in the database.
Unit version	The official version of the DVMS unit.
Number of cameras	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.

Item	Description
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 DVR 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	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 or **PAL** : the PAL standard is mainly used in Germany, Great Britain, China, Australia and Brazil.
Estimated remaining images	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	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	The rate code value. This value indicates the aggregate recording rate for the DVR 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	The total number of images in the remote unit's database.
Version compatibility	Compatibility between the versions of the DVR unit and the application interface used.
Number of text	The numbers of text data streams available from the DVMS. The text data source may be a cash register or other device.

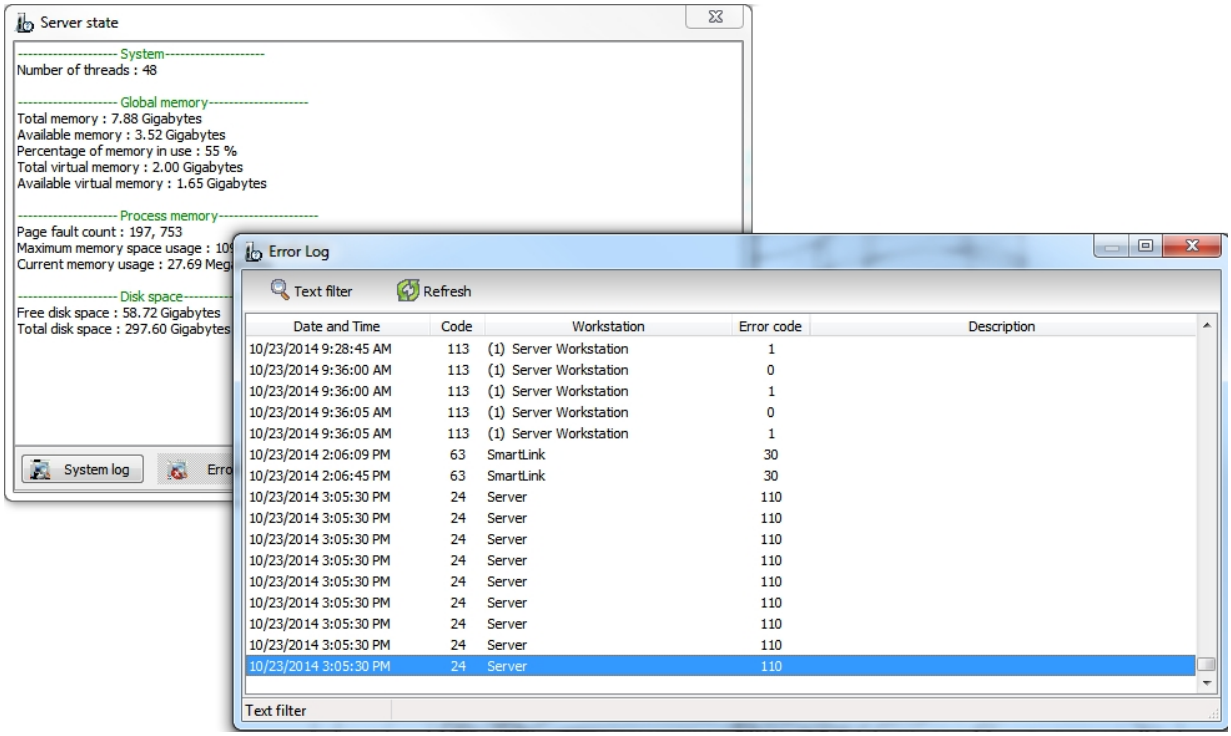
Server State

The **Server state** dialog allows users to view detailed information on the server such as system information, system global memory, system process memory and system disk space.

- **System log** button: Click to display the system log.



- **Error log** button: Click to display the error log.



Logins

This feature allows you to see how many operator our actually logged in the system for each application.

To access Logins, click the **Logins** button from the **Status** toolbar. The displayed window shows the following columns:

- **EntraPass application** : The application name in which the operator is logged in.
- **SmartLink** : The application (EntraPass Web or EntraPass Go) to which the operator is logged in.
- **Operator name** : The operator's name.
- **Login name** : The login name.
- **Login since** : The date and time from which the operator is logged in.

NOTE: *You can use filters for EntraPass application, Account and SmartLink columns by clicking the arrow displayed when the cursor is hovering the column title.*

NOTE: *At the bottom of the window, you can see the total number of operators logged in.*

NOTE: *When an operator logs in, a number is displayed in the details column of the event (Message desktop) to indicate the number of operators logged in the system. That value is also displayed in reports.*

NOTE: *Under **Security level/Workstation/Status**, you will find an option that allows to give access or not to the **Logins** button.*

NOTE: *You can force another operator to log off EntraPass. Right-click on the operators name and select **Force logout**. To stop the operator logging back in to the system right-click on the operators name and select **Force logout and Disable operator***

Manual Operations on Gateway

Manual operations on the gateway feature allows operators to communicate with the gateways to refresh and reload gateway data.

Icon	Definition
	Reset TCP and UDP sockets: releases the TCP and UDP controller communication sockets and then recreates them.
	Reload: deletes the content of the gateway database, restarts the gateway and reloads the data from the system database. Reload is available on the CE, GE and KT-NCC gateways.

Note...

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

Selecting a Gateway

1 - From the EntraPass workstation, click the **Operation** tab, and then click **Gateway** from the menu. The **Gateway** window displays and lists all the gateways connected to your system.

2 - To view gateway statistics, point to the multi-site gateway you want, and double-click.

Viewing Gateway statistics

The gateway status window outlines the current gateway statistics, these include the following details:

- **Connection**
- **Number of cards**
- **Number of threads**
- **Number of messages waiting**
- **Version**
- **Number of sites**
- **Number of sites Ok**
- **Number of failed sites**
- **Total memory**
- **Available memory**
- **Available virtual memory**
- **Local time**
- **Last startup**

Note...

When you define modem connections on a gateway, you need to manually check their online status as EntraPass does not show modem connections in the gateway status window under ***Number of site Ok*** *or* ***Number of failed sites.*** *The* ***Number of sites Ok*** *represents the number of sites successfully connected by broadband connections on the gateway, modem connections are not counted. The* ***Number of failed sites*** *represents the number of sites that failed to connect by broadband connections on the gateway, modem connections are not counted. The* ***Number of sites****, represents the number of sites defined on the gateway.*

Performing a Hard Reset

Note...

Execute reset commands with caution. Before you carry out a controller reset operation, we recommend you contact our Technical Support. For more information, see ***Technical Support****.*

1 - Select the gateway for which you want to perform a hard reset.

2 - Click the **Hard reset** button. This command erases the existing gateway database and reloads it with new information.

Reloading Gateway Data

EntraPass allows operators to reload data in order to refresh system parameters with new data from the system database. When should you reload a 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 (for example, when it does not receive data).

After a reload operation, the gateway reorganizes the data received and communicates the new data to all the sites and controllers.

Note...

Communication with controllers is suspended during a reload operation.

1 - Select the gateway for which you want to reload the data.

2 - Click the Reload data button. Gateway data will be updated.

Manual Operations on Sites

The manual operations on site and connection 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.

Icon	Description
	Connect to remote site: Click to connect to a remote site using a pre-configured dial-up connection.
	Disconnect remote site: Click to **close** the connection between this EntraPass workstation and the remote connection.
	Force disconnect site: Force disconnect remote connection immediately, even if the system is reloading. This option is only available in a multi-site Gateway.
	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 connection: After selecting connection, click to connect and update parameters.
	Update all remote connections: Click to connect and update parameters on all connection starting with the first connection on the list.
	Remove connection from connect and wait list: Select a connection then click to suspend connection after all connections had been set for update.
	Reload IP Link firmware: will force a reload of the selected Kantech IP Link firmware. NOTE: For security reasons, the System Administrator may disable this button.
	Broadcast IP Device: will send a signal to the selected Kantech IP Link and also the KT-400 IP Secure.

Note...

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

Performing Manual Operations on a site/connection

1 - From the **Operation** window, click on the **Site and Connection**button to open the **Site and Connection** window, then select the site/gateway to which the site/connection is connected.

2 - To poll a controller that is not assigned, click the **Controller** button. A message is sent to an unassigned controller, asking it to identify itself. When the controller receives the call from the connection, 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 connection. If the percentage is too low (below 75% for instance), it may indicate that the connection is not communicating efficiently. Communication problems may stem from various reasons such as interferences, damaged cables, etc.

Communication Status Messages Available in the List

The messages in the list area of the dialog indicate the connection communication status. In the following example, you will see communication status messages for multi-site Gateways.

Multi-site Gateways

Message	Description
Connection Communication OK	All controllers can communicate with the gateway.
Connection Communication Trouble	At least one of the controllers can't communicate with the gateway.
Connection Communication Failure	Communication failed between the controllers and the gateway.
Connection Communication Cannot be Opened	The gateway cannot open the communication port.

Manual Operations on Controllers

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

Icon	Definition
	Soft reset: will not affect the controller database. This command sends new information to a controller to update its physical components (relays, inputs, doors and outputs)
	Hard reset: will erase the existing controller database and reload it with new information in the controller database Reset commands should be executed with caution. Before you carry out a controller reset operation, we recommend you contact our Technical Support. For more information, see **Technical Support**.
	Reload: will reload the controller database; if for example a controller database is not reloaded correctly due to an erratic operation

Icon	Definition
	Reload controller firmware: will reload the firmware of the controller (KT-100, KT-300).
	Clear buffered events: offline controllers buffer events until they reconnect to the server. This operation will discard saved events on the controller. This operation is only available for KT-400 and KT -1 controllers.
	Unlock reader keypad: will unlock the reader keypad for KT-100 controllers.
	Reset reader power: will reset the controller reader power. You can only perform this operation on the KT-1, KT-400, and the KT-300 controllers.
	Forgive: will reset to zero the cards-in and cards-out counters or card counters from controller local area
	Anti-passback cards list: displays the number of cards per local area, obtain a card list in local area controllers, move cards (when you have a KT-400 system) and allows you to get position a card. This feature is used only for Multi-site Gateway.
	Request unassigned modules: will provide the serial numbers of all ioSmart readers connected but not defined in the system, for example, Controller #1, ioSmart reader, 14001560.
	Reload module firmware: will reload the firmware of the ioSmart module.

Note...

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

Selecting a Controller

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

2 - From the **Gateway/Site** pane, select a gateway or site. Controllers attached to this gateway/site appear in the right-hand pane.

- From the **Controller** list, select the controller where the operations will take place. It has to be highlighted. To perform the operation on a group of controllers, select **Controller Group** (lower right-hand pane).

Note...

If only one site or gateway is defined in the system, the Site Controller or Gateway list pane will not

appear on the Controller window.

The **Controller Group** bottom panel is available only to the selected site or to a selected connection not linked to a site.

Performing a Controller Soft Reset

A soft reset will refresh the data in the controller.

1 - In the **Controller** dialog, select desired controller or controller group.

2 - Click the **Soft reset** button in the toolbar. This command will sends new information to the controller to update its physical components (relays, inputs, doors and outputs, etc.)

Performing a Controller Hard Reset

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

Note...

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

1 - In the **Controller** dialog, select desired controller or controller group.

2 - Click the **Hard reset** button in the toolbar. This command will sends new information to the controller to update its physical components (relays, inputs, doors and outputs, etc.)

Reloading a Controller Manually

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

1 - In the **Controller** dialog, select desired controller or controller group.

2 - Click the **Reload** button in the toolbar. The controller's database will be reloaded.

Manually Reloading a Firmware Controller

EntraPass allows you to reload a controller firmware database for KT-100 and KT-300. You will perform a firmware reload after a system or firmware upgrade.

1 - In the **Controller** dialog, select desired controller or controller group.

2 - Click the **Reload controller firmware** button in the toolbar.

Manually clearing buffered events

Offline controllers buffer events. When offline controllers are reconnected to EntraPass buffered events can be downloaded or cleared. To clear buffered events complete the following steps:

1 - In the **Controller** dialog, select the controller you want.

2 - Click the **Clear buffered events** button in the toolbar.

This option is also available when you right-click on the controller you want. This operation is only available for KT-400 and KT -1 controllers.

Manually Unlocking a Reader Keypad

EntraPass allows you to unlock the reader keypad for KT-100 controllers from a workstation.

1 - In the **Controller** dialog, select desired controller or controller group.

2 - Click the **Unlock reader keypad** button in the toolbar.

Resetting Cards In and Cards Out Counters or all Controller local areas

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

1 - In the **Controller** dialog, select desired controller or controller group.

2 - Click the **Forgive** button in the toolbar. Card holders will not be considered inside or outside until the next use of their card at an entry or exit reader.

Calculating Number of Cards In and Cards Out

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

1 - In the **Controller** dialog, in the **Gateway/Site** section, select **KT-400-IP** . Then in the **Controller** section, the list of appropriate controllers relative to the selection display.

2 - Select desired controller or controller group.

3 - Click the **Get Card List** button in the toolbar. The system will display the number of cards in or cards out for the selected controller or controller group.

Note...

This operation is performed only on one controller at a time as it may be a lengthy operation. The option is only available on a Multi-site Gateway.

Card Location

1 - Right-click the appropriate local area number, and then click **Find card position** .

2 - In the **Get card position** dialog, click **Start with** , **Begin with** or **Contains** to filter the search criterion.

3 - In the list, select the wanted card position, and then click **Get position** .

Resetting Cards In and Cards Out Counters or all Controller local areas

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

1 - In the **Controller** dialog, select desired controller or controller group.

2 - Click the **Forgive** button in the toolbar. Card holders will not be considered inside or outside until the next use of their card at an entry or exit reader.

Requesting unassigned modules

This feature provides the serial numbers of all ioSmart readers and ioModules connected to a controller but not defined in the system. Use one of the following methods to view unassigned modules in a **Message List** window:

- In the **Operations** tab, select a controller, right-click and select **Request unassigned modules**.
- In the **Operations** tab, right-click in the toolbar and click **Request unassigned modules.**

To edit a module, right-click an event, click **Edit**, and choose one of the following options:

- **Controller**: use to open the **Controller** window and edit the definition for the controller.
- **Assign**: performs the following actions:
  - Populates the data into the controller's configuration page in the **ioSmart** tab, or the **ioModule** tab. If necessary, rename the reader or change the configuration details, and click **Save.**

Full status

Use **Full status** to review the controller's communication settings and configuration.

Module status

Use **Module status** to review the module's status.

Note...

If you want to view to the **Full status** and the **Module status** windows at the same time, click **Full status**, and on the controller window, click **Module Status**.

Edit

Use **Edit** to open the **Controller** window and edit the definition for the controller.

Manual Operations on Doors

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

Icon	Definition
	Lock door or group of doors: will manually lock the selected door or group of doors.
	Unlock door or group of doors: The selected door or group of doors will be manually unlocked and will remain unlock until the next valid change of the unlocking schedule or an operator manually locks the door or group of doors

Icon	Definition
	Temporarily lock/unlock door or group of doors: Temporarily unlocks a door or group of doors for a preset delay. Once the delay expires, the door or group of doors re-lock automatically.
	Return to schedule: Will re-apply the locking schedule for a door or a group of doors.
	Enable card reader: Will enable a previously disabled door reader.
	Disable card reader: Will disable a door reader and user will not be able to access that door, even if they have access rights.
	Arm door (Multi-site Gateway with KT-400 only): Does a Request to arm on the alarm panel.
	Disarm door (Multi-site Gateway with KT-400 only): Does a Request to disarm on the alarm panel.
	Soft reset reader: will restart the reader by powering it off and then on again.
	Hard reset reader:will restore the reader to its original factory state. It deletes all programmed settings.

Note...

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

There are various reasons why you would want to perform one of these operations; for example you may need to “disable a reader” for a short period in order to deny access to the door, etc. This operation allows an operator to lock a door that was previously unlocked by an operator or a schedule. When a door is manually locked through the **Operation** menu, it remains locked until:

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

Selecting a Door or a Door Group

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

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

- The left-hand pane displays the list of all **Sites/Gateways**. You may select all or select one site/gateway.
- The individual doors associated with the site/gateway selected on the left are displayed in the top right side of the pane. If you select **All** on the left, all doors in the system will be listed on the right. You can select one, several or all doors.

Note...

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

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

Note...

The **Door Group** bottom panel is available only to the selected site or to a selected connection not linked to a site.

Locking a Door Manually

1 - In the **Door** dialog, select desired door(s) or door group.

2 - Click the **Lock-door** button in the toolbar.

Unlocking a Door Manually

1 - In the **Door** dialog, select desired door(s) or door group.

2 - Click the **Unlock-door** button in the tool bar. The selected door(s) will be manually unlocked. The system will prompt for operator confirmation. A door defined with an automatic unlocking schedule will remain unlocked until:

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

Unlocking a Door Temporarily

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

Note...

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

1 - Click the **Temporarily unlock** button. The **Change delay on action** dialog will popup.

2 - Enter the **New time delay (m:ss)** and click **OK** . The selected door will be temporarily unlocked by an operator.

Note...

If a door contact is installed, the door will re-lock as soon the system sees a “door open-door closed”

transition. There is no “Animation” for this type of operation.

Resetting a Door Schedule

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

1 - In the **Door** dialog, select desired door(s) or door group.

2 - Click the **Return to Schedule** button. This option will reset the schedule for the selected components.

Enabling a Door Reader

1 - In the **Door** dialog, select desired door(s) or door group.

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

Disabling a Door Reader

1 - In the **Door** dialog, select desired door(s) or door group.

2 - Click the **Reader-disabled** button. This option disables a previously enabled reader. Disabling a reader prohibits users from accessing the door, even if access rights have been granted.

Modifying access level schedule

Using the door's operation menu you can manage the access levels of the door directly.

1 - In the **Door** dialog, select a door.

2 - Right-click on the door and select **Access Level**. This window displays all access levels where the door can be assigned.

3 - To create a new schedule, right-click on the **Schedule** section and select **New**.

4 - To edit existing schedules, right-click on the **Schedule** section and select **Edit**.

5 - To apply an existing schedule to an access level, click on the drop-down list beside the schedule.

For more information about access levels, click **here**.

Manual Operations on Elevator Doors

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

- The cardholder pushes an “up/down” button, the elevator door opens,
- The cardholder presents its card at the reader (usually inside the cab),
- The system checks if the schedule assigned to this door is valid. If yes, the system checks which floor group is associated to this door,
- Then the system verifies each floor of the floor group (in the floor group menu) and checks if the schedule associated to each floor of the group is valid or not valid.

- Only floors that have a valid schedule will be available for selection by the user (the elevator panel will enable the buttons corresponding to the floors).

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

Note...

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

Selecting an Elevator Door

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

2 - Click the **Enable animation** button to view a real-time display of the elevator door status.

- The left-hand pane displays the list of all **Sites/Gateways**. all **Sites/Gateways**. You may select all or select one connection/gateway.
- The individual elevator doors associated with the connection/gateway selected on the left are displayed in the top right side of the pane. If you select **All** on the left, all elevator doors in the system will be listed on the right. You can select one, several or all elevator doors.

- **Elevator door groups** associated to the connection/gateway selected on the left are displayed at the bottom right of the pane. If you select **All** on the left, all elevator door groups will be listed at the bottom right. You can select one or several or all elevator door groups.

Note...

The **Door Group** bottom panel is available only to the selected site or to a selected connection not linked to a site.

Locking Floors from Elevator Doors

1 - Select an elevator door or a group of elevator doors.

2 - Click the **Lock** button in the toolbar. This command will manually lock the floor group that was previously unlocked by an operator or a schedule.

Note...

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

Unlocking Floors from Elevator Doors

1 - Select an elevator door or a group of elevator doors.

2 - Click the **Unlock elevator floors** button in the toolbar to unlock a previously locked floor. This command will only enable the elevator floors that are defined with an “X” in the “” column of the Floor group Definition menu. If you do this, the system will prompt the you to select a floor group that should be unlocked (available). Once the group is selected, the system will prompt the operator to confirm the operation.

Note...

For a door defined with an “automatic unlocking schedule”, floors will remain available until the next valid change of the unlocking schedule, or an operator manually locks the door.

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

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

Unlocking Floors from Elevator Doors Temporarily

EntraPass allows you to temporarily unlock a floor from an elevator door for a preset delay. Once the delay expires, the elevator door re-locks automatically. The maximum unlock time: 4:15 (255 seconds).

1 - Click the **Temporarily unlock** button. The **Change delay on action** dialog will pop up.

2 - Enter the **New time delay (m:ss)** and click **OK** . The selected elevator floor will be temporarily unlocked by an operator.

Note...

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

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

Resetting an Elevator Door Schedule

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

1 - In the **Elevator door** dialog, select desired elevator door (s) or door group.

2 - Click the **Return to Schedule** button. This option will reset the schedule for the selected components.

Enabling an Elevator Floor

1 - In the **Elevator floor** dialog, select desired floor(s) or floor group.

2 - Click the **Enable elevator floor** button. This option enables previously disabled elevator floors or floor group.

Disabling an Elevator Floor

1 - In the **Elevator door** dialog, select desired floor(s) or floor group.

2 - Click the **Disabled elevator floor** button. This option disables a previously enabled elevator floor. Disabling a floor prohibits users from accessing the floor, even if access rights have been granted.

See Also...

Manual Operations on Relays

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

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

Icon	Definition
	Deactivate relay: allows an operator to deactivate a relay which was previously activated by an operator, event, schedule or input in alarm.

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

Note...

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

Selecting Relays

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

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

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

Note...

*The **Relay Group** bottom panel is available only to the selected site or to a selected connection not linked to a site.*

Deactivating a Relay Manually

1 - Select a relay or a group of relays.

2 - Click the **Deactivate Relay** button.

Note...

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

Activating a Relay Manually

1 - Select a relay or a group of relays.

2 - Click the **Activate Relay** button. 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.

Activating a Relay Temporarily

1 - In the right-hand pane, you may select a relay in the upper part of the window, **All Relays** in the lower part of the window.

2 - Click the **Activate relay temporarily** button. The **Change delay on action** window will popup on screen.

3 - Enter the **New time delay (m:ss)** and click **OK** . The selected relay will be temporarily activated by an operator.

Note...

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

Resetting a Relay Schedule

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

1 - In the **Relay door** dialog, select desired relay(s) or relay group.

2 - Click the **Return to Schedule** button. This option will reset the schedule for the selected components.

Manual Operations on Inputs

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

Icon	Definition
	Input normal: returns an input to its normal state as setup in the Device menu.
	Input continuous supervision: will monitor the selected input at all times.

Icon	Definition
	Input with no supervision will terminate the input monitoring, regardless of its schedule, and will start monitoring with the next pre-defined schedule.
	Input no supervision temporarily (Shunt): will stop input monitoring for a pre-set period of time.

Note...

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

Performing Manual Operations on Inputs

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

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

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

Note...

The **Input Group** bottom panel is available only to the selected site or to a selected connection not linked to a site.

Returning an Input to Its Normal State Manually

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

1 - Select an input or a group of inputs.

2 - Click the **Input normal button** . The selected input returns to its normal state as defined in the **Device** menu.

Stopping Monitoring an Input

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

1 - Select an input or a group of inputs.

2 - Click **Input no supervision** . The selected input will not be monitored.

Stopping Input Supervision (Shunt) Temporarily

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

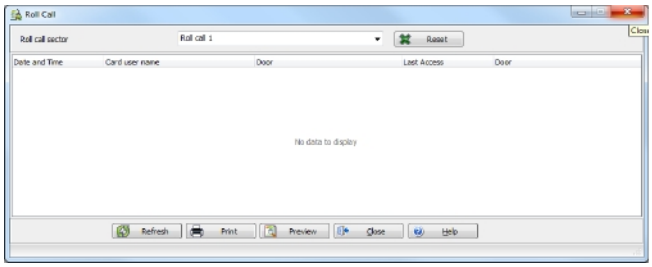
1 - To temporarily shunt an input, select the input, then click the **Temporarily shunt** button. The input will not be monitored temporarily.

2 - Click **Input no supervision temporarily.** The **Change delay on action dialog** will popup.

3 - Enter the **New time delay (m:ss)** and click **OK** . An button next to the input will indicate that it is temporarily shunt. If an alarm occurs, or if the input is disconnected, no message will be sent to the **desktop Message list**.

Manual Operations on View Roll Call

This feature is used to visualize the users entering a pre-defined perimeter. When a user enters this area, the corresponding data is displayed in the following dialog:



Manual Operations on Integrated Panels

1 - From the **Operations** toolbar, select the **Integrated Panel** button.

2 - If required, select a specific component from the **All components** drop-down menu.

3 - Select a **panel** from the left column and then right-click to view its contextual menu.

4 - Select **Full status** to view the panel status details.

5 - Select **Virtual Alarm Panel** to view the virtual keypad.

6 - Select a **partition** and right-click to view its contextual menu.

7 - Select **Arm partition** or **Disarm partition** as required.

8 - Select a **zone** and right-click to view its contextual menu.

9 - Select **Zone bypass** or **Zone unbypass** as required. When the panel is next disarmed, the zone will return to its unbypassed state.

Manual Operations on Action Scheduler

Use the Action scheduler to create actions with the option to program one-time actions or recurring actions. The initial input interface is a calendar layout, to open a new action in the scheduler window, double-click a date. You can view existing actions in a daily, weekly, monthly or yearly format and use the Action scheduler tag to filter the type of actions displayed.

The initial view includes a list of programmed actions, and include the following details: who requested it, the date and time it is scheduled for, what the action is, a full description of the action, whether it is a recurring action or not and, the used and total recurring count.

You control permissions for the Action scheduler in Action Scheduler under the **Operations** menu. The icon is a calendar page with a timer, and is automatically installed on a system update. A security item is also added for this feature and it is located under the **Operation** menu, **Action scheduler** of the security level menu.

Note...

To program actions the default security setting for Installer and Administrators is, allow which, is indicated by a green icon, the default security setting for Operators is, not allow indicated by a red icon. To change this, expand the **Operation** tree and select **Action Scheduler**.

Icon	Definition
	Action Scheduler: This creates actions that are either one-time actions or recurring actions. It provides a calendar view of all programmed actions with filter, search and tag capability.

Programming the Action scheduler

The following table outlines the controller compatibility and firmware requirements for this feature.

Controller	V3 Assa-Abloy firmware compatibility	Gateways	Fail-soft mode
KT-1, firmware 2.00 and higher	Yes	Multi-site, Global, KT-NCC	Yes
KT-400, rev 1, firmware 1.29 and higher	Yes	Multi-site, Global, KT-NCC	Yes
KT-400, firmware 1.23 and higher	Yes	Multi-site, Global, KT-NCC	Yes
KT-300	No	Global, KT-NCC	No
KT-200	No	Global, KT-NCC	No

Table Controller and firmware compatibility

To program the Action scheduler complete the following steps:

1 - Click the **Operation** tab, and select **Action scheduler** from the menu.

2 - From the calendar interface, double-click the date you want, or click the **Add** button on the upper left panel.

3 - In the **Action scheduler** window, enter a name for the action in the primary or secondary fields.

4 - From the **Action** list, select the appropriate action, the default action is **Unlock door.**

Note...

Execute task is a new action that selects an existing task builder as a component, an option to select a specific time zone is available, where the default is based on the location of the local server. When you create a new action schedule by right-clicking a component from the **Operation** menu, the menu only displays actions appropriate to that component.

For wireless door connections, use V3 of the Assa-Abloy firmware with any of the compatible controllers listed in the table, Controller and firmware compatibility.

5 - In the **Schedule date and time** fields, select the appropriate values. The default day is the current day, and the default time is one hour later than the current time.

Note...

If you select a temporary action, an end time box appears. If an action has a dual function such as

Activate and Deactivate, **Date and Time** fields appears.

6 - In the **Action scheduler tag** field, create a name to tag the action scheduler. The tag populates a list used to filter all actions. Each new name generates a new tag, 50 tags is the maximum amount possible. If no action uses a tag, it is automatically removed from the list.

7 - Optional: Select the **Recurring** checkbox if you want the action to repeat. In the **Frequency** list, choose from **Daily**, **Weekly**, **Monthly** or **Annually**. Set the counter to the amount of times you want the action to repeat, this is a static setting and 99 is the maximum amount of times available. A dynamic counter is visible in the lower section of the calendar view.

8 - Select the **Delete when expired** check box to delete the action after the programmed amount of recurrences.

Note...

To ensure different time zones are adhered to, EntraPass deletes actions 24 hours after midnight of the day of execution. For example, an action programmed for Monday 15:00 is deleted the following Wednesday at 00:00.

9 - You must use one of the eight **Component** fields for an action.

Note...

If you want the action to work in stand-alone mode, use only new generation controllers such as the KT-1, KT-400, KT-400 rev1.

10 - Click the **Save** button.

The KT-NCC, Global Gateway and the Action scheduler

If a KT-NCC or Global Gateway is used, the **Action scheduler** will function with all types of controllers, as the Global gateway is responsible for all decisions. If a KT-1, KT-400, or KT-400 rev 1 is used in stand-alone mode and loses connection with the KT-NCC, the KT-1 takes responsibility for the **Action scheduler** actions.

If you use a KT-100, KT-200, or KT-300 controller and the KT-NCC is offline when an action is triggered, the action will not trigger as the **Action scheduler** uses date and time to trigger an action, and the date and time is not buffered when the KT-NCC is offline.

Programming the Action scheduler from the Door or Relay windows

The following steps outline how to program the Action scheduler from the **Door** window, the same steps apply if programming the Action scheduler from the **Relay** window:

1 - Click the **Operation** tab, and click **Door** from the menu.

2 - In the **Door** panel, select the appropriate door and right-click.

3 - Click **Action schedule** to open the **Action scheduler** window.

4 - Complete steps 3 to 9 in **Programming the Action scheduler** procedure.

Printing the Action scheduler calendar

A report on all **Action scheduler** actions is available. To print the report, complete the following steps:

1 - From the **Action Scheduler** window, click the **Print** button.

2 - Select the actions you want to include in the report, use **Select all** or **Unselect all** to assist your choice.

3 - The report lists actions beginning with the nearest date and time to the furthest away.

4 - Actions include the following items:

- Name
- Action
- Which components
- Date
- Time, start time, and end time
- Recurring schedule with counter
- Time zone if applicable

Access Exception

Use the **Access exception** tab to link a specific schedule to a door.

1 - From the left panel, select a door.

2 - From the right panel, select a schedule using the drop-down list. Use the and buttons to add or remove doors from the list on the right.

3 - Under the Access column, choose between **Allow** or **Deny**.

NOTE: Only doors with an associated schedule will be saved.

Warning: *User list report does not take Access Exception into account.*

To enable the **Access level exception** feature, please refer to **Credentials Parameters**.

Access Levels Definition

Access levels determine where and when the card will be valid. Pre-programmed card access groups allow quick selection of access levels for various gateways. A total of 248 access levels can be programmed per connection . 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.

1 - 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.

2 - From the Users toolbar, select the **Access level** button. The Access level window appears.

3 - C lick on **New** , then assign a meaningful name to the access level you are creating.

NOTE: Components that are displayed in the Doors and Schedule or Floor group columns have to be pre-defined for selection. To define Doors: Devices > Door. To define Schedules: Definition > Schedule. To define Floors groups: Groups > Floor group.

4 - From the **Doors** list, select the doors to which the cardholder has access.

5 - From the **Schedule** column, select the schedule during which the cardholder will have access to the corresponding door.

6 - From the Floor group column, select the floor group, if applicable.

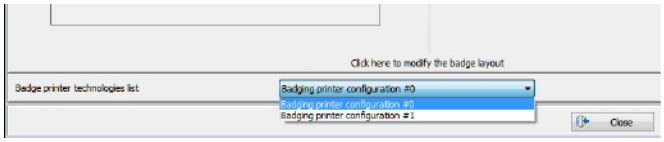
7 - Click the **Comment** tab to had comments to the current access level. You can double-click in the blank space to display the edition window.

Badges Designing

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

Creating a Badge Template

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



*NOTE: The printer configuration description must be first entered from the **System Parameters/Credentials** menu (see Badge Printer for more information).*

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

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

To Specify Properties for a Badge Layout

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

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

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

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

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

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

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

To Edit a Badge Layout

The Badge design utility allows users to edit the badge layout, to add background colour 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 button in the Badge window toolbar.

To Modify the Number of Card Sides

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

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

3 - Click the **Save** button to save the new badge information.

To Modify the Background colour

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

2 - Click the **Click here to modify the card layout** button (located in the lower part of the window) to open the Badge design window.

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

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

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

5 - Select the appropriate options for the template:

- **No background** (default setting)
- **Use colour as background:** this option will allow you to apply a background colour 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.

To Add Objects to a Badge Layout

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

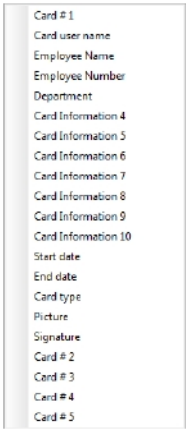
- Card fields information
- Bar codes

- Text boxes
- Current date
- Previously saved images and logos (BMP, JPG, GIF, etc.)
- Border
- Rectangle (including rounded rectangle and 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.

To Incorporate Card Information Fields

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



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

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

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 card holder's photo will be displayed. When a badge is assigned to a card, the appropriate card holder's photo is displayed.

To Align Objects in the Template Layout

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

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

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

NOTE: To disable the grid deselect ***Show grid line*** *in the Align menu.*

To Modify Card Fields Properties

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

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

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

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

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

- Font (name, colour, style (bold, italic, underline)),
- Background (transparent or solid with a colour),
- 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 re-size the field.

To Modify Picture Properties

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

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

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

3 - You may select another image from file or modify the image properties:

- **Stretch ratio** : select this option if you want the image to be centered in the image holder space, while keeping the proportion of the original image.
- **Transparent mode** : if you choose this option, there is no background colour,

- **Draw frame** : select this option if you want a frame around the picture object,

- **Frame colour** (enabled when a Frame option is selected): select this option if you want to apply a specific colour to the image frame. The Frame colour drop-down list enables you to select a custom colour 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.

To Add Static Text Objects

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

1 - From the Badge design tool bar, click the text button. To re-size 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 To Align Objects in the Template Layout.

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.

To Add Bar Codes

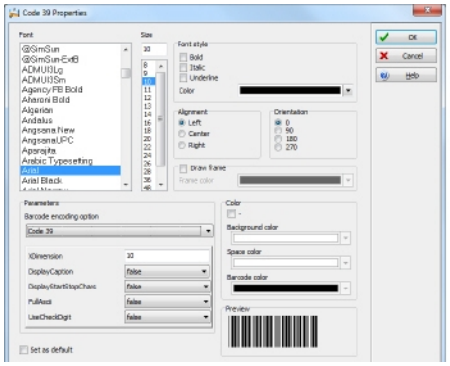
The Badging feature allows users to add bar codes to badges. By default, the bar code value is the card number, if no other value is specified.

1 - From the Badge design window, click the **Bar code** button, then click in the Badge design work area.

2 - To align the bar code, see To Align Objects in the Template Layout.

To Set Up Bar code Properties

1 - From the Badge design window, right click the bar code to open the Bar code Properties window.



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

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

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

To Add the Current Date

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

1 - From the Badge Design template, select the **Current date** button, 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 To Align Objects in the Template Layout.

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

5 - From the Current date properties window, you can:

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

To Add an Image

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

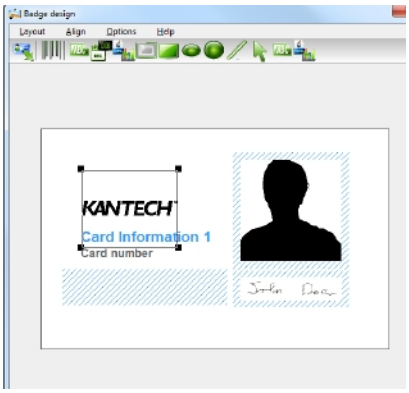
1 - From the Badge design window, select the **Picture** button.

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

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

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

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 re-size it to its original size as illustrated on the following image.

5 - Using the sizing handles, adjust the image to the desired size, then move it to the right-hand position; you can use the grid to align it properly. For more information, see To Align Objects in the Template Layout.

6 - Right click the image to modify its properties. For details, see **To Modify Picture Properties**.

To Place Other Design Objects

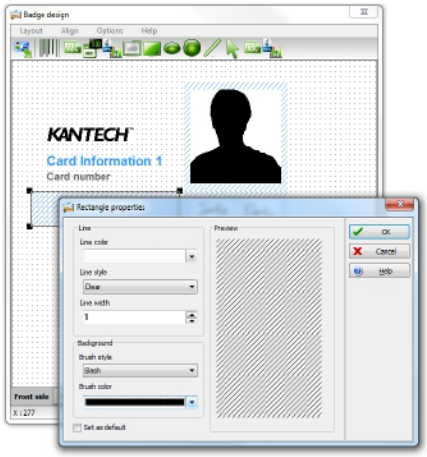
The Badging feature lets you add borders, rectangles (regular, rounded, ellipse), lines and pointers, just as you add any other design object, by a click in the toolbar, then a drop in the design work area.

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

2 - To modify the border properties, select the border colour, 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 window, select the rectangle tool (next to the Border tool), then click in the work area.



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

2 - From the Rectangle properties window, you may define the rectangle properties before importing it:

- Line colour,
- Line style,
- Line width,
- Background (brush style and brush colour).

1 - From the **Users** menu, select **Badge**.

2 - Click the **Print sample** button. The system is prompting to select which user to use for the badge sample.

NOTE: If the badge is 2-sided, the word Sample will be printed on both sides.

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.

Performing Operations on a Group of Cards

1 - From the **Users** toolbar, click the **Batch operations** button.

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

3 - Select a card filter to narrow the batch operation among the selected type of cards.

*NOTE: The card filter drop-down list is available for a registered **hattrix** option only (see **Adding System Components** for more information).*

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

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

5 - Check the option you want to modify for the selected type.

- **Card** : If a card state is selected, the system will assign this new card state to all the cardholders of the selected card type.

- **Maximum card usage** : If a maximum card usage is selected, the system will assign this value to all the cardholders of the selected card type.

- **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, two scroll lists become available to modify card access groups for the selected **Card type** . The first scrolling list defines the action to perform on the selected card type. The second scrolling list contains the card access groups (already defined in EntraPass) that will be used to perform the action.

  - **Replace card access group (Replace)** : Replaces the current access level with the one selected in the scrolling list.

  - **Update card access group (Update)** : Updates the current access level with the one selected in the scrolling list except where sites were set to none in the current access level. No new access levels will be added.

  - **Add new access level (Add)** : This option is used in situations when new sites are added and the sites' access levels must be added to the current access level list. All sites that are set to none in the current access level list will be updated with the sites in the new access level list.

  - **Update add access level (Merge)**: Merges the sites in both lists. The new sites have precedence over the current ones.

Examples of batch operations on card access levels

Current Access Level	New Access Level	Replace	Update	Add	Merge
connection Y1	connection X1	connection X1	connection X1	connection Y1	connection X1
connection Y2	connection X2	connection X2	connection X2	connection Y2	connection X2
connection Y3	None	None	connection Y3	connection Y3	connection Y3
None	connection X4	connection X4	None	connection X4	connection X4

- **Card layout:** If checked, the list of card layout templates will be listed.
- **Card filter** : Apply the selected card filter to all cardholders of the selected card type

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

7 - Click **Yes** if you want to continue. As soon as the process is initiated, a red indicator is displayed at the bottom left of the dialog. The indicator will remain red until the end of the process.

Card Access Groups Definition

Pre-programmed card access groups allow quick selection of access levels for various sites of the system. This card access group can be recalled during card programming instead of re-entering the access levels for each connection. It is only the card access group information that is associated with the card. Therefore, you can modify the card access group information without modifying the card access information.

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

1 - From the **Users** toolbar, click the **Card access group** button.

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 **connection** column displays the connection associated with a card access group.

3 - From the **Access level** drop-down list, select the access level that will determine the access to the doors of the selected connection.

Card Options Definition

Use the **Miscellaneous** tab to specify and view card 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. You also need to set the expiration hour (00 to 23) . The default is 00 (midnight). When the end date is reached, the **Card state** field is set to "Expired".

NOTE: The expiration hour uses the current hour of the connection if the firmware is updated. Please ensure that this is correct for your installation. Only available for KT-400 and KT-1 controllers.

3 - Check the **Delete when expired** option (if applicable). This option can only be used with the **Use end date** option. When selected, the card information will automatically be deleted on the expiry date (using the end date specified), otherwise the **Card state** field will be modified to "Expired".

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

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

5 - **Editable PIN number**: The operator can enter the number of digits needed by the reader/keypad to grant access (see **Defining a Card Display Format** for more information).

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

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

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

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.

7 - Check the **Disable passback** option if you want the card to override the passback option when defined.

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

NOTE: If your are issuing a card for a cardholder with disabilities, check the Extended door access delay option. To enable this option in the system, you have to define appropriate delays in the Door definition. This option is also available when defining visitor cards.

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

8 - Allow multiple-swipe (KT-400 and KT-1 only): Enable the multi-swipe action (see Card Multi-Swipe for more information).

Card Printing

Use the Print feature to print a specific range of all the cards that are stored in the database. You can select various filters to customize the card list. You can preview your list so that you can modify or verify the settings (fields) before printing. You can also use the **Font** button to set a different font and font size for your report.

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

1 - From the **Card** dialog, click the **Printer** button.

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** : Check the option and then select the desired state. The system will include cards that have this card state selected in the **Card** window (**Miscellaneous** tab).
- **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 window.
- Select the **Exist trace** for the system to include cards that have the "Card Trace" option in their definition (Card window, **Miscellaneous** tab).
- Select the **Exist comment** option for the system to include cards that have information in the **Comment** field in their definition (Card window, Comment tab).
- Select **Exist PIN** : The system will include cards that have a PIN.
- Select **Exist delete when expired** : The system will include cards that have information in the **Delete when expired** field (Card window, **Miscellaneous** tab).
- Select **Exist wait for keypad** for the system to include cards that have information in the **Wait for keypad** field (Card window, **Miscellaneous** tab).

5 - To include specific data fields, select the **Print selected fields** check box, and select the fields you want to appear in the card profile report. Save the files in a CSV format.

6 - Click the **Select door 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 window to preview your report.

Card Type Definition

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 of card.

NOTE: *The system is preset with five card types: administrator, employee, security, maintenance and visitor. A card type can be assigned to a card access group. This way, if a cardholder is issued a card type associated with a card access group, the access information of the card access group will automatically be transferred to the cardholder.*

Creating a New Card Type

1 - From the **Users** toolbar, click the **Card type** button. The **Card type** window appears.

2 - In the **Card type** window, click the **New** button in the toolbar and enter the necessary information in the language section.

3 - From the **Card access group to assign** list, select a card access group or create one. For details about card access groups, see **Card Access Groups Definition**.

4 - To assign a card type to a cardholder, see **Cards Definition**.

Cardholder Access Levels Assignation

An access level must be assigned to each card. Access levels determine where and when the card will be valid. The access level allows the cardholder entry to selected locations during specified schedules. For information on defining access levels, see **Access Levels Definition**.

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.

Assigning an Access Level to a Cardholder

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

2 - Click the **Card access group** button (displayed on the left of the connection or Gateway list) to copy information from a Card access group to a card. The **Gateway / connection** column The **Gateway / connection** 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 card holder's access to the doors of the selected connection. If you do not want this cardholder to have access to the door of this connection, leave this field to **None** .

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

Card Options Definition

Use the **Miscellaneous** tab to specify and view card 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".

3 - Check the **Delete when expired** option (if applicable). This option can only be used with the **Use end date** option. When selected, the card information will automatically be deleted on the expiry date (using the end date and hour 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.

5 - **Editable PIN number** : The operator can enter the number of digits needed by the reader/keypad to grant access (see **Defining a Card Display Format** for more information).

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

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

- **Valid** : The card is functional,
- **Invalid** : The card is NOT functional,
- **Lost/Stolen** : The card is NOT functional,
- **Pending** : The card is not yet functional.

- **Expired** : The card has reached its expiry date,

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.

7 - Check the **Disable passback** option if you want the card to override the passback option when defined.

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

NOTE: If your are issuing a card for a cardholder with disabilities, check the Extended door access delay option. To enable this option in the system, you have to define appropriate delays in the Door definition. This option is also available when defining visitor cards.

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

8 - Allow multiple-swipe (KT-400 and KT-1 only) : Enable the multi-swipe action (see Card Multi-Swipe for more information).

Adding Comments to a Card

1 - From the **Card** window, 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.

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

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

3 - From the **Maximum card usage** 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 Maximum card usage , the Current card usage 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 when 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 a Picture from a File

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

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

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:

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.

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

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

- **Paste picture** : This option allows you to paste a picture from the clipboard. To use this option, you have to copy the picture, then paste it into the picture window.

NOTE: 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 capture** tab.

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

1 - Right-click the picture area.

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

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

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 **Badges Designing**.

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 options > Badge printer . If these buttons are enabled, you can preview and print the card holder'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.

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

2 - From the shortcut menu, make the appropriate choice:

- **Get signature from file** : Allows you to select a previously saved signature,
- **Paste signature** : Allows you to paste a signature that was previously copied to the clipboard. The option is enabled when there is content in the clipboard.

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

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

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**).

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

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

3 - Click **OK** to paste the signature in the card window.

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).

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

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

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

- **Auto contrast** : This feature gives better contrast by intensifying lights and shadows: it makes the darks darker and the lights lighter. In general, this auto contrast feature gives a good result when a simple contrast adjustment is needed to improve an image's contrast.

- **Sharpen** : This feature provides more definition to blurry images by applying sharpening only when an edge is found.

- **Brightness** : This feature allows you to add light to the image by sliding towards the positive values.

- **Reset all:** This feature allows you to undo all the changes and to restore the original image.

4 - Click **OK** to close the **Picture** editing window.

5 - From the Badge layout pull-down menu, select a layout to associate with the card you have defined To define a badge layout, see **Badges Designing**.

Printing Badges

You may print badges, **visitor cards** and **daypasses** from a **Card** or from all **Badge preview** windows. The software is set up to let you print one single or double-sided badges.

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

Selecting a Badge Printer

1 - From the EntraPass Workstation window, select the **Options** toolbar, then click the **Printer Options** button.

2 - From the **Printer options** window, select the **Badge printer** tab.

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

3 - Check the **Badge printer** option to indicate to the system that a badge printer is selected. If the **Badge printer** option is checked, the Print badge and Preview badge are displayed in windows where you can print badges (Card, 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** window allows you to preview a badge layout with card information (if the badge layout is associated with a card) or with default values (if the template is not yet associated with a particular card). The program permits you to print single or double sided badges.

1 - From the Card, Visitor or Daypass window, click the **Preview badge** button.

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

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

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

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

Cards Definition

Cards are defined by the following properties: card number, card user name, card type, access level and status (valid, invalid, pending, lost/stolen or expired). If you have enabled the **Use card multiple format**

option in the Card format dialog (see **Defining a Card Display Format**), you will be able to change the card format for each card individually from the Card dialog. This option allows more flexibility in assigning multiple cards to the user or in assigning user cards for sites equipped with different reader technologies. In other words, when creating a new card for a user, the operator will be able to select a card format directly in the Card dialog, according to the reader type used in the area where the user will be accessing the building. If you have enabled the **Enhanced user management** feature in the System parameters dialog (see **Credentials Parameters**) , card definition will be slightly different. In this type of environment, EntraPass allows for the creation of a user card with no number assigned to it. In both cases, cards will be defined by: card user name, card type, card access level and status (valid, invalid, pending, lost/stolen). Card records can be searched, sorted and deleted.

An activity report icon on the toolbar becomes available when you select a card. Use this icon to generate a quick report based on time parameters. The report contains the following information on the user's card: date and time, event message, card number, and many description columns. For more information on the report options, see **Previewing reports**.

Icon	Description
	Activity report: this generates a last transactions report based on the time parameters you enter. On completion of the report, EntraPass generates an event with details of who requested the report, and for what user.

Issuing a New Card

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

*NOTE: If you enabled the Enhanced User Management, move to the next section to see **Issuing a New Card in Enhanced User Management Environment**.*

2 - Click the **New** button (first button) 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 card holder’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 template 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 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 **Card Type Definition**.

*NOTE: From the Card type window, 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 on the upper right-hand side of the Card dialog.

7 - Fill out the **Card Information 1 to 20** fields. These are user definable fields. They are used to store additional information regarding the cardholder. For example, you could use Card Information 1 to store the employee number; Card Information 2, Department where the employee works; Card Information 3, employee address, etc. Later, card information fields will be used to index reports, customize cardholder lists, etc.

NOTE: The information field labels are editable. 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** button.

Issuing a New Card in Enhanced User Management Environment

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

2 - Click the **New** button (first button) in the toolbar. The **Card user name** field is enabled to enter the card holder's name. You can enter up to 50 characters.

3 - Click **Save** .

4 - Double-click on the **Card type** field to open the **Card type** window. 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 **Card Type Definition**.

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

5 - Click on the **Card number** tab, double-click on **Card #1** if you want to change the label.

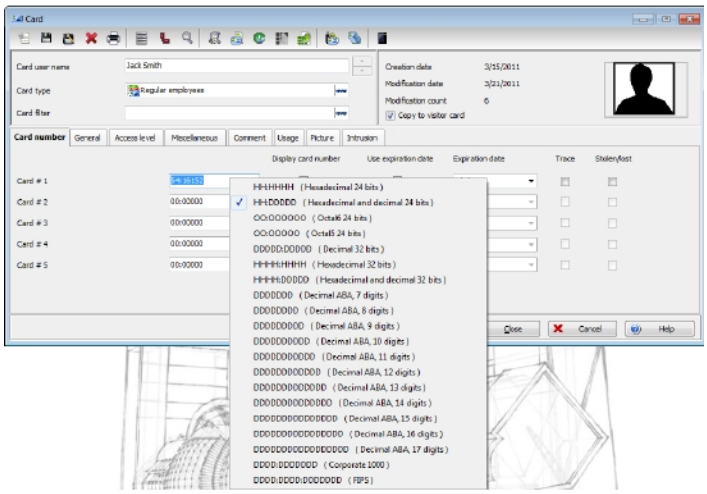
6 - Enter the **Card number** .

- If EntraPass was previously configured for **Multiple Card Format** , you can modify the card format by right-clicking the **Card number** field, see **Defining a Card Display Format** to enable the multiple card formats and select a new default card format for Card #1 to Card #5 . The default card format is HH:DDDDD (Hexadecimal and decimal 24 bits).

*NOTE: The **Access Level** will apply to the user which means all 5 cards.*

- When the **Multiple Card Format** is enabled: A list of all card formats will be displayed when you right-click in the card number field.

- When a card format has been defined by the system administrator, the card format (the one in use) has a check mark next to its description.



7 - As an option, you can assign the **Card number** immediately.

8 - If your access rights allow it, you can decide to **Display card number** or not, then the user card number in reports and message lists in the EntraPass workstation s .

NOTE: The system automatically displays the Creation date, the Modification date and the Modification count information on the upper right-hand side of the Card dialog.

9 - Check the **Use expiration date** option and select the corresponding date.

10 - 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.

11 - Check the **Stolen/Lost** option, if the card has been stolen or lost. The card will not be functional anymore.

12 - Repeat Steps 5 to 11 for Card #2 to Card #5, if applicable. The selections can be different for the 5 cards.

Card audit trail

Use the Card audit trail icon to view who made changes, and when the changes occurred on a card.

To provide access to the Audit trail functionality, you must give permission to the operator to use **Audit** in the **System** group, for more information, see **Security level**.

1 - Click **Users**, click **Card**, and select a cardholder from the **Card user name** list.

2 - To open the **Audit** window, in the toolbar, click the **Audit trail** icon.

The **Audit** window contains two tables the first table contains the following card information:

- **Color coded column**: indicates if the card was created, modified, or deleted.
  - Green: **Create**
  - Blue: **Modify**
  - Red: **Delete**
- **Date and time**: the date and time an operator created, modified, or deleted the card.
- **Operator**: the name of the operator who made the change.
- **Count**: the number of fields that were changed.

The second table contains the following card information:

- **Reference type**: the connection, site, or gateway connected to the card that changed.
- **Reference**: the item the change references.
- **Field name**: the name of the GUI field.
- **Old value**: the value before the change occurred.
- **New value**: the value when the system saved the change.
- **Field description**: description of the field name.

To access the following column options, click the **Filter** icon on the upper left of the table.

- **Data type**: the database data type:
  - **Time**
  - **Integer**
  - **Object**
  - **Components**
- **Table name**: the database table name.

*NOTE: Define the results based on the amount of records, or by date. For more information see, **Server logs** in **System parameter.***

To access the context menu, select a table entry, and right-click. The following options are available:

- **CSV export selected**: export the selected entry of the card audit trail to a CSV format file.
- **CSV export all**: export the entire content of the card audit trail to a CSV format file.
- **View old value**: view a window with the value before the change.
- **View old value parent**: view a window of the parent of the selected component with the value before the change.
- **View old value link**: view a window representing a link to the component with the value before the change.
- **View new value**: view a window with the value after the change.
- **View new value parent**: view a window of the parent of the selected component with the value after change.
- **View new value link**: view a window representing a link to the component with the value after the change.

Quick Access to Door List per Card

This feature allows to quickly and conveniently display the list of doors with an associated schedule for all access levels of the selected user.

1 - From the **Users/Card** menu, click the **Door access list** button:

The information is displayed over five columns:

- Gateway/connection button
- Gateway/connection description
- Door description
- Schedule description

NOTE: This information can be exported to a CSV file for printing and report purposes.

The same information is also available from the View card information window by clicking the Door access list button:

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.

1 - Type required changes into specific fields in the Card window and click the **Save as** button. This feature allows you to create a new card under a new card number.

2 - Enter the new card number in the **New card number** field.

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

Issuing Cards Using the "Batch Load" Feature

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

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

2 - From the **Door** drop-down list, select the door that will be used to read the cards.

3 - Check the following options:

- **Refresh an access granted** : if this option is checked, each time an access is granted the information displayed will be refreshed with data relative to the card.

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

NOTE: When this option is selected, the first card presented to the door reader will be saved only when presenting a second card or by pressing the save button.

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

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

Viewing and Verifying PINs

EntraPass enables you to view and validate each configured cardholders’ PINs in the Card and Visitor windows.

Viewing Cards Assigned the Same PIN

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

2 - From the **Card** or **Visitor** window, click the **List of PIN owners** button.

3 - Enter the PIN number you wish to validate and click OK. A list containing all operators that have a PIN number will be displayed on the screen.

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

Card Handling

Editing a Card

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

Finding a Card

You can perform two types of card searches from the Card dialog toolbar:

- Find the card information
- Find archived card information

*NOTE: You can also type a user name into the **card user name** field. When you begin to type an auto-complete will be displayed to help you find existing card user names.*

*NOTE: For more information on how to search information in EntraPass, see **Finding Components**.*

Deleting a Card

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

1 - Locate the card you want to delete.

2 - Click the **Delete** button, 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 under the **General** tab according to your organization requirements. These fields can contain any information. They can be used as edit boxes or drop-down lists.

1 - In the Card definition dialog, select any card, then double-click the **Card information** label under the **General** tab. The system displays the **Change labels** window .

2 - Select the field you want to modify on the left, and enter the name in the field on the right. If your system operates in two languages, two fields will be available to enter the field name in both languages. For example, if you want to rename Card Information 1 to Employee number , double-click the **Card Information 1** label and enter the new name in the field(s) on the right.

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 that this field is not left empty.

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.

NOTE: The operator can make a search based on any of the 40 fields of card information.

Cardholder Access Levels Assignation

An access level must be assigned to each card. Access levels determine where and when the card will be valid. The access level allows the cardholder entry to selected locations during specified schedules. For information on defining access levels, see **Access Levels Definition**.

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.

Assigning Additional Access Levels (Multi-site gateway only)

Using the KT-400, KT-400 rev1, and KT-1 up to five total access levels per user/connection are possible.

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

A small box in the far right column indicates the connection has controllers which accept multiple access levels. If the box is black, no additional access levels have been added. If the box is green, at least one additional access level has been assigned. If the box is yellow, the access level has doors from legacy controllers, which prevent additional levels to be assigned.

2 - Select the desired Gateway or connection by clicking the small box in the far right column. The Additional access levels window will appear with the different Gateways and Connections.

3 - From the Additional access levels window, additional access levels can be assigned.

NOTE: If there is a warning exclamation sign in the right column beside the Access level, there are controllers associated with access level which do not support additional access levels, such as the KT-100, KT-200 and the KT-300.

Assigning an Access Level to a Cardholder

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

2 - Click the **Card access group** button (displayed on the left of the connection or Gateway list) to copy information from a Card access group to a card. The **Gateway / connection** column The **Gateway / connection** 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 card holder's access to the doors of the selected connection. If you do not want this cardholder to have access to the door of this connection, 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.

Access Exception

Use the **Access exception** tab to link a specific schedule to a door.

1 - From the left panel, select a door.

2 - From the right panel, select a schedule using the drop-down list. Use the and buttons to add or remove doors from the list on the right.

3 - Under the Access column, choose between **Allow** or **Deny**.

NOTE: Only doors with an associated schedule will be saved.

Warning: *User list report does not take Access Exception into account.*

To enable the **Access level exception** feature, please refer to **Credentials Parameters**.

Card Options Definition

Use the **Miscellaneous** tab to specify and view card 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".

3 - Check the **Delete when expired** option (if applicable). This option can only be used with the **Use end date** option. When selected, the card information will automatically be deleted on the expiry date (using the end date and hour 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.

5 - **Editable PIN number**: The operator can enter the number of digits needed by the reader/keypad to grant access (see **Defining a Card Display Format** for more information).

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

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

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

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.

7 - Check the **Disable passback** option if you want the card to override the passback option when defined.

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

NOTE: If your are issuing a card for a cardholder with disabilities, check the Extended door access delay option. To enable this option in the system, you have to define appropriate delays in the Door definition. This option is also available when defining visitor cards.

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

8 - **Allow multiple-swipe (KT-400 and KT-1 only)**: Enable the multi-swipe action (see Card Multi-Swipe for more information).

Adding Comments to a Card

1 - From the **Card** window, 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.

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

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

3 - From the **Maximum card usage** 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 Maximum card usage , the Current card usage 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 when the maximum value is reached.

*NOTE: **Smartlink** must be running for this feature be available.*

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. For capturing signatures, signature pads such as Topaz are recommended.

Assigning a Picture from a File

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

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

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:

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.

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

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

- **Paste picture** : this option allows you to paste a picture from the clipboard. To use this option, you have to copy the picture, then paste it into the picture window.

NOTE: 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 capture** tab.

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

1 - Right-click the picture area.

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

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

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 **Badges Designing**.

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 options > Badge printer . If these buttons are enabled, you can preview and print the card holder'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.

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

2 - From the shortcut menu, make the appropriate choice:

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

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

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

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**).

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

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

3 - Click **OK** to paste the signature in the card window.

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).

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

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

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

- **Auto contrast** : this feature gives better contrast by intensifying lights and shadows: it makes the darks darker and the lights lighter. In general, this auto contrast feature gives a good result when a simple contrast adjustment is needed to improve an image's contrast.

- **Sharpen** : this feature provides more definition to blurry images by applying sharpening only when an edge is found.

- **Brightness** : this feature allows you to add light to the image by sliding towards the positive values.

- **Reset all:** this feature allows you to undo all the changes and to restore the original image.

4 - Click **OK** to close the **Picture** editing window.

5 - From the Badge layout pull-down menu, select a layout to associate with the card you have defined To define a badge layout, see **Badges Designing**.

Printing Badges

You may print badges, **visitor cards** and **daypasses** from a **Card** or from all **Badge preview** windows. The software is set up to let you print one single or double-sided badges.

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

Selecting a Badge Printer

1 - From the EntraPass Workstation window, select the **Options** toolbar, then click the **Printer Options** button.

2 - From the **Printer options** window, select the **Badge printer** tab.

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

3 - Check the **Badge printer** option to indicate to the system that a badge printer is selected. If the **Badge printer** option is checked, the Print badge and Preview badge are displayed in windows where you can print badges (Card, 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** window allows you to preview a badge layout with card information (if the badge layout is associated with a card) or with default values (if the template is not yet associated with a particular card). The program permits you to print single or double sided badges.

1 - From the Card, Visitor or Daypass window, click the **Preview badge** button.

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

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

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

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

Creating a New Import/Export Pattern

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

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

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

3 - To move an available field to the **Import / Export fields** area, double-click the item in the **Available fields** area, or select the item and use the **left** and **right hand** buttons. Once you select the fields, use the **red Up / down** arrows to organize information, this indicates how to arrange the information in the CSV file.

NOTE: The card number must always be selected for every pattern including a specific card. For example, if you select the field ***Card #3 - Stolen/Lost*** *, you must also select the field* ***Card #3 - Card Number*** *.*
If you select the Unique ID field, you can import without a card number. You can also delete users without a card number.

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 "-". Field separators can be: tab, space, comma, semicolon (;) and other.

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. Other date formats are:

- MM/DD/YYYY
- DD/MM/YYYY
- YY/MM/DD
- MM/DD/YY

- DD/MM/YY

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

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

9 - Enter the pattern name, then click **OK** . The system automatically returns to the Export/Import CSV file window. The pattern you have just created is displayed in the **Available patterns** list.

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

Creating a Visitor Card When Creating a New Card

1 - Select the **Card** button from the Users toolbar. 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.

CSV Files Import and Export

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

- Your company has a new database: instead of having to reprogram all the information already available in the card database, the system administrator could export the data contained in the card database (names, departments, card numbers, etc.) into a CSV file that can be imported into the target database.

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

To Import/Export card information, you may use Kantech pre-defined patterns or you may create your custom patterns.

Using a Predefined Pattern

Two patterns are available: the EntraPass (1,2,3) and the WinPass64 model. You may use the template "as is" or you may edit it.

1 - From the **Users** toolbar, select the **Import/Export CSV file** 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 pattern** button if you want to edit the pattern.

Creating a New Import/Export Pattern

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

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

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

3 - Double-clicking on the **available fields** or using the **left** and **right hand** buttons moves the field back and forth. Once the fields are selected, you can use the **red Up / down** arrows to organize information (this will indicate how information will be arranged in the CSV file).

*NOTE: The card number must always be selected for every pattern including a specific card. For example, if you select the field **Card #3 - Stolen/Lost** , you must also select the field **Card #3 - Card Number** .*
If you select the UniqueID field, you can import without a card number. You can also delete users without a card number.

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 "-". Field separators can be: tab, space, comma, semicolon (;) and other.

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. Other date formats are:

- MM/DD/YYYY
- DD/MM/YYYY
- YY/MM/DD
- MM/DD/YY
- DD/MM/YY

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

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

9 - Enter the pattern name, then click **OK** . The system automatically returns to the Export/Import CSV file window. The pattern you have just created is displayed in the **Available patterns** list.

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

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.

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

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

3 - From the **Available patterns** list (left-hand pane), select the pattern you want to use when exporting cards. If necessary, you may edit the pattern so that it matches the target application pattern, else, you may create a new one. (For more information on how to create a pattern, see **Creating a New Import/Export Pattern**).

4 - For the **Transaction file, click on the three-dot** , then 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 to the Import / Export CSV file window.

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

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

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

NOTE: The Transaction file field shows the target file name and location. By default, the export file is saved in the specified folder (Exportdata, in this example). The status bar (lower part of the window), shows the number of imported cards (1, in this example). The default name is YYYYMMDD.csv. You can open the target file with NotePad for instance.

Importing Cards

1 - From the **Users** toolbar, select the **Import/Export CSV File** button. The Import / Export CSV file dialog will display on screen.

2 - In the **Select Operation** drop-down list, select Import.

3 - Click the **Available patterns** button to select the pattern that will be used to import the cards information (for more information on how to create a pattern, **Creating a New Import/Export Pattern**).

4 - For the **Transaction file, click on the** three-dot, browse your hard drive to the CSV file that contains the data to import into the card database **.**

5 - Once the file has been selected, click **Open** . You will return to the Import / export CSV file window.

6 - If no errors are present (or once you have corrected errors), click **Import** to complete the operation.

NOTE: The system scans the file to be imported; then it displays the results using a colour code. Each entry is identified by a colour 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.

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.

1 - Click the **Import or Export** button to start the transaction (the following example illustrates a case of importing CSV data). The lower part of the window displays the number of cards in the list.

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

2 - Click the **Import** button.

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

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

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

5 - In the Import/Export CSV window, double-click the pattern you have used for the Import transaction (Custom, in the example above).

6 - From the **Field separator** drop-down list, select **Comma** as the field separator, then click **OK.** Data in the **Card number** field indicates that the import transaction will be successful.

Customizing Card Information Fields

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

1 - In the Card definition dialog, select any card, then double-click the **Card information** label under the **General** tab. The system displays the **Change labels** window .

2 - Select the field you want to modify on the left, and enter the name in the field on the right. If your system operates in two languages, two fields will be available to enter the field name in both languages. For example, if you want to rename Card Information 1 to Employee number , double-click the **Card Information 1** label and enter the new name in the field(s) on the right.

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 that this field is not left empty.

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.

Day Passes Definition

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). You can also use an existing day pass to create a new one.

Creating a Day Pass

1 - From the **Users** toolbar, select the **Daypass** button. The Daypass window appears.

2 - You can fill out the fields or browse the card databases to the desired card.

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 **Creating a Visitor Card When Creating a New Card**. The Picture tab allows you to display the cardholders picture and signature as well as to preview and print badges.*

Creating a New Day Pass Using the "Save As" Feature

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

1 - From the **Users** toolbar, select the **Daypass** button. The Daypass window appears.

2 - To locate an existing card, click the binoculars and select the card you want to duplicate.

3 - Type required changes into specific fields and click the **Save as** button.

4 - You will be prompted for a new card number.

Issuing a New Card in Enhanced User Management Environment

*NOTE: See **Credentials Parameters** for more details on how to enable the **Enhanced User Management** environment.*

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

2 - Click the **New** button (first button) in the toolbar. The **Card user name** field is enabled to enter the card holder's name. You can enter up to 50 characters.

3 - Click **Save** .

4 - Double-click on the **Card type** field to open the **Card type** window. 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 **Card Type Definition**.

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

5 - Click on the **Card number** tab, double-click on **Card #1** if you want to change the label.

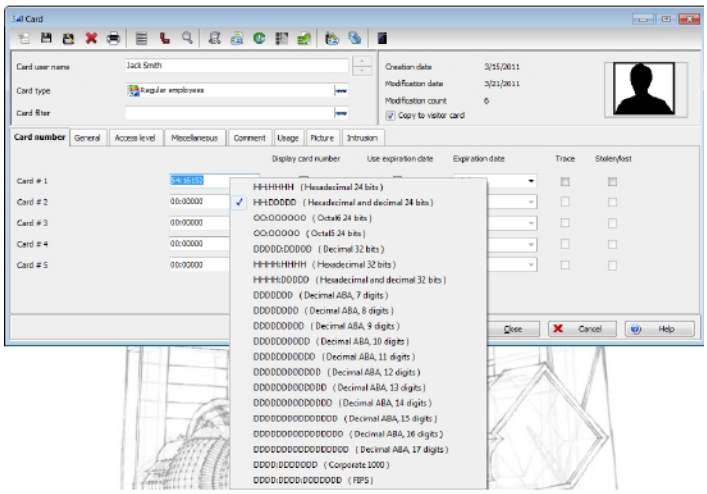
6 - Enter the **Card number** .

- If EntraPass was previously configured for **Multiple Card Format** , you can modify the card format by right-clicking the **Card number** field, see **Defining a Card Display Format** to enable the multiple card formats and select a new default card format for Card #1 to Card #5 . The default card format is HH:DDDDD (Hexadecimal and decimal 24 bits).

*NOTE: The **Access Level** will apply to the user which means all 5 cards.*

- When the **Multiple Card Format** is enabled: A list of all card formats will be displayed when you right-click in the card number field.

- When a card format has been defined by the system administrator, the card format has a check mark next to its description.



7 - As an option, you can assign the **Card number** immediately. If you are using the EntraPass Web, you can leave the field empty and assign the card number at a later time.

8 - If your access rights allow it, you can decide to **Display card number** or not, then the user card number in reports and message lists in the EntraPass workstation s .

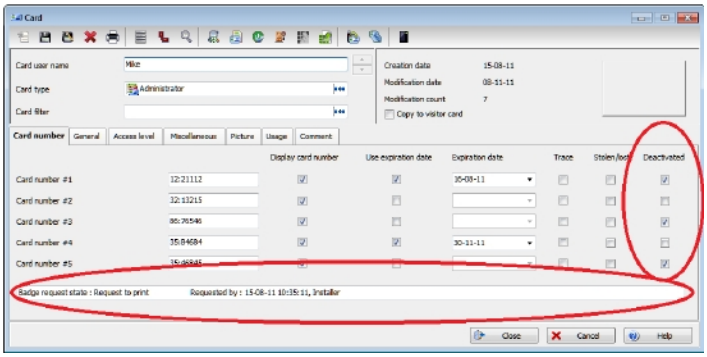
NOTE: The system automatically displays the Creation date, the Modification date and the Modification count information on the upper right-hand side of the Card dialog.

9 - Check the **Use expiration date** option and select the corresponding date.

10 - 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.

11 - Check the **Stolen/Lost** option, if the card has been stolen or lost. The card will not be functional anymore.

12 - Repeat Steps 5 to 11 for Card #2 to Card #5, if applicable. The selections can be different for the 5 cards.



Issuing Cards Using the Batch Load Feature

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

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

2 - From the **Door** drop-down list, select the door that will be used to read the cards.

3 - Check the following options:

- **Refresh an access granted** : if this option is checked, each time an access is granted the information displayed will be refreshed with data relative to the card.

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

NOTE: When this option is selected, the first card presented to the door reader will be saved only when presenting a second card or by pressing the save button.

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

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

Last Transactions Display

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

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

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

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

Viewing the Last Transaction

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

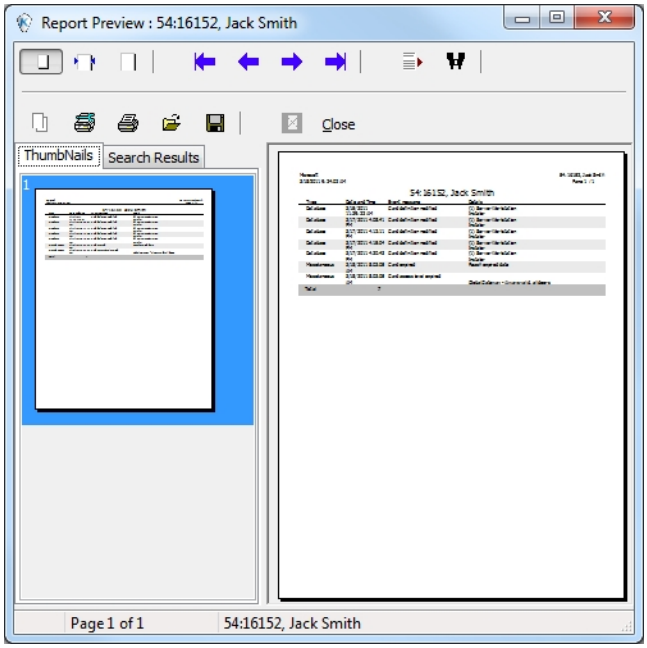
- **Type:** Displays the event category.
- **Date and time:** Displays the date and the time stamp of the event message.
- **Event message:** Displays the event message that was sent to the server (and to the authorized EntraPass workstation) when this event occurred. This is the same message as in the 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 column lists the EntraPass applications from which the card was modified as well as the operator name.

- **Refresh:** This button can be used to refresh the window with new transactions as they happen. As cardholders generate events, new information is available.

- **Parent:** To view the parent component of a selected component. For more information, see **Basic Functions**.

- **Print:** Use this button to print an exact copy of the window. For more information, see **Basic Functions**.

- **Preview** : The **Preview** button request the selection of a printer and then displays the **Report Preview** dialog.



Quick Access to Door List per Card

This feature allows to quickly and conveniently display the list of doors with an associated schedule for all access levels of the selected user.

1 - From the **Users/Card** menu, click the **Door access list** button:

The information is displayed over five columns:

- Gateway/connection button
- Gateway/connection description
- Door description
- Schedule description

NOTE: This information can be exported to a CSV file for printing and report purposes.

The same information is also available from the View card information window by clicking the Door access list button:

Tenants List

The tenant is a resident in an apartment building or an employee in a company. The tenant can grant access to a visitor. Tenants list can be created in EntraPass to be used with the KTES.

Creating a New Tenants List

1 - From the **Users** toolbar, select the **Tenants list** button.

2 - Edit the **Tenants list** name. Default value is **New tenant list** .

3 - Select the **Tenant ID length** (1 to 5). Default value is 4.

4 - Select the **Tenant PIN length** (4 to 6). Default value is 4.

5 - Select the **Wiegand display format on LCD** . Possible values are:

- Hexadecimal 24 bits
- Hexadecimal and decimal 24 bits
- Hexadecimal 32 bits

- Hexadecimal and decimal 32 bits
- Decimal ABA 8 digits
- Decimal ABA 10 digits

Default value is Hexadecimal 32 bits

Adding New Tenants to the List

1 - Select the **General** tab.

2 - Click the **Add** (**+**)button. You can use the **Legend** button to display the actual status of each tenant.

3 - Configure the tenant parameters:

- **Tenant name** : Enter the tenant's name (20 characters maximum) . Default value is **New tenant** .
- **Tenant ID** : Enter the tenant's ID. The tenant's ID is an identification code consisting in a 1 to 5-digits number a visitor can use to call a tenant. The number of digits available for an ID has already been configured when the list was created. Default value is 0000.
- **First phone number** : Enter the first phone number. The first phone number is used when a visitor select the tenant from the KTES directory. If no phone number is entered, the tenant cannot be called by the KTES system and will not be displayed in the KTES directory either (15 digits maximum). Default value is empty.
- **Second phone number** : Enter a second phone number. The second phone number is used by the KTES to contact the tenant when there is no answer to the first number (15 digits maximum). Default value is empty.
- **PIN** : A Personal Identification Number (**PIN**) consists of a 4 to 6-digits number configured for each tenant. The number of digits available for a PIN has already been configured when the list was created. Default value is 0000.

- **Access schedule**: Enter the access schedule. For security reasons, an **Access Schedule** should be configured in order to link a schedule with the tenant access rights. A tenant can access the building according to specific time, days and holidays defined in the system. Default value is **Always valid**. Refer to see **Schedules Definition** for more information on schedules definition.

- **Tenant admin level** : Select the administration level for the tenant (Installer, Owner, Maintenance or Tenant). Default value is **Tenant** .

- **Tenant language**: Select the default language used by the KTES for the tenant (System, English, French, Spanish, Custom). Default value is **Default** (for more information on the system language, see **Kantech Telephone Entry System (KTES) Configuration**.

- **Disabled Tenant** : A **Disabled Tenan** t status allows the activation of a relay and/or the generation of an alarm. Default value is deselected (**enabled**).

- **Trace** : The trace option allows the activation of a relay and/or the generation of a traceability event. Default value is deselected (**not traced**).

- **Hide tenant** : This option is used if you want the current tenant's name to be displayed or hidden. Default value is deselected (**displayed**).

- **Extended door access delay** : The extended delays correspond to the additional time lapse a door should stay unlocked and could be kept opened (for instance, a handicapped person could need more time to access to a building). Default value is deselected (**no extended delay**).

- **Extended ring** : The system can allow an extended number of rings in order to give more time for the tenant to answer. Default value is deselected (**no extended ring**).

4 - Select the **Advanced options** tab.

5 - Set the **Tenant validation date** :

- **Start date** : The **Start date** is the date from which the tenant can access the system. Enter the date in the field (mm/dd/yyyy) or click on the **calendar** button to select a date. Default value is empty.

- **Use end date** : The **end date** is the date at which the tenant cannot access the system anymore and its status is no more valid. Select the checkbox to enable the end date. Default value is deselected (**no end date used**). Enter the date in the field (mm/dd/yyyy) or click on the calendar button to select a date. Default value is empty.

6 - Set the **Do not disturb** option. This functionality is used to place the tenant in a "Do not Disturb" (DnD) status if the selected schedule is active. You would check the **Hide tenant** check box if you would like the tenant to remain hidden from the list or for search option while in the DnD status.

7 - The **Call second phone number** option enables the use of a second phone number immediately (bypassing the first number) when the schedule is active. If you would like to use the second phone number only when the selected schedule is active, you would need to make sure the **Call second phone number only on schedule** box is checked.

8 - Set the **Wiegand interface for access granted** :

- **Tenant card number** : A 64-bit number associated to each tenant. This number is used by the tenant to get access from the KTES.

- **Card holder for access granted (not available in EntraPass KTES Edition)** : This card holder's number will be the first card number to be used by the tenant to get access from the KTES.

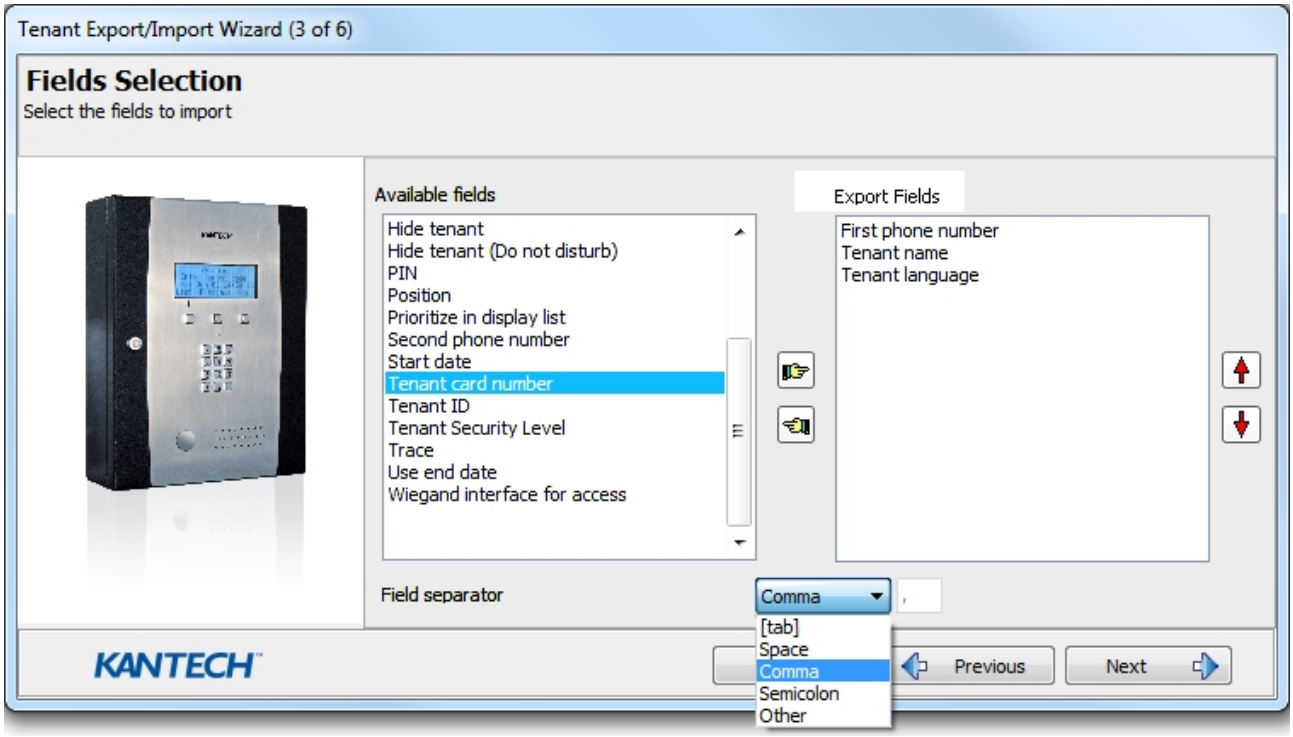
Importing a Tenant List

In order to ease the process of importing tenant lists, an automated procedure has been implemented to guide you through the various steps.

Step 1: Click the **Import** button to run the **Tenant Export/Import Wizard**.

Step 2: Click the **Next** button and select a CSV format source file.

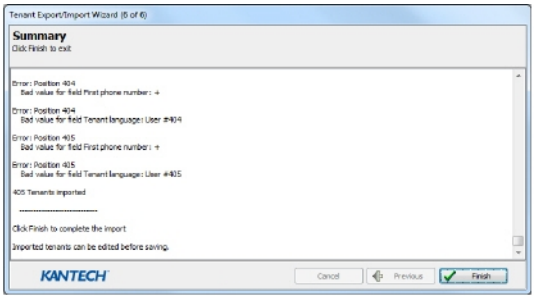
Step 3: Click the **Next** button and choose the field to be imported from the list at right. Use the left and right "hand" buttons to add or remove data fields. A different field separator can also be selected (default is Comma).



Step 4: Click the **Next** button and select the tenants to be imported.

Step 5: Click the **Next** button and then the **Import** button to complete the operation.

Step 6: Click the **Next** button to see a summary of the imported data.

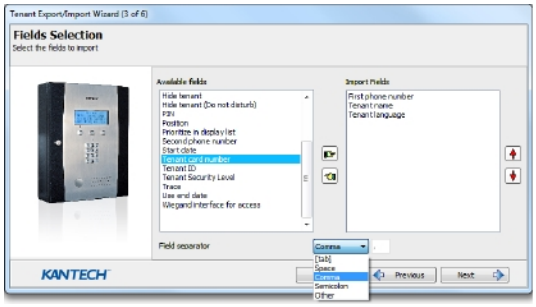


Exporting a Tenant List

As for the importation, an automated procedure has been implemented to guide you through the various steps of exporting a tenant list.

Step 1: Click the **Export** button to run the **Tenant Export/Import Wizard**.

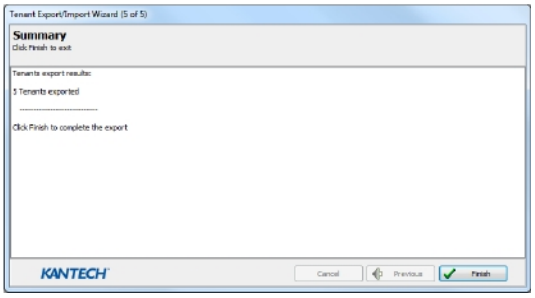
Step 2: Click the **Next** button and choose the field to be exported from the list at left. Use the left and right "hand" buttons to add or remove data fields. A different field separator can also be selected (default is Comma).



Step 3: Click the **Next** button and select the tenants to be exported.

Step 4: Click the **Next** button and select a CSV format destination file. Click the **Export** button.

Step 5: Click the **Next** button to see a summary of the exported data.



To Add 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,

- Bar codes,
- 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.

To Modify Picture Properties

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

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

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

3 - You may select another image from file or modify the image properties:

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

Validating Card Access

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

1 - From the Card window, select a card.

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

3 - Select a site/gateway/connection from the **Site/Gateway/Connection** list .

4 - 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).

Visitor Cards Definition

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.

Creating a Visitor Card When Creating a New Card

1 - Select the **Card** button from the Users toolbar. 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.

Creating a Visitor Card Using the Card Template

1 - Select the **Visitor** button from the **Users** toolbar.

2 - Enter the required information.

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

Schedules Definition

A schedule indicates when the system will execute certain operations such as automatically unlocking doors, permitting access to employees, running automatic reports, monitoring inputs, etc. It also determines when events are to be acknowledged or when to activate relays controlling different functions (lighting, heat, etc.). You can use the same schedule in different menus, but it is recommended to create a different schedule for each application, because it is much easier to modify a particular schedule without affecting other applications.

Each schedule is composed of four intervals. Each interval has a starting and ending time. Each of these intervals can be individually selected for the seven days of the week, and for 4 holidays. EntraPass gives you the possibility of programming 99 schedules per gateway and an unlimited number of system schedules. To do so, you must activate the **Upgrade to advanced schedule capability** option in the **System parameters** dialog (Options toolbar > System parameters > Server) .

*NOTE: For more information, please see **System Parameters Configuration**.*

EntraPass supports two groups of schedules :

- **System schedules** : System schedules for global functions such as operators login schedules and video triggers. These are not loaded in controllers.
- **Multi-site schedules** : These are defined per connection. You can define 99 schedules per connection for such purposes as: power supervision (controllers), unlock schedule (doors), Rex schedule (doors), activation mode (relay), monitoring schedule (input).

Definition

Schedules Definition

If you are assigning or defining schedules, make sure that you are selecting the proper category for this schedule. For example, if you are assigning or defining a system schedule (for workstation, operators, alarm notifications, video triggers) this schedule will be available for selecting components of this category. If you are selecting a schedule for physical components such as controllers, doors, inputs, their schedules will be grouped by site if you are using a multi-site Gateway . If you have defined two sites in your system, there will be two separate groups of schedules for each site. You can define up to 99 schedules for each site.

Defining a Schedule

1 - From the EntraPass main window, click the **Definition** tab. Then click the **Schedule** button.

*NOTE: If you have checked the Upgrade to advanced schedule capability option (System parameter > Server > Schedule tab), the Gateway/Site drop-down list appears for selection. From the Gateway/site drop-down list, select a **Site** or a System schedule (applicable to system components such as video triggers and operator login).*

2 - From the **Schedule** drop down list, select the schedule you want to modify or select the schedule applicable to the category selected in previous step, or click the **New** button to create a new one.

3 - Assign a name (or modify an existing one) to the schedule. It is recommended to choose a meaningful name.

4 - You can click the **Holiday** button in the toolbar to view the list of holiday that are defined in the system.

NOTE: EntraPass supports four types of holidays.

5 - **Specify the Start time** : This is the scheduled time when the interval becomes valid. It will become invalid when the end time has been reached.

6 - **Specify the End time** : This is the scheduled time when the interval is no longer valid.

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

7 - Check the **Days of the week** during which this schedule interval will be valid. To do this, click in the checkbox below each day.

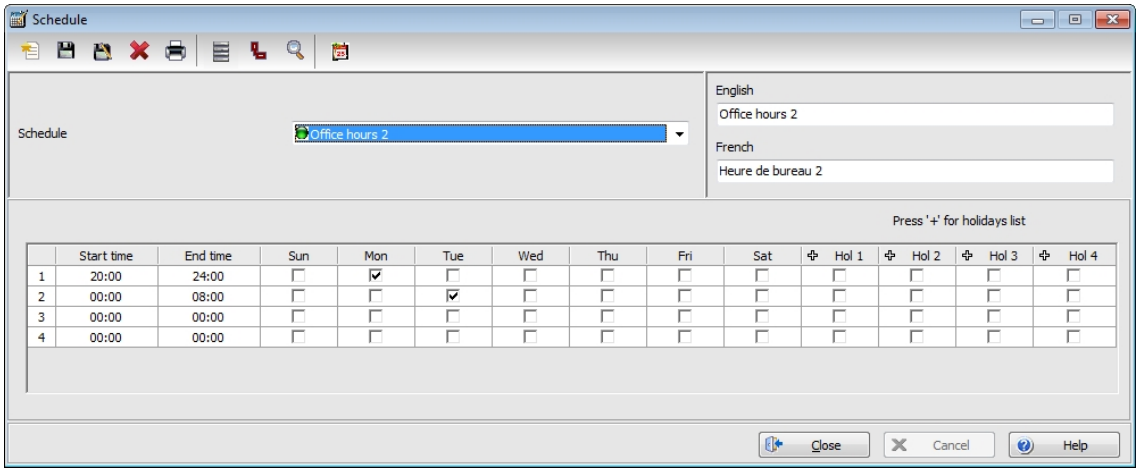
8 - Check the **Holiday type** (**Hol1, Hol2,** etc.) column checkbox if you have defined four holidays in the Holiday definition menu and you want this interval to be valid during a holiday. You can also click on the + sign to display a calendar for the next 12 months showing holidays in one of the three colours identified in the legend.

*NOTE: The legend is different from the one used to define holidays. See **Holiday Definition** for more information.*

To Create 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.

Extended Schedule

This feature allows increasing the number of schedule intervals to 20.

NOTE: Schedules with 20 intervals in stand-alone mode can be used with KT-400 and KT-400 V1 controllers only.

Floors Definition

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

1 - In the **Definition** tab, click the **Floor** button.

2 - From the **Site/Gateway/Connection** drop-down list, select the Site/Gateway/Connection 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** button to create a new floor group.

4 - Assign a meaningful name to the floor, then click the **Close** button. The system prompts you to save.

Graphics Definition

A graphic corresponds to the secured area of the system where components (EntraPass applications, controllers, inputs, relays, etc.) are located on a connection. With graphics, operators can easily view the exact location of a component installed on a connection, or the status of components and devices such as doors, contacts, motion detectors, controllers, panels assigned to the graphic. Operators can perform manual operations directly from the displayed component (for example, locking/unlocking a door). Operators can execute tasks with or without confirmation. You can create as many graphics as you need. Each graphic can display up to 250 components including using live video as a background. You may also import graphics or maps from other programs in the following formats (BMP, EMF, WMF, JPEG, GIF, PCX, PNG, TIF or PCD).

NOTE: *EntraPass offers users four sample floor plans. You can customize them to suit your system needs. The sample floor plans are located at: C:\Program Files\Kantech\Server_ CE \Generaldata\Demobmp folder .*

Defining Components of a Graphic

1 - In the **Definition** tab, click the **Graphics** button.

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

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

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

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

NOTE: If the 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 button can be positioned on a graphic layout and its status can be retrieved by clicking on the video button. In addition to standard options, 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 the **Options** menu to display a pull down menu of drawing options. A check mark appears next to an option that is activated. **Show** hints provides the component's name (component's address and name) when you point your mouse cursor over that graphic.

- **Draw transparently** will place a transparent button on top of a background picture for a blended effect.
- **Draw frame** draws a frame around the component. **Frame colour** indicates the current frame colour and allows you to change the colour.
- **Auto display video view** lets you add a video view.
- Select **Edit background picture** to edit the background of the selected graphic. From this window you can modify the graphic's frame and background colour and add annotations.
- Select **Add live video as background** to have live video as background.
- Select **Add Web page as background** to have a Web page as background. Enter the **URL address** of the connection and press **Enter** on the keyboard, or click **Test** . The **Login** and **Password** are not required unless the Web page you want to access requires it. Click **Test** to see that the page is loading properly. Then, click **Save** .

- Select **Clear background** in order 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.

Designing the Background for the Graphic Window

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

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

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

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

- To insert shapes and text in the background image, select a rectangle, a circle, an ellipse, etc. in the toolbar, and drag and drop it in your background.

- To modify a shape you've just placed in the burgeoned window, right-click it to open the **Properties** dialog. and make the appropriate modifications (colour, position, etc.).

- You can setup the system to display the **Properties** dialog as you drop the shape into the design window. To do so, select the **Show properties on Drop** from the **Options** menu.

- To retrieve shapes that were previously saved to a disk, select the **Load annotations** option in the **Image** menu. When you add shapes to a graphic, you have the option of saving them as annotation on a separate file in order to retrieve them later.

- To save annotations on a separate file from your graphic, select the **Save annotations** option in the **Image** menu. You will be able to retrieve them for later use.

- To clear the shapes, select **Clear annotation** in the **Image** menu. If you save the graphic with the shapes, the shape become permanent.

- Use the **View** menu to define how the graphic will be displayed.

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

Assigning System Components to Graphic Icons

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

2 - Once you have positioned the component, and released the mouse button, the **Assign From** dialog will pop up on the screen.

3 - Select the system component you want to assign to the button on the screen.

4 - Click **OK** to go back to the previous window.

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

Printing System Components and Graphics

1 - From the **Definition** tab, click the **Graphic** button and select a graphic from the drop-down list.

2 - Click on the **Print** button from the **Graphic** dialog toolbar.

- Select the graphics to be printed using the checkboxes. You can also use the **Select all** or the **Clear all** buttons.

- Select **Print empty fields** to include the titles of the fields even if they are empty.

- Select **Print component references** to print the component reference numbers.

- Use the **Font** button to display the standard Windows Font dialog and modify the font attributes accordingly.

- Click on the **Preview** button to display a general view of the printing layout.

3 - Click on **Print** to send the graphic to the printer.

Holiday Definition

A holiday is treated differently than other days. It is recommended to program holidays at the beginning of the year; this helps to modify floating holidays for the current year (Easter, Thanksgiving, etc.). A holiday may be identified by a specific type (Hol 1, 2, 3, 4). The same day may be defined as a holiday at one connection, but as a regular day in another connection.

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

2 - To create a new holiday, select the **New** button.

3 - To create a global holiday, proceed with the holiday definition. If you want to define a holiday for a specific gateway/connection, select the gateway/connection from the drop-down list.

4 - Assign a name to the holiday.

5 - From the **Date** pull-down menu, select a the holiday date from the calendar.

6 - Check the **Recurring** option if this is the case for the holiday you are defining.

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

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

8 - Click on the + Holiday list button to display a calendar for the next 12 months showing holidays in one of the three colours identified in the legend.

9 - If the holiday is to apply to specific sites only, the **Selective Holiday** checkbox must be selected.

10 - Drag & drop system, sites or global gateways to the appropriate holiday case. You can also use the and buttons to move them.

NOTE: *The legend is different from the one used to define schedules. See* ***Schedules Definition*** *for more information.*

Trigger and Alarm (previously Event Trigger)

Create a New Trigger.

1 - From the **Definition** toolbar, select the **Trigger and Alarm** button and click the **General** tab.

2 - Click on **New** and enter a name for the trigger.

3 - Select a component from the **Component type** drop-down list.

4 - Select between **Single component**, **Trigger group** and **All components** as a trigger source.

5 - Click on the **three-dot** to select a door.

6 - Click on the **three-dot** to select a trigger schedule.

7 - To use an extended filter, select the **Use extended filter** option.

8 - From the **Event category selection** drop-down, select the type of events.

9 - In the **Trigger destination** section, click on the **three-dot** to select the **SmartLink** .

10 - Click on the **three-dot** to select a task (refer to **Task Builder Definition** for detail about task creation).

11 - To use a trigger value variable, check the **Use task variable** box and click on the **Variable** tab. Select the variable type #1 from the drop-down list and the variable type #2 if needed..

12 - From the **Events** tab, select events.

13 - Click the **Extended filter** tab.

14 - Click the **Add** button to add a new filter.

15 - Select a **Filter type** and a **Component filter**.

16 - Repeat the previous step for as many cards as required.

17 - Click on **Save** and **Close**.

Disable a Trigger

1 - From the **Definition** toolbar and select the **Trigger and Alarm** button.

2 - Choose an **Event Trigger** from the drop-down list.

3 - Check the **Disable trigger** box.

*NOTE: Alarm notification menu is only available when **Event Operator** mode is enabled.*

Create a new Alarm notification

1 - Click on the **Alarm notification** tab.
2 - Select an **Alarm schedule** to define when to treat a trigger as an alarm.
3 - Select the **Desktop popup schedule** to define when alarm notifications pop up on an operator's desktop.
4 - If you want the operator to acknowledge the alarm, select an acknowledge option from the drop-down list.
- **a - No acknowledge**. No acknowledge popup is displayed. The message is listed in the **Alarm Messages List**.
- **a - Acknowledge for all connected workstations**. An acknowledge popup messages is displayed on all online and logged on workstations.
- **a - Acknowledge for all connected and selected workstations**. An acknowledge popup messages is displayed on all online and logged on workstations selected in the **Selected Workstations** tab.
- **a - Acknowledge first, based on operator level**. EntraPass determines the highest acknowledge priority of all logged on operators. The acknowledge popup message is first sent to these operators. If the popup message is not acknowledged within the time defined in **Time-out acknowledge delay**, the popup message is sent to all online and logged on workstations.

a - **Acknowledge first, based on workstation level**. EntraPass determines the highest acknowledge priority of all logged on workstations. The acknowledge popup message is first sent to these workstations. If the popup message is not acknowledged within the time defined in **Time-out acknowledge delay**, the popup message is sent to all online and logged on workstations.

a - **Acknowledge first, based on operator and workstation levels**. EntraPass determines the highest acknowledge priority of all logged on operators and all workstations. The acknowledge popup message is first sent to the highest priority candidate. If the popup message is not acknowledged within the time defined in **Time-out acknowledge delay**, the popup message is sent to all online and logged on workstations.

5 - If you require the operator to add a comment on the alarm, select the **Mandatory comment** check box.

6 - Select the **API popup schedule** to define when alarm notification popups are active for third-party applications.

7 - Select the **Instruction** option to associate an instruction with the alarm.

8 - Select an **E-mail notification schedule** to send e-mails during an alarm. The e-mail recipients are defined in the **E-mail notification** box.

9 - Select the **Allow e-mail acknowledge** box to allows alarms to be acknowledged using e-mail. If this option is selected, e-mail recipients defined in the **E-mail notifications** box are sent a link to acknowledge the alarm. E-mail addresses must seperated by a semi-colon ";". The e-mail contains the date and time of the event, the event name, the details of the event and the instructions linked to the trigger (if defined).

*NOTE: Allow e-mail acknowledge requires a Web Service defined under at least one **Smartlink**.*

10 - Select the language from the drop-down list.

11 - Click on **Save** and **Close**.

Receiving notification e-mails for video triggers

When you configure an alarm notification for a video event, you must configure the e-mail notification schedule field. The component that triggers the event must have a camera or video view link in order to receive the notification e-mail containing the thumbnails. When an event trigger occurs, EntraPass sends an e-mail containing four thumbnail views of the event. If the device has multiple cameras attached, the first camera in the view is used. For the timing of the thumbnails, see the following steps:

1 - Five seconds before the event occurred.

2 - At the time of the event.

3 - Two seconds after the event.

4 - Five seconds after the event.

*NOTE: You must enable the **New event operator mode** to receive the thumbnails e-mail. Both e-mails use the task builder and alarm notifications to send the e-mails.*

Task Builder Definition

Minimum Requirements

The **Task Builder** and **Event Trigger** buttons will only display if the SmartLink component has been installed on a workstation and registered with the EntraPass server.

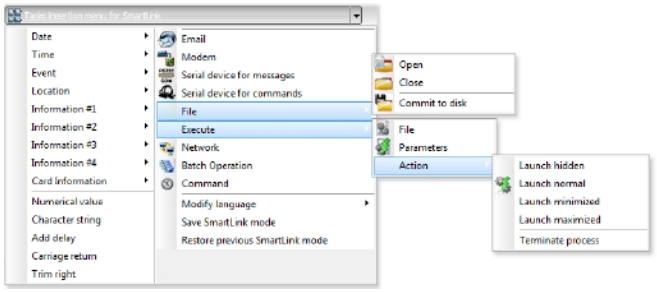
Task Builder Dialogs Description

1 - From the **Definition** toolbar, select the **Task Builder** button.

The **Task Builder** menu allows you to create SmartLink tasks. When you have a SmartLink application installed, the **Task insertion** menu for SmartLink button is enabled. It allows operators to send built-in task commands to the SmartLink.

NOTE: A new command has been added to SmartLink (BATCHMODIFY) allowing batch modifications to a group of cards. It is now possible to change parameters for a group of cards of the same type. Only the data fields indicated in the command will be modified. For more information on task commands, refer to your SmartLink Reference Manual DN1327.

2 - Click on the **Task insertion** menu for SmartLink button and a menu will be displayed, or use the **buttons** corresponding to the most common insertions.



NOTE: When creating SmartLink tasks, only commands that are written in the primary language are considered as valid commands. For more information on task commands, refer to your SmartLink Reference Manual, DN1327.

Options of the Task Insertion menu

Parameter	Description
Date	Insert a date in the task. Options are: **Year**, **Month**, **Day**, **YYYY/MM/DD** or **MM/DD/YYYY**
Time	Insert a time in the task. Options are: **Hour**, **Minute**, **Second**, **HH:MM:SS** or **HH:MM**.
Event	Insert event description in the task. You can select to display event name **Text** or **Number**.
Location	Insert the location where the task must take place. Options are: **EntraPass Application**, **Gateway** or **connection**.
Information #1 to 4	Insert event information. Options in the database are: **Index Number**, **Index Text**, **Component ID** and **Component Text**.

Parameter	Description
User Information	Insert card information in the task. Options are: **Card Number**, **Card User Name**, **Card Information #1 to #10** or **Comment**.
Numerical Value	Insert a number in the task.
Character String	Insert a string of characters (free text) in the task.
Add Delay	Insert a delay in 1/10 secs in the task.
Carriage Return	Insert a carriage return in the task.
Trim Right	Will delete the last character to the right of the task.
Email	To insert and email in the task that will be sent automatically when the event occurs.

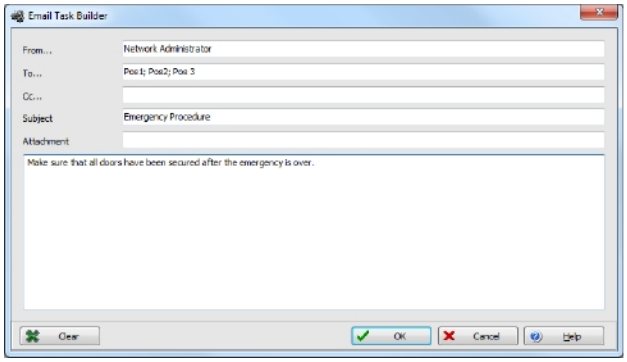
Parameter	Description
Modem	To insert a message in the task that will be sent automatically through a pager when the event occurs.
Serial Device for Messages	Select the **Serial Com Port** and **Baud rate** to send the message.
Serial Device for Commands	Select the **Serial Com Port** and **Baud rate** to send the command.
File	**File** opens the Select a file name dialog that allows you to locate a file (or create a new one) where all event information entered in the task will be logged when an event occurs. **Close** will close the file. **Commit to disk** will save the file to disk. This command will not close the file.

Parameter	Description
Execute	**File** opens the Select a file name dialog that allows you to locate the executable that will be used with the task command. **Parameters** open the Enter Character Strings dialog allowing you to type a string of characters that will be added to the task command. **Action** allows you to define how you want to launch the task (**Launch Hidden**, **Launch Normal**, **Launch Minimized**, **Launch Maximized** or **Terminate process**).
Network	Insert a **Network Tag**.
Command	Insert a **Command Tag**.
Modify Language	You can modify the command language to **English** or **French**.
Save SmartLink Mode	Insert in the SmartLink command to interrupt and place current SmartLink mode in the background (for example sending and email). This command must **always** be used with **Restore Previous SmartLink Mode**.

Parameter	Description
Restore Previous **SmartLink Mode**	Insert in the SmartLink command to restore the previous SmartLink mode. This command must **always** be used with **Save SmartLink Mode**.

Adding an Email to a Task

1 - Once you have selected an existing task or created a new one, click the **Mailbox button.** The **Email Task Builder** dialog will display on screen.



2 - Enter the your email address in the **From...** field.

3 - Enter the email address(es) where the message should be sent in the **To...** field. Each address should be separated by a semi-colon (;).

4 - If you wish to send a copy of this email to other people, enter their name in the **CC...** field.

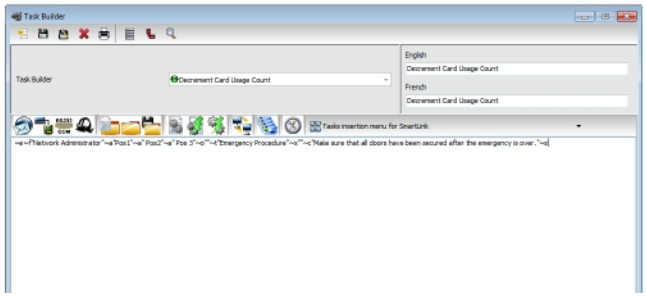
5 - Enter the **Subject** .

6 - If you want to attach a file to the email, enter the entire path to the file in the **Attachment** field. Each file must be separated by a semi-colon (;).

7 - Enter the message in the text area.

NOTE: Variables can be added to the email subject and body.

8 - Click **OK** to attach the email to the SmartLink task. The message will appear in the window.



Inserting a Pager Command in a Task

When building a task using SmartLink, EntraPass allows you to insert a command that will send a message to a paging system.

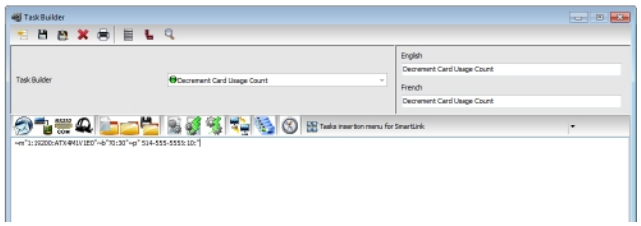
1 - Click the Modem button. The **Modem task parameters** dialog will display on screen.

2 - The **Modem serial port** parameter should already be setup.

3 - Enter **Dial information** such as the pager Phone number.

4 - Check the **Pager** options and enter the **Message** that will display on the pager (if the receiving pager has the option to display) and the **Delay before message (seconds)** will be sent to the pager. The time range value is 00:00 and 09:59 min.

5 - Click **OK** . The phone number and message will appear in the window :



Inserting Serial Device for Messages

1 - Click the **Serial device for messages** button. The **Serial com port** dialog will display on screen.

2 - Select the **Port Number** and the **Baud rate** .

3 - Click **OK** .

Inserting Serial Device for Commands

1 - Click the **Serial device for commands** button. The **Serial com port** dialog will display on screen.

2 - Select the **Port Number** and the **Baud rate** .

3 - Click **OK** .

Inserting a File

1 - Click the File (Open) button. The **Select a file name** dialog will display on screen.

2 - Enter the **file name** or browse to find the file.

3 - Click **OK** .

Executing a File

1 - Click the Execute (File) button. The **Select a file name** dialog will display on screen.

2 - Enter the **file name** or browse to find the file.

3 - Click **OK** .

Executing Parameters

1 - Click the Execute (Parameters) button. The **Enter character string** dialog will display on screen.

Entering a Network Tag

1 - Click the Network button. The **Enter network tag** dialog will display on screen.

2 - Enter the **network tag** . The range value is 0 to 999,999.

3 - Click **OK** .

Entering Commands

1 - Click the Command button. The **SmartLink Task Builder** dialog will display on screen.

2 - Select a component type from the **Component type** list.

3 - Select a command from the **Command list** .

NOTE: *The **toggle** command is only available with specific component types such as **Door** , **Input** and **Relay** .*

4 - Select a variable from the **Variables list** . There are three categories of variable that can be linked to a component type and a command.

- Message Value
- Trigger
- Card Information 1 to 10

Task Building Examples

The following procedures will involve each of the three variables that can be linked to a component type and a command.

Building a Task with a Message Value Variable

1 - From the **Definition** toolbar, select the **Task Builder** button.

2 - Click on **New** and enter **Decrement Card Usage Count** as the task name.

3 - Click on the **Command** button.

4 - From the **SmartLink Task Builder** window, select **Card** from the **Component type** drop-down list.

5 - Select **Decrement count usage** from the **Command list** .

6 - Select **Message Value** from the **Variable list** . The task displays at the bottom of the dialog. Click **OK** .

7 - The SmartLink task now displays in the text field.

8 - Click **Save** and close the **Task Builder** dialog.

9 - From the **Definition** toolbar, select the Event Trigger button.

10 - Click on **New** and enter **Decrement Card Usage** as the event trigger name.

11 - In the **Trigger source** section, select **Door** from the **component type** list.

12 - Click on the **three-dot** to select the **component** .

NOTE: You c an also select a group of components or all the components as a trigger source.

13 - In the **Trigger destination** section, click on the **three-dot** to select the **SmartLink** .

14 - Click on the **three-dot** to select **Decrement Card Usage Count** as the task.

15 - From the **Events** tab, select events.

16 - Click on **Save** and **Close** .

Building a Task with a Trigger Value Variable

1 - From the **Definition** toolbar, select the **Task Builder** button.

2 - Click on **New** and enter **Trigger value** as the task name.

3 - Click on the **Command** button.

4 - From the **SmartLink Task Builder** window, select **Relay** from the **Component type** drop-down list.

5 - Select **Toggle relay activation** from the **Command list** .

6 - Select **Trigger variable #1** from the **Variable list** . The task displays at the bottom of the dialog. Click **OK** .

7 - The SmartLink task now displays in the text field.

8 - Click **Save** and close the **Task Builder** dialog.

9 - From the **Definition** toolbar, select the **Event Trigger** button.

10 - Click on **New** and enter **Trigger value** as the event trigger name.

11 - In the **Trigger source** section, select **Door** from the **component type** list.

12 - Click on the **three-dot** to select the **component** .

NOTE: You can also select a group of components or all the components as a trigger source.

13 - Click on the **three-dot** to select **Always valid** as the **Trigger schedule** .

14 - Check the **Use extended filter** option.

15 - In the **Trigger destination** section, click on the **three-dot** to select the **SmartLink** .

16 - Click on the **three-dot** to select **Trigger value** as the task.

17 - Check the **Use task variable** option.

18 - From the **Events** tab, select the **Access granted** event.

19 - Click on **Save** .

20 - Click on the **Variable** tab.

21 - Select **Relay** for both as the variable type.

22 - Click on the **Extended filter** tab.

23 - Select **Card** as the **Filter type,** then select the **component filter** and both **variables** .

24 - Repeat Step 23 for as many cards as required.

25 - Click on **Save** and **Close** .

Building a Task with a User Information Variable

1 - From the **Definition** toolbar, select the **Task Builder** button.

2 - Click on **New** and enter **Toggle Relay via User Information** as the task name.

3 - Click on the **Command** button.

4 - From the **SmartLink Task Builder** window, select **Relay** from the **Component type** drop-down list.

5 - Select **Toggle relay activation** from the **Command list** .

6 - Select **User Information 1** from the **Variable list** . The task displays at the bottom of the dialog. Click **OK** .

7 - The SmartLink task now displays in the text field.

8 - Click **Save** and close the **Task Builder** dialog.

9 - From the **Definition** toolbar, select the **Event Trigger** button.

10 - Click on **New** and enter **User Information** as the event trigger name.

11 - In the **Trigger source** section, select **Door** from the **component type** list.

NOTE: You can also select a group of components or all the components as a trigger source.

12 - Click on the **three-dot** to select the **component** .

13 - Click on the **three-dot** to select **Always valid** as the **Trigger schedule** .

14 - In the **Trigger destination** section, click on the **three-dot** to select the **SmartLink** .

15 - Click on the **three-dot** to select **Toggle Relay via User Information** as the task.

16 - From the **Events** tab, select the **Access granted** event.

*NOTE: Make sure the **User Information** is entered correctly. Check below for an example from the **Users** toolbar > **Card** Dialog > **General** tab. Number 1505 is the RELAYID of the relay that will toggle when the task is performed.*

17 - Click on **Save** and **Close**.

Controller Group Creation

The Controller group menu is used to group a number of controllers of the same connection.

1 - From the Groups window, select the **Controller** button.

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

3 - From the **Gateway/connection** drop-down list, select the connection or gateway from which you want to group controllers.

4 - To create a new group of controllers, click the **New** button. 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 connection, check the controllers that are to be assigned to the group.

*NOTE: For more information on controllers, see **Controllers Configuration**.*

Door Group Creation

The Door group menu is used to group doors of a specific connection. The door group can later be used to carry out manual operations such as unlocking a group of doors.

1 - From the Groups window, select the **Door** button.

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

3 - From the **Gateway/connection** drop-down list, select the connection 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** button to create a new group, then enter the necessary information.

5 - From the **Door list** , select the doors that must be assigned to the group.

*NOTE: For more information on doors, see **Doors Configuration**.*

Relay Group Creation

The Relay group menu is used to group relays of a specific connection. This relay group can later be used to carry out manual operations such as temporarily activating relays.

1 - From the Groups window, select the **Relay** button.

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

3 - From the **Gateway/connection** drop-down list, select the connection 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** button 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 **Relay Configuration**.*

Input Group Creation

The Input group menu is used to group inputs of a controller connection. This input group can later be used to carry out manual operations such as shunt on inputs.

1 - From the Groups window, select the Input button.

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

3 - From the **Gateway/connection** drop-down list, select the connection 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** button 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 **Input Configuration**.*

Access Level Groups Grouping

The Access level group dialog is used to group access levels of the same connection.

1 - From the Group window, select the Access level group button.

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

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

4 - Click the **New** button to create a new group access level, and assign a name in the **English** field.

5 - Check the boxes that correspond to the access level group.

Floor Group Creation

This menu is used to group the floors that were created in the floor definition menu. Floor groups are also used for various operations in the system such as: manual operations (unlocking schedules), access levels, etc.

1 - From the **Groups** tab, select the **Floor Group** button.

2 - Select the **View hierarchy** button to display all the sites defined in the system; then from the **Gateway/connection** drop-down list, select the connection 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** button 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 - From the **Schedule** column, select a schedule for each floor in the group.

- When assigning a floor group and an unlock schedule to an elevator door (see **Defining Elevator Doors** for details), the system scans the schedule column of that group and unlock each floor accordingly.
- The schedule assigned to the floor group will be used to validate the access card and its unlock schedule. This way, the floors will be unlocked only when the two schedules (the floor and the access card) are valid.

NOTE: *The unlock schedules are effective even when the controllers are in* ***Fail soft mode*** *(communication failure).*

Trigger Group Creation

Trigger groups are used to configure triggering elements from a group of sub-components.

1 - Under the **Groups** tab, click the **Trigger group** button to open the **Trigger group** dialog.

2 - From the **Trigger group** drop-down list, select an existing group if you want to modify it; or click the **New** button to create a new group. Then, enter the name of the group in the language section.

3 - From the **Component** drop-down, select a component. Check the boxes corresponding to the sub-components you want as part of the trigger group.

4 - Click the **Save** button.

Application Configuration

The minimum configuration of an EntraPass software package includes a server, a workstation application (EntraPass monitoring application) and a gateway application. The gateway application can be integrated with the EntraPass workstation on the same computer. The software package comprises a number of applications including:

- A workstation application
- A server application,
- One multi-site Gateway application,
- And a number of utilities such as the Vocabulary editor, the Express Database utility, etc.

NOTE: *For a single gateway, limits are 2048 connections, 10,000 doors, 100,000 cards, 100,000 inputs and outputs.*

It is recommended to install the EntraPass server on a dedicated computer for system stability. The **Application** dialog allows operators to configure computers where EntraPass is installed. This includes configuring computers where you have installed: the EntraPass Workstation software, the Gateways, the Mirror Database and Redundant Server programs, as well as computers where you have installed the SmartLink Interface, if applicable. To configure the Application, you have to define:

- General parameters applicable to all computers where EntraPass is installed.
- Security parameters (applicable to all EntraPass applications).
- Filters (to define which gateways and EntraPass applications will send messages to the Workstation application being configured).
- Message / alarm controls.

Configuring an Application

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

Note...

Items displayed in the Application window vary depending on the selected EntraPass application. For example, if the selected application in a workstation-type application, tabs such as Workstation , Gateway and site , etc., are displayed. If the selected application is a Redundant server, the Redundant server tab appears.

---

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

3 - Assign a name to the selected application. If you are running the software in two languages, for example in English and French, you may assign a name in English and in French.

4 - Click the **Save** button to activate the new application.

Defining General Parameters

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

1 - Select the **Send to tray on idle** if you want the applications to be minimized when there is no action on the keyboard. If you do this, you have to specify the period after which the application will be minimized

---

if there is no action on the keyboard. In the **Send to tray on idle**, enter the delay after which the applications will be minimized and sent to the task bar.

2 - Select the **Automatic Logout on idle** option if you want the application to log out 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).

3 - If the **Video** feature is enabled, the **Video view** field appears. If this is the case, select the Video view in which you want the defined component to appear. For details on defining video views, see **Video Views Definition**.

4 - From the **Graphic** list, you may select the graphic to which the application is assigned, if applicable. For details on defining graphics, see **Graphics Definition**.

5 - For the **Mirror Database** application, select the **Automatic Backup** check box if you want the application to automatically do a backup of the database. When you click the **Configure Automatic backup** button you can define options for the backups in the **Backup Scheduler.**

Note...

You must configure the Backup Scheduler for the Mirror Database and Redundant server independently from the Backup Scheduler for the primary server.

---

a - You also have the option to start a backup immediately from the Mirror Database and Redundant Server application when you click the **Backup ALL NOW** button. By doing so, the Mirror Database performs a backup of all four databases: Data, Archives, In/Out and Video following the parameters set in the Backup Scheduler. An option to execute an immediate backup of a specific database type is also available from the Status window:

- In the Status window, select the Application button.
- From the root tree menu, right-click the Mirror Database.
- Click backup now and then click the database type you want from the sub menu.

Note...

To execute automatic backups, the Mirror Database application must be online and in Updating Mode with the primary server.

Defining Parameters

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

1 - From the **Application** window, select a workstation and move to the **Parameters** tab.

2 - Make the appropriate choices:

- **Disable application** : If selected, the operator will not be able to start the application. This field must be used with caution.
- **Disable authentication to server:** When this option is checked, it is no longer possible to register the application to the server.
- **Auto disable authentication:** I f selected, the system will automatically disable authentication when the application has authenticated itself for the first time.
- **Display Login List** : If checked, this option tells the system to save the five last login names to make them available for selection when opening new sessions. This option offers a fast way to open a session since an operator has only to select a user name and enter a password. You may however leave this field to its default setting (unchecked) for increased security; this will oblige operators to enter both a valid user name and password before accessing EntraPass.

- **Single Sign On (SSO):** When this check box is visible, the Active directory application is active. It is unchecked by default. To activate SSO you need to select the application or applications you want from the drop-down list.

  - If SSO is on in EntraPass, the next time you start the application you are not required to enter a username and password.

  Note...

  If you log out and the application remains open, the next time you log in you are required to enter your EntraPass username and password.

  - If SSO is off in EntraPass and the operator has disabled synchronization you are required to enter your EntraPass username and password.

  - If SSO is off in EntraPass an Active directory operator can still have their credentials validated against their profile if they enter their *domain**username* for login.

  Note...

  *EntraPass supports cross-domain log in but first the operator must create and save Login names, passwords and the domain in EntraPass in **Creating or Editing an Operator**. Cross-domain usernames use the following format, domain\username. Cross-domain brings the added benefit that EntraPass is not required to run on a Windows platform this facilitates EntraPass Web and Go.*

- **Must be login to close application** : Checking this option will oblige operators to log in before they exit an EntraPass program.

- **Suspend messages:** If this option is selected, all incoming messages for this application will be suspended. Use this option for an EntraPass workstation that is used only to configure components or when messages are not required.

- **Operator must login to view events** : Checking this option will oblige the operator to log in at least once with a valid user name and password before system event messages can be viewed.

- **Disable video** : Check this option to hide the video view options from this EntraPass workstation user interface. If this option is checked, the Video Events List, Video Playback and Video desktop options are disabled in the system. Operators with appropriate user permissions will be able to configure the Video option but will not be able to view live or recorded video segments.

- **Notify when remote sites must be updated** : Check this option to tell the system to send a notification before updating remote sites. When this option is enabled, operators will receive a notification before updating site communicating via a modem. If this option is selected, operators will receive a notification each time data related to sites (such as schedules, controllers, etc.) are modified. They will have the choice of updating remote sites (**Yes**), refusing the change (**No**) or clicking **Details** so that they can select specific sites to be updated.

- **Use for custom and quick reports**: Select this option so the **Mirror Database and Redundant Server** application will have access to the queue of reports. This option allows the Mirror database or the Database access application to run quick or custom reports in order to reduce the workload on the Server application.

Defining Message Controls

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

Note...

*Messages desktops are configured in the **Desktop definition** menu. For details, see **Message List Desktop**.*

---

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

- Specify the number of **Messages that will be kept on the server** when the EntraPass workstation is off-line, that is, when it is not connected to the server. The server buffers a maximum of 10,000 messages per EntraPass workstation (default: 500).

- Specify the number of messages that will be **kept on the workstation** . There is a maximum of 100,000 messages per EntraPass workstation. By default, it keeps 5,000 messages.

Note...

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

---

3 - Specify if the server should keep newest or oldest messages when its buffer reaches the defined maximum number:

- **Keep older messages:** The Server will keep the oldest messages and archive the newest messages when the EntraPass workstation is off-line and when the Server buffer is full.

- **Keep newer messages:** The Server will keep the newest messages and archive the oldest messages when the EntraPass workstation is off-line and when its buffer is full. Messages are processed on a first in - first out basis.

4 - In the **Clear Message Desktops** section, specify when messages should be cleared:

- **On logout** (on a regular logout by an operator).

- **On workstation shutdown** (when the EntraPass workstation is completely shutdown).

5 - In the **Picture information** section, select the field content that will be displayed below the cardholder picture. The **Show cardholder information with picture** drop-down list contains 10 definable fields (User information 1, User information 2, etc.).

Note...

By default, the field displays "User information #1" to "User information #10". These labels may be customized. For more information on renaming card information labels, see ***Customizing Card Information Fields****.*

---

6 - In the **Status button refresh delay** section, specify the time interval at which the application refreshes the condition reported by the status button visible in the status bar. Refresh delays range from 0.01 to 5.00 min. in increments of 0.01 sec.

7 - Select the **Dedicated event desktop** option to enable the **Dedicated Desktop** tab. Using dedicated desktop, you can configure specific events to be displayed on specific workstations. For example a workstation which is dedicated to a specific site can be configured to only see events from that site. Operators logged onto workstations with **Dedicated Event Desktop** enabled will default to the workstations event filter configuration.

8 - You can define the **Maximum number of records** that can be retrieved from archived files and displayed on screen for the **Historical Report Desktop** . The maximum is 200,000.

Defining Alarm Controls

1 - Click the **Alarms** tab to define how alarms should be processed when the EntraPass workstation is connected (or not) to the server .

Note...

Alarms desktops are configured in the ***Desktop definition*** *menu. For details, see* ***Alarms Desktop****.*

---

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

- Specify the number of alarms that will be **kept on server** when the EntraPass workstation is off-line, that is, when it is not connected to the EntraPass Server. The EntraPass Server buffers a maximum of 100,000 alarms per EntraPass workstation (default: 500).

- Specify the number of alarms that will be **kept on workstation** . There is a maximum of 100,000 alarms per EntraPass workstation. By default, it keeps 5,000 alarms.

Note...

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

---

3 - Specify if the server should keep newest or oldest alarms when its buffer reaches the defined maximum number:

- **Keep older alarms:** The EntraPass Server will keep the oldest alarms and archive the newest alarms when the EntraPass workstation is off-line and when the Server buffer is full.

- **Keep newer alarms:** The EntraPass Server keep the newest alarms and archive the oldest alarms when the EntraPass workstation is off-line and when its buffer is full. Alarms are processed on a first in - first out basis.

4 - In the **Clear Alarms Desktops** section, specify when alarms should be cleared:

- **On logout** (on a regular logout by an operator).

- **On workstation shutdown** (when the EntraPass workstation is completely shutdown).

5 - 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.

6 - You can check the **Disable auto display of video views** option to prevent video views from being automatically displayed by this workstation. In fact, video views defined as alarms and associated with components are automatically displayed when the component goes in alarm.

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 deskto**p. For more information on EntraPass desktops, see **Alarms Desktop** .

Comment

For more details about the **Comment** entry box, please refer to **Comment Field**.

Configuring a Gateway Application

The EntraPass Gateway converts the information received from a controller or a site and transmits the converted data to the server that in turns transmits it to the appropriate application. It also converts the information received from the EntraPass workstation and transmits it to controllers. The gateway interfaces the sites and the application. The gateway application allows you to monitor the controller sites connected to the gateway. You may add up to 40 multi-site Gateways.

Configuring General Parameters for a Gateway

From the **Application** drop-down list, select the gateway application you want to configure. When the selected application is a gateway type, the **Application type** field in the **General** tab displays "Gateway".

Configuring an Oracle/MS-SQL Interface (CardGateway)

The Oracle/MS-SQL Interface creates a real-time mirror copy of the EntraPass card databases (Card table, Card group table, Card type table and Badge table) in MS-SQL or Oracle database. 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 from the EntraPass card database. The card information is updated in all the databases, whatever the program used to modify or to update the database; MS-SQL Interface ensures that the modifications are conveyed to the server and then sent to the workstations.

Note...

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

---

*The **Card Gateway** is not compatible with windows server 2008 64 bits. Client 32 bits must be installed.*

Make sure that the MS-SQL or Oracle client software is installed on the same computer as the Oracle/MS-SQL Interface. It is not recommended to install the Oracle/MS-SQL Interface on a computer where EntraPass is installed. Installing the two applications on the same computer may cause problems during data exchange between EntraPass and the Oracle or MS-SQL Server. To configure the Oracle/MS-SQL database Interface you have to define:

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

---

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

2 - Define the application on which you have installed the Oracle/MS-SQL Interface.

3 - Select the **Parameters** tab to define security parameters for the Oracle/MS-SQL Interface. For details, see **Defining Security Parameters**.

4 - Select the **ORACLE/MS-SQL 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 server, Oracle 7.3 server or SQL server. 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 Interface will not communicate and will not be able to connect to the server.

---

6 - Enter the database **Server name** .

7 - Type the name of the requested Oracle or SQL **Database Name** .

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

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 user name and password.

Note...

It is important to check this box. If you do not, you must manually create the database, the user name and password in the database server.

---

10 - Enter the **Administrator user name** and **Administrator password** . The program will automatically create the database, user name and password in the server database

11 - In the **Database access** area, enter a user name and password which will be used by the CardGateway to connect to the Oracle/SQL database.

Note...

The database access procedure does not allow the CardGateway 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 Interface database.

Note...

If you do not select this option, deleted records will be physically and permanently erased from the

Oracle/MS-SQL database. 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. For more information, see the next section, ***Creating Server Databases Manually****.*

---

13 - Click the **Service** tab to define login information when the Oracle/MS/SQL interface runs as a service and a report needs to be printed.

14 - Click the **Service** tab to define login information when the Oracle/MS/SQL interface runs as a service and a report needs to be printed.

- The **Login to EntraPass service application** box must be checked to activate this option.
- Enter the Oracle/MS-SQL Interface **Domain name** and **Login name** .
- Type in the **Password** and **Password confirmation** .

Creating Server Databases Manually

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.

Creating an Operator Manually in the ORACLE/MS-SQL Server

The first step in integrating ORACLE/MS-SQL 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.

Creating a Kantech Operator for an MS-SQL Server

You have to create an operator that the Oracle/MS-SQL Interface will use to log in 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 window 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.

Creating a KANTECH Operator for an Oracle Server

1 - Login 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 login profile. Default user name 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.

Comment

*For more details about the **Comment** entry box, please refer to **Comment Field**.*

Configuring the Mirror Database and Redundant 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, except the Oracle/MS-SQL card database.

Synchronization between the system database and the Mirror Database can be configured to be synchronous or asynchronous. Synchronous mirroring synchronizes the mirrored database in real time. Asynchronous mirroring synchronizes the mirrored database at user defined intervals (5 minutes, 15 minutes, 30 minutes, 60 minutes, 2 hours and 4 hours). Asynchronous mirroring can improve the performance of the system by reducing the number of server transactions.

Note...

Asynchronous mirroring is only available for Archive, In/out and Video events. Synchronous mirroring is used for all other data.

When communication between the Mirror Database and the Primary Server fails, the Mirror Database automatically initiates the delay after which the Redundant Server is automatically started to replace the Primary Server. The Mirror Database and Redundant Server program cannot run on the same computer as the EntraPass software server. The Mirror Database and Redundant Server should be installed on a dedicated computer.

Note...

You can operate the system with more than one Mirror Database and Redundant Server. The Mirror Database and Redundant Server feature requires an additional license.

To configure the **Mirror database and Redundant Server** workstation, you must define:

- General parameters applicable to the Mirror Database and Redundant Server, including security parameters.
- Redundant Server parameters.

- Security parameters.

1 - From the **Application** drop-down list, select the **Mirror Database and Redundant Server** application.

2 - To define parameters in the **General** tab, see **Defining General Parameters.**

3 - Select the **Parameters** tab to define security parameters for the Mirror Database and Redundant Server. For details, see **Defining Security Parameters**.

4 - Move to the **Redundant Server** tab to define communication parameters for the Mirror Database and Redundant Server.

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

Note...

When you select TCP/IP, the Redundant server address field is enabled to allow you to enter the TCP/IP address of the computer hosting the Mirror Database and Redundant Server.

*If **Automatic** is checked, the IP address of the computer hosting the Mirror Database and Redundant Server 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 or if the computer is connected to a DHCP server.*

---

6 - Enter the **Redundant server IP address .**

7 - Select the course of action the redundancy server must take in cases of **start up with no server communication** .

8 - Specify the options for starting the Redundant Server when the main server shuts down: this may be automatically on a normal shutdown (when an operator shuts down the EntraPass server) or on an abnormal shutdown. The Mirror Database will start the Redundant 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 Redundant 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.*

---

9 - Specify the system's course of action when the server returns to normal (**On server restore**): enter the delay after which the Redundant Server will be stopped when the primary server returns to its normal functioning. During this time, the Redundant Server will continue to prevail (maximum allowed: 59 min:59 secs).

10 - Move to the **Restore Parameters** tab to define the redundant server's course of action when the main server comes back up after a shut down.

- To automate the restore process from the redundant server, check the **Automatic process on restore** box. The rest of the options become enabled.

- Check the appropriate boxes depending on the features you have installed, and the restore process you want to activate:

  - **Restore** : Will transfer the whole database that contains all the transactions from the redundancy server to the main server and overwrite any data created on the main server.

  - **Merge** : Will only transfer data from the redundancy server when the transactions cannot be found on the main server.

Note...

*When using the **Merge** feature, data will not be transferred in cases where, for example, a card has been modified on the redundant server and the main server simultaneously while the main server was disconnected.*

---

11 - Click the **Async updates** tab to define the mirror database synchronization settings. These setting determine whether the mirror database synchronization is synchronous (**Live**) or asynchronous (**Every 5 minutes**, **Every 15 minutes**, **Every 30 minutes**, **Every 60 minutes**, **Every 2 hours** and **Every 4 hours**).

Note...

*To check the status (pending transfers and next synchronization) of an asynchronous transfer the user can check the **Mirror Database and Redundant Server** connections in the **Status Tab** under **Application**.*

---

12 - Click the **Service** tab to define login information when the **Mirror Database and Redundant Server** run as a service and a muster report needs to be printed.

- The **Login to EntraPass service application** box must be checked to activate this option.
- Enter the Mirror database and Redundancy Server **Domain name** and **Login name** .
- Type in the **Password** and **Password confirmation**.

Comment

*For more details about the **Comment** entry box, please refer to **Comment Field**.*

Configuring the SmartLink Application

The SmartLink application allows operators to interface the EntraPass access control software with any intelligent device such as video matrix switchers, paging systems, email 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, reports or commands, and to communicate with client applications.

Note...

The SmartLink 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, DN1327.

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

2 - Define the workstation on which you have installed the SmartLink interface. For more details, see **Defining General Parameters**.

3 - Configure the SmartLink workstation security parameters. For more details, see **Defining Security Parameters**.

4 - Configure the SmartLink workstation messages. For more details, see **Defining Message Controls**.

5 - Configure the SmartLink workstation email reports. For more details, see **Defining Email Report Options**.

6 - Click the **SmartLink** tab to view and setup the SmartLink connection parameters.

7 - From the **Mode enabled** drop-down list in the **SmartLink serial connection** section and the **SmartLink network connection** section, select the appropriate mode of transmission:

- **Messages only** : SmartLink will only receive messages.
- **Commands only** : SmartLink will only execute commands (tasks).
- **Messages and commands** : SmartLink will receive messages and execute commands.

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 other than "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.

---

8 - In the **SmartLink tasks** section, you may define **start up** or **Default** tasks. The task you assign will be processed automatically when the **SmartLink** application is started. For details on defining SmartLink tasks, see **Task Builder Definition**.

9 - Click the **SmartLink email** tab to view and setup the SmartLink connection parameters.

10 - In the **Email server (SMTP or Exchange server)** field, enter the IP address of the Email server that will be used for sending emails.

11 - In the **Email Port** field, enter the number of the port that will be used for sending emails (usually 25).

12 - Select the encryption method.

- Unsecured (No SSL/TLS)
- Gmail(SSL/TLS)
- Secured (SSL/TLS)
- Office 365 (STARTTLS)

13 - Enter a valid email address in the **Email sender** field. This email address will be used for authenticating the email server.

14 - Authentication: These options can be used to configure the authentication method.

- **No authentication** : No authentication will be applied.
- **SMTP authentication** : An authentication, sent on the SMTP port, must be validated before the message is released.

- **POP3 authentication** : An authentication, sent on the POP3 port, must be validated before the message is released.

15 - User name : Enter a user name for the authentication process.

16 - Password : Enter the password for the user name.EntraPass supports SMTP connection passwords with a maximum length of 64 characters.

17 - E-mail server (POP3) : Enter the POP3 server address for a POP3 authentication.

18 - E-mail port (POP3): Enter the POP3 port number for a POP3 authentication.

19 - Delete e-mail(s) when maximum reached: The maximum amount of e-mails that will be kept in the buffer when the feature is active is 9999. The minimum (and default value) is 1000.

20 - Delete e-mail(s) when older than (hh:mm): The maximum amount of time e-mails will be kept in the buffer when the feature is active is 24:00. The minimum value is 02:00 and the default is 05:00.

21 - Send to : Recipient's address for the message to be sent.

22 - Test button: Send a test message with the selected parameters. According to the test results, different error or success messages could be displayed.

Note...

The email port value is set to 25 by default. You may leave it as is or change this value to another available port on the network (between 0 and 65,535). For information about setting of the email server, contact the network administrator.

---

23 - To define the EntraPass web parameters, click the **SmartLink Web and API** tab, and complete the following steps:

a - Click **Web Service**, and click the **Use Web Service** check box.

b - In the **Connection name** field, type a name for the connection.

c - In the **Web Service Name** field, type the name of the Web service.

---

d - Choose one of the following communication options:

- Select **IP address**, and type the IP address of the SmartLink.
- Select **Domain name**, and type the domain name, click **Test DNS** to test the connection.

e - In the **Web Service Port** field, type the port number.

f - In the **Web Service Protocol** field, select one of the protocols.

g - In the **EntraPass web link for welcome email** field, view and edit the EntraPass web path.

h - In the **Mobile link for welcome email** field, view and edit the path for EntraPass go, EntraPass go Install, and EntraPass go Pass.

i - To choose, which application you want to connect to the selected SmartLink, select one of the following options:

- Include EntraPass web link
- Include EntraPass go link
- Include EntraPass go Install link
- Allow go Pass request

24 - Enter the **Connection timeout on idle (mm:ss)** : When the connection timeout has been reached, the operator must log back in to continue. All changes, after the last save, are lost. The default connection timeout is 5:00 min. The time range value is 00:30 to 20:00 min.

Note...

If you have updated the EntraPass system, the connection timeout has not been modified automatically, it will remain as it was. Make sure to check its value.

---

25 - Click the **Service** tab to define login information when the SmartLink server runs as a service and a report needs to be printed.

26 - Click the **Service** tab to define login information when the SmartLink server runs as a service and a muster report needs to be printed.

- The **Login to EntraPass service application** box must be checked to activate this option.
- Enter the SmartLink **Domain name** and **Login name** .

- Type in the **Password** and **Password confirmation**.

Comment

*For more details about the **Comment** entry box, please refer to **Comment Field**.*

Configuring the EntraPass Video Vault Application

The EntraPass Video Vault application addresses the need for better video data archiving. This application retrieves video segments from the Video Servers connected to EntraPass and saves these video segments for future reference. In fact, video segments can be kept on the video server for a limited period of time. This period depends on the video server disk capacity and settings. In order to take full advantage of the Video Integration capability, EntraPass users who are running a video monitoring software need EntraPass Video Vault to manage their video archive database. To register the video vault, you need a license and a confirmation code. Each registered video vault increases your **Kantech Advantage Program** (KAP) amount by one.

After installing and registering the EntraPass Video Vault application, you must define its environment among other applications. For details about registering EntraPass Video Vault, see **Adding System Components**. For details about using EntraPass Video Vault, see **EntraPass Video Vault**.

To configure the EntraPass Video Vault Application, complete the following steps:

1 - Click the **Devices** tab, and select **Application** from the menu.
2 - From the **Application** list, select **Video Vault**.
3 - In the **General** tab, there are two check boxes available, **Use as a vault** and **Use as a Video Server Gateway**. By default, EntraPass selects the **Use as a Video Server Gateway** check box, all new exacq video server connections connect to any available Video Vault.

Note...

- In the Outbound connections port, the default value is 35111, exacq DVRs use this port to connect to the vault.

To establish the outbound connection to the exacq DVR, select one of the following communication options:

- In the **IP address** field, enter the IP address requied for exacq to reach the video vault.
- In the **Domain name** field, enter the domain name required for exacq to reach the video vault.

Note...

The **Connected Video Servers** field displays the amount of connected video servers reporting to the video vault. You cannot delete a video vault if it has one DVR linked to it.

4 - To define General parameters for the EntraPass Video Vault application, see **Defining General Parameters**.

5 - To define security parameters for the EntraPass Video Vault application, see.**Defining Parameters**.

6 - Select **the Folder** tab to specify the video file location and name structure. The settings defined in this window will be reflected in the way the video files will be displayed in the Browse Video Vault window (**Video** tab > **Browse Video Vault**).

- **Destination drive(s)** : specify the list of drives where video segments will be archived. Video segments will be saved according to the disk space available on the drive and according to order of the selected drives.

Note...

Destination drives that are displayed for selection correspond to the mapped network drives on your computer. They differ from a computer to another.

By default, drives are listed alphabetically. You may decide to change this order according to the space available on each disk. The up/down green arrows allows you to change the sequence of drives to use for archiving. displayed for selection correspond to the mapped network drives on your computer. They differ from a computer to another.

- **Minimum free disk space (MB):** Enter the minimum free disk space allowed before the system sends a message that there is no more disk space in the EntraPass Video Vault and archiving will stop. The value can be up to 99,999 MB.

- **Disk free space threshold (MB):** Enter the maximum threshold space allowed before the system sends a message that the EntraPass Video Vault has reached its disk free space threshold but will continue archiving until it has reached the **minimum free disk space** . The value can be up to 99,999 MB.

- **Date field separator:** You can define the date field separator that will appear in the archived video directory.

- **Destination folder** : Select the folder that will be used to archive video data. If you do not specify a target folder, no video segment will be archived. By default, video segments will be archived in C:\KantechVideoArchive folder.

- **Sub-folder structure** : Each combo box contains the criteria that will be used to create a sub-directory where to archive video data. For example, selecting **Video Server Name** will create a sub-directory for each video server where all corresponding video segments will be stored. If you go down further and select Day-yyyy-mm-dd, another sub-directory will be created under Video Server Name to store video segments daily. You can go down to 5 levels of sub-directories.

7 - Select the **File** tab to define the file naming convention.

- **File name structure:** Check the boxes that correspond to the information you wish to include in the file name.

- **Separators:** You can define a field separator for the file name as well as data and time.

8 - Select the **Process** tab to tell the system how archived video segments will be processed.

- **Default Video file format for your video archives:** You can archive video segments using the KVI, KVA, AVI, IMG or PS formats.

  - **KVI** stands for Kantech Video Intellex format. The KVI file contains thumbnail and video context information and places a watermark on embedded.img. It must be viewed with the Intellex Video Player that uses the American Dynamics API. You must make sure that the API has been installed on the client's computer.

  - **KVA** stands for Kantech Video AVI format. The KVA file contains thumbnail and video context information with no watermark on the embedded .avi. Video files can be viewed using Windows Media Player or any other AVI player on the market.

- **AVI** stands for Audio Video Interlaced format. AVI video files are viewed using Windows Media Player.

- **IMG** is the Intellex native format. Video data are stored in Intellex format (.img) and can be viewed using the Intellex Video Player.

- **PS** : HDVR native compressed video format.

Note...

KVI and KVA formats enable users to protect video files with a password and to specify key frames for any selected video event. Key frames offer a fast way for retrieving video segments based on a still image (bmp) representing the whole video sequence.

- **Simultaneous video segment transfers:** Select the number of simultaneous downloads. You cannot retrieve more than one video segment from one video server at a time. However, it is possible to retrieve more than one segment from more than one video server simultaneously. The minimum value is 1; the maximum is 8.

Note...

A high number of retrievals requires more network bandwidth. As the flow of video data requires a great amount of network bandwidth, contact the Network administrator for these settings.

- **Video segment duration limit:** Specify the minimum and maximum duration of the video segment to be archived. The maximum duration is 59 min:59 secs. Moving the cursor over the editable field will activate a hint indicating the minimum and maximum duration. This feature can prove useful if you want to restrict the number of archived video segments. For example, the restriction can be based on the size of the record. For example, you can tell the system to ignore all video recordings with a duration of less than 10 seconds.

- **Default password for KVI and KVA file formats** : For increased security, check the box if you want to protect the archived video segments by a password. The KVI and KVA formats add the benefit of protecting your archived data with a password. Make sure to enter identical information in the **Password** and **Password Confirmation** fields. Operators with appropriate permission for viewing archived video segments will be required to enter a valid password before viewing the video segment.

- **Kantech server polling frequency (m:ss):** Using the slide bar to specify how often the EntraPass Video Vault will poll the EntraPass server.

Note...

Keep in mind that network traffic will be affected by the polling frequency between the EntraPass Server, Workstations, Gateways and Video servers. Faster polling means higher network bandwidth use.

---

9 - Click the **Significant Frame** tab to define the key images that will be used as thumbnails to preview video segments in the directories.

- You must select a setup type:

  - **Significant Frame:** The most representative still image of the video segment. This key image serves as a summary for the video segment. It can be used as a thumbnail, for example, when searching for a specific video segment.

  - **Significant Frame on Sequence:** This feature is used only with dome cameras where a pattern has been set for the camera to follow and the most representative still image of the video segment must be defined within that pattern.

  - **Significant Frame on Preset:** This feature is used only with dome cameras where preset positions have been defined. The most representative image of the video segment can be set taking in consideration the time needed by a camera to move from the first frame to the next preset position.

- You can select one of the **Default Key Frame types** for each significant frame setup type:

  - **No image:** There will be no thumbnail for this video segment.

- **First frame:** The video segment will be represented by a still image of the pre-alarm recording. This automatically enables the **Delay for Significant Frame (ss:cc)** parameter, which is the delay calculated after the first frame to select the thumbnail image that will represent the video segment. Moving the cursor over the editable field will display the min./max. time range admissible.

- **Event Frame:** The video segment will be represented by the image that was captured when the alarm occurred.

10 - Click the **Service** tab to define login information when the EntraPass Video Vault server runs as a service and a report needs to be printed.

11 - Click the **Service** tab to define login information when the EntraPass Video Vault server runs as a service and a muster report needs to be printed.

- The **Login to EntraPass service application** box must be checked to activate this option.
- Enter the EntraPass Video Vault **Domain name** and **Login name** .
- Type in the **Password** and **Password confirmation**.

Comment

*For more details about the **Comment** entry box, please refer to **Comment Field**.*

EntraPass Gateways Configuration

EntraPass Gateways convert the information received from a controller or a connection and transmits the converted data to the server. Gateways also convert the information received from the server and transmit it to controllers. The gateways may be installed on a dedicated computer, or integrated with another EntraPass workstation.

NOTE: For a single gateway, limits are 2048 connections, 10,000 doors, 100,000 inputs and 100,000 outputs.

Multi-site Gateway features

Capacities	Multi-site Gateway
Number of Gateways	41
Local connections	32 sites with serial and USB
On-line remote connections	512 sites with Kantech IP Link* and KT-400
Dial up modems at host connection	32 per gateway
Remote dial up connections	512 per gateway
Controllers per gateway	17,408 total (32 KT per connections
Readers/keypads per gateway	34,816
Events for timer on/off	34

* System requirements may differ according to the size of the connections and the number of events generated per day

Configuring a multi-site Gateway

1 - From the **Devices** definition tab, click the **Gateway** button.

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

3 - Under the **General** tab:

- Select a **Graphic** and **Video view** to which the Gateway is assigned, if applicable. The video view feature will only be activated If the video feature is enabled in EntraPass.
- If your multi-site Gateway connects to the first controller of a remote site via modem, click the **Host Modem Definition** button to configure the modem communication options.
  - Click the **New** button to add a modem to the modem selection list.
  - Configure the modem as per the example entries shown in the previous window and click **OK** to return to the **Device definition** window.

Note...

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

4 - Under the **Multi-Site Gateway** tab, set the **IP address** and the **Domain name** for the gateway. A multi-site Gateway is configured to manage KT-100, KT-200 or KT-300 related events.

5 - Under the **KT-100/KT-200/KT-300 Events** tab, set the **LED Timer on** and **Timer off** for each event. A multi-site Gateway is configured to manage KT-100, KT-200 or KT-300 related events.

6 - Under the **KT-400/KT-1 Events** tab, set the **LED Pulse on** and **Pulse off** for each event. A multi-site Gateway is configured to manage KT-400 related events.

7 - Under the **KTES Events** tab, set the **LED Pulse on** and **Pulse off** for each event.

Note...

EntraPass may support up to 41 multi-site Gateways.

All the events available in a multi-site Gateway

Access granted	Arming request denied	Time-out on waiting for a second card
Access denied	Postpone granted	Access denied - Waiting for a second card
Time-out on access granted	Postpone denied	Access denied - Reader locked
Waiting for keypad (*Note 1*)	Door opened	Exit delay
Time-out on keypad	Door forced open	Entry delay
Bad code on keypad	Pre-alarm door opened too long	Access granted by tenant (*Note 3*)
Valid floor selection	Door open too long	Access denied by tenant (*Note 3*)
Invalid floor selection	Door alarm on relock	Auxiliary relay activated by tenant (*Note 3*)
Time-out on floor selection	Door unlocked	Postal lock request granted (*Note 3*)
Request to exit granted	Reader disabled	Postal lock request denied (*Note 3*)

Request to exit denied	Door armed	.
Arming request granted	Waiting for a second card (*Note 2*)	.

Note...

*The activation period for the event **Waiting for keypad** is defined under the **Keypad delays** tab.*

8 - Under the **Keypad delays** tab, define keypad options.

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

Note...

The maximum time allowed for both the inter-digit and time-out on keypad delays is 2 minutes and 7 seconds, and for KT-400 this is 4 minutes and 15 seconds.

- In the **Delays (Not applicable to KT-200)** section, using the up/down arrows, determine the number of **Invalid attempts before keypad disabled**. Users have a maximum of 255 invalid attempts before the keypad is disabled.
- Enter the **Keypad disabled duration delay (h:mm)**. The maximum duration allowed is 4 hours and 15 minutes. When the counter reaches the maximum, the keypad will be disabled for all cards. It is disabled for the delay specified in the **Keypad disabled duration** field.
- 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 minutes and 15 seconds. If the value entered is greater than the maximum allowed, then the system will use the previous correct value.

Comment

*For more details about the **Comment** entry box, please refer to **Comment Field**.*

Site Configuration

A site, as opposed to a physical connection, is composed of one or many physical connections (see **Connection Configuration** for more information about connections).

This way, it is possible for a large number of “controllers”, communicating over IP within an EntraPass system, to be linked together into a common “virtual site” regardless of their physical connections.

NOTE: Dial-up connections are not supported by virtual sites.

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

2 - If you are defining a new **Site** , click the **New** button, assign a name to the new site and click the **Save** button. The bullet next to the site name will turn green.

3 - Enter or edit the description in both languages.

General Parameters

1 - Click the **General** tab.

2 - In the **Connection list** section**,** you will find all the connections for that site. Right-click on a connection to view or edit it.

3 - Select a **Graphic** and a **Video view** to which the gateway is assigned, if applicable. The video view will only be activated If the video feature is enabled in EntraPass.

Information

1 - Click the **Information** tab.

- Enter site information in the fields (up to 20).
- The first 10 fields have already been populated. Double-click on a field to edit it (please refer to **Change Site Labels** for more details).

Comment

1 - Click the **Comment** tab:

- For more details about the **Comment** entry box, please refer to **Comment Field**.

Merge Connection Options

The **Merge existing connection** tab allows existing connections to be added to the site. By doing so, all logical and physical components linked to the connections will be transferred to the site. During the merge process, the system will combine access levels from the site and the merged connections. This process will create new access levels and assign them to users. These merged access levels will be renamed with the prefix “Combination:” followed by the names of merged access levels. Multiple instances of “Combination” in the name is the result of multiple access level merged between each connections.

Note...

Please ensure the total count of logical components of the site and the connections merged will not reach the limit site components. (100 Groups of each [Controller, Relay, Input, Access Level], 250 Access Levels, 100 Schedules, 256 Floors, 250 Floor groups). Otherwise, components will be lost if the limit is reached during the merge.

To merge connection(s) into a site,

1 - Click the **Merge existing connection** tab.

2 - Select the connections to be integrated with the site.

3 - Click the **Save** button. The system will then prompt the **Merge connection options** dialog (all are checked by default):

- **Merge Identical Schedules**: This option allows the system to find duplicate schedules between the site and the connection(s), and merges them into one. If not selected, all schedules from connection(s) will be transferred to the site even if duplicates exist.
- **Add Site Name as Prefix to Component's Name**: When selected, this option add the site name as a prefix to all physical components name (controllers, doors, inputs, outputs and relays). For example, for a site named "Montreal Office", a door named "Main Door" will become "Montreal Office, Main Door.

4 - Click **OK** to continue.

5 - Edit access level names from the list in both languages as needed. Click **OK**.

6 - The **Merge results** dialog will be displayed. Check for any error during the merge process. Click the **Close** button.

7 - To complete the merge process, you must close the **Site definition** window. A reload data of gateway (s)/ account will then be started.

Linked Component

Large EntraPass installations across multiple sites can contain many components(graphics, intrusion panels, and video servers). To simplify the management of a large number of components use **Linked components** to associate components with sites. Components can be linked and unlinked from a site. To create a linked component, complete the following steps:

1 - Click the **Linked component** tab.

2 - Select a component from the menu under the component type: **Panel**, **Graphic**, **Video Server**, or **Video View**.

3 - Select the link button to add the component to the **Site**.

4 - To unlink a component, select the component from the list and select the unlink button.

Change Site Labels

1 - Select a site information field from the list on the left.

2 - Edit the site information captions. You can enter two different descriptions and use the **Swap** button to swap the first and second captions.

3 - Click **OK** to keep your changes or **Cancel** to return.

Connection Configuration

A connection is composed of controllers attached to the same communication port. The system can manage up to 32 connections per multi-site Gateway. EntraPass also allows users to add up to 2048 connections per multi-site Gateway. multi-site Gateway connections are composed of KT-100, KT-200, KT-300, KT-400 and KT-1 controllers.

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

NOTE: *For a single gateway, limits are 2048 connections, 10,000 doors, 100,000 inputs and 100,000 outputs.*

Seven types of connections are available: Direct (RS-232 and USB), Secure IP (KT-400), Secure IP (KTES), Secure IP (IP Link), Secure IP KT-1, Ethernet (polling) and Dial-Up (RS-232) modem. Check the following table for the connection type versus the gateway.

Connection Type	Multi-site Gateway (*Note*)	Global Gateway (*Note*)	KT-NCC (*Note*)
Direct (RS-232 or USB)	Yes	Yes	Yes
Ethernet (polling)	Yes	Yes	Yes
Secure IP (KT-1)	Yes	Yes	Yes
Secure IP (KT-400)	Yes	Yes	Yes

Connection Type	Multi-site Gateway (*Note*)	Global Gateway (*Note*)	KT-NCC (*Note*)
Secure IP (KTES)	Yes		
Secure IP (IP Link)	Yes		
Dial-up (RS-232) modem	Yes		

Note...

The multi-site Gateway is available in all EntraPass Editions. Even though, it is not referred as a multi-site Gateway, the EntraPass Special Edition includes an imbedded multi-site Gateway.

The KT-NCC and the Global Gateway are only available with EntraPass Global Edition.

---

1 - From the **Devices** window, click the **Connection** button.

2 - Select a **Site filter** from the first drop-down list.

3 - select the **Gateway**.

4 - From the **Connection** drop-down list, select the connection where the controller is located.

5 - If you are defining a new **Connection** , click the **New** button. Assign a name to the new connection and click the **Save** button.

6 - Under the **General** tab:

- In the **Hardware definition** section **,** specify the number of controllers for the connection. There may be up to 32 controllers per connection. If the number specified is greater than the maximum allowed, the system will set the value to 32.

Note...

*When the connection type is **Secure IP (KTES),** the number of KTES is automatically limited to a single KTES per connection.*

- Select a **Time zone**: This setting will allow events from the remote site to be displayed at local gateway time on EntraPass workstations located in different time zones.

- Select a **Graphic** and **Video view** to which the gateway is assigned, if applicable. The video view will only be activated If the video feature is enabled in EntraPass.

- Use the scroll list to select the **Connection type between the computer and the gateway**. This will determine which tabs will be displayed for configuration.

Setting up Communication Timing

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

Configuring a Direct RS-232 Connection Type

This type of connection can be configured in EntraPass Corporate Edition for multi-site Gateways to communicate via a RS-232 gateway.

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

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

Configuring an IP Device Connection Type

This type of connection can be configured in a multi-site Gateway with EntraPass Corporate Edition to communicate via a Kantech IP Link, a KT-400, a KT-1 or a KTES.

Note...

For additional information on configuring the Kantech IP Link, please refer to the Kantech IP Link Installation Manual , DN1670.

For hardware information on the KT-400*, please refer to the KT-400 Installation Manual , DN1726.*

For hardware information on the KT-1*, please refer to the KT-1 Installation Guide.*

If you choose ***Secure (IP KT-400)*** *as a connection type, the primary controller must be a KT-400.*

For the KTES, the only controller in the loop must be a KTES. For hardware information on the KTES, please refer to the KTES Installation Manual, DN1769.

---

1 - When you specify **Secure IP (IP Link)** , **Secure IP (KT-400)**, **Secure IP (KT-1)** or **Secure IP (KTES)** from the **Connection type** drop-down list in the **General** tab, you will be able to access three extra tabs: **IP Device IP configuration** , **IP Device Automated Connection** and **IP Device Parameters** .

- **MAC address**: Enter the device MAC address. The first 6 characters in the MAC address (00-50-F9) cannot be modified.

- The **Online** box is selected by default.

  - **Obtain IP address automatically**: Check this option when configuring the device with a **Reserved DHCP IP** address.

  - **Use the following IP Address**: Check this option when you want to assign a static IP address to the device . When selected the next three parameters will become available.

  - **IP Address:** The static IP address should be provided by the System Administrator.

  - **Subnet Mask**: This address should be provided by the System Administrator.

  - **Gateway (Router):** This address should be provided by the System Administrator.

- **DNS server address:** This address should be provided by the System Administrator (for Kantech IP Link, KT-400 and KT-1 only).

- **Protocol: Used to specify the communication protocol, UDP or TCP.**

- **Port:**

- **For TCP:** Should be 18802 for the host site. Not required for the remote site.

- **For UDP** : Port 18810 is automatically assigned to the device by default. It should not be modified unless the IP device is at a remote location, like in a **WAN**.

Note...

Port 18802 should be used with KT-400, KTES, KT-1 and IP Link.

- The **multi-site Gateway IP address** will be used or click **Override Gateway IP Address**.
  - **Auto Discovered IP**: This is a read only field that automatically displays the gateway IP address. When the radio button is selected, the system overrides the IP address and reloads the connections with that new information.

Note...

*The **Auto Discovered IP** field is always filled and updated with an IP address even when not selected.*

*For a new gateway, the **Auto Discovered IP** radio button is not selected by default. The IP Address field is still the default selected option.*

- **IP address:** You will enter the gateway computer IP address.

- **Domain name:** If you don't have the gateway IP address, you can enter the domain name provided by the System Administrator (for Kantech IP Link, KTES, KT-400 and KT-1 only) .

Note...

You must select to either enter the IP address or the domain name. You cannot enter both at the same time (for Kantech IP Link, KTES, KT-1 and KT-400 only) .

- **Test DNS**: Once you have entered the domain name, click on the **Test DNS** button. This should display the corresponding IP address (for Kantech IP Link, KTES, KT-1 and KT-400 only) .

2 - Move to the **IP Device Automated Connection** tab if you are in a **WAN** environment.

- The **Broadcast configuration** box must be checked at all times.
  - **Private IP Address (LAN):** Will assign the IP address automatically.
  - **Public IP Address (WAN)**: This IP address should have been provided by your internet provider. This corresponds to the IP of the remote site.
  - **Domain Name (WAN)**: This information should be provided by the System Administrator. This corresponds to the IP of the remote site.
- **Enable KT-Finder diagnostic for IP device**: Check this box if you want to use the KT-Finder as a configuration and troubleshooting tool.

3 - Move to the **IP Device Parameters** tab to configure security and communication parameters.

- **Encryption key**: You will enter a 16-Digit hexadecimal code to secure your site.
- **Controller's loop baud rate**: Enter the controller's loop baud rate.

Note...

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

- In the **Delays** section:
  - **Heartbeat frequency (mm:ss)**: Enter the frequency to which you want the IP device to send a signal to the gateway to indicate it is online (00:15 to 10:00).

- **Fail to report after (mm:ss)**: Enter the delay before acknowledging communication failure (01:30 to 59:59).

- **Fail-soft delay on gateway communication failure (mm:ss)**: Enter the delay before the IP device will consider communication with a controller has been lost and the controller is in fail-soft mode.

- **Retry Count:** Enter the number of times the IP device will try to communicate with a controller within the delay setup in the previous parameter before acknowledging communication failure (1 to 15).

- **Maximum wait on send command (s.cc)**: When applicable, enter the maximum delay period that the gateway will allow for the IP device to acknowledge reception of a command from an EntraPass workstation (1.00 to 9.99).

Configuring an Ethernet Polling Connection Type

This type of connection can be configured in with the gateway via the network (Lantronix).

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

- Enter the terminal server **IP address** and **Port number**.
- Select the communication protocol:
  - **TCP** if the communication is made with the gateway through a terminal server using TCP protocol. In this case, you have to configure the terminal server. To do this, follow the manufacturer's instructions or refer to the Terminal server documentation.
  - **UDP** (User Datagram Protocol), uses the IP protocol to send datagrams from one Internet application to another. It is called "connectionless" because the sender and the receiver are not

required to connect before the transmission of data. Check this option if the connection you are configuring uses this protocol.

Configuring a Dial-Up (RS-232) Modem Connection Type

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

Note...

The Dial-up option is only available when selecting a multi-site Gateway.

---

1 - Select the **Modem options** tab to set outgoing call behaviour to site modem.

Note...

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

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

- Enter the **Remote phone number** .

Note...

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

The Modem init settings cannot be changed.

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

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

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

Note...

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

---

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

- Check the **Use a callback connection** option to force the gateway modem to hang up after initial connection to the remote site modem and to stand by for an acknowledgement call from the remote modem. You may also want to customize the **Fail to callback delay.** Default is set to 1:30 (1 min 30 secs.).

- This option only applies to the KTES. Check the **Enable multiple KTES line sharing** option to change the **Identification delay (ss)** between each KTES. The time range value is between 00 and 20 seconds.

- Select the **Primary host modem** in the drop down list. If available, select a backup modem in the **Secondary host modem.** This setting is useful when the primary modem is busy or fails to take the call.

- Check **After reception stay online for** if you wish to limit in-call time to a predetermined amount of time which can be set to anywhere between 00.03.00 and 23.59.59.

- Check the **Call immediately when secondary controller communication failure** to be alerted in the event that a secondary controller fails to send data to the primary controller (the one carrying the modem).

- Check the **Call immediately when buffer 70% full** to force download of a site controller's event buffer as soon as it reaches 70% capacity.

Note...

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

Migrating KT-Standalone Back-up Data to an EntraPass Server

You can migrate backup data from a KT-Standalone controller to an EntraPass server; compatible controllers include the KT-1, firmware v2.01 and higher, and the KT-401, firmware v2.00 and higher. The backup includes the following data:

- Controller definitions
- Door definitions
- Relay definitions
- Schedule definitions
- Holiday definitions
- User definitions
- Action scheduler

Note...

The following features are not included in the migration:

- Time zone
- Alarm panel integration
- Multi-swipe settings on exit door.

Icon	Description
	KT-Standalone: selects backup files from a KT-1, firmware v2.01 and higher, and the KT-401, firmware v2.00 and higher, standalone controllers.

Before you migrate your data, you must configure EntraPass to use the same **card format**, **Global Card Format**, and **PIN length** as the standalone settings:

1 - Navigate to the **Account** tab, and select **System** from the menu.

2 - To open the **Display Format** window, click the

3 - In the **Default card format** area, select the **Card #1** format to match the **Card #1** format in the standalone controller, repeat for Card # 2 to Card # 5.

NOTE: *If card #1 and card #2 use a different display format, EntraPass migrates into card #4 or card #5.*

4 - In the **Global Card Format** area, choose the appropriate global card format.

5 - Select the appropriate PIN length from the **Number of PIN digits (KT-400 and KT-1)** list.

To migrate backup data complete the following steps:

1 - On the **Devices** tab, select **Connection** from the menu.

2 - Click the **KT-Standalone** button on the menu bar to display the KT-standalone backup CFG files for the KT-1, firmware v2.01 and higher, and the KT-401, firmware v2.00 and higher.

3 - Select a file to see the backup information:

a - Backup date and time

b - Controller type

c - Controller MAC/Serial number

a - Controller firmware version

b - Amount of users

c - Amount of schedules

d - Amount of holidays

e - Amount of action scheduler

f - Amount of doors

g - Amount of relays

h - Amount of input

4 - A window displays with the message “Are you sure you want to import the following data?” If you click **Yes: import data**, the following message displays, “Migration completed”, click **OK**. If you click **No**, the message window closes.

The Unassigned Controllers List

When EntraPass receives data from the KT-1 enrolment process it adds the controller to the controllers unassigned list. the "Controller was added to the unassigned list” event is then generated with the following parameters:

- Gateway description
- MAC Address
- Device type

The unassigned controllers list displays:

- Date and time (when it was added to the list) of the gateway
- Controller model

- MAC Address
- Serial Number
- Broadcast received IP address

Note

The unassigned controller list can have a limited number of 100 entries.

---

*For more details about the **Comment** entry box, please refer to **Comment Field**.*

Setting up Communication Timing

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

Controllers Configuration

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

The controller definition tells the system how a controller is being used and what devices are associated with it: (doors, input zones, relays and output devices). Controllers may be defined during a gateway or connection configuration; or in the controller definition menu, by selecting either the controller button (**Devices > Controller**) or by using **Express Setup program**. EntraPass supports five types of controllers:

KT-100, KT-200, KT-300, KT-400 and KT-1. 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	Door(s)	Wireless Doors (licensed)	Relays	Input Zones	Auxiliary Outputs
KT-100	1	not supported	4	4	2
KT-200	2	not supported	2	16	4
KT-300	2	not supported	2	8	4
KT-400	4	8	4	16	16
KT-1	1	2	2	5	5

Note

Unassigned modules

To find a list of modules communicating with a controller but unassigned, click the **Request Unassigned Modules** icon. A window with the following information displays:

Module Type: ioSmart or ioModule.

Module Serial Number: of the module.

To define an unassigned module, right-click the module, and click **Assign module**, it automatically populates the module's data into the controller's configuration page in the **ioModule** tab, or the **ioSmart** tab. If required, rename the module, or change the configuration details, and click **Save**. When you define the module, the system removes it from the list.

Configuring General Parameters for Kantech Controllers

1 - From the **Devices/Controller** window, select a **Site filter** from the first drop-down list.

2 - Select the **Gateway** (please refer to **Gateway Configuration** for more details about configuring a gateway) .

3 - From the **Connection** drop-down list, select the connection where the controller is located (please refer to **Connection Configuration** for more details about configuring a connection) .

4 - 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.

5 - From the **KT controller type** drop-down list, select a controller type. Once selected, the language section is enabled. You may rename the selected controller.

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

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

Note

EntraPass offers you the ability to install two types of readers on the same controller (primary and secondary). This feature is only available with KT-100 and KT-300. For KT-400/KT-1, 8 different reader types can be loaded (this feature is supported with firmware 1.06 and later).

On a given controller, all reader types must be the same (Wiegand or ABA).

6 - Select the reader installed on your controller from the **Reader type** drop-down lists. Check Table 1 for the reader types versus the controller type.

Note...

The *button allows you to install a custom driver for a specific controller. Moreover, using this button allows you to add the driver in the Reader+ Driver table, making it available the next time you want to configure a new controller.*

Table 1: Reader Types

Reader Types	KT-100	KT-200	KT-300	KT-400/KT-1
ABA with Type CNPID Cards	Yes	Yes	Yes	
BC-201 - CF100	Yes	Yes	Yes	
BC-201 Bar code with Polaris Cards	Yes	Yes	Yes	Yes
CARDKEY	Yes	Yes	Yes	
CASI-RUSCO 26/28-Bit Wiegand	Yes	Yes	Yes	
CHECKPOINT Sielox Format	Yes	Yes	Yes	
CHUBB	Yes	Yes	Yes	
DORADO ABA clock and data	Yes	Yes	Yes	
DORADO ABA Wiegand	Yes	Yes	Yes	
DORADO EMPI 26-Bit	Yes		Yes	
DORADO EMPI 34-Bit	Yes	Yes	Yes	

Reader Types	KT-100	KT-200	KT-300	KT-400/KT-1
FIPS 201 75-bit no expiry date				Yes
FIPS 201 75-bit with expiry date				Yes
h20302, 37-Bit	Yes	Yes	Yes	Yes
HID CORPORATE 1000 Generic	Yes	Yes	Yes	Yes
HID iClass 37-Bit No Party				Yes
HID KSF (Kantech Secure Format)	Yes	Yes	Yes	Yes
HUGHES 36-Bit - CF104	Yes	Yes	Yes	
INDALA old 27-Bit Format	Yes	Yes	Yes	
INTERCON	Yes	Yes	Yes	
ioProx Dual Driver (26-Bit and XSF)	Yes	Yes	Yes	Yes
ioProx Kantech 26-Bit Wiegand	Yes	Yes	Yes	Yes
ioProx Kantech XSF Format	Yes	Yes	Yes	Yes
ioProx UK 31-Bit Wiegand				Yes
ioSmart Kantech SSF Format (Wiegand)	Yes	Yes	Yes	Yes
ioSmart Kantech SSF Format (RS-485)				Yes
KRONOS Card with Bar Code Reader	Yes	Yes	Yes	
Mifare 32-Bit CSN	Yes	Yes	Yes	Yes
Mifare 34-Bit AID 517A	Yes	Yes	Yes	
Mirage 135	Yes	Yes	Yes	
NCS	Yes	Yes	Yes	
Northern 32-Bit with NR1 Reader	Yes	Yes	Yes	
Northern 34-Bit with Hughes Reader	Yes	Yes	Yes	

Reader Types	KT-100	KT-200	KT-300	KT-400/KT-1
Paramount Farm 32-Bit Wiegand	Yes	Yes	Yes	Yes
Polaris 1 - CF101	Yes	Yes	Yes	
Polaris 1 with 10-Digit Cards	Yes	Yes	Yes	
Polaris 1 with 16-Digit Cards	Yes	Yes	Yes	
Polaris 1 with Polaris Cards	Yes	Yes	Yes	Yes
Polaris 2 ABA with 10-Digit Cards	Yes	Yes	Yes	
Polaris 2 ABA with 16-Digit Cards	Yes	Yes	Yes	
Polaris 2 ABA with Polaris Cards	Yes	Yes	Yes	Yes
Polaris 2KP ABA with 10-Digit Cards	Yes	Yes	Yes	
Polaris 2KP ABA with 16-Digit Cards	Yes	Yes	Yes	
Polaris 2KP ABA with Polaris Cards	Yes	Yes	Yes	Yes
Polaris 32/35/37 CHRS - CF103	Yes	Yes	Yes	
RBH 50-Bit Card Driver				Yes
SCHLAGE 1030 and 1040 Card Format	Yes	Yes	Yes	
Sensor 26-Bit Wiegand Standard	Yes	Yes	Yes	Yes
Sensor 34-Bit Wiegand	Yes	Yes	Yes	Yes
SFT-R50 26-Bit	Yes	Yes	Yes	
Shadow PROX	Yes	Yes	Yes	Yes
Siteguard Format	Yes	Yes	Yes	
Wiegand 26/28-Bit - CF102	Yes	Yes	Yes	
WLS Wireless 26-Bit	Yes	Yes	Yes	
WLS Wireless Shadow Prox and HID	Yes	Yes	Yes	

7 - Select the keypad installed on your controller from the **Keypad type** drop-down list. Check Table 2 for the keypad types versus the controller type.

Table 2: Keypad Types

Keypad Types	KT-100	KT-200	KT-300	KT-400/KT-1
KP-1003H	Yes	Yes	Yes	
KP-500, KP-2000, KP-2500, KP-3000	Yes	Yes	Yes	
ioProx with Integrated Keypad (8-Bit Burst)	Yes	Yes	Yes	Yes
POL-2KP - 5-Digit Integrated Keypad	Yes	Yes	Yes	Yes

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

Note...

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

---

9 - Select the **Vital LED** mode (for KT-1 only). Please refer to KT-1 Installation manual D29008966 for details.

10 - Select between **On demand** and **Always on** for the **Status LED** (for KT-1 only) . Please refer to KT-1 Installation manual D29008966 for details.

11 - Select a **Graphic** and **Video view** to which the gateway is assigned, if applicable. The video view will only be activated If the video feature is enabled in EntraPass.

Changing controller type

Controller types can be updated to newer controllers without resetting the controller configuration. To change the controller type do the following:

1 - From the **Devices** tab select **Controller**, then select a **Controller** from the drop-down list.

2 - Select a new controller type from the **KT controller type** drop down list.

3 - Click the save button. A warning message asks if you want to continue. Press **Yes** to continue. This launches the **Express Setup** window.

4 - Any undefined components can be configured using the **Express Setup** window. For example when changing from a KT-1 to a KT-400, the undefined doors can be configured.

5 - Click **OK** to complete the process.

6 - During the process the option **Disable controller polling** is automatically checked. Ensure that this option is unchecked

This function only supports updating controllers to newer controllers. The rules for updating controller types are summarized in the following table.

Original controller type	Supported update controller types
KT-100	KT-300, KT-1, KT-400
KT-200	KT-300, KT-400
KT-300	KT-400
KT-1	KT-400

Note...

When converting from KT-100 or KT-1 to KT-400 exit readers are converted to a second door.

Note...

It is not possible to change the controller type if a KT-IP has been used.

Note...

Combus and SPI modules associated with a controller cannot be transferred. To change the controller type, definitions for combus and SPI modules must first be removed.

Configuring Specific Controller Parameters

1 - Select the **controller** tab (KT-100, KT-200, KT-300, KT-400 or KT-1) from the **Controller** window.

2 - Enter the controller serial number in the **Serial number** field. Usually, the number is found on the controller label. The field is defined to accept only numeric characters, except for the first character which may be an a or A . If a lower case character is entered, the system converts it to a capital letter.

3 - For KT-400 only:

- To configure SPI modules, please refer to **Expansion Modules Setup**.
- To configure the elevator floor associations, please refer to **Defining the KT-400 Elevator Floor Associations**.

4 - For KT-300 only:

- To configure Combus Modules, please refer to **KT-300 Combus Modules**.

- To configure the elevator floor associations, please refer to **Defining the KT-300 Elevator Floor Associations**.

5 - For KT-200 only:

- To configure KT-200 Auxiliary devices , please refer to **Configuring KT-200 Auxiliary Devices**.
- To define REB-8 relays, please refer to **Defining REB-8 Relays**.
- To configure REB-8 elevator controllers, please refer to **Programming REB-8 Elevator Controllers.**
- To configure KT-2252 elevator controllers, please refer to **Programming KT-2252 Elevator Controllers**.

6 - Enter the **Wait for second access card delay**. The maximum time allowed is 2 minutes and 7 seconds. This feature is useful for secured areas where two cards are required to access a secured door. If the value entered is greater than the maximum allowed, the system will use the existing value.

7 - 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.

8 - In the **EOL resistor (5.6K)** drop-down list, select the resistor type used with your system. By default, this choice is set to **None** . This feature is used as a supervision device for all inputs. In fact, if this feature is enabled and if an input is disconnected, an alarm message is generated and sent to the **Alarm message** desktop (or other desktop configured to receive such events).

9 - Select a value from the **RS-485 baud rate** list.

10 - In the **Reader template** list, click the **more options** button to select a reader template. Selecting a template ensures any reader connected to the controller inherits the template properties.

11 - Click the **Save** button.

Configuring the Status Relay Activations (multi-site gateway only)

Select the **Status relay** tab to program a relay or group of relays that will be activated when an event occurs. Click the button to select a relay or a group of relays (not available for KT-100).

Configuring Licensed Wireless Doors

*The **Licensed Door** feature must be installed prior to use. See System Registration for details.*

The licensed wireless door feature supports the addition of Assa Abloy wireless doors in EntraPass. For more information about configuring the Assa Abloy interface, refer to the Application Note, *ASSA ABLOY Wireless Locks integration (AH30 hub, serial)*. To configure your EntraPass installation for licensed wireless doors do the following.

- From the **Devices/Controller** window, select the controller you want to configure. If the controller supports licensed wireless doors the licensed door icon will be available from the **Controller** menu bar.
- Select the Licensed doors symbol.
- If no integrated panel has previously been linked to that controller EntraPass will automatically create a new integrated panel.
- Select **Configuration** to open the **Licensed Doors** window. The number of **Purchased** licences and **Available** (remaining) licenses is displayed.
- To add a door select **+**.
- You must input a description of the door and the device address. The device address (EAC address) has been configured during the configuration of the wireless lock. For more information about configuring the Assa Abloy interface, refer to the Application Note, *ASSA ABLOY Wireless Locks integration (AH30 hub, serial)*.
- Check the correct box to indicate whether the door has a **contact** (to indicate open or close) or a **REX** (Request To Exit) functionality.

- To delete a door select **Delete** followed by **OK**.

- If an integration panel has previously been linked to the selected controller the **Licensed Doors** window will be displayed. Here you can edit existing wireless doors.
- To view the status of the wireless lock select the wireless lock from the **Operation/Integrated Panel**. The icon will signify if the device is operational. To view details double-click on the device. The possible states are listed in the table.

Parameter	Possible States
Door Number:	
Tamper:	• Tamper in alarm • Tamper in normal condition • [Unknown State: NOTHING DISPLAYED]
Device communication status :	• Device Online, as per Hub Status • Device Offline, as per Hub Status • [Unknown State: NOTHING DISPLAYED]

Parameter	Possible States
Door side:	• Door side: Inside • Door side: Outside • Door side: Both inside and outside • [Unknown State: NOTHING DISPLAYED]
Handle State:	• Handle not used • Handle used • [Unknown State: NOTHING DISPLAYED]
Key Cylinder State:	• Key cylinder not used • Key cylinder used • Key cylinder is in Specific position: 1 (or 2 or 3) • [Unknown State: NOTHING DISPLAYED]

Parameter	Possible States
Lock State:	• Door unlocked • Door locked • Door lock secured • Door lock jammed • [Unknown State: NOTHING DISPLAYED]
Door State:	• Door opened • Door closed • [Unknown State: NOTHING DISPLAYED]
Protocol version:	
Version Number:	
Vendor ID:	
Mac Address:	
Hub Mac Address:	

Parameter	Possible States
On abnormal behaviour:	• Controller firmware does not support this integration • No Reader Driver available • Door not configured • Input not configured

Note

Licensed wireless doors can be identified by a blue icon. Wired doors have a green icon in EntraPass.

There are less configurable parameters for wireless doors when compared to wired doors. There are also some differences to the operation of wireless doors.

- Some manual features such as **Arm Door**, **Disarm Door**, **Door contact back to schedule** and **Disable Door Contact** are not available for wireless locks.

- Wireless locks will go into a sleep mode to conserve power. When you send a manual operation to these locks you must wake up the lock (by interacting with the lock) for the manual operation to be processed. This is also true of unlock schedules which require the lock to be woken up to operate correctly. To wake a lock you may need to swipe your card twice.
- On initial power up the **Tamper State** will be reported as **Unknown** until the lock cover has been opened.
- If a wireless hub looses power it will not retain the last status of it wireless locks.
- The buzzer and LED cannot be controlled through EntraPass.

- When switching the length of the pin code, the wireless lock must be configured through it's own interface.
- The current status of the lock is only updated on an event.
- The wireless lock cannot be operated when disconnected from the controller.
- The lock state refers to deadbolt of he lock. When the dead bolt is engaged the lock state becomes unknown.
- Currently only 26-bit drivers are supported for wireless locks.

Note

*If you select **Devices / Integrated Panel...Print** you can see the number of licensed doors associated with that integrated panel.*

Note

Currently, wireless licensed doors are only supported for KT-1 and KT-400 controllers.

Defining Controller Options

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

- Anti-passback (for synchronizing entry/exit readers)
- Duress function (for defining a panic button)

- Card count options (for specifying cards in an area), etc.

Note...

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

---

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

2 - Determine the **Duress** options . When a duress option is selected, you have to assign a duress key, that is a silent panic key.

- **Duress on access granted** : This option enables the duress key when access is granted.
- **Duress on access denied** : This option enables the duress key, even when access is denied.

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

Note...

For added security, you may select both options. The anti-passback programming is only available on a multi-site Gateway.

---

4 - From the **Anti-passback options** (multi-site Gateway only) , select the **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 anti-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 " **Access granted - Passback bad location** " event is sent to the **Message desktop**.

- **Hard anti-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. Only an " **Access denied - Passback bad location** " event is sent to the Message desktop.

- **Controller local area:** This selection enables the **Controller local area** tab. This option is only functional with the KT-400; the **Controller Local Area** tab will only appear with a KT-400 (please refer to **Defining the KT-400 Controller Local Areas** for more details).

5 - In the **Forgive schedule** section, click the three-dot button to set a schedule for resetting the anti-passback option on all other cards.

Note...

*The **Forgive Schedule** section is enabled only when Soft anti-passback or Hard anti-passback item is selected.*

---

6 - In the **Miscellaneous** section, indicate options for **Enable fail-soft delay (10-255 s)** . During a fail-soft mode, the controller operates in stand-alone mode, following a communication failure.

7 - Enter the **32-bit card family code** (optional). You can locate this hexadecimal code on the access card.

8 - In the **Card count options** , use the up or down controls to set the maximum card number. The **maximum card number** allowed is 2,147,483,647. The system keeps track of the number of monitored cards that are in the monitored area and activates a relay when the count is reached. When users exit the area, the counter decrements and the relay will eventually reset when the count is smaller than the value defined.

---

9 - You may configure the system to **activate a single relay** or a **group of relays** 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.

Note...

*The **Activate relay** section is enabled only when Soft anti-passback or Hard anti-passback item is selected.*

Supervision Schedule

1 - Select a schedule for the **Power supervision** (not available for KT-1).

2 - Select a schedule for the **Tamper switch** (not available for KT-100 and KT-300).

Note

*Please refer to **Schedules Definition** for more details about schedule configuration.*

KT-200

Defining KT-200 Auxiliary Devices

---

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

2 - In the **Auxiliary devices** section, select the type of devices used with KT-200 controller.

- Check the **REB-8 relay** option if REB-8 expansion boards are used as relays. Only 16 relays can be defined. If two REB-8 are added, the last two relays (the 17th and 18th relays) can be used to perform different actions. You have to specify the additional actions for the two relays in the **Extra relay** drop-down list.

- Check the **KT-2252 elevator controller and REB-8 relay** option if KT-2252 are used as elevator controllers and REB-8 are used as relays on the same door controller. A maximum of four KT-2252 can be connected to the controller.

- Check the **REB-8 Elevator Controller** option if REB-8 are used for elevator control. Up to four REB-8 can be used for elevator control.

Note...

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

Programming KT-2252 Elevator Controllers

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

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

---

2 - In the **Auxiliary devices** section, select **KT-2252 elevator controller** , or **KT-2252 elevator controller and REB-8 relay** . The **Elevator** tab appears.

3 - To configure elevator controllers, select the **Elevator** tab. When KT-2252 elevator controllers are used, the **Elevator mode** section is enabled.

4 - In the **Elevator mode** section, check the appropriate number of floors. This indicates how the floors are controlled with the KT-2252.

- Select 16 Floors if there is one KT-2252 for two cabs sharing the same floors.
- Select 32 Floors if there is one KT-2252 per cab.

Note...

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

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

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

Number of Cabs	Number of Floors	Number of KT-2252
2	32	2
2	64	4

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

Note...

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

Programming REB-8 Elevator Controllers

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

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

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

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 (in the **Floor** 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 **Doors Configuration.**

Note...

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

Defining REB-8 Relays

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

1 - Under the **KT-200** tab, 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 REB-8 relay** option. In either case, the REB-8 definition section is enabled.

3 - In the **REB-8 Definition** section, select the appropriate option: **No REB-8, One REB-8** or **Two REB-8.**

4 - If two REB-8 are added (for a total of 18 relays), the last two relays can be used to perform different actions: select the use for the extra relays from the **Extra relay** drop-down list.

5 - Select the **Status relay** tab to program a relay or group of relays that will be activated when an event occurs.

KT-300

Defining the KT-300 Elevator Floor Associations

Note...

*The **Elevator** tab displays only when Combus modules have been defined as elevators under the **KT-300** tab.*

Associating Floor Numbers

1 - In the **Controller** window, click the **elevator** tab to define the floor associations.

2 - From the **Floors** drop-down menu, for each number select a floor.

3 - Click **Save** .

Note

*To define floors, please refer to **Floor Definition**.*

KT-400

Configuring the KT-400 Expansion Modules

The KT-400 support expansion modules through its SPI expansion port. The SPI port is a 6-conductor cable bus to which several expansion modules are daisy-chained to add inputs, outputs and relays.

Note...

The KT-400 SPI port maximum current draw is 500 mA, when the 12V AUX terminals are not used. External power supply (12 VDC, 2 Amps) for the expansion module is required when the total current draw exceeds 500mA on the SPI Port. For additional hardware details, please refer to the KT-400) Installation Manual , DN1726.

Three expansion module types are available:

- **KT-MOD-INP16** : The KT-MOD-INP16 is an input module that adds 240 zones to the KT-400 controller. Up to 15 input modules (16 input modules if used for elevator configuration) can be connected to a KT-400 for a total of 240 external inputs. Adding the 16 onboard inputs of the KT-400 gives a total of 256 inputs per KT-400. For further details, check the KT-MOD-INP16 KT-400 Expansion Module 16-Zone Input with SPI Cable, Install Sheet , DN1776.

- **KT-MOD-OUT16:** The KT-MOD-OUT16 is a 16-output module. It can be used for elevator access control with additional hardware. Up to 16 output modules can be connected to a KT-400 for a total of 256 outputs. For further details, check the KT-MOD-OUT16 KT-400 Expansion Module 16-Output with SPI Cable, Install Sheet , DN1781.

- **KT-MOD-REL8:** The KT-MOD-REL8 is an 8-relay outputs expansion module used as general relays or elevator control outputs. Up to 32 relay modules can be connected to a KT-400 for a total of 256 relays. For further details, check the KT-MOD-REL8 KT-400 Expansion Module 8-Relay Output with SPI Cable, Install Sheet , DN1786.

The following table summarizes the options associated with each module:

Expansion Module	Options
KT-MOD-INP16	Controller inputs (up to 256) and/or elevator inputs (up to 64 per elevator door)
KT-MOD-OUT16	Outputs relays (up to 256) and/or elevator outputs (up to 64 per elevator door)
KT-MOD-REL8 (***Note***)	Relays (up to 256) and/or elevator outputs (up to 64 per elevator door)

Note...

*There are already 4 relays available on the KT-400. Make sure to check the **relay number assignments** to prevent redundancy unless it has been planned on purpose.*

The 9-16 relay configuration is set by default.

1 - If an expansion module(s) is(are) connected to a KT-400, click the **SPI module configuration** button. The **Expansion modules setup** appears.

If you want to	**then** go to
configure an input module KT-MOD-INP16	Step 2.
configure an output module KT-MOD-OUT16	Step 5.
configure an output module KT-MOD-REL8	Step 6.
modify an existing expansion module configuration	Step 7.

2 - To add a KT-MOD-INP16, select the **Input Module** tab and then click on **Add** . If there is more than one input modules listed, make sure that you select the correct one before changing the input assignments. Assign names to the modules in the language fields and choose the options.

3 - Select the **DEOL: Double end-of-line resistor JP4 On** checkbox to define a KT-MOD-INP16 module in DEOL.

Note...

The entire expansion board is used to provide 8 inputs with DEOL. These 8 inputs are added of the next group of 8 inputs. For example, if inputs #33-40 are linked to a DEOL module, inputs #33-40 and #41-48 will not be available for other modules.

Controller inputs 1-16 are reserved to the inputs on the KT-400.

---

4 - Selection of the inputs numbers can be done in two ways; using the drop-down menu or the **Extended selection box**. Right-click on the inputs menu selection to view the **Extended selection box**, see **Using the Extended Selection Box**

Note...

---

*This is an exclusive condition. You cannot select the same item in the **Inputs** drop-down menu and in the **Elevator inputs** drop-down menu because it will be a duplicate, and the system does not accept any duplicate. For example, **Inputs # 17-24** cannot be selected twice. Another way to let you understand this concept, is that in the **Elevator inputs** menu the same item will not be available for the same door. The same concept applies for the **Elevator outputs** menu.*

---

5 - To add a KT-MOD-OUT16, select the **Output Module** tab and then click on **Add** . When you click on the **Add** button, a menu appears and lets you select which output module you want to add. Assign names to the modules in the language fields and choose the options.

6 - To add a KT-MOD-REL8, select the **Output Module** tab and then click on **Add** . When you click on the **Add** button, a menu appears and lets you select which output module you want to add. Assign names to the modules in the language fields and choose the options.

Warning: There are already 4 relays available on the KT-400. Make sure to check the relay number assignments to prevent redundancy unless it has been planned on purpose.

7 - From the **Summary** tab, you can modify all the modules. Make sure to highlight the module you want to modify in the left column before doing any modifications on the right side.

8 - When you have finished configuring the expansion modules, click the **OK** button to go back to the KT-400 configuration window.

Note...

*For more information, **Connection Configuration**.*

---

ioModule

To define a KT-MOD-IO16 for a KT-400, or a KT-1 controller, click the **ioModule** tab, and complete the following steps:

1 - Select a controller from the **Controller** list, and click the **ADD** button.

2 - In the **ioModule** area, type the name of the ioModule in the language field.

3 - In the **Serial Number** field, type the serial number.

4 - Select one of the following terminal banks:

- Terminals 1 - 4
- Terminals 5 – 8
- Terminals 9 – 12
- Terminals 13 – 16

For each terminal select one of the following action options:

- **Not in use**: this is the default setting. Select to indicate that terminals are not in use.
- **Use as input**: select to use terminals of inputs/outputs as inputs. EntraPass uses the same setting for EOL as the controller settings. If you want to change EOL settings, use the **Input** menu. For more information see, **Configuring Specific Controller Parameters**In the **Inputs** field, select an input bank from the list.

Note:

You cannot use an input bank on multiple devices. When you use it on one device, it is no longer available, until you delete the configuration.

- **Use as relay**: select to use terminals of inputs/outputs as relays. In the **Relays** field, select a relay bank from the list.

Note:

You can define a relay bank on multiple devices, they mirror each other.

- **Use as elevator**: select to use terminals of inputs/outputs as elevators doors. Two further options become available:
  - **Use as outputs**
  - **Use as floor confirmation (inputs)**

Use as outputs

a - In the **Elevator** field, select an elevator from the list.

b - In the **Elevator outputs** field, select the elevator output bank from the list.

Note:

You can define an elevator output bank on multiple elevators they mirror each other.

Use as floor confirmation (inputs)

a - In the **Elevator** field, select an elevator from the list.

b - In the **Elevator inputs** field, select an elevator input from the list.

Note:

You cannot use an input bank on multiple devices. When you use it on one elevator, it is no longer available, until you delete the configuration.

Terminals 9 – 12

In addition to the **Not in use**, **Use as input**, **Use as relay**, and **Use as elevator** options, **Use as SPI** is available for Terminals 9 – 12.

Use as SPI: select to use terminals 9 – 12 as SPI relays. In addition to the 32 SPI relay modules defined directly in the **SPI** tab, you can add another 32 relay SPI modules using the **ioModule** tab.

To continue the configuration, complete the following steps:

a - Click the **SPI** tab, and click the **Output module** on **ioModule** tab.

b - If you have defined more than one **ioModule**, select the one you want from the **ioModule** list.

c - In the **Relay 1 - 8** tab, select one of the following options:

- **Not used**
- **Used as relays**
- **Use as elevator equipment**

Note:

You can define relays on the SPI expansion module, and on the ioModule. For example, for the KT-1 controller, if you define relays 1 - 4 on an ioModule, and an SPI expansion module, it lights up on the controller, the ioModule, and the SPI expansion module.

5 - To remove a module, click the **REMOVE** button.

Enable Exit Reader

This feature is to bring up the number of readers to 8 (on 4 doors) for KT-400 and KT-401 controllers (only) when using ioProx XSF or IoProx UK 31 bits readers. This way, a second reader can be connected to the controller. That second reader will keep the same values as the first one for:

- Door lock mode
- Unlock time
- Open time
- Extended Unlock time
- Extended Open time
- Unlock Schedule
- Video View
- Graphic
- All “Door Contact” features
- Relay Activation for Door events except “Door forced open”

The second door will automatically be labelled with the first door name plus the word **EXIT** at the end.

1 - From the **KT-400** tab, under **Enable exit reader**, select the doors for which the reader has to be enabled.

2 - Click **Save** .

Notes

- The feature is available only when IoProx XSF or IoProx UK 31-Bit readers are used under **General/Reader and keypad**. If another type of reader is selected, the option is not available.
- A number of option fields are not available for the 2nd reader since values are already programmed in the first one.
- If you deselect the exit reader under controller, the exit reader will be disabled. It is not possible to DELETE an exit reader.

Defining the KT-400 Controller Local Areas

Note...

*The **controller local area** option is only available with a KT-400 controller on a multi-site Gateway (see **Defining Controller Options** for the procedure to enable the **Controller local area** tab) .*

---

1 - Click the **Controller local area** tab to define up to 4 local areas.

2 - Assign a name for both languages for the 1st controller local area.

3 - Select the **Forgive schedule** from the drop-down menu.

4 - Enter the maximum number of cards allowed in the **Cards threshold** field.

5 - Check the **Deny access on area full** box to prevent more users to enter the area after the cards threshold has been reached.

---

6 - Click on the three-dot to select the relay or the relay group to activate when the cards threshold has been reached.

7 - Repeat **steps 2** to **6** for each controller local area.

Defining the KT-400 Elevator Floor Associations

Note...

*The **Elevator** tab displays only when expansion modules have been defined as inputs or outputs for elevators under the **KT-400** tab.*

For KT-400 controller, it is possible to choose up to four patterns to define door and floor numbers that will be associated with each pattern. By default, pattern 1 specifies all door numbers.

1 - In the **Controller** window, click the **elevator** tab to define the floor associations.

2 - In the **Elevator** tab, click **Pattern #2** , and then select the appropriate **Door** number check box(es).

3 - From the **Floors** drop-down menu, select the appropriate item or floor number to associate with the door number and the pattern number.

4 - Repeat **Steps 2** and **3** for each pattern.

5 - Click **Save** .

Note

To define floors, please refer to ***Floor Definition.***

KT-1

enrolment Button

The enrolment button is used to send an “enroll me” request to EntraPass with the controller status which includes:

- IP address
- How it is powered (PoE or 12 VDC)
- Full Status

1 - The installers press the enrolment button.

2 - The controller then sends information for a period of 10 minutes at 30 seconds intervals.

3 - Once the 10 minutes delay is expired, the controller stops sending information.

Note...

For the enrolment process to be allowed for a given operator, it must first be enabled in ***System/Security Level/Devices/Connection/enrolment****.*

When an enrolment request is received, a circled digit will be displayed at the bottom right side of the workstation main window. The digit indicates the number of unassigned controllers. When there is only one unassigned controller, double-click on the circle to open the **enrolment Wizard**. Follow instructions on the screen. You can also do a right-click on it to display a contextual menu that contains the following options:

- **Define**: Display the enrolment Wizard.
- **Full Status**: Displays the full status window. Provide a pop-up box with the IP address, how it is powered (IP or 12 VDC) and the full status information.
- **Delete**: Remove the selected controller from the list.
- **Assign to an account**.

The Unassigned Controllers List

When EntraPass receives data from the KT-1 enrolment process it adds the controller to the controllers unassigned list. The "Controller was added to the unassigned list" event is then generated with the following parageters:

- Gateway description
- MAC address
- Device type

The unassigned controllers list displays:

- Date and time (when it was added to the list) of the gateway
- Controller model
- MAC address
- Serial number

- Broadcast received IP address

Note

The unassigned controller list can have a limited number of 100 entries.

Video Gateway or Video Vault enrolment

When the video gateway or video vault receives an outbound connection, it receives the following incoming information from the DVRs:

- Name
- Serial number
- IP address

The above list remains in wait mode, ready for assignment to a hattrix account or a defined Corporate Edition, or Global Edition system. In the workstation, the enrolment pending count displays on the lower right section of the status bar. Double click the **enrolment pending** label to open the following report:

Column	Description
Request date	Date request received.
Account	Identifies if the account is selected or assigned.
Icon	Video server.

Column	Description
Model	exacq model.
MAC adress	MAC address of the DVR unit.
Request received from	IP address of the DVR that sent the request.

When you select an enrolment, double-click the enrolment to bring up the context sensitive menu. The following options are available:

Column	Description
Define	Opens the **Video Server** window that EntraPass pre-populates with information received from the outbound connection, which is the active account. Rename the DVR and save it.
Delete	Prompts to confirm and remove the unit from the list.

When you define a DVR using enrolment, the **Video Server** window opens, with fields pre filled with information received from the outbound connection. When you define a DVR unit, EntraPass removes it from the list.

If you input the incorrect log in credentials, an error message is displayed. If the import is successful, a confirmation window is displayed. When you click the **Save** button, the camera details are automatically called. You can then rename the DVR in the **Server Parameters** tab. To maintain the name of the imported cameras, select the **Override Camera name from DVR** check box, if you clear the check box, operators can change the name of imported camera.

Adding an ioSmart reader

Follow the steps in **How to setup the ioSmart** to add an ioSmart reader.

Controller Event Buffer Overflow Message

When a controller is disconnected from the server, the controller buffer starts collecting the controller's events. When the buffer is full, it transfers the oldest events in a secondary buffer (50 to 100 bytes) that always contain 50 events. When the communication is restored, the system then starts sending messages to the **Desktop Message List** to indicate that the buffer is full and that events are being deleted from the buffer.

- The controller will delete messages in **FIFO** order (First In, First Out). The oldest message will therefore be deleted first.

- When the controller is reconnected to the server, the controller events will be sent to the **Message list** all at once, in the following order: events in the controller's secondary event buffer; a single **Event Buffer Overflow** will display, followed by the list of events generated while the controller was disconnected from the server.

Comment

*For more details about the **Comment** entry box, please refer to **Comment Field**.*

KT-300 Combus Modules

Five Combus modules can be connected to a KT-300:

- **KT-PC4108** (8-zone input expansion module). This module has a tamper contact input.
- **KT-PC4116** (16-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-LCD3** (Kantech 32-character liquid crystal display). The LCD is green (normal status), red (power failure) and yellow (trouble).

1 - If a Combus module is installed to the KT-300 controller, click the **Combus module configuration** button. Undefined Combus terminals are identified by red flags/bullets. Once a module has been defined, it is identified by a green flag.

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

3 - Enter the module's serial number, then click **OK**.

Note...

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

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

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

Note...

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

The options associated with each module

Combus type	Options	Additional options
KT3-LCD	Combus low power, display date and time	No additional options
KT-PC4108	Tamper alarm, Combus low power	8-input module
KT-PC4116	Tamper alarm, Combus low power	16-input module
KT-PC4204	Tamper alarm, Combus low power, Low battery, Power failure, lower auxiliary power	Used as relays (1-4)
KT-PC4216	Tamper alarm, Combus low power	Used as outputs

6 - Check the **Combus low power** option so that the KT-300 will report any Combus low power condition.

7 - Check **Display date and time** option so that LCD can display the date and time.

8 - When you have finished configuring the Combus module, click the **OK** button to go back to the **Status relay** tab.

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

Note...

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

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

Note...

*For more information, see **Connection Configuration**.*

Expansion Modules Setup

Input Module KT-MOD-INP16 Configuration

1 - To add a **KT-MOD-INP16**, select the **Input Module** tab and then click on **Add**. If there is more than one input modules listed, make sure that you select the correct one before changing the input assignments. Assign names to the modules in the language fields and choose the options.

2 - Select the **DEOL: Double end-of-line resistor JP4 On** checkbox to define a KT-MOD-INP16 module in **DEOL**.

Note...

The entire expansion board is used to provide 8 inputs with DEOL. These 8 inputs are added of the next group of 8 inputs. For example, if inputs #33-40 are linked to a DEOL module, inputs #33-40 and #41-48 will not be available for other modules.

Controller inputs 1-16 are reserved to the inputs on the KT-400.

3 - Selection of the inputs numbers can be done in two ways: using the drop-down menu or the **Extended selection box**. Right-click on the inputs menu selection to view the Extended selection box, see **Using the Extended Selection Box**.

Note...

*This is an exclusive condition. You cannot select the same item in the Inputs drop-down menu and in the **Elevator inputs** drop-down menu because it will be a duplicate, and the system does not accept any duplicate. For example, Inputs # 17-24 cannot be selected twice. Another way to let you understand this concept, is that in the Elevator inputs menu the same item will not be available for the same door. The same concept applies for the **Elevator outputs** menu.*

Output Module KT-MOD-OUT16 Configuration

To add a KT-MOD-OUT16, select the **Output Module** tab and then click on **Add**. When you click on the **Add** button, a menu appears and lets you select which output module you want to add. Assign names to

the modules in the language fields and choose the options.

Output Module KT-MOD-REL8 Configuration

To add a KT-MOD-REL8, select the **Output Module** tab and then click on **Add**. When you click on the **Add** button, a menu appears and lets you select which output module you want to add. Assign names to the modules in the language fields and choose the options.

Warning...

There are already 4 relays available on the KT-400. Make sure to check the relay number assignments to prevent redundancy unless it has been planned on purpose.

Modify an Existing Expansion Module Configuration

1 - From the **Summary** tab, you can modify all the modules. Make sure to highlight the module you want to modify in the left column before doing any modifications on the right side.
2 - Click the> **Output from an ioModule** tab to define outputs created in the ioModule tab. For more information, see **ioModule**.
3 - When you have finished configuring the expansion modules, click the **OK** button to go back to the KT-400 configuration window.

Note...

*For more information, see **Connection Configuration**.*

Kantech Telephone Entry System (KTES) Configuration

The Kantech Telephone Entry System (KTES) is a telephone entry system that is suited for small and large applications with a separate access control system, or in applications that require telephone entry access only. This system provides visitor access control for a variety of applications: apartment buildings, gated communities, condominiums, office buildings, factories, and industrial sites. Visitors use the KTES to communicate directly with a tenant and are easily identified by voice communication. The tenant can grant or deny the visitor access directly from a telephone land line or a cellular phone.

Designed as a stand-alone unit, the system controls one door, auxiliary relay, and supports postal lock access. For larger commercial installations, the KTES integrates with EntraPass through a multi-site Gateway and KT-controllers to provide a complete access control solution. The entire programming of the system can be done directly on the keypad or remotely from a PC via a modem, Ethernet connection or RS-485 interface.

The system reports all events directly to EntraPass, where you can obtain a detailed event log. Additionally, programmed alarms can be reported to a pager and/or to the EntraPass system via an integrated modem. For more information on the KTES, please refer to the *KTES Installation Manual, DN1769*.

Note...

For reliability and configuration consistency, Kantech currently supports the US Robotics Sportster external modem only. Even if other type of modem are available, we strongly recommend using the officially supported external US Robotics.

Defining General Parameters for the KTES

1 - In the **Devices** toolbar, select the **KTES** button.

Note...

You must select a multi-site Gateway when configuring a KTES.

*As shown in the above picture, using the **KTES Setup Wizard** will help you setup the Kantech Telephone Entry System (KTES) in a few quick easy steps.*

Note...

*See **Configuring a KTES Using Express Setup** for more details.*

2 - Select a **Site filter** from the first drop-down list.

3 - Select the **Gateway**.

4 - From the **Connection** drop-down list, select the connection where the controller is located.

5 - From the **KTES** drop-down list, select the KTES you want to define. Once selected, the language section is enabled. You may rename the selected KTES.

Note...

*See **Connection Configuration** for more information on connection configuration.*

6 - From the **General** tab, specify the **visitor call settings** :

- **Talk time**: This is the maximum talk duration in seconds for a normal call between a visitor and a tenant (10 secs to 59 min:59 secs). Default value is 40 secs.
- **Extended talk time**: This is the maximum talk duration in seconds for a extended call between a visitor and a tenant (10 secs to 59 min:59 secs). Default value is 60 secs.
- **Talk time remaining warning** : The system sends a warning ring (a beep sound), a certain number of seconds (depending on the value entered) to indicate the end of the allowed talking period (1 sec to 59 min:59 secs). Default value is 10 secs.
- **Number of rings before answer** : This is the maximum number of rings allowed for a tenant to answer (4 to 16). Default value is 5.

- **Extended number of rings before answer** : This is the maximum number of rings allowed, for a tenant with the extended option, to answer (4 to 16). Default value is 10.

7 - Specify the **Postal Lock options** :

- **Postal lock contact**: This is the input corresponding to the door postal lock (0 to 4). Select an input and click **OK**:

Note...

*See **Input Configuration** for more information.*

- **Postal lock Schedule** : This is the schedule inside which the input, corresponding to the postal lock, generates a valid postal lock request when that input is in alarm.

Note...

*See **Schedules Definition** for more information about schedule definition.*

8 - Disable KTES polling option: Select this checkbox when you need to put the KTES in disable mode. In disable mode, the KTES will never be polled and all status requests from this specific. Default value is selected.

9 - Specify the **Tenants list** options:

- **Tenants list capacity** : By default, the capacity is 250 tenants unless you have registered for 500, 1000 or 3000 tenants total.

Note...

Remember that you are limited by the options purchased with the software. If you have registered many KTES options for additional capacity, make sure to assign it to the correct KTES site.

- **Tenants list** : Select a tenants list. Default value is empty.

Note...

*See **Tenants List** for more information about Tenants list definition.*

- **Use all tenants from list** : Check this box to include all the tenants from the list. Otherwise, leave the check box empty and click the **Customize** button. Select the check boxes for tenants to be included and/or displayed on the LCD. Default value is selected.
- Use the **Print** button to send a printout of the tenants list to a printer of your choice. Sort by **name** or by **code** and **preview** before printing.
- Select a **Graphic** and **Video** view to which the gateway is assigned, if applicable.

Defining the Kantech Telephone Entry System parameters

1 - From the **KTES** window, select the **Kantech Telephone Entry System** tab.

2 - Specify the **General options** :

- **Serial number** : The serial number is unique to each **KTES** . It is used for communication between the **KTES** and the EntraPass software. Default value is 00000000.

- **Enable fail-soft delay** : Enter the delay before EntraPass enters fail-soft mode and consider communication with the KTES lost . Values range from 10 secs to 4 min:15 secs. Default value is 45 secs.

- **EOL resistor** : This parameter defines the input termination as: **None** for no end-of-line resistor (dry contact), **Single** for single end-of-line resistor (5.6K) or **Double** for double end-of-line resistor (2 * 5.6K). Default value is **None**.

3 - Specify the **Regional configuration** parameters:

- **Line Type** : Set this parameter to select the telephone line type used by the system. Possible values are **Tone** or **Pulse** . Default value is **Tone**.

Note...

For New Zealand, pulse dialling cannot be used.

- **Telephone line regional setting** : The Telephone line regional setting must be set to specify which telephone line country code should be used by the KTES. Default value is USA/Canada (0). Click the drop down list to display the available countries:

- **Time base** : Main time base comes from the AC power input (**50 Hz** or **60 Hz**) for best accuracies over large operating temperatures. Time base will be automatically switched to internal **Xtal** in case of AC power failure. Time base can be forced to internal **Xtal** when DC power only or unstable AC source is used. Default value is 60Hz.

- **Line monitoring** : The telephone line is monitored when busy or disconnected, when this option is selected. Default value is selected.

Note...

In order to comply with New Zealand Telepermit requirements, line sensing must be turned on.

4 - Specify the **Tenant response setting** :

- **Keypad key for access granted by tenant** : This telephone key can be used by a tenant to grant access to a visitor. Default value is 9.

- **Keypad key for access denied by tenant** : This telephone key can be used by a tenant to deny access to a visitor. Default value is *.

- **Keypad key for auxiliary relay activated by tenant** : This telephone key can be used to grant access to a visitor that is using a secondary entrance. Default value is empty.

5 - Specify the **Wiegand interface** options:

- **Reader type** : This is the Wiegand Interface output format to be sent to the KTES. Default value is **Kantech XSF** .

- **Reader's Driver download**: Click on the button to open the selection window and select a driver to download:

- **Wiegand integration with an access controller** : Selecting this option indicates that the KTES is connected to an access controller. Otherwise it is operating in Standalone mode .

- **Card holder used for postal activated** : This is the card number used by the KTES to generate a Wiegand code when the postal lock is activated . Default value is empty.

Defining the Language and Welcome Message Parameters

1 - From the **KTES** window, select the **Languages and Welcome messages** tab.

2 - Specify the **Enabled languages** : Select the languages available in the KTES LCD Display. Default values are deselected.

3 - Specify the **Custom language** : Select the custom language available in the KTES LCD Display, chosen by the customer (in addition to the enabled languages). Use the **+** button to add other languages. Default value is **None** .

Note...

*See **Vocabulary Editor** for more information about Custom language definition.*

4 - Specify the **Default KTES language** : Select the default language used by the KTES . Default value is **None**.

5 - Define the **Welcome Messages** :

- Enter the message to be displayed on the KTES LCD for each enabled language. Default value is empty. Use the button next to the **Display delay** text box to centre the message text.
- Enter the displaying delay in seconds (0 sec to 4 min:15 secs). Default value is 2 secs.
- Repeat both steps for the second message.

6 - Click the **Save** button.

Special Characters

By combining the commands listed in the following table, you can display the **KTES** current hour and date according to different formats. For example:

- The complete current date in the international format: &yyy/&o/&d = 2007/01/18
- The complete current date in the American format: &o/&d/&y = 01/18/07
- The complete current hour in 24 hours format: &h:&m:&s = 14:50:55
- The complete current hour in am/pm format: &h:&m:&s&a = 02:50:55pm
- The current day in 3 letters format: &ww = mon
- The current day in 10 letters format: &wwwwwwwww = wednesday
- The current month in 3 letters format: &oo = jan
- The current month in 9 letters format: &Ooooooo = January
- The complete current date in letters and digits format: &ww &oo &d &yyy = thu jan 18 2007

Display	Format
Hour displayed in 24 hours format	&h
Hour displayed in 12 hours format	&h&a
Minutes	&m
Seconds	&s
Ten of years	&y
Year	&yyy
Month	&o
Date	&d
Day of the week	&ww to &wwwwwwwww
Current month in text format	&oo to &ooooooooo

Defining the Options Parameters

1 - From the **KTES** window, select the **Options** tab.

2 - Specify the **LCD setting** :

- **Hide PIN number** : Select this check box to hide the tenant's PIN numbers on the LCD. Default value is deselected.
- **Backlight delay** : The**Backlight Delay** is the maximum delay of inactivity before the LCD backlight turns low (0 sec to 4 min:15 secs) . Default value is 20 secs.
- **Next character delay** : The**Next Character Delay**is the maximum delay allowed between each key press before considering a next character entrance when entering a text string at the keypad (0 sec to 4 min:15 secs) . Default value is 2 secs.
- **Find user timeout delay** : After pressing the**Find**option key, the **Find user timeout delay**is the maximum delay allowed between each key press before cancelling a find sequence (5 sec to 4 min:15 secs). Default value is 15 secs.
- **Programming PIN timeout delay** : The **Programming PIN timeout delay** is the maximum delay allowed to enter a complete valid **PIN** number before entering in system programming mode (5 sec to 4 min:15 secs) . Default value is 20 secs.
- **Programming mode timeout delay** : The **Programming mode timeout delay**is the maximum delay allowed between each key press before exiting from the programming mode and returning to the welcome messages (5 secs to 9h:59 min). Default value is 60 secs.

3 - Specify the **Duress** options. A Duress alarm is used by employees or tenants to signal for help:

- **Duress on access granted** : Allows a tenant to trigger a duress alarm after a valid PIN entry. Default value is deselected.
- **Duress on access denied** : Allows a tenant to trigger a duress alarm after an invalid PIN entry. Default value is deselected.
- **Keypad duress key** : Set this parameter to configure the symbol that will activate the duress functions. A Duress alarm is used by employees or tenants to signal for help(0 to 9, # and *). Default value is 9.

4 - Specify the **Supervision Schedule** options:

- **Power supervision schedule** : To define the schedule applicable to KTES power monitoring. Select a schedule from the list and click **OK**. Default value is empty.
- **Tamper switch supervision schedule** : To define the schedule applicable to KTES tamper switch monitoring. Select a schedule from the list and click **OK**. Default value is empty.

5 - Click the **Save** button.

Note...

*See **Schedules Definition** for more information about schedule definition.*

Defining the Status Relay Parameters

1 - From the **KTES** window, select the **Status relay** tab.

Note...

*See **Relay Configuration** for more information about relay configuration.*

2 - Specify the **Relay activation** parameters:

- **Power failure** : This is the relay that can be activated when a KTES AC power failure occurs. Default value is none.
- **Battery trouble** : Relay that will be activated if the 12 volts standby battery is disconnected or comes low (under 11.5 volts DC). Default value is none.
- **Tamper in alarm** : This is the relay that can be activated when a KTES tamper switch event occurs. Default value is none.
- **Buffer 70% full** : Relay that will be activated if the event buffer for the EntraPass software has reach a 70% capacity. Default value is none.
- **Lock power trouble** : T his parameter defines the relay to be activated in the event of a door lock problem, locking device disconnected or shorted to ground. Default value is none.
- **Other troubles** : Relay that will be activated when any other trouble on the KTES occurs. Default value is none.
- **Heater kit activated** : Relay that will be activated when cabinet inside temperature falls below +5oC. Default value is none.
- **Postal lock** : Relay that will be activated with an entry request from the front door postal lock. Default value is none.

3 - Specify the **Pager call type** :

- For each event you can configure a pager call type. You can select **No call** (the relay activation for that event will not be sent to the pager), **Immediate call** (the relay activation for that event will be sent immediately to the pager) or **Schedule call** (the relay activation for that event will be sent to the pager according to the pager call schedule). Default value is **No call** .

Note...

To specify pager call types for each events, the Pager reporting function must be enabled.

Defining the Pager Options

1 - From the **KTES** window, select the **Pager** tab.

Note...

For New Zealand: This equipment shall not be set up to make automatic calls to the Telecom "111" Emergency Service.

2 - Specify the **Pager Reporting** options:

- **Pager phone number** : The pager phone number to which events will be reported (24 characters maximum). Default value is empty.
- **Pager call schedule** : The schedule number from which the KTES can communicate programmed events, alarms and troubles to the pager. Select a schedule from the list and click **OK**.

Note...

*See **Schedules Definition** for more information about schedule definition.*

- **Unit ID** : The Unit ID identifies the**KTES** that sent the pager code(0001 to 9999). Default value is 0001.
- **Restore code** : The **Restore code**is the pager code corresponding to the general event that triggered a zone restore condition (0 to 999). Default value is 0.
- **Alarm code** : The **Alarm code** is the pager code corresponding to the general event that triggered a zone alarm condition (0 to 999). Default value is 1.
- **Tamper code** : The pager code corresponding to the general event that triggered a zone tamper condition (0 to 999). Default value is 2.
- **Trouble code** : The pager code corresponding to the general event that triggered a zone trouble condition (0 to 999). Default value is 3.
- **Field separator** : The **Field separator** is the character to be used as a field separator or delimiter (*, # or ,). Default value is *.
- **Field ending** : The**Field ending** is used to indicate that the call is completed. Remember that you can enter any signs for the ending parameter (*, # or ,). Default value is #.

3 - Specify the **General event** pager codes:

- **Tamper in alarm** : The pager code that corresponds to a tamper switch problem (0 to 999). Default value is 100.
- **Power failure** : The pager code that indicates an AC power failure on the **KTES** (0 to 999). Default value is 101.
- **Battery trouble** : The pager code that indicates a low battery problem on the**KTES**(0 to 999). Default value is 102.
- **Buffer 70% full** : The pager code sent to indicate that the event buffer for the EntraPass software has reach a 70% capacity (0 to 999). Default value is 103.
- **Other troubles** : The pager code that corresponds to any other system event that can occur (0 to 999). Default value is 104.
- **Door forced open** : The pager code thatcorresponds to a forced open door (0 to 999). Default value is 120.
- **Door open too long** : The pager code that corresponds to a door opened for too long (0 to 999). Default value is 121.
- **Door alarm on relock** : The pager code that corresponds to a door left opened (0 to 999). Default value is 122.

- **Lock trouble** : The pager code that corresponds to a problem with the door locking device supervision (0 to 999). Default value is 123.
- **Keypad disabled** : The pager code that corresponds to a keypad disabled condition (when the option is enabled (0 to 999). Default value is 124.
- **Duress alarm** : The pager code that corresponds to a duress alarm. A Duress alarm is used by employees or tenants to signal for help (0 to 999). Default value is 125.
- **Access granted** : The pager code thatcorresponds to a granted access. An access granted code is sent when the tenant was granted access using his PIN (0 to 999). Default value is 140.
- **Invalid access schedule** : The pager code that corresponds to a denied access. An access denied code is sent when the tenant was denied access using his PIN (0 to 999). Default value is 141.
- **Access granted by tenant** : The pager code that corresponds to an allowed access by a tenant to a visitor (0 to 999). Default value is 142.
- **Auxiliary relay activated by tenant** : The pager code that corresponds to an allowed access by a tenant to a visitor at an alternate entrance, different from the main entrance usually used by the tenants or visitors, for example(0 to 999). Default value is 143.
- **Access denied by tenant** : The pager code that corresponds to a denied access by a tenant to a visitor (0 to 999). Default value is 144.
- **Tenant traced** : The pager code thatcorresponds to a granted access for a traced tenant(0 to 999). Default value is 145.
- **Disabled tenant** : The pager code that corresponds to an access attempt from a tenant with an invalid status (0 to 999). Default value is 146.
- **Other access denied** : The pager code thatcorresponds to an access attempt from a tenant outside of his assigned schedule(0 to 999). Default value is 147.

Configuring Tenant Administration Level Parameters

1 - From the **KTES** window, select the **Tenant administration level** tab.

2 - Specify the access parameters rights: Use the scroll boxes to set the administration level for the four different tenant types (**Full access, Read only** or **No access**).

Comment

*For more details about the **Comment** entry box, please refer to **Comment Field**.*

Doors Configuration

This menu is used to define the door parameters on which readers and/or keypads are installed. A door can be an elevator door, a In/Out door, an entry door for anti-passback, an exit door for anti-passback or an access door. It depends on how the settings are programmed. The controlled door may be secured at all times or only during defined schedules. The common locking devices used are electric door strikes and electromagnetic locks. A door may be equipped with one or two readers; one reader on 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.

***NOTE:** For a single gateway, limits are 2048 connections, 10,000 doors, 100,000 inputs and 100,000 outputs.*

Defining General Parameters for a Door

Note...

When you are using the KT-300 system, you are working with h:mm:ss and the range value can be from 00:00:01 to 9:06:07. Each time you are using a KT-400 system, you are working with hh:mm:ss and the range value can be from 00:00:01 to 04:15 (255 sec.) for a KT-100, KT-200 and KT-300; or to 18:12:15 (65535 seconds) for a KT-400 . So, please take this difference into consideration.

1 - In the **Devices** toolbar, select the **Door** button.

Note...

*The **Local areas** options are only available for a KT-400 controller on a multi-site Gateway with the*

Controller local area *property enabled* (see **Configuring the KT-400 Controller** for more information) .

The ***Miscellaneous*** *,* ***In/Out*** *, and* ***Door Anti-Passback*** *options are not available for a KTES door.*

2 - Select a **Site filter** from the first drop-down list.

3 - select the **Gateway**.

4 - From the **Connection** drop-down list, select the connection where the controller is located.

5 - 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.

6 - From the **Door** drop-down list, select the door you want to modify or define. New items are identified with a red button. The button turns green once the item has been defined and saved.

7 - From the **General** tab, specify the **Door lock mode** : Depending on the lock device used, the locked state will energized or de-energized to lock. Default value is **Fail-secure** .

- **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 (electromagnetic locks).

8 - If the door is for a **KTES** then go to **Step 13 .**

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. Default value is unchecked.

10 - Specify the **In/Out type from the drop-down list (default is None)** :

- **None** : The reader is considered as an access reader. An access reader generates only “Access granted/Access denied” events.
- **Entry** : An entry door is an entry point. 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. In order for the system to record an exit, the door must be opened after a valid access (if a door contact is installed).

11 - If the **Controller Local Areas** are enabled then go to **Step 11 .**

12 - Specify the **Door Anti-Passback type (default is Access)** :

- **Access** : The reader is considered as an access reader. **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. 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. In order for the system to record an exit, the door must be opened after a valid access (if a door contact is installed).

13 - Go to **Step 13** .

Note...

None** , **Soft anti-passback** and **Hard anti-passback** are used only with the KT-400 and **Controller Local Areas.

14 - Specify the **Door Anti-Passback** type (default is **Access**):

- **None** : The anti-passback option is disabled.

- **Soft anti-passback** : If the destination area is under **Deny Access on Local Area Full**, access is denied. When a user is passing his access card to a local area, for example, the system will allow him to access another local area even if the user was not in the **Local area before** . The system will generate the event: “ **Access granted - Passback bad location** “.

- **Hard anti-passback** : If the destination area is under **Deny Access on Local Area Full**, access is denied. 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. The system will generate the event: “ **Access denied - Passback bad location** “.

15 - Specify the **Local area before** and **Local area after** . These items are enabled and can be specified only for **Controller Local Area** .

16 - Specify the **Door access delay**:

- **Unlock time (hh:mm:ss)**: 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). The time range value can be from 00:00:01 to 04:15 (255 sec.) for a KT-100, KT-200 and KT-300; or to 18:12:15 (65535 seconds) for a KT-400. 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. Default value is 10s. For more information, see **Input Configuration.**

- **Open time (hh:mm:ss)** : 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. The time range value can be from 00:00:01 to 04:15 (255 sec.) for a KT-100, KT-200 and KT-300; or to 18:12:15 (65535 seconds) for a KT-400. 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 (**Door** window, **Contact** tab) to sound the door piezo when half of this delay has expired. It will continue to sound until the door is closed. Default value is 30s.

17 - The **Extended door access delay (hh:mm:ss)** feature allows to keep the door open for an extended period in order to allow people with disabilities to pass through without triggering an alarm. If you want to use this option, specify the delays in the **Unlock time** (default is 40s) and **Open time** (default is 2 min) fields. The time range value, for both delays, can be from 00:00:01 to 04:15 (255 sec.) for a KT-100, KT-200 and KT-300; or to 18:12:15 (65535 seconds) for a KT-400.

18 - **Unlock Schedule** will allow the system to unlock the door for a predetermine period of time that you will select.

19 - **First PersonIn** option (Not for KT-200): keeps door locked until the first granted card access while an unlock schedule is valid. Default is unselected.

- For KT-400 and KT-1 only, it's now possible to specify an **Unlock Grace Period (mm)**. This feature allows the door to be unlocked under its unlock schedule if the first card access is granted inside the selected time period before the unlock schedule starts. Time range value can be from 0 (disabled) to 59 minutes. Default value is 0 minute. For example, if the door has an unlock schedule that goes from 8:00am to 5:00pm and the **First Person In** is enabled with an **Unlock Grace Period** of 15 minutes, a valid access between 7:45am and 7:59am will allow the door to unlock automatically at 8:00am.

20 - Select **Enable Multi-Swipe** to turn the visibility of the Multi-Swipe tab ON or OFF.

21 - Select a **Graphic** and **Video view** to which the gateway is assigned, if applicable. The video view will only be activated if the video feature is enabled in EntraPass.

Note...

Under a Corporate Gateway, EntraPass offers the ability to program an extended door access delay and to specify specific unlock and open time delays reserved for people with disabilities. In addition to setting this special access delay, the user's access card must be programmed with this feature. Only available with KT-100, KT-300 and KT-400.

Defining Door Keypad Options

For KT-100 and KT-300 Controllers

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

For KT-400 Controllers

Doors can be defined with relay or relay group activation by pressing any specified key on the keypad.

Note...

*The Keypad tab is enabled only if you have selected a **Keypad type** while defining the controller associated with the door being defined. There are 4 keys. The first 2 keys: # and * are fixed keys and they are similar and play the same role as in the KT-300 system. The 2 other keys: Key 3 and key 4 are variable according to the client's needs.*

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

2 - Specify how access to the door is controlled (default is **Reader only**):

- **Reader only** : Select this option if access is granted using a reader. A reader only installation is the most common application.
- **Reader or keypad** : Select this option if access is granted using a reader or a keypad only. A keypad only installation is generally considered less secure than a reader only installation, because a user may "lend" its PIN to another person but cannot prevent further use (in comparison to getting a card back).

Note...

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

- **Reader and keypad** : Select this option if both a reader and a keypad are used to permit access to this door. The keypad will only be used when the "keypad schedule" is valid. Adding a keypad to a reader significantly increases the level of security. PIN code requirement can be limited by a schedule for use only outside business hours, for example, rather than during high traffic hours.

3 - From the **Card and PIN schedule** menu, select a schedule during which cardholders will have to enter their PIN after a valid card read. The time allowed between a valid card read and entering the PIN at the keypad is set in the Gateway definition menu (**Time-out on keypad** option).

4 - Check the **Enable duress function on keypad** option, if desired. The default value is unchecked.

5 - Select the **Keypad relay activation** key(s):

- **For KT-100 and KT-300 Controllers** : For doors defined with keypad or reader and keypad, you can program the star key (*) or pound key (#) to activate a relay. When this feature is enabled, users can activate a relay simply by pressing the appropriate key.
- **For KT-400 Controllers** : For doors defined with keypad or reader and keypad, you can program *, # or any key to activate a relay or a relay group. When this feature is enabled, users can activate a relay or a relay group simply by pressing the appropriate key.

Defining Door Contact Options

In most applications, the low cost door contact is the only supervisory element that protects the investment made to control access to the door. The door lock and card reader (or keypad) provide security and prevent unauthorized entry only when the door is closed and locked. A simple door contact allows the ability to monitor several door conditions such as: door forced open, door open too long, interlock options (mantrap), etc.

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

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

3 - In **Shunt Door Schedule,** select a schedule.

Note

A door contact cannot be assigned to more than 2 readers.

Note...

This feature allows associating a schedule to a door contact in order to bypass the events / alarms related to the door contact supervision. If no schedule is selected, the system will continue to work as usual. If a valid schedule is selected, the system will hide following conditions in the events monitoring desktop:

- Door Forced open
- Door forced open restored
- Door open too long (unless otherwise indicated)
- Pre-Alarm door open too long
- Door left open

4 - Check **Enable door open too long notification** to continue to receive the **Door open too long** event and the **Pre-Alarm door open too long** in the desktop. If there is no schedule selected, this checkbox is not available for selection (greyed out).

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.

5 - Check the door reading options:

- **Door open reading** : If selected, this option allows the system to read cards while the door is open. However the system will not unlock the door if it was locked. If selected, the event "Access granted" is generated. Otherwise, the event "Access granted - Door open" is generated. Default is checked.
- **Door unlocked reading** : If selected, this option allows the system to read cards while the door is unlocked manually by the operator or by a valid unlock schedule. If selected, the event "Access granted - Door unlocked" will be generated on access. To ignore all access events while the door is unlocked, leave this option deselected. Default is checked.
- **Unlock on access door opened:** If selected, this option allows the system to unlock access on door opened at any time. Default is unchecked.
- **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. Default is unchecked.

Note...

If the door is a KT-400 and if the value entered is higher or equal than the open time and if the checkbox is selected, a pop up will appear explaining that the delay value is incorrect. Value range can be between 00:00:01 and 18:12:15 and must be lower than the door open time.

6 - Select the appropriate **Relock on access** option. You may choose to relock an access **On door opening** or **On door closing. Default value is On door opening.**

Defining REX (Request to Exit) Options

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

1 - From the door window, select the **REX** tab, then check the appropriate **Relock on Rex** options (default is **On door closing**):

- **On door opening** , if you want the door device to re-lock following a valid access.
- **On door closing** , if you want the door device to re-lock when it closes.

2 - For the **Primary** and **Secondary REX options (the Secondary REX options does not apply to KTES)** , make the appropriate choices:

- Assign the **REX contact** : The input to which a "request to exit" detector can be connected. This input must be local; it has to be one of the inputs on the controller operating the door.
- Select a **Rex schedule**: When this schedule becomes valid, the controller will detect request to exit signals originating for the exit contact. This option applies only to a door defined with a REX contact.
- Select a **Rex Bypass Message schedule**: When this schedule becomes valid, the event will NOT be stored in archives . When invalid, event is sent to the gateway for archives. On EntraPass updates, all existing REX will have the 'Bypass REX message schedule' set to **NONE** or to **no schedule**. On a new door definition, **Bypass REX message schedule** is set to **always valid** by default.

Note...

*The primary and secondary **Rex Bypass message schedule** options will be available upon activation in **System parameters**. Please refer to **System Parameters/Schedule** for additional information.*

- **Unlock on REX**: The door will be unlocked if a valid request to exit is permitted by the controller. This option may be useful on exit doors such as interior doors, shipping doors or other push doors through which people carrying packages may pass. The system will permit the exit and generates the "request to exit granted" event rather than "door forced open" event.
- **Resettable REX function** : The unlock time is restarted on a valid request to exit. Open and unlock times are defined in the door definition (**Devices** > **Door** > **General**). Select this option for high traffic area doors such as manufacturing doors where many users may need to exit at short intervals (for example after a work shift) to prevent unwanted door open too long or door forced open events.

Note...

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

Card Multi-Swipe

This feature allows using double and triple card swipe actions with the new KT-400 firmware (KT-400: 1.08; KT-400 V1: 1.11).

1 - Select the **General** tab.

2 - **Enable Multi-swipe**: Check to enable the multi-swipe function. The Multi-Swipe tab will appear. Deselecting will disable the multi-swipe function but keep the parameters entered previously for future use. Deselecting the box will make the Multi-Swipe tab disappear.

3 - Select the **Multi-swipe** tab.

4 - **Schedule** : The schedule applies to both the double swipe and triple swipe actions and will need to be valid when the person swipes the card a second time or a third time for the corresponding action to occur.

5 - **Delay** : There is a maximum delay of 3 seconds between two card swipes to be considered by EntraPass as a double or triple swipe. A beeping sound will be heard two times for the double swipe and three times for the triple swipe. A long beep indicates a denied entry.

6 - **Relay** : Select a relay to be triggered.

7 - **Relock on access on double/triple swipe** : Relock on access on double swipe or triple swipe checkbox controls are used to lock the door before executing the double or triple swipe action.

Note...

*By default the system sets the unlock time for the door to 10 seconds and the open time to 30 seconds. If the door is kept open for more the 15 seconds after a valid swipe, a **pre alarm door open too long** (see the **Contact** tab) will be triggered and the buzzer on the reader will start to beep.*

*The pre alarm door open too long delay will override the default setting for the Open time. For example, an unlock time of 10 seconds and an open time of 2:00 minutes. If the **pre alarm door open too long** option is selected with a time delay of 00:00:20, 20 seconds before the end of the open time, the system will trigger a pre alarm door open too long alarm and the buzzer will start to beep on the reader.*

This feature is only available on KT-400 with firmware higher then 1.08.

Double/Triple swipe actions

- **Activate relay** : A relay or relay group can be selected.
- **Deactivate relay** : A relay or relay group can be selected.
- **Lock door** : Relock on access on double/triple swipe will be automatically checked and disabled
- **Request to arm granted - Alarm interface** : Equivalent to an arm door manual operation including panel partitions arming functionality.
- **Temporarily activate relay** : A relay or relay group can be selected. A delay can be entered. (between 00:00:01 and 18:12:15).
- **Temporarily unlock door** : Relock on access on double/triple swipe will be automatically checked and disabled. A delay can be entered (between 00:00:01 and 18:12:15).
- **Toggle door lock:** Relock on access on double/triple swipe will be automatically checked and disabled.
- **Toggle relay** : A relay or relay group can be selected.
- **Unlock door** : Relock on access on double/triple swipe will be automatically checked and disabled.

Defining Interlock Options (Mantrap)

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

Note...

The Interlock options do not apply to a KTES door.

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

2 - From the **Door** drop-down list, select the first door for which you want to define interlock options (mantrap).

3 - From the**Interlock contact**list, select the first input for the interlock options (mantrap). The selected input has to be the door contact of the second door .

4 - Return to the **Door** drop-down list to select the second door for which the interlock options (mantrap) are being defined; then select the interlock contact for this second door. It has to be the door contact of the first door.

5 - Select the**Interlock schedule** : The two doors must have the same interlock schedule. This is the schedule according to which the interlock is checked by the controller before access is granted to users.

Note...

The interlock options (mantrap) are not available on doors controlled by a KT-100.

6 - The **Suspend report delay on door relock (hh:mm:ss)** indicates the time during which the selected inputs will not be monitored when the door unlocks. It is not possible to shunt a door contact since the system will automatically shunt it. Values range from 00:00:01 to 18:12:15. Default is 15 secs.

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

Note...

The Shunt input items vary depending on the KT-300 or KT-400 system used.

Defining Elevator Doors

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

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

2 - From the**Unlock schedule #1** list **,** select the applicable unlock schedule. By default, you may select the **Always valid** schedule. You may also create a new schedule (**Definition** menu, **Schedules**).

3 - From the **Floor group #1** list, select the appropriate floor group associated with the **Unlock schedule #1** . Only floors that have a valid schedule in the **Floor group definition** will be unlocked or available for selection when the **Unlock schedule #1**becomes valid.

4 - From the **Unlock schedule #2** list, select the schedule applicable to the second group of floors.

5 - **From the Floor group #2** list **,** select the appropriate floor group. Only floors that have a valid schedule in the **Floor group** definition will be "unlocked" or available for selection when the **Unlock schedule #2** becomes valid.

Important Notes:

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

*For more information on how to program elevator control using REB-8 relays, see **Controllers Configuration**.*

Configuring Door Events (multi-site gateway only)

1 - In the **Door** window, select the **Door events** tab. This is to define the relays (or relay groups) that are to be activated on specified events. However, when you are using a controller other than KT-400, this tab is used to define relays only.

2 - Select the relay that will be activated locally for each event **.**

3 - **Pager call type** (applies to **KTES** only): You can select **Do not call** (the relay activation for that event will not be sent to the pager), **Call immediately** (the relay activation for that event will be sent immediately to the pager) or **Call when scheduled** (the relay activation for that event will be sent to the pager according to the pager call schedule). Default value is **Do not call** .

Note...

*To specify pager call types for each events, the **Pager reporting** function must be enabled. See **KTES Configuration**.*

Note...

4 - Once all door event features have been set, select the **Access events** tab to define relays (or relay groups if you are using KT-400) that are to be activated on miscellaneous events.

Note...

*EntraPass offers you the ability to define a relay that will be activated if the **Extended delay** feature is used. The card used must be defined with this feature. Only KT-100, KT-300, KT-400 and KTES can be configured with the Extended door access delay feature.*

5 - Select the relay that will be activated locally or the relay group (if you are using KT-400) for each event .

6 - **Pager call type** (applies to **KTES** only): You can select **Do not call** (the relay activation for that event will not be sent to the pager), **Call immediately** (the relay activation for that event will be sent immediately to the pager) or **Call when scheduled** (the relay activation for that event will be sent to the pager according to the pager call schedule). Default value is **Do not call** .

Note...

*To specify pager call types for each events, the **Pager reporting** function must be enabled. See **KTES Configuration**.*

Note...

Defining Door Options for Controllers and the KTES (multi-site gateway only)

The following tab only appears when KT-100, KT-300, KT-400 controllers and the KTES have been configured in a multi-site Gateway.

Select the **Options and alarm system** tab (or **Options** for a KTES).

- **Supervised door lock device:** This feature is used in specific applications such as bank vaults to compensate for the slow motor locks. Adding this delay avoids false door forced open alarms if a user is opening the door before it has been completely secured at the end of unlocking delay. Check this option if you want to enable it in EntraPass. Default is unchecked.

- **Motor lock delay (does not apply to KTES)** : Enter the time period (hh:mm:ss) after which the door will be considered locked. Values range from 0s to 18 h:12 min:15 secs. The default value is 0:00 for inactive. For example, if this delay is set to 5 seconds and unlocking delay is 20 seconds after access granted; the lock output will d deactivate after 15 seconds and no door forced open alarm will be generated if the door is opened during the last 5 seconds.

- If a second card read is required, select a schedule from the **Second card schedule required (two-man rule)** list **(does not apply to KTES)** .

- **Relay to follow lock output** (Only available for KT-400 and KTES): The relay follows the lock output status.
- **Multi-factor authentication**: available for go Pass cardholders presenting at a door with an ioSmart reader. To define multi-factor authentication for go Pass, select one of the following options.
  - **None**: multi-factor authentication is not enabled, present a card to the reader.
  - **go Pass**: present a card to the reader, or go Pass to the door.
  - **go Pass + Disable card**: present go Pass to the door only, disables the reader.

The option you select saves as a global setting and is the default setting when you create a new account and enable go Pass. You can change the setting as required.

Note...

The first type of authentication is an activation e-mail. The second type of authentication depends on the smartphone, use a PIN or biometric identification.

- **Enable duress function on keypad** (KTES only): Set this parameter to enable the duress function on the door controller keypad. Employees or tenants use the duress alarm to signal for help. The operator must enable the duress function. The duress function is unchecked by default. For more information, see **KTES Configuration.** For more information on the duress function for doors only, see **Defining Door Keypad Options**.

Note...

When KT-100, KT-300 and KT-400 are installed in a multi-site Gateway, the system offers the ability to interface an external alarm system.

Configuring External Alarm System Interfaces (multi-site Gateway Only)

The following option is only available when KT-100, KT-300, KT-400 and KT-1 controllers have been configured in a multi-site Gateway. KT-100, KT-300, KT-400 and KT-1 controllers 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 (does not apply to a KTES door). There are two ways of arming/disarming or postponing an external alarm system:

- On a valid card read and with the trigger of an arming input.
- On a valid arming code entered and with the trigger of an arming input.

There may be a combination of the 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.

1 - Click the **External alarm system options** button located under the **Options and Alarm System** tab in the **Door** dialog. The **Alarm system options** dialog will display on screen.

2 - Under the **Arming request** tab, select the **Arming request input** . This is the input that is activated on an external alarm arming request.

3 - Once you have selected an arming request input, you have to **Enable arming request schedule** during which the request will be valid.

4 - If applicable, select an **Arming access level** .

- The **Group** option allows you to select all access levels.
- The **Single** option allows you to select a specific level.
- If the level you want does not appear in the list, you may right-click in the **Arming access level** field to create a specific level to arm the external alarm system.

5 - To increase the security of your alarm system:

- **Wait for access granted to arm** will force the user to present a valid card before pressing the selected **Keypad button** option.
- **Relock door on request to arm** will be used in conjunction with the **Wait for access granted to arm** to override the schedule.

- **Relock door on arming after exit delay** will relock the door and arm the system after the pre-configure exit delay is over.

- **Prevent arming request on input status** will prevent arming the system if an input is in alarm.

6 - Specify the **Exit delay and Entry delay (hh: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 18:12:15 for both the exit and entry delays. When the KT-300 system is used, the maximum values are 9:06:07. Usually the entry delay is shorter than the exit delay.

7 - Select the input that will indicate the **External alarm system panel status** . 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.

- Using the checkboxes, select the appropriate input where you want an external alarm system to supervise them. Also select the appropriate item for which you want to suspend supervision (on entry, on exit, or when the alarm system is disarmed).

9 - Select the **Disarming request** tab to select the **Input to postpone arming .**

10 - Select the applicable schedule from the **Enable postpone arming schedule** .

11 - You may check the **Wait for access granted to postpone** box. 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 (**Partition and Relays** for the KT-400 to define 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.*

Managing Door Access Levels

Select the **Access Level** tab to manage the access level schedule for this door. This tab displays all the access levels where the door can be assigned.

- To create a new schedule, right-click on the **Schedule** section and select **New**.
- To edit existing schedules, right-click on the **Schedule** section and select **Edit**.
- To apply existing schedules to an access level, click on the drop-down list beside the schedule.

For more information about access levels, click **here**.

Comment

*For more details about the **Comment** entry box, please refer to **Comment Field.***

Relay Configuration

The output control relays provided on each KT-100, KT-200, KT-300, KT-400 and KTES can be used to activate alarms or other devices such as lighting control, ventilation, and air conditioning. These relays can be activated according to schedules, events reported by the system. They can also be activated to indicate the status of an alarm system or a combination of different logic conditions.

Defining Relays

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

2 - Select a **Site filter** from the first drop-down list.

3 - Select the **Gateway**.

4 - From the **Connection** drop-down list, select the connection where the controller is located.

5 - From the **Relay** drop-down list, select the relay you want to define. Once selected, the language section is enabled. You may rename the selected relay.

6 - From the **General** tab, 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.

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

8 - Specify the **Disable relay action** : When this schedule is valid, the relay will be deactivated (or activated) according to the predefined operating mode .

9 - Set the **Temporary activation timer** to indicate the delay during which the relay will be temporarily triggered following a temporary activation.

Note...

When the timer is set to zero, the default activation delay is set to five seconds. Maximum time allowed: 9:06:07 (9 hours, 6 minutes and 7 seconds). When you are using the KT-400, the maximum time allowed is 18:12:15 (18 hours, 12 minutes and 15 seconds).

---

10 - Select a **Graphic and Video view** associated with the relay, if applicable.

Comment

For more details about the **Comment** entry box, please refer to **Comment Field**.

Input Configuration

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

- **For KT-200 controllers** : 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.

- **Inputs 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.

- **For KT-400 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 (REX Door #1) of the controller. Input 5 should be reserved for contact on door 2 while input 6 should be used for request to exit device for door 2 of the controller. Input 9 should be reserved for contact on door 3 while input 10 should be used for request to exit device for door 3 of the controller. Input 13 should be reserved for contact on door 4 while input 6 should be used for request to exit device for door 4 of the controller.

NOTE: *For a single gateway, limits are 2048 connections, 10,000 doors, 100,000 inputs and 100,000 outputs.*

Defining Input

You may define inputs from the **Input** button of the **Devices** toolbar. You can also define inputs using the **Express Setup** when defining a controller (see**Express Setup Program**).

1 - From the **Devices** toolbar, select the Input button.

2 - Select a **Site filter** from the first drop-down list.

3 - select the **Gateway**.

4 - From the **Connection** drop-down list, select the connection where the controller is located.

5 - From the **Input** drop-down list, select the input you want to define. Once selected, the language section is enabled. You may rename the selected input.

6 - From the **General** tab, 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.

7 - Specify the **Normal condition** for the input: it may be **Closed** or **Opened** .

Note...

*When using single or double EOL resistors, set input **Normal Condition** to **Closed** .*

8 - Specify the **Notify abnormal condition** for the input: it may be **Alarm** or **Activate** .

9 - By default, EntraPass will not select the **Suspend status update when not monitored** . This is to keep data traffic at a minimum. However, this option can be enabled if necessary.

10 - Specify the **Input response time.** This delay corresponds to a period within which an input must remain in the same state before a transition is recognized. This delay is expressed in minutes (mm:ss:cc). **Values range from 10 secs to** 10 min:55 secs:35 cc for both the alarm response and alarm restore times.

- **Alarm response time (mm:ss:cc)**: The delay before the system generates the input and alarm event. Default is 50 cc.
- **Restore response time (mm:ss:cc)** : The delay before the system generates the input restore events (multi-site Gateways only). Default is 50 cc.

Note...

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

11 - Specify the **Telephone Entry System** options (applies to KTES only).

Note...

*To access the **modem call type** feature, the site connection type must be set to **Modem**. For more information, see **Connection Configuration**. The modem call type feature is supported by multi-site Gateways only.*

- **Pager call type** : You can select **Do not call** (the relay activation for that event will not be sent to the pager), **Call immediately** (the relay activation for that event will be sent immediately to the pager) or **Call when scheduled** (the relay activation for that event will be sent to the pager according to the pager call schedule). Default value is **Do not call** .
- Under **modem call type** , assign the call type option that best suits event reporting. Default value is **Do not call**.
- **Input pager ID** : Enter the pager code corresponding to the selected input. Possible values are 201, 202, 203 and 204.

Note...

*To specify pager call types for each events, the **Pager reporting** function must be enabled. See **KTES Configuration**.*

12 - **For KT-400 and KTES only**, check **Override default EOL (56K)**, and then, in the drop-down menu, select the appropriate item. Default is unchecked.

13 - Select a **Graphic** and **Video view** associated with the input, if applicable.

Defining 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.

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

3 - **Activate relay temporarily** will activate the relay according to the **Temporary activation parameters** defined in the **Relay** dialog. Default is unchecked.

4 - In the **Temporary Shunt Timer (h:mm:ss)** field, specify the period during which an input is not monitored. Setting the timer to 0:00:00 will instruct the relay to follow the input state. The maximum value for the **Shunt delay (hh:mm:ss)** is 18:12:15 when you are using the KT-400 or the KTES. Default is 0s.

Note...

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

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

6 - If applicable check **Shunt input temporarily** and **Reset delay for shunt temporarily** options. Default is unchecked for both.

7 - **Delay before unshunt** : Values range from 1 sec to 18 h:12min:15 secs.

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.

Defining Tamper and Trouble

1 - Select the **Tamper and trouble** tab to associate a relay or a group of relays to activate in case of an input in trouble or in tamper. This tab is visible for a zone in **DEOL** (double end-of-line) only.

2 - From the **Activate relay list** (Tamper alarm), select a relay or a relay group that will be triggered when this input is in tamper.

3 - **Activate relay temporarily** will activate the relay according to the **Temporary activation** parameters defined in the Relay dialog. Default is unchecked.

4 - From the **Activate relay list** (Input in trouble), select a relay or a relay group that will be triggered when this input is in trouble.

5 - **Activate relay temporarily** will activate the relay according to the **Temporary activation** parameters defined in the Relay dialog. Default is unchecked.

Defining an Input for an Elevator Door

When the input being defined or edited is used for elevator control, an **Elevator** tab is displayed in the Input definition window. You may associate an input to a push button. It can then be used by a guard or by a receptionist to temporarily enable the floors defined in the Floor group activation section.

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

Note...

*Only the floors marked with an "X" in the state column in the Floor group menu will be available for selection. The system will temporarily enable floor selection according to the delay defined in the **Unlock time** of the Door 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.

Enabling Remote Event Reporting (multi-site Gateway Only)

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).

Note...

The relay group is only available when you are using KT-400.

3 - Under **modem call type** , assign the call type option that best suits event reporting. Default value is **Do not call** .

Note...

*To access the **modem call type** feature, the site connection type must be set to **Modem**. For more information, see **Connection Configuration**. The modem call type feature is supported by multi-site Gateways only.*

Comment

*For more details about the **Comment** entry box, please refer to **Comment Field**.*

Output Device Configuration

Outputs usually control the reader LED and buzzer. There are four outputs available per KT-200, KT-300 (2 per door), but there are 16 outputs for KT-400 controllers (4 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.

NOTE: For a single gateway, limits are 2048 connections, 10,000 doors, 100,000 inputs and 100,000 outputs.

Defining General Options for an Output

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

Note...

*The **Miscellaneous** section is hidden in the case of using the KT-400 system because the items are already defined in the Gateway/KT-400 events.*

---

2 - Select a **Site filter** from the first drop-down list.

3 - Select the **Gateway**.

4 - From the **Connection** drop-down list, select the connection where the controller is located.

5 - From the **Output** drop-down list, select the output you want to define. Once selected, the language section is enabled. You may rename the selected output.

6 - From the **General** tab, specify the **Operating mode** for the output device (default is **Normal**):

- **Normal** : The output is switched to ground when it is activated.
- **Inverse** : The output is an open circuit (not grounded) when it is activated.

7 - In the **Selected doors** section, select which door will affect the output you are configuring:

- **First door**: Only the first door port will follow the state programmed for these events.
- **Second door** : Only the second door port will follow the state programmed for these events.

Note...

This option is not available with KT-100 and KTES.

---

8 - 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. It will leave the output activated indefinitely, regardless of the activation type. Values range from 1 sec to 4 min:15 secs. Default is 5 secs.

Note...

This option is not available when you are using the KT-400 or the KTES.

*If you are using the **Video Integration** feature, EntraPass enables you to assign all system components into a video view, the same way you assign them to a system interactive floor plan (graphic). To do this, you simply select the video view where you want the system component (Workstation, site, gateway, controller, etc.) to appear.*

Associating Events with Auxiliary Outputs

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

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

2 - In the **Options** column, associate an event with an output state. Default is **None** .

- **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 **EntraPass Gateways Configuration**. Events for timer on/off vary depending on the type of the selected gateway.*

Comment

*For more details about the **Comment** entry box, please refer to **Comment Field**.*

Reader Templates

Use a reader template to define how a reader is configured. Reader templates can only be used for ioSmart card readers in RS-485 mode. Creating a template allows the same configuration to be shared across a number of card readers. To create a reader template complete the following steps:

1 - Click the **Devices** tab.

2 - Click **Reader template** from the menu. When the Reader template window appears, click the **New** icon to enable editing.

3 - Select the Status bar **LED color**, **Buzzer**, and **Backlight** setting for each **State** of the reader.

4 - Select the **Send UID** option for the reader. Use this option to define which type of card is accepted by the reader.

- **Never**. Only send card ID from ioSmart Cards
- **When not ioSmart card**. Send card ID from ioSmart cards and UID from non ioSmart cards.
- **Always (No encryption)**. Always send UID from a card.

5 - Select the **HID 125 kHz** and **ISO 14438B** options to define the card technology.

6 - If the controller connects to ioSmart readers and you want to enable the BLE technology, select the **BLE** check box. EntraPass selects the **BLE** check box by default as all ioSmart readers are BLE enabled.

7 - Select the **Keypad backlight intensity when in idle mode**.

8 - Set the delays for the **LED flash duration (ms)**, **Buzzer signal duration(ms)**, and **Keypad backlight duration(s)**.

Integrated Panel Configuration

Minimum Requirements to View and Use the Integration Buttons

- The Integration DLL must have been loaded at the **EntraPass Server**. If the toolbar doesn't display the

two buttons, see **System Parameters Configuration**.

- The third party hardware must be connected on the serial port of the **multi-site Gateway** or the serial port of a pass-through KT-400 controller.
- The third party hardware must be powered up.

Note

Before defining an integration panel in EntraPass, ensure that none of the partitions is armed. If there is at least one armed partition, it will not be possible to program the panel.

1 - From the **Devices** toolbar, click the **Integrated Panel** button.

2 - Click on the **New** button and assign a name for both languages.

3 - Select a **Panel** from the drop-down list.

General Tab

1 - Select a **Connection type** from the drop-down list.

2 - Select a **Panel model** from the drop-down list.

3 - If the **Video feature** is enabled, the **Video view** field appears. If this is the case, select the Video view in which you want the defined component to appear. For details on defining video views, see **Video Views Definition**.

4 - From the **Graphic** list, you may select the graphic to which the application is assigned, if applicable. For details on defining graphics, see **Graphics Definition**.

5 - Click on the **Configuration** button to display the **Panel Configuration** dialog. A different dialog is displayed according to the selected connection type:

Panel Configuration Parameters Summary

Parameters	NEO connected to serial or IP controller	NEO connected to serial or IP gateway	PowersSeries or MaxSys connected to serial controller	PowersSeries or MaxSys connected to serial gateway	Bentel Kyo320 connected to gateway IP	Honeywell Galaxy connected to gateway IP	Simplex 4100 & 4007ES connected to serial controller	Simplex 4100 & 4007ES connected to serial gateway
Virtual Zone management: Select **Single controller** to limit the integration to the controller it is connected to. Select **Multiple controllers** so the integration can use events/components for any controller of the same gateway.	Yes							
Intrusion model : Select the access management. **By partition** means that the default user code will be used to arm/disarm the system. **By users** means that the user card will be used to arm/disarm the system.	Yes		Yes					
Controller selection for pass-through: Select the controller to which the panel is connected in order to establish communication.	Yes		Yes				Yes	

Parameters	NEO connected to serial or IP controller	NEO connected to serial or IP gateway	PowersSeries or MaxSys connected to serial controller	PowersSeries or MaxSys connected to serial gateway	Bentel Kyo320 connected to gateway IP	Honeywell Galaxy connected to gateway IP	Simplex 4100 & 4007ES connected to serial controller	Simplex 4100 & 4007ES connected to serial gateway
Integration identification number: Enter the DSC TL280R code to establish communication.	Yes	Yes						
Integration access code: The DSC TL280R code that can be configured by the user.	Yes	Yes						
Number of digits : Enter the number of digits for the master access code.	Yes	Yes	Yes	Yes	Yes			
Master access code: Enter a code that will be used to program the panel.	Yes	Yes	Yes	Yes				
Default user access code: Select a default user access code from the drop-down list.	Yes	Yes	Yes	Yes				
Communication port COM: Select a port from the drop-down list. This port is used for manual operations and when the system use the "managed by partition" mode.		Yes		Yes				

Parameters	NEO connected to serial or IP controller	NEO connected to serial or IP gateway	PowersSeries or MaxSys connected to serial controller	PowersSeries or MaxSys connected to serial gateway	Bentel Kyo320 connected to gateway IP	Honeywell Galaxy connected to gateway IP	Simplex 4100 & 4007ES connected to serial controller	Simplex 4100 & 4007ES connected to serial gateway
Communication type: Select between Serial (RS-232), IP-TCP and IP-UDP physical connections.	Yes	Yes						
Connection filter(NEO connected to serial or IP controller): Used to filter controllers on the gateway. Selected controllers will be used for virtual zones.	Yes	Yes						
Baud rate: Default is 9600.				Yes				
Ethernet IP address: Enter the controller IP address to allow communication.					Yes	Yes		
Domain name address: Enter the controller domain name to allow communication.					Yes	Yes		
DSL Port: Enter the panel communication port.					Yes			

Parameters	NEO connected to serial or IP controller	NEO connected to serial or IP gateway	PowersSeries or MaxSys connected to serial controller	PowersSeries or MaxSys connected to serial gateway	Bentel Kyo320 connected to gateway IP	Honeywell Galaxy connected to gateway IP	Simplex 4100 & 4007ES connected to serial controller	Simplex 4100 & 4007ES connected to serial gateway
IP ports: Select the three (3) IP ports that are used to communicate with the Galaxy panel.						Yes		
PIN value: Enter the remote panel PIN number (the displayed value is the default value from the Galaxy panel).					Yes			
Check **Always validate MAC address upon startup** in order to verify that it is the right panel.					Yes			

Parameters	NEO connected to serial or IP controller	NEO connected to serial or IP gateway	PowersSeries or MaxSys connected to serial controller	PowersSeries or MaxSys connected to serial gateway	Bentel Kyo320 connected to gateway IP	Honeywell Galaxy connected to gateway IP	Simplex 4100 & 4007ES connected to serial controller	Simplex 4100 & 4007ES connected to serial gateway
Import IDNet points (Simplex 4100 panel): Select **Import IDNet points** to auto-matically import the panel points defined into the IDNet boards located on the Fire Panel. The information imported is the point addresses consisting in the **Slot number**, the point value and the subpoint value with the corresponding point label.							Yes	Yes
Import panel button points (Simplex 4100 panel): Select Import panel button points to retrieve the button addresses in order to generate an EntraPass specific named event for the following buttons: • System Reset key • Alarm Silence key • Master Fire alarm Ack key • Master Supervisory Ack key • Master Trouble Ack key • Master Priority Ack key							Yes	Yes

Note...

*When selecting the **Access managed by user**, a tab named **Intrusion** will become available in the **Users** toolbar **> Card.***

For the KT-400 version, an additional drop down list is available to select a controller for pass-through.

Panel Component Tab (Bentel, DSC Maxsys, NEO, PowerSeries)

Note...

This feature depends on the type of intrusion panel. The device has to be first created in EntraPass for the DLL to be downloaded into the corresponding gateway or KT-400. Once downloaded, the auto-detection becomes active.

1 - Define the **Zone**, **Partition , User** and **Virtual Zone** parameters. These parameters have the following maximum values:

Parameter	PC1616	PC1832	PC1864	HS2016	HS2032	HS2064	HS2128
Zones	32	32	64	16	32	64	128
Partitions	2	4	8	2	4	8	8
Users	48	72	95	48	72	95	95
Virtual Zones				16	32	32	32

2 - Select the number of **Zones**. Click the button on the left to display a table that shows all the defined zones. Click the **View** or the **Edit** button to see/edit the selected zone from the **Integrated Component** window.

3 - Select the number of **Partitions**. Click the button on the left to display a table that shows all the defined partitions. Click the **View** or the **Edit** button to see/edit the selected partition from the **Integrated Component** window.

4 - Select the number of **Users**. Click the button on the left to display a table that shows all the defined users. Click the **View** or the **Edit** button to see/edit the selected user from the **Integrated Component** window.

5 - Select the number of **Virtual zones** (only available for Neo panels connected to KT-1/KT-400). A corresponding number of virtual inputs will be added in **Integrated Component**. Remember that configuring virtual zones in **Integrated Panel** allows you to see all zones in one page as opposed to configuration in **Integrated Component** that will display one zone at a time.

Note

*The number of **Virtual Zones** default value is the maximum value described in the above table. The purpose of that feature is to create "virtual" zones in an alarm panel that will receive commands from groups of*

selected input, doors and other events of a gateway. These commands are then transmitted from the panel to a central station.

The Neo 1.1 integrated panel can support 16 or 32 virtual zones.

- *16 virtual zones for HS2016.*
- *32 virtual zones for HS2032, HS2064 and HS2128.*

Note...

That feature is only available using KT-400 and KT-1 controllers. A new firmware is required (1.16.xx for KT-400, 1.22.xx for KT-401, 1.02.xx for KT-1).

6 - Click the **Virtual Zone List** button. The displayed table allows you to map Kantech components to DSC virtual zones.

Note...

*The **Physical Zone** column is displayed only with a valid DSC panel communication.*

- For each **Door**, **Input** or **Event** (use the corresponding tabs), select a physical zone number and the type of event (**Alarm**, **Trouble** or **Tamper**) to be sent to the central. Please note that you can see the remaining available zones from the counter at right.

Events sent to the virtual zone

Component	EntraPass Event	Report Alarm	Report Trouble	Report Tamper
Input	Input in alarm / Input restored or in normal condition	X		
	Input in trouble/ Input in trouble restored		X	
	Input tamper in alarm / Input tamper restored			X
Door	Door forced open / Door forced open Restored	X		
	Door open too long / Door open too long restore		X	
	Door lock device failure / door lock device failure restored		X	
Duress	Duress feature	X		

Component	EntraPass Event	Report Alarm	Report Trouble	Report Tamper
Controllers	Controller AC power failed / Controller AC power restored		X	
	Tamper switch in alarm / Tamper switch restored			X
	Controller Auxiliary power failure / Controller Auxiliary power restored		X	
	Controller reader power failure / Controller reader power restored		X	
	Controller battery power failure / Controller battery power restored		X	
	Controller module communication failure /Controller module communication restore		X	
	Controller DC power failed / Controller DC power restored		X	
	Controller lock power failed / Controller lock power restored		X	
	Controller power trouble (KT-1)		X	
Access Denied	Access denied - Bad card status		X	
	Access denied - Card lost or stolen			X
	Access denied - Card expired	X		

- Click the **Add** button to add a new event in the list or click the **Remove** button to remove the selected event.
- Click **Save** or **Cancel** to return to the **Integrated Panel** window.
- **Printing**: Use the **Print** button from the **Virtual Zone Summary** section to send the virtual zone configuration parameters to the central.

NEO Virtual Zone	NEO Physical Zone	Component Type	Component	Report Alarm	Report Trouble	Report Tamper
1	110	Door	Door #1	✓		✓
2	111	Door	Door #5	✓	✓	
3	112	Input	Input #1	✓	✓	✓
4	114	Controller	Controller #4	✓		

RS-232 Tab

1 - Select the **Communication port COM** and the **Baud rate** from the drop-down lists.

2 - Click **Save**.

Integrated Component Configuration

The **Integrated Component** dialog can handle any type of panel components (partition, zone...etc) under any type of panel (intrusion, temperature control,...etc).

1 - From the **Devices** toolbar, select the **Integrated Component** button.

2 - Select the **Component** from the drop-down list.

Note...

You can use the drop down list in the toolbar to sort the displayed components by type.

3 - Select the **Component type** .

4 - Click on the **Configuration Form** button to display the **DSC Power Series** dialog.

5 - For a **User** component type, enter the **User access code**. This code is a **PIN** number used for arming or disarming a partition.

6 - For a **Simplex** panel, select proper values to define the fire panel device point. Once the device is granted an address (manually or automatically from IDNet import), the user will not be allowed to change it unless the point is deleted and another one is created.

7 - For a **Virtual Zone**:

The purpose of that feature is to create "virtual" zones in an alarm panel that will receive commands from groups of selected input, doors and other events of a gateway. These commands are then transmitted from the panel to a central station.

Note...
The Neo 1.1 integrated panel can support 16 or 32 virtual zones. 16 virtual zones for HS2016. 32 virtual zones for HS2032, HS2064 and HS2128.

Note...

That feature is only available using KT-400 and KT-1 controllers. A new firmware is required (1.16.xx for KT-400, 1.22.xx for KT-401, 1.02.xx for KT-1).

- Select a **Component type** from the drop-down list (Door, Input or Event).
- For an **Event** component type, select an event (please refer to the following table for a list of events based on the selected component type).

Events sent to the virtual zone

Component	EntraPass Event	Report Alarm	Report Trouble	Report Tamper
Input	Input in alarm / Input restored or in normal condition	X		
	Input in trouble/ Input in trouble restored		X	
	Input tamper in alarm / Input tamper restored			X
Door	Door forced open / Door forced open Restored	X		
	Door open too long / Door open too long restore		X	
	Door lock device failure / door lock device failure restored		X	
Duress	Duress feature	X		

Component	EntraPass Event	Report Alarm	Report Trouble	Report Tamper
Controllers	Controller AC power failed / Controller AC power restored		X	
	Tamper switch in alarm / Tamper switch restored			X
	Controller Auxiliary power failure / Controller Auxiliary power restored		X	
	Controller reader power failure / Controller reader power restored		X	
	Controller battery power failure / Controller battery power restored		X	
	Controller module communication failure /Controller module communication restore		X	
	Controller DC power failed / Controller DC power restored		X	
	Controller lock power failed / Controller lock power restored		X	
	Controller power trouble (KT-1)		X	
Access Denied	Access denied - Bad card status		X	
	Access denied - Card lost or stolen			X
	Access denied - Card expired	X		

- For a **Door** or **Input** component type, indicate the component source (controller)
- Check the appropriate **Component action** to be reported for the virtual zone and click **OK**.

8 - If the **Video feature** is enabled, the **Video view** field appears (for zones and partitions only). If this is the case, select the Video view in which you want the defined component to appear. For details on defining video views, see **Video Views Definition** .

9 - From the **Graphic** list, you may select the graphic to which the application is assigned, if applicable (for zones and partitions only). For details on defining graphics, see **Graphics Definition** .

Note...

*The **Details** button is available only for a **User** or a **Virtual Zone** component type.*

10 - Click **Save** .

See **Manual Operations on Integrated Panels** to complete the configuration.

Trigger and Alarm tab

The alarm and trigger tab is available for the following menu items:

- Devices ... Gateway
- Devices ... Connection
- Devices ... Controller
- Devices ... Door
- Devices ... Relay
- Devices ... Input
- Devices ... KTES
- Definition ... Alarm System
- Definition ... Area
- Definition ... Guard Tour

This tab displays a summary of all alarms and triggers that are associated with the selected device. The following information is displayed in the tab:

heading	description

heading	description
Event	The name of the event. For example "Door locked by an operator". Note: this heading is only available when **Event Operator** mode has been enabled.
Trigger description	The name of the trigger. This is given when then trigger is created
Source	Indicates if the trigger is a single trigger or part of a trigger group
Event Trigger	Indicates that an event trigger has been created for this event
Alarm	Indicates if an alarm is associated with the trigger
Disabled	Indicates if the trigger is disabled
Trigger Group	If the trigger is part of a group it will be listed here

To view, add, edit, and, delete a trigger, select a trigger from the list and right-click to open the menu. Deleting a trigger will only remove the trigger, it will not remove the application or selected event from the trigger.

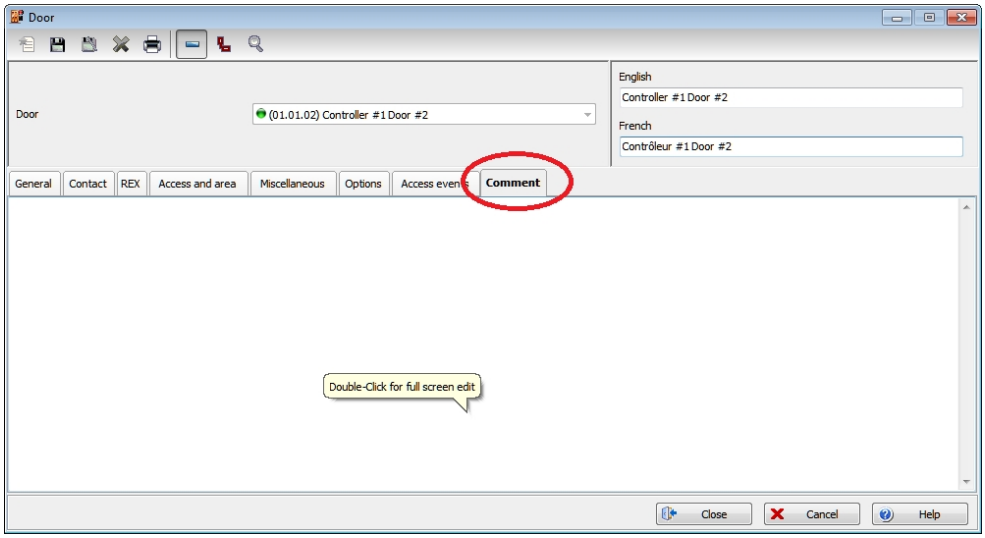
Comment Field

A comment field is available for the following components:

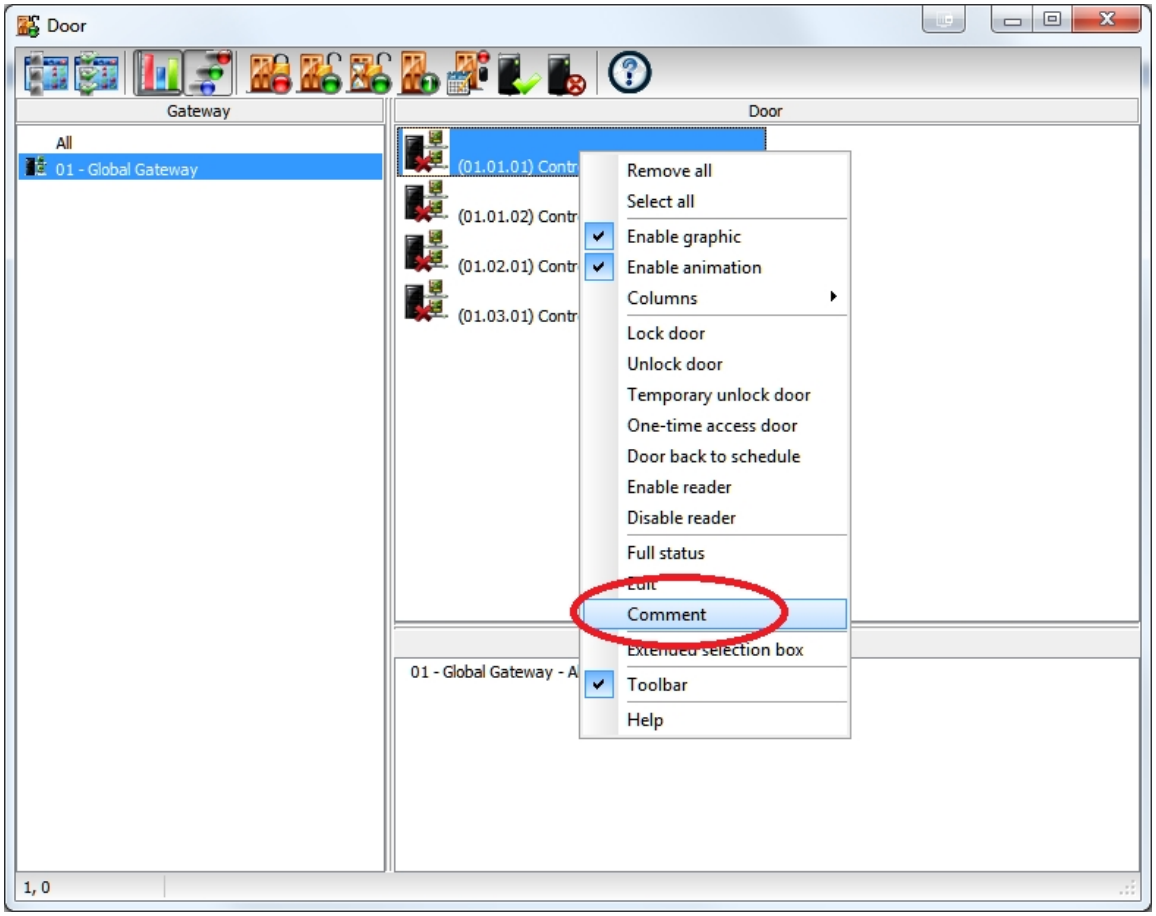
- EntraPass application
- Active directory
- Gateway
- Site
- Connection
- Controller
- Door

- Relay
- Input
- Output

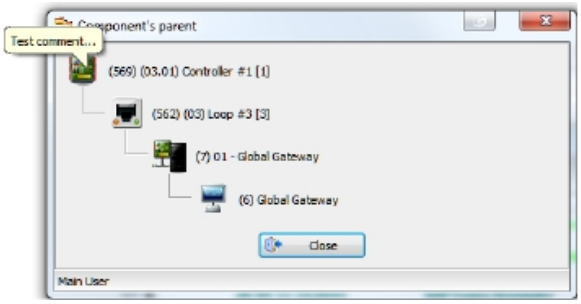
The comment field can be modified or deleted at all time. Its length is unlimited. Here is an example from the **Devices/Door** menu:



- Use a double click in the field to enable the edit mode.
- Comments can also be visualized from the Operation window using a right click on a component:



- Comments can also be visualized through the **Messages List** or a graphic (right-click on a component and select **View parent/controller**). The following window is displayed:



- Move the mouse pointer over the controller to display the associated comment.

Camera Definition

EntraPass offers you the ability to assign names to cameras, presets, and patterns for easy identification in the Video desktop and in all system video events.

The definition of a camera includes identifying its:

- Types (fixed or dome)
- Presets (for dome cameras)
- Patterns (for dome cameras)

The camera name is displayed when viewing live or recorded video events (Intellex only). The default names are Camera1 through Camera n (where n is the last camera number).

Defining a Camera

1 - From the Video window toolbar, click the **Camera** button. The Camera window appears.

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

3 - Select the **Camera type** from the drop-down list.

- **Fixed camera:** no preset/pattern; operators cannot control a fixed camera.
- **Dome:** preset and pattern (Intellex only) available; selecting this option allows operators to control the camera. If you select this option, assign descriptive names to the camera presets.

4 - Check the **Show camera** option for the camera to be accessible for selection and display in the Video view desktop. It is important to check this option if you want the camera to be enabled in EntraPass. Only operators with appropriate permission will be able to view a camera with the **Show camera** option not checked (Hidden/covert cameras). To assign permission to an operator: **System** > **Operator definition** > **Privileges** .

NOTE: If you leave the Show camera box unchecked, the camera will not appear in the Video view component window (Video view > Modify video view components) and will not therefore be assigned in the Video desktop for view. This feature allows to hide a camera from all view. Operators who do not have appropriate permission will not be able to view, search, export or carry any other operation on a camera for which they do not have access permission. However, all links and references to this camera will be kept. This feature is different from deleting a camera since links to a deleted camera are deleted as well.

5 - Check the **Select specific events** option if you want this camera to record specific events. By default all camera events are displayed in the Video Events List. However, you can decide which events will be recorded by a specific camera by checking this option. When you do this, the **Event** tab appears. You can then select it and specific events will be recorded by the camera being defined. If this option is checked, you have to select events that will be recorded by this camera.

6 - Using the **Up/down** controls, adjust the number of presets and patterns for the selected camera if the selected camera is a dome. When you do this, the **Preset** or **Pattern** tabs appear in the Camera window.

7 - Select the view type you want to display when an alarm occurs.

- **Video View:** The video view selected will be displayed when an alarm occurs on this camera.
- **Graphic View:** The graphic view selected will be displayed when an alarm occurs on this camera.

Associating a Camera with an Icon

EntraPass offers you the ability to associate a specific button with a camera for easy identification in the Video desktop and system Graphic.

1 - From the Camera window, select the camera you want to associate with an button, then click or double-click the button next to the camera type drop-down list. The **Select an button** window opens.

2 - Choose an appropriate button to associate with the selected camera, then double-click it to close the window. When you do this, a camera is associated with an button using the button index.

- The Camera button in the Camera window toolbar allows you to add custom buttons to the list of available buttons. The list of buttons is displayed when you click the Camera button in the toolbar.

Defining Presets and Patterns

1 - From the Video server window select the **Preset** (or **Pattern**) tab to assign custom names to your presets.

2 - Select a table cell, then overwrite the default name. If you are running the system in two languages, enter the name in both the primary and secondary language, then click **Close** to close the Preset (or Pattern) window.

NOTE: If you select a preset or pattern and click the Default button, the assigned name is replaced by the default name.

Defining Events Recorded by a Camera

If the **Select specific events** option is checked in the **General** tab, you have to:

- Select events that will be recorded by the camera being defined and that will be sent to the EntraPass Server. This option is disabled when a camera is connected to an Intellex LT DVR.

- Select or define a schedule that will be used by the video server to report selected events to the EntraPass Server. This schedule can be used as a filter to limit the message flow from the Video Server to the EntraPass Server. For instance, choosing an Always valid schedule will send all the selected events to the EntraPass server. Specifying a limited period of time will allow to send events that occurred during a targeted period of time.

To Select Camera Events and Schedules

1 - From the Camera window, select the **Event** tab. Typical camera events are displayed in the window. These are specific to the selected DVR.

2 - Select a schedule for camera event reporting. Only events that will be recorded during the specified period of time will be sent to the EntraPass server. Right clicking the Event report schedule field enables operators to create a new schedule or to select an existing one. To define a schedule , make sure that you are selecting the proper category for this schedule. For example, if you are assigning or defining a

system schedule (for workstation, operators, video triggers) this schedule will be available for selecting components of this category. If you are selecting a schedule for physical components such as controllers, doors, inputs, their schedules will be grouped If you have defined two sites in your system, there will be two separate groups of schedules for each connection. You can define up to 99 schedules for each connection.

3 - Select camera events that you want to send to the EntraPass server. Specifying events to be sent to the video server is a way of saving on controlling the flow of the video data, and hence of decreasing bandwidth usage. The list of events is specific to the video server:

- **Camera advanced motion alarm (Intellex only)** : the camera will send any event related to a motion alarm.
- **Camera alarm (Intellex only)** : the camera will send any event related to a change that occurred in the target area.
- **Camera light alarm (Intellex only)** :
- **Camera motion alarm** : the camera will send to the EntraPass server all video segment events related to any movement that occurred in the target area.
- **Camera override (Intellex only)** :
- **Camera perimeter (Intellex only)** : the camera will send all video segment events related to an object, that has crossed into or out of the target area, to the EntraPass server.
- **Camera text alarm (Intellex only)** :

4 - Select the **Video Vault Comment** tab if you want to add information regarding the camera being defined. KVI and KVA file formats from this camera that will be saved in EntraPass Video Vault will be displayed with the comment entered in this window.

5 - Enter the comment you want to associate with the camera being defined, then save and close the window.

Comment

*NOTE: For more details about the **Comment** entry box, please refer to **Comment Field**.*

Current Recording

The Current recording feature allows users to view the list of all on-going recordings. The information displayed depends on the source of the recording request:

- Started by a video trigger
- Started by an operator
- Started by an alarm on the video server

Viewing the Current Recordings

1 - From the Video toolbar, click the **Current recording** button. The current recording window appears, it shows all on-going recordings.

The following table shows the information displayed in the Current recording window depending on the source of the recording.

Initiated by	Information
Video server alarm	• Initiated by • Event name • Start date and time
Video trigger	• Initiated by • Video trigger • Recording parameter • Event • Start date and time • Remaining time for the recording

Initiated by	Information
Operator	• Initiated by • Workstation • Operator name • Start date and time • Remaining time for the recording

EntraPass Video Vault Browsing

EntraPass Video Vault offers an easy way for preserving important video data for future reference. In fact, video recordings have a limited life span depending on the video server settings and capability. Moreover, since video recordings require a great amount of disk space, using an archive management tool such as EntraPass Video Vault enables organizations to better manage and easily retrieve video contents. The archiving activity is monitored from the EntraPass Video Vault user interface. The Browse EntraPass Video Vault interface offers a Windows-like navigation pane that enables operators (with appropriate permission) to play video segments archived on EntraPass Video Vault.

Viewing Video Segments Archived in the EntraPass Video Vault

1 - From the Video main window, select the Browse Video Vault button.

2 - To view a specific segment, select a video segment, then click the **Play from Video Vault** button.

Exported Video Viewing

EntraPass enables users to view all exported videos. This feature makes it possible to browse the list of all exported videos and to preview a key frame of the exported videos sequence for all KVI and KVA formats. Moreover, users can preview the exported video segment before viewing it.

1 - From the Video toolbar, select the **View exported video** button. The Video folder opens automatically, with the list of all exported video sequences that have been exported.

2 - Select a video sequence. The video thumbnail appears in the lower left part of the window. The directory contains the **Date and Time** the video was taken, the video file format (**Type**) and the **File Name** . You can then click the **Preview** button for details about the exported video.

Exporting Video Files

EntraPass exports video segments in four formats: KVI and KVA.

- KVI (Kantech Video Intellex format). Video data are stored in Intellex format (.img). A simple double-click allows you to view the file using VideoPlayerIntellex.exe.
- KVA (Kantech Video AVI format). Video data are stored in AVI format (.avi). A double click opens the video file using VideoPlayerWindow.exe.
- AVI format
- IMG format
- PS format

EntraPass users have two options when exporting videos:

- From the Video event list (without previewing the video)
- From the video playback window: in this case, the video is previewed before it is exported.

1 - From the video event list, select the video event you want to export.

2 - Click the **Export** button. The **Enter a video filename** window opens.

3 - Enter a file name in the **File name** field. By default, the file is assigned the Kantech KVI format. The file will be saved among EntraPass program files:\Kantech\Server CE\Video. Later you can call this file simply by double-clicking it.

*NOTE: Video files can be viewed in the **Exported video** window (Video tab > Exported video). The video file is displayed with its name, date and time. Key frames (if any) associated with a video clip can also be previewed in this window.*

4 - Click **Save** to close the **Enter filename** window. When you do this, the **Description and password** window appear.

Finding Video Events

Under **Video > Video event list**, use the **Search** button to locate and view video segments. If the **Search** button is not displayed on screen, click the **Menu** button to make it appear.

- The **Video server** tab allows you to search for a video segment on a specific video server.
- The **Events** tab allows you to filter events.
- The **Options** tab allows you to determine the size of the video you are looking for. Appropriate user access rights are necessary for performing this task.
- The **Archive state** tab allows you to filter archived events according to their status.

1 - From the Video Events List, click the **Search** button. The Find video event window appears.

*NOTE: If the **Menu** and **Legend** buttons are not activated, the window will not show the legend nor the buttons in the lower part.*

2 - From the **Find video events** window, select the **Start date and time** and the **End date and time** for the video segments you are looking for.

*NOTE: The **Legends** button allows you to display a status legend related to video events. The Play and Copy from Video Vault buttons are enabled when the selected video events have already been archived on EntraPass Video Vault.*

3 - Select the video server that you want to include in the search. You can select **All video servers** if you want to search through all video servers defined in the system.

NOTE: If an event was registered by more than one video server, at least one of the servers must be selected for the event to be included in the list.

4 - Select the **Events** tab to filter events to be included in the report. If you select **All events,** all the specific events will be checked.

5 - Select the **Options** tab to filter video segments according to their duration.

6 - Check the **Video segment duration limit** option, then enter the duration in the **Greater than (mm:ss)** and **Smaller than (mm:ss)** fields. The value entered is in minutes and seconds. This feature allows you to target video segments meeting specific duration criteria.

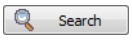
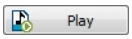
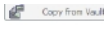
7 - Select the **Archive State** tab to filter events according to the archive status.

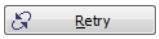
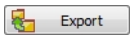
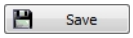
8 - Check the **Archive State** option if you want to specify which events will be included in the filter. If you want to include all events, leave these options unchecked.

9 - Click **OK** to go back to the **Video event list** window.

*NOTE: The **Play** and **Copy from Video Vault** buttons are enabled when the selected video event has been archived on EntraPass Video Vault. Archived events are identified by a green flag.*

10 - Do one of the following using the buttons described bellow:

Button	Use description
	Use this **Search** button to search for events associated with a video segment.
	Use the **Play** button to view a video event. When you click this button, the Video desktop displays the video event. If only one camera was used, which is most often the case, the system displays the duration of the video event. If the video event was recorded by more than one camera on a single server, the video server will use the most optimal display layout. If the video event was registered by more than one server, it is possible to select a specific video server. For example, 2x2 for a maximum of 4 camera, 3x3 for a maximum of 9 camera and 4x4 for a maximum of 16 cameras. For events with various length, events will be played based on the longer event. Note that this feature shows limitations when used in systems not configured for continuous recording as it will not display cameras involved outside the selected time frame.
	The **Copy from Vault** button allows operators to retrieve video segments that have been archived on EntraPass Video Vault.
	The **Play from Vault** button enables operators to view a video event that has been archived on EntraPass Video Vault

Button	Use description
	The **Retry aborted** button enables operators to trigger any archiving process that was suspended.
	Use the **Menu** button to display the buttons in the lower part of the window and the **Legend** button to display a legend about the status of the displayed video recording events.
	The KVI (Kantech Video Intellex), KVA (Kantech Video AVI), IMG, AVI and PS formats are available for your **Export** needs. These formats allow users to store all the data relative to a video event such as the event button or key frame, description, etc.
	The **Save** button is enabled when an operator enters data in the **Comment** field. It enables operators to save comments associated with a video event.
	The **Cancel** button is enabled when the **Comment** field is modified. It enables operators to discard the comment and to go back to the previous value.

Recording Parameters

The **Recording Parameters** menu enables users to define parameters that control video recording and to associate recording parameters (such as video source, cameras, etc.) with a video trigger. For each recording event, you must specify parameters such as the video server source, the camera, etc.

A recording can be stopped by a timer (maximum recording time) or by a trigger when a stop recording trigger is used. A source component must be specified for each type of triggering event. For example, the "door" component must be specified for the "Door forced" event message. The resulting action (whether to start or stop recording) must also be specified.

EntraPass offers you the ability to associate multiple recording parameters with one trigger. In this case, all recordings will be associated with the single event and it will be possible to save all record segments as a single event recording.

Setting Up Recording Parameters

The Video record window lets you configure how EntraPass Video records videos. You must possess the appropriate privileges to set up this feature. There is no limit to the number of definable recording parameters. The following information can be defined:

- Name in two languages (for systems in two languages)
- Video source (server and camera)
- Preset and patterns
- Start recording trigger
- Pre-alarm time
- Maximum total recording time, etc.

1 - From the Video toolbar, click the **Recording parameters** button. The **Recording parameters** window appears with the **General** tab enabled.

2 - Click the **New** button to create new **Recording parameters** (or select one from the Recording parameters drop-down list) and assign a descriptive name to the Recording parameters.

3 - From the **Video server** pop-up window, select the video server that will be used for the Recording parameters.

4 - From the **Camera** drop-down list, select the camera for this Recording parameters.

*NOTE: If the selected camera is a dome, you can specify the **Preset or Pattern** name and number. Defining these options allows you to direct the camera to a specific position for recording. However, the pre-alarm time feature may not work well with the preset/pattern option. In fact, the pre-alarm may be triggered when the camera is directed to a location different from the one where the video recording event occurred.*

5 - From the **Start recording trigger** pop-up window, select the Video trigger you want to associate with the Recording parameters being defined. The Video trigger pop-up window displays all video triggers defined in the system.

6 - In the **Timings** section, specify:

- **Pre-alarm time (m:ss)** : This option enables users to retrieve from the video server, segment that was recorded before recording was triggered. For example, if a recording was triggered at 2:00 PM and if the Pre-alarm time is 1min. 0 seconds, the record segment will start at 1h 59.

- **Maximum total recording time (m:ss)** : This options allows you to specify a maximum length for the recording. This includes the pre-alarm time but not the post-alarm recording delay. The maximum allowed is 5 minutes.

Setting Up Stop Recording Trigger Parameters

If you want to associate the defined recording parameters with a trigger for stopping recording, check the **Stop recording trigger** option. If you do this, the **Stop recording trigger** tab appears in the Recording parameters window.

1 - From the Recording parameters window, select the **Stop recording trigger** tab.

- **Post-alarm recording delay (m:ss)** : this delay enables the system to end recording when an "end recording delay" condition has been used. Moving the mouse pointer over the field shows the value range allowed in the field.

- **Trigger** : select one (or more) trigger(s) that will stop recording.

NOTE: You can create new stop recording triggers by right-clicking the triggers display area.

Video Desktop

The Video Desktop allows operators to display and monitor, in real-time, video cameras configured and connected to the network.

Displaying a Video View

1 - From the EntraPass main window, select the **Desktops** tab, then select the desktop dedicated to Video. The Video View window appears in the desktop.

NOTE: The Video desktop will be empty the first time you open it and "No video view selected" is displayed.

2 - **Select video view** from the drop-down list at the bottom of the window. You can edit the view (**Video view** > select a specific **View** > **Modify Video view components** button).

3 - The 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.
	These buttons are configured in the Operator security level. They enable operators to perform pre programmed tasks such as viewing video playback with a fixed or variable delay, generating video events with fixed or custom parameters. For details on programing this buttons, see **Security Level Definition**.
	Use these buttons to **Create** and **Edit** video views.
	Use this **Show view selector** button to display a mosaic view of all the cameras, or one of the cameras defined in the system.
	Help and **Close** buttons. These are EntraPass standard buttons.

4 - 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 pattern. For instance, if you select a cell in the View selector, the sequence is interrupted to display the selected cell.

NOTE: When you open the Video view selector while a camera is recording, the camera button will blink until the end of the recording.

5 - From the displayed view, you can click a dome camera button 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 pre programmed movement patterns, you can define a view displaying a pattern composed of one or many of these patterns. For more details, see **Video Views Definition**.*

Video Event List

The Video Event List window displays all video segments recorded in the system and stored in the Video server database as well as video segments archived in EntraPass Video Vault . These video segments can originate from three sources:

- Video triggers
- Manual requests from operators
- Automatic recordings from video servers

> ***NOTE:*** *Operators must have access rights to the video server in order to perform operations on events displayed in the Video Event list. For example, if an operator has not been assigned permission to use a specific video server, he/she will not view events originating from this server. User permission are assigned while defining the security level: System > Security level .*

Using the Video Event List

The **Video event list** window displays all video events as well as their description. EntraPass operators can:

- Search for a specific event associated with a video segment based on the date and time when the video was recorded
- Play a video segment
- Export the video segment for future consultation
- Stream or copy video segments from EntraPass Video Vault
- Retry all aborted transfers: these are transfers of video segments that were tagged for archive but which were not transferred to EntraPass Video Vault.

Finding Video Events

Under **Video > Video event list**, use the **Search** button to locate and view video segments. If the **Search** button is not displayed on screen, click the **Menu** button to make it appear.

- The **Video server** tab allows you to search for a video segment on a specific video server.
- The **Events** tab allows you to filter events.

- The **Options** tab allows you to determine the size of the video you are looking for. Appropriate user access rights are necessary for performing this task.

- The **Archive state** tab allows you to filter archived events according to their status.

1 - From the Video Events List, click the **Search** button. The Find video event window appears.

*NOTE: If the **Menu** and **Legend** buttons are not activated, the window will not show the legend nor the buttons in the lower part.*

2 - From the **Find video events** window, select the **Start date and time** and the **End date and time** for the video segments you are looking for.

*NOTE: The **Legends** button allows you to display a status legend related to video events. The Play and Copy from Video Vault buttons are enabled when the selected video events have already been archived on EntraPass Video Vault.*

3 - Select the video server that you want to include in the search. You can select **All video servers** if you want to search through all video servers defined in the system.

NOTE: If an event was registered by more than one video server, at least one of the servers must be selected for the event to be included in the list.

4 - Select the **Events** tab to filter events to be included in the report. If you select **All events,** all the specific events will be checked.

5 - Select the **Options** tab to filter video segments according to their duration.

6 - Check the **Video segment duration limit** option, then enter the duration in the **Greater than (mm:ss)** and **Smaller than (mm:ss)** fields. The value entered is in minutes and seconds. This feature allows you to target video segments meeting specific duration criteria.

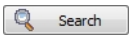
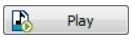
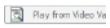
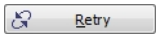
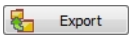
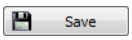
7 - Select the **Archive State** tab to filter events according to the archive status.

8 - Check the **Archive State** option if you want to specify which events will be included in the filter. If you want to include all events, leave these options unchecked.

9 - Click **OK** to go back to the **Video event list** window.

*NOTE: The **Play** and **Copy from Video Vault** buttons are enabled when the selected video event has been archived on EntraPass Video Vault. Archived events are identified by a green flag.*

10 - Do one of the following using the buttons described bellow:

Button	Use description
	Use this **Search** button to search for events associated with a video segment. For details, see **Finding Video Events**.
	Use the **Play** button to view a video event. When you click this button, the Video desktop displays the video event. If only one camera was used, which is most often the case, the system displays the duration of the video event. If the video event was recorded by more than one camera on a single server, the video server will use the most optimal display layout. If the video event was registered by more than one server, it is possible to select a specific video server. For example, 2x2 for a maximum of 4 camera, 3x3 for a maximum of 9 camera and 4x4 for a maximum of 16 cameras. For events with various length, events will be played based on the longer event. Note that this feature shows limitations when used in systems not configured for continuous recording as it will not display cameras involved outside the selected time frame.
	The **Copy from Vault** button allows operators to retrieve video segments that have been archived on EntraPass Video Vault.
	The **Play from Vault** button enables operators to view a video event that has been archived on EntraPass Video Vault
	The **Retry aborted** button enables operators to trigger any archiving process that was suspended.
	Use the **Menu** button to display the buttons in the lower part of the window and the **Legend** button to display a legend about the status of the displayed video recording events.
	The KVI (Kantech Video Intellex), KVA (Kantech Video AVI), IMG, AVI and PS formats are available for your **Export** needs. These formats allow users to store all the data relative to a video event such as the event button or key frame, description, etc.
	The **Save** button is enabled when an operator enters data in the **Comment** field. It enables operators to save comments associated with a video event.

Button	Use description
Cancel	The **Cancel** button is enabled when the **Comment** field is modified. It enables operators to discard the comment and to go back to the previous value.

Playing Video Segments

The Video Event List window is divided in two panes: the left-hand pane displays all video events that were retrieved according to the search criteria. The lower pane of the window displays the legend explaining the status of each event. It also contains buttons that enable operators to perform operations on video recordings. The right-hand pane contains three tabs:

- The **Details** tab displays the text description of the video event such as the video server that recorded the event, the operator who was logged on, etc.
- The **Cameras** tab shows cameras that are associated with a selected event.
- The **Image** tab contains the key frame for the video sequence. The key frame serves as preview of the video sequence. It is from this pane that you can associate a video key frame and link it to the video segment.

*NOTE: Video recordings can be streamed from the left-hand pane (Play button) or from the Camera tab. You can also view camera recordings from the **Message** desktop. To do so, you have to select a video recording event (identified by a camera button in the Message desktop), right-click it and select **Video recording > Play** from the shortcut menu.*

1 - From the Video event list, select an event, then click the **Play** button. The video clip appears in the Video Playback window.

2 - You may select the **Cameras** tab to view information about the camera that captured the selected event.

- **Start/End dates and times** when the recording event occurred.
- **Recording time (mm:ss)** : duration of the video segment. This duration is specified when defining recording parameters (**Video** menu > **Recording parameters**).

- **Video trigger** , if any: the video trigger is defined in the **Video trigger** menu and then selected in the **Recording parameters** definition.

NOTE: The status indicator next to the video server name indicates the current connection status of the server.

3 - You can:

- Click the **Play** button to view this video segment of the selected camera for the duration of the recording. The video appears also in the Video desktop (**Desktop** menu)
- Click the **Export** button to export it for future use. For details, see **Exporting Video Files**.

Linking Video Clips with Key Frames

EntraPass users have the ability to save a still image that best represents a video sequence linking this image to the whole video recording. This may be useful for example if one event was registered by more than one camera and you want to associate the recording with a more explicit image. Viewing the video event will enable users to identify the best image for this video event, to snap it, paste it and save it as the best sequence for the video clip. It is also possible to retrieve a previously saved image and to link it to a video segment, or to paste a previously snapped image.

1 - From the **Video event list** , select an event, then click the **Image** tab (right pane).

2 - From the image window, you can:

- **Import image** : click the **Import** button to retrieve a previously saved or exported image from a file.
- **Paste image** : click this button to paste a previously snapped image. The **Paste image** button is enabled only when you have snapped (copied) an image while viewing it. You can first play a video clip, snap it and then paste it.
- **Clear** : click the clear button to delete the displayed image from view.

Exporting Video Files

EntraPass exports video segments in four formats: KVI and KVA.

- KVI (Kantech Video Intellex format). Video data are stored in Intellex format (.img). A simple double-click allows you to view the file using VideoPlayerIntellex.exe.
- KVA (Kantech Video AVI format). Video data are stored in AVI format (.avi). A double click opens the video file using VideoPlayerWindow.exe.
- AVI format
- IMG format
- PS format

EntraPass users have two options when exporting videos:

- From the Video event list (without previewing the video)
- From the video playback window: in this case, the video is previewed before it is exported.

1 - From the video event list, select the video event you want to export.

2 - Click the **Export** button. The **Enter a video file name** window opens.

3 - Enter a file name in the **File name** field. By default, the file is assigned the Kantech KVI format. The file will be saved among EntraPass program files:\Kantech\Server CE\Video. Later you can call this file simply by double-clicking it.

*NOTE: Video files can be viewed in the **Exported video** window (Video tab > Exported video). The video file is displayed with its name, date and time. Key frames (if any) associated with a video clip can also be previewed in this window.*

4 - Click **Save** to close the **Enter file name** window. When you do this, the **Description and password** window appear.

Protecting a Video with a Password

You can protect exported videos using a password. Users must enter this password to view exported videos.

NOTE: The password protection is applicable to KVI and KVA video formats only.

1 - Select the video you want to export, then click the **Export** button.

2 - Enter a description for the video segment, in the Enter Video file name window, then click **Save** . The Description and password window appears.

3 - Check the **Use password** box if you want to add more security to this video segment. Users will have to enter this password in order to view the saved video segment.

4 - Enter a password and confirm the password in the displayed field.

5 - Click **OK** to close the Description and password window. Click **OK** to close the system message confirming the export.

Video Playback

The Video Playback feature offers the ability to view recorded video of up to 16 cameras simultaneously. To do so, you have to specify the period of time for the playback. A maximum of one hour is allowed:

- Select cameras in the left-hand pane.
- Drag and drop them into the View playback area.

Viewing a Video Playback

1 - From the Video playback window, specify the **Start date** and **time** and **End date** and **time** for the video you want to view. The maximum allowed is 1 hour. Therefore you may stream video events that occurred on the same date and for a maximum of one hour.

2 - From the left-hand pane, select a camera then drop it into the right pane. It plays for the time specified in the start and end time. Use the controls in the lower part of the Playback window (right pane) to play, fast forward, rewind or stop the video playback.

NOTE: If the requested video is not available, a message appears in the lower part of the window; the Snap and Export buttons remain disabled. If a video is available, the message Requesting video is displayed.

- **Snap** : copy the displayed image and save it in the \tmp\image folder and use it as a still image representing the video sequence. Later, the snapped image will automatically appear in the View exported video when browsing the exported videos. It is recommended to add a comment to the snapped image; the comment will appears next to the image.

- **Export** : export the video clip for future usage

- Tag to archive : mark the video sequence so that it is queued for archive.

NOTE: You can drag the slider at the bottom of the right-hand pane to increase or decrease the speed of the video clip your are playing.

3 - To save a specific video image, click the **Snap** button.

4 - Accept the default name or enter a specific name for the video recording. The video recording is saved in: Program files\Kantech\Server_CE\Tmp\Image. The video image can then be viewed using a Windows® image viewer such as Paint. Simply, double-click the video image to view it.

NOTE: For the TVR II, the video sequence can only be played forward. That is why the slider can be moved to the right side only. Also, a new button has been added to jump 30 seconds before the beginning of the current sequence.

Video Server Configuration

A video server is connected to EntraPass through a specific IP address. The video server captures, stores and distributes video data to the EntraPass desktops for monitoring and surveillance purposes. Video data can then be accessed by any EntraPass workstation (with appropriate permission) through the network. In order to use the video feature in EntraPass, the video server must be identified to EntraPass. To do this, you have to:

- Define the video server communication settings

- Specify video parameters including the number of cameras connected to the server

- Set communication delays

- Define parameters for use with EntraPass Video Vault, etc.

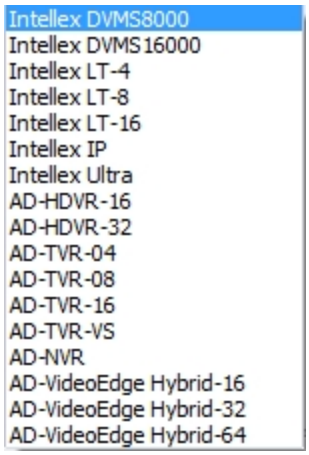
NOTE: Panasonic and American Dynamics video integrations are not compatible with Windows Server 2003 and 2008 operating systems.

Defining the Video Server Communication Settings

1 - From the EntraPass main window, click the **Video** tab, then click the **Video server** button in the Video window toolbar. The Video server window appears with the **General** tab enabled.

2 - From the **Video server** drop-down list, select the Video server you want to configure (or click the **New** button to create a new one), then assign it a descriptive 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.

3 - From the **Video Server type** drop-down list, select the DVR type for the Video server you are configuring.



NOTE: The current version of the software integrates with American Dynamics Intellex and HDVR . EntraPass supports HDVR-2U, HDVR-4U, all versions of Intellex: DVMS8000 (Up to 8 cameras) and DVMS16000 (Up to 16 cameras), Intellex IP (up to 16 network video streams), Intellex Ultra (16 channels) and Intellex LT. This later version limits the number of cameras to 4, 8 or 16 depending on the selected Intellex LT (LT-4, LT-8 or LT-16). EntraPass also supports the following models:

- **AD-TVR-04** : AD TVR 04 video channels (models ADTVR04050 and ADTVR04100).
- **AD-TVR-08** : AD TVR 08 video channels (models ADTVR08100 and ADTVR08200).

- **AD-TVR-16** : AD TVR 16 video channels (models ADTVR16050, ADTVR16100, ADTVR16200 and ADTVR16400).

- **AD-TVR-VS** : AD TVR-VS 4 video inputs.

- **AD-NVR:** Allows users viewing, managing and controlling the video being recorded on the AD-NVR through the EntraPass software:

  - Can support up to 128 IP cameras
  - Up to 400 Mb/sec image streaming
  - Base model includes minimal video analytic and can be upgraded to a full analytic package
  - One pre-configured video playback button
  - Connect to EntraPass through an IP connection. No other interface needed.
  - Video with live and playback views on the same screen:

4 - Check the **On-line** option to tell EntraPass that the video server is on-line.

NOTE: *The On-line option must be unchecked when the server is off-line for long periods such as maintenance reasons, for example. Otherwise, EntraPass will continue polling the video server; this may cause the system to hang.*

5 - In the **IP address** field, specify the static IP address of the Video server. Make sure that the Video server is set to a static IP address. For specific information about the video server IP address, contact your network administrator.

6 - **Domain name** : Video server domain address.

7 - Specify the port information for **Video (Intellex only)** , **Communication (Intellex, HDVR and TVR II)** and **Event (Intellex only)** . Make sure that these are the same used by the DVR (Digital Video Recorder).

NOTE: The TCP port (Transmission Control Protocol) is used by the 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 with the Digital Video Recorder (DVR) vendor.

8 - Check the **Bypass Ping for identification (Intellex only)** option if you want to save on bandwidth utilization. In fact if this option is not checked, the workstation will continually poll for server identification.

9 - Check the **Specify video server login (Intellex only)** option if you want users to enter their credentials before accessing the Video server. If this option is checked the **Login** tab appears in the Video Server window.

10 - Check the **Bypass DVR Messages** option if you want to cancel all the messages coming from Intellex.

11 - In the **Video server parameters** section:

- Enter the **Number of cameras.** The number of cameras connected to the video server (or use the up/down arrows) or click the **Import camera details** button to get this information from the video server. Using the **Import camera details** button offers a fast way to define cameras connected to the video server. In fact, when you click this button, EntraPass will connect to the Video server and get the number and default names for cameras connected to the DVR.

- Specify the **Polling frequency (mm:ss)** . The polling frequency refers to the delay between two polls from the Kantech Server to the Video Server. This operation is processed by the Kantech Video Server Interface.

- Specify **Polls before Communication failure** . This refers to the number of unsuccessful polls before the EntraPass Server declares the video server offline. For example, if you enter 4 in this field, EntraPass will attempt to connect four times to the video server before it declares that the server is down.

- Indicate the **Time zone adjustment.** Using the up/down arrows, specify the **Time zone adjustment** if the EntraPass server and the DVR server are not in the same time zone. The time zone adjustment refers to the time zone difference between the DVR server and the EntraPass server. Adjusting the time zone enables workstations to retrieve events generated by the DVR server at the EntraPass Server's time.

- Check the **Time for clock synchronization (Intellex only)** box. The Time synchronization refers to the time of the day when the video server will synchronize with the Kantech server for date and time. This operation is processed by the Kantech Video Server Interface.

NOTE: The EntraPass server serves as the reference time source. The video server will process the time according to the EntraPass Server's time. For example, if the EntraPass Server's time is 3:00 and that of the video server is 2:00, the Timezone adjustment data will be -1 so that the video server can display the correct information about an event that occurred at a specific time.

Enhancing the Security of Video Servers

1 - If your Intellex video server is secured by Policy Manager, EntraPass operators must use a domain name, a specific login and password to access the video server. In that case, you will check the **Specify Video server login** box in the **General** tab.

NOTE: Login name and password are mandatory if a HDVR or a TVR II video server type is used

NOTE: For details about the video server security parameters, contact the network administrator.

2 - If the **Specify video server login** option is checked, the **Login** tab is displayed.

3 - Enter the login data in the displayed fields:

- **Domain name** : enter the domain name used by the Intellex Video server **(not used for HDVR and TVR II)** .

- **Login name** : enter the login name used for accessing the video server.

- **Password** : enter the password specific to the domain controller.

- **Password confirmation** : the password for confirmation must be identical to the password entered in the previous field. If you get an error message, make sure that the Caps Lock key is not activated. For a HDVR or a TVR II, it corresponds to the DVR server password.

Remote Video Connection

This function allows controlling server video from many occurrences of the RemoteVideoProcess.exe application, on the server computer or any computer connected on the same network.

Once the Remote video connection option is registered, new parameters can be configured in the Video server window.

- IP address

- Domain name (from which the RemoteVideoProcess.exe will be executed)

- Communication port (port opened by the RemoteVideoProcess.exe application to monitor incoming requests from the EntraPass server)

*NOTE: The **RemoteVideoProcess.exe** is not accessible from the redundant server*

*NOTE: The **Video Viewer** option, accessible from the EntraPass installation process, must be used for the RemoteVideoProcess function to work.*

*NOTE: Installation of the **Remote Video Connection** will add 128 new video servers.*

Defining the EntraPass Video Vault

The EntraPass **Video Vault parameters** tab allows you to specify settings such as archiving schedule or transfer frequency for EntraPass Video Vault if this application has been activated in EntraPass and has been configured for use within the EntraPass applications.

- For details about installing EntraPass Video Vault, see **Adding System Components**.

- For details about configuring the EntraPass Video Vault application, see Configuring the EntraPass Video Vault Application.

- For details about using EntraPass Video Vault, see **EntraPass Video Vault**.

1 - From the **Video server** window, select the **Video Vault parameters** tab.

2 - Enter information for the EntraPass Video Vault application:

- **Video Vault application** : the name of the EntraPass Video Vault application associated with the selected video server.

- **Archive schedule** : the selected schedule indicates the period during which video segments will be saved. When this schedule is valid, all video segments from user-defined triggers, video server triggers or manual triggers will be saved for archiving purposes.

3 - Define the **Video segment transfer parameters** :

- **Transfer interval (hh:mm)** : the interval specified in this field indicates the period during which videos segments are retrieved from the video server. This feature restricts data retrieval and the availability of the video server during a specified period of time.

NOTE: The server allows one video retrieval at a time. If, for instance, the specified period is 02:00 --> 04:00, video segments will be retrieved for two hours per day. If the specified period is 18:00 --> 06:00, this indicates an interval of twelve hours starting from 6:00 PM to 6:00 AM.

- **Notify on transfer failure (days)** : this number indicates the number of days allocated for the video retrieval. If a video segment was not retrieved after the number of days specified in this field, the video segment will be considered unrecoverable for archiving and EntraPass Video Vault will notify the operator of the failure.

- **File language** : This option is applicable to KVI and KVA formats only. Users can choose between English and French as the language that will be used to describe the archived data.

- **Video file format** : select the format for the video file that will be retrieved:

  - **Video Vault default** : this is the format defined for the selected EntraPass Video Vault (**Devices** > **EntraPass Applications** > (Select **Video Vault application**) > **Video Vault Process** tab).

- KVI (Kantech Intellex Video) Format : The KVI file contains thumbnail and video context information and places a watermark on embedded .img. It must be viewed with the Intellex Video Player that uses the American Dynamics API. You must make sure that the API has been installed on the client's computer.

- **KVA (Kantech Video AVI) Format** : The KVA file contains thumbnail and video context information with no watermark on the embedded .AVI. Video files can be viewed using Windows Media Player or any other AVI player on the market.

- **AVI (Audio Video Interlaced) Format**: This is the standard AVI format, with no watermark. Video files can be viewed using, Windows Media Player or any other AVI player on the market.

- **IMG Intellex Format** : This format places a watermark on the video. It must be viewed with the Intellex Video Player using the American Dynamics API. You must make sure that the API has been installed on the client's computer.

- **PS Format** : HDVR native compressed video format. Use eplayer to play.

4 - For increased security, check the **Use a password for KVI and KVA file formats** option if you want to protect the KVI and KVA archived video segments by a password. Make sure to enter identical information in the **Password** and **Password confirmation** fields. Before viewing video segments archived on the EntraPass Video Vault being defined, operators will have to enter this password. Archived video files can be viewed from the Browse Video Vault window.

Comment

*NOTE: For more details about the **Comment** entry box, please refer to **Comment Field**.*

Programming the exacq DVR using EntraPass Corporate or Global system

To use EntraPass workstation to program the exacq DVR, complete the following steps:

1 - Navigate to the **Video** tab, and select **Video server** from the menu.

2 - Click **Import camera details**. The DVR can be local or remote. In the case of a remote DVR, hattrix uses a dedicated IP address that you program on the customer site or a dedicated domain name with the port forwarded to the DVR units. EntraPass pushes the EntraPass video gateway into the outbound connection for the exacq DVR.

Programming the exacq DVR to connect to EntraPass

To use the exacq DVR to program the IP address of the Video Gateway (Video Vault), complete the following steps:

1 - In the exacqVision client, click the **Config (Setup)** window icon.
2 - From the navigation tree, expand the server node and select **Configure System**.
3 - Click the **Outbound Connections** tab, and select the **Show Advanced** configuration check box.
4 - Click the **New** icon.
5 - Enter the IP address of the video vault in the **Address** field, and the port you want to use in the **Port** field.
6 - Click **Apply**.

NOTE: If the DVR fails to define in EntraPass, EntraPass add the device to the enrolment list. For more information, see ***Video gateway enrolment.***

Video Triggers

Video triggers are system events that start or stop recording. Any event related to the selected component type can trigger recording including exception events originating from a video server. A source component must be specified for each type of triggering event. For example, the “door” component must be specified for the “Door forced” event message. There is no limit to the number of definable video triggers.

Defining Video Triggers

The following information can be defined:

- A name in two languages
- The component type: type of component to be programmed for the trigger. Events are related to system components: gateway, connection, controller, etc.

Based on an event that occurred on the selected system component, the trigger will start or stop recording.

NOTE: The list of parameters depends on the video server type connected to EntraPass. It can vary depending on server feature availability and decisions on subsequent implementation. All EntraPass events can be associated with the video trigger function.

1 - From the Video toolbar, select the **Video trigger** button. The Video trigger window appears.

2 - Click the new button (or select an existing trigger if you want to modify one). Assign a descriptive name to the trigger.

NOTE: An alert message appears when you attempt to save before selecting the component type as well as the component for the trigger being defined.

3 - From the **Component type** drop-down list, select the component that will trigger the recording event. It may be a door controller, for example.

4 - As a trigger source you can select **Single** , **group** or **All components** from the component radio buttons.

5 - Use the three-dots button to select a component.

6 - From the **Trigger schedule** select a schedule for the trigger to be valid. If necessary, you can define a specific schedule for this trigger (**Definition** > **Schedule**). If there is no schedule selected for a trigger, the trigger will be disabled.

7 - From the **Event category selection** , choose between the **EntraPass** or **Intrusion** groups of events from the drop-down list.

NOTE: This field is available only when an intrusion panel has been configured in the system.

8 - Click on the **Events** tab and select events from the list.

Video Views Creation and Modification

Video presets and patterns enable users to perform automatic actions on domes. They are configured for view in the desktop dedicated to Video viewing. They enable to optimize the time dedicated to video viewing when displaying videos using pre-programmed views.

EntraPass enables users to define a wide variety of views, depending on their needs:

- Single camera
- Multiple cameras

- Multiple graphics and cameras
- Server-specific view: these are created by dragging a server into the display
- Multiple video servers: depending on their needs, EntraPass users can create views from multiple video servers.

Modifying a Video View

1 - From the Video view window, click the **Modify Video view components** button to edit or create content for the Video view desktop.

2 - From the left-hand panes, select a camera, a camera preset, or a camera pattern, then drag it into a right-hand pane cell. A camera is identified by its name and corresponding button. A preset is identified by the camera name and the preset name.

*NOTE: A specific camera can appear in more than one cell; in this case, the **Enable video sequence** option must be enabled. A graphic can appear only in one cell.*

NOTE: A Video view may only includes cameras of the same DVR type (HDVR, Intellex, TVR).

NOTE: The maximum number of TVR available is 40 .

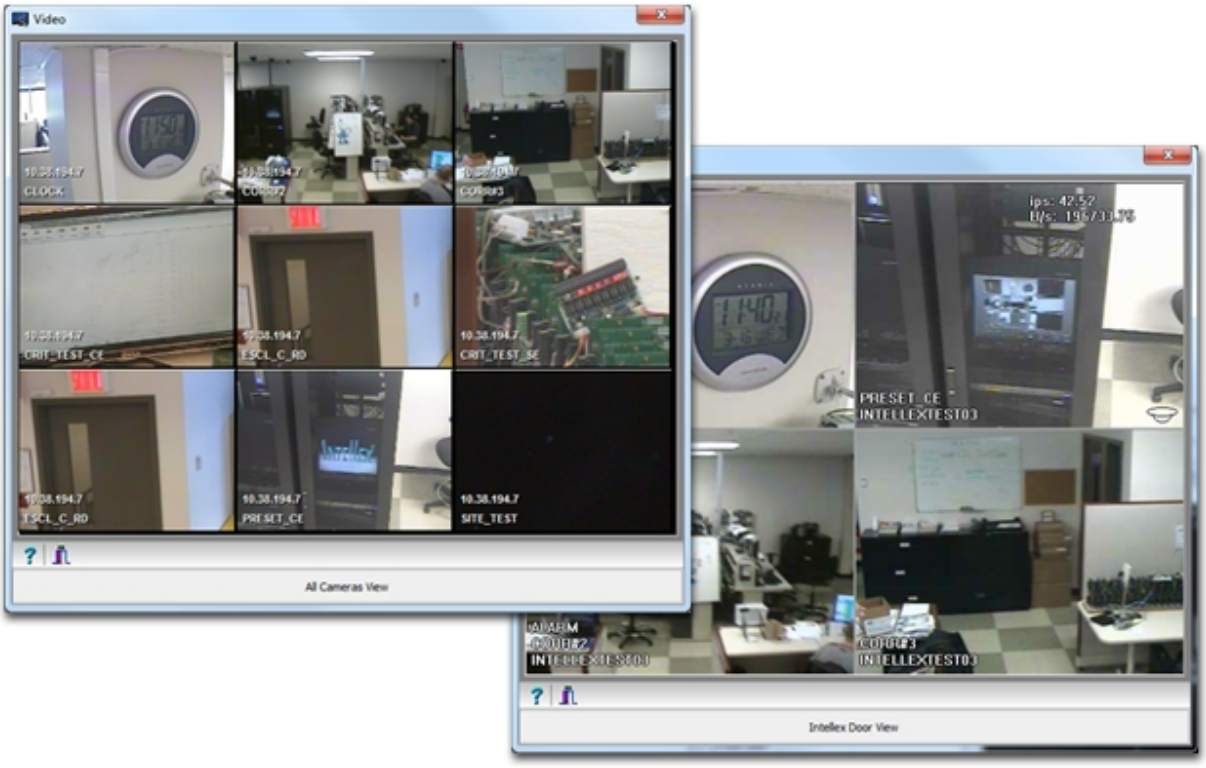
3 - Select the camera layout you want by clicking on the corresponding button in the upper part of the right pane to specify the number of images you want to display:

- Click 1 X 1 to display 1 image
- Click 2 X 2 to display 4 images
- Click 3 X 3 to display 9 images
- Click 4 X 4 to display 16 images.

NOTE: You can create a view by dragging a video server into the display. This view will contain all cameras from this specific server.

NOTE: *The number of 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 Video view appears in the Video desktop for video monitoring and surveillance (**Desktops** > Desktop dedicated to video monitoring).



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

5 - Click the **Close** button (bottom left or the "X" top right) to close the Video test window.

Video Views Definition

Once the video server is defined and its cameras identified, operators can define video views that will be displayed in the Video desktop for viewing and monitoring purposes. EntraPass operators will then call previously configured presets and patterns.

EntraPass Devices (workstations, gateways, sites, controllers, etc.) can be associated with video views. Later, the video view can be selected in the components definition in order to display the component in the video view.

Defining General Parameters for a Video View

1 - Select the **Video view** button from the Video toolbar. The Video View window appears with the **General** tab enabled.

2 - From the **Video view** drop-down list, select a video view (or click the **New** button 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 **Video server** drop-down list, select a video server type (Intellex, HDVR or TVR).

4 - From the **Default size on 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 Video window with another window.

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

5 - 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).

6 - Specify the **Refresh rate percentage** using the **Up/down** arrows.

*NOTE: The **Refresh Rate Percentage** is related to the image compression/quality. The image quality impacts the system performance: the higher the quality, the lower the compression and the lower the system performance will be. If you set the Refresh Rate 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	Result
80 and Over	Super quality	Images are recorded at the highest image quality, using the lowest level of compression. This setting requires the highest amount of storage space and network bandwidth.
50	Normal, Default	Images are recorded at normal image quality. This setting provides a balance between compression and storage space requirements. The smaller, more subtle changes between images are ignored.
40	Low quality	Images are recorded at low image quality, using the highest level of compression. This setting requires the lowest amount of storage space and network bandwidth.

7 - Check the **Re-initialize video view delay (mm:ss)** option 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. This feature is very useful if the defined camera view includes patterns or presets.

8 - From the Video control section, make the appropriate choices:

- **Show overlay Intellex and HDVR only)** : check this option if you want the camera identification (camera name and server) to appear in the Video desktop.
- **Show camera control:** check this option for use with dome cameras. Selecting this option allows operators to control a dome camera. It is not available with fixed cameras.
- **Show metrics (Intellex only)** : 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 Video window (and in the Video desktop).
- **Auto-hide text (Intellex only)** : if this option is checked, the system will not display the information related to a camera.

- **Enable image zoom (Intellex only)** : check this option if you want to display the zoom value for the selected camera.

9 - Check the **Enable video pattern** box to alternate video images in the Video window. If you have defined a 2X2 view, then the video pattern will be composed of four images alternating in the video display according to the delay specified in the **Camera display** delay field. If you do not check this option, the video view will display all the cameras simultaneously.

NOTE: The Enable video pattern section is enabled once components have been assigned to the video view.

10 - Check **Delay before launching sequence (m:ss)** box to specify the transition delay before the images start alternating in the Video window.

11 - Specify the **display delays for Cameras** , **Presets** , **Patterns** and **Graphics** .

NOTE: These delays indicate the time interval during which a video or graphic appears in the Video display before it is replaced by another. Refer to the following table for the minimum/default delays. The maximum delay is 9:59 seconds.

Delay	Minimum (sec.)
Delay before launching sequence	2 seconds
Camera display delay	3 seconds
Preset display delay	5 seconds
Pattern display delay	10 seconds
Graphic display delay	5 seconds

12 - Select the Details tab to view data about the selected view: video servers, cameras, and when applicable, camera presets and patterns.

Active Directory

The Active directory (AD) feature enables EntraPass to import and synchronize Users from AD with Operators and users in EntraPass. EntraPass uses Lightweight Directory Access Protocol (LDAP) to share information across the network between the EntraPass server and the clients AD. The sync feature eliminates the manual creation and maintenance of AD Users in EntraPass while the AD integration permits Single Sign On (SSO) authentication. This means Operators are authenticated by their Windows credentials and are automatically logged on to EntraPass Workstation using a single click. Users can also be managed through the AD connection simplifying the management of users. Up to ten AD connections are possible at the same time.

*NOTE: To run the EntraPass LDAP service you need to install Microsoft's .NET Framework. Install **.NET version 4.6.1** on the same machine where **SmartLink** is installed.*

You are required to enter network and AD settings for the server you want to connect with.

1 - Under the **System** tab, select the **Active directory** button. The Active directory window appears with the **General** tab enabled.

2 - Click the **New** button to create a new Active directory and enter the necessary information in the language section.

*NOTE: The **Enable active directory service** check box is automatically selected.*

3 - Enter the **IP address** or the **Domain name** for the server that stores the Active directory. The LDAP application uses the dedicated Port 389 for both TCP and UDP transmission.

4 - The **Sync interval (hh:mm:ss)** field specifies the time interval between the last Sync and the next Sync. Enter the interval time in hours, minutes and seconds.

NOTE: After first installing the LDAP application EntraPass completes a full Sync. However, for a restart, EntraPass completes a partial Sync where SmartLink only updates new or modified entries.

5 - You need to assign a **SmartLink** to the Active directory because the LDAP application connects to the SmartLink Web service.

NOTE: Several SmartLink connections are possible on the same SmartLink. The maximum number of Active Directories defined in EntraPass is ten.

6 - Under the **Active directory settings** complete the following fields:

- **LDAP Base DN (Operator) :** the name used for the starting point for directory server searches for EntraPass Operators, for example EntraPass.
- **LDAP Base DN (User) :** the name used for the starting point for directory server searches for EntraPass users, for example EntraPassUser.
- **LDAP Binding DN:** the user name of the AD User Account that you want to connect to the Active directory.
- **LDAP Password:** the Active directory password for the AD User Account.
- **LDAP Password confirmation:** confirm the password.

NOTE: If connection is successful then synchronization will occur. You will see LDAP service status at several locations, these are: System / Active directory, Status / Application / SmartLink, Windows system tray / LDAP Service Control, and the SmartLink application window.

7 - Select the **IMPORT AD/LDAP** button. If the connection is successful the **Imported fields** box is populated with the number of fields available from the AD server.

*NOTE: The **Import AD\LDAP** button will be greyed out if LDAP Base DN (User) is blank, or AD server IP or Domain name is blank.*

8 - For user's the **User Mapping** tab defines which Active Directory Attributes are mapped to which EntraPass database field. Here you can customize the fields used in the users synchronization. **Table 1** below describes which EntraPass database fields can be mapped.

9 - Use the **Sync now** button to manually start synchronization with the selected Active Directory server.

NOTE: The button is shaded if the Active directory is not connected.

10 - For operators, under the **Operator Mapping tab** there are thirteen fields that EntraPass can synchronize with. The first nine are mandatory and read-only but the remaining four are optional depending on your requirements. The majority of read-only fields relate to the Active directory password and the various conditions associated with it. The reason for this is EntraPass does not store passwords in its database. Active directory fully controls passwords.

If you select the **Use expiry date** and the **Operator expiry date** Active directory controls when the account expires. If you deselect these fields, the EntraPass settings remain operational. Select the **Picture** field if you want to store images of the operator, EntraPass can import both jpeg and thumbnail photo types. When you select the **E-mail** field it is possible to import and store either one or many email addresses for an operator.

11 - Please click here for information on the **Comment tab.**

Table 1 : EntraPass database fields for user mapping. The TBD field can be customized by you.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card User Name	Display Name (DisplayName)	(mandatory)
Card Type (integer)	TBD	AD fields drop list returns attributes of types: • integer • numerical string • enumeration
Start Date (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time
User End Date (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean

EntraPass fields	Active Directory fields	Possible AD fields Syntax
End Date (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time
Card # 1 - Card Number (char)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card # 1 - Display Card Number (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 1 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 1 - Expiration Date and Hour (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time
Card # 1 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 1 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 2 - Card Number (char)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card # 2 - Display Card Number (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 2 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 2 - Expiration Date and Hour (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time
Card # 2 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 2 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 3 - Card Number (char)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card # 3 - Display Card Number (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 3- User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 3 - Expiration Date and Hour (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time
Card # 3 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 3 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 4 - Card Number (char)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card # 4 - Display Card Number (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 4 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 4 - Expiration Date and Hour(date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time
Card # 4 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 4 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 5 - Card Number (char)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card # 5 - Display Card Number (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 5 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 5 - Expiration Date and Hour (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time
Card # 5 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 5 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card Information 1 (up to 10 with EP Corporate)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 2	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 3	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 4	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 5	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 6	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 7	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 8	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 9	TBD	AD fields drop list returns attributes of types: - • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 10	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 11 (up to 40 with EP Global)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 12	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 13	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 14	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 15	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 16	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 17	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 18	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 19	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)
Card Information 20	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 21	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 22	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 23	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 24	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 25	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 26	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 27	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 28	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 29	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 30	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 31	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 32	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 33	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 34	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 35	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 36	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 37	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 38	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 39	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 40	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Filter (Hattrix only) (integer)	TBD	AD fields drop list returns attributes of types: • integer • numerical string • enumeration
Privileged Operation (Global Gateway only) (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • • boolean

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Supervisor level (Global/Hattrix only) (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Delete when expired (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Wait for Keypad (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
PIN (char)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card State (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Disable Passback (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Extended Door Access	TBD	AD fields drop list returns attributes of types: • integer • enumeration
Allow Multi-Swipe (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration
Picture (binary)	TBD	AD fields drop list returns attributes of types: • replica link (type received from AD as octet string) • octet string • SID (type received from AD as octet string)
Badge Layout (integer)	TBD	AD fields drop list returns attributes of types: • integer • numerical string • enumeration
Bar Code (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration
Value (char)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Enable usage restriction (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration
Maximum card usage (integer)	TBD	AD fields drop list returns attributes of types: • integer • numerical string • enumeration
Manual Operation only (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration
Card access group (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration
Comment (char)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)

Associations

Associations is a mechanism to logically group devices. When one of the devices in the association changes its state the other devices in the association are made available. For example, an association could include a door and two cameras in the same area. If the door is opened a direct link is made to the two cameras in that association. This feature is required for the EntraPass Go Install application.

NOTE: A maximum of 8 devices are supported in each association.

To create a new association complete the following steps.

1 - Select the **Associations** button under the **Devices** tab.

2 - Click the **New** button to create a new association.

3 - Add a descriptive name to the association. For example "Main Entrance".

4 - Each tab contains a list of supported devices under that category. For example, under the **Doors** tab, all supported doors are displayed. Select the check boxes of the devices you want to add to the association.

NOTE: Doors, Inputs, Relays, Cameras (Exacq only), Partitions (DSC only), and Zones (DSC only) are supported in associations.

5 - Click the **Save** button to save the association.

6 - To remove an association, select the association from the drop-down list and select the **Delete** button.

7 - To modify an association, select the association from the drop-down list, make changes and click the **Save** button.

NOTE: If a camera and door are added to an association, that camera is also automatically added to that door's definition. If the camera was previously added to another door, a video view will be automatically added to the doors definition. If more than one camera is added to a door the first camera will be added to the door's definition.

Commissioning

Commissioning is a tool which performs a series of tests to verify each device has been installed correctly. The commissioning process maintains a commissioning status of each supported device which can be used to generate a commissioning report. This feature is required for the EntraPass Go Install application.

Commissioning is available for the following items:

- Doors.
- Inputs.
- Relays.
- Zones (DCS only).
- Cameras (Exacq only).
- Partitions (DSC only).

To view a devices commissioning status, select the device from the **Devices** tab.

If commissioning is supported by the device a **Commissioning** tab will be available. This tab contains the following items:

- Test results - including historical data.
- Date and time of commissioning.
- Comments.
- Pictures.

The status of each device can be **Not Done**, **Requested**, **Pass** or **Fail**. The operator can change the status of a device to **Requested** to force the device to perform a commissioning test.

*NOTE: A commissioning report is available in the **Report** tab.*

Creating/Modifying an Operator Security Level

Assigning security levels is critical to the system. In fact, if a security level is given full access to a system menu, operators who are assigned this security level will be able to modify system parameters. Make sure that each operator is given the security level corresponding to his/her tasks.

Items in the Security Level window are presented in a root tree with all components available for selection. This structure makes it possible to target specific components when granting security level for manual operations. Each security level is identified by a colour: full access (green), read-only (yellow) and no access (red). The security manager or an operator with appropriate permissions can easily change or assign a component to a lower level security level by double clicking an item until it changes to the desired colour code.

NOTE: Operators will not be able to see items for which they have not been given access.

1 - Under the **System** tab, select the **Security level** button. The Security level window appears with the **Menu** tab enabled.

2 - From the drop-down list, select the **Security level** you want to modify.

- To create a new security level, click the **New** button and enter the necessary information in the language section.

3 - Under the **Menu** tab, double-click an item until it reaches the desired status: **No access** (red) **, Read-only** (yellow) **or Full access** (green) **.** You can also check the appropriate items on the left to be more specific about the allowed rights.

NOTE: A user with Read-only rights will not be able to print components in EntraPass.

Configuring the security level in EntraPass Web to allow access to configure exacq DVR

To configure DVRs and cameras through EntraPass Web, click the **System** tab, and select **Security Level** from the menu. Choose the appropriate security level from the **Security Level** list, and click the **EntraPass Web** tab. The configuration options are the same as the workstation Security Level Definition.

Creating or Editing an Operator

1 - From the **System** tab, select the **Operator** button to open the Operator window.

> ***NOTE:*** *The upper right-hand corner shows the last EntraPass workstation where the operator logged on and the last login date.*

2 - Enter the operator **Name** . The operator name is composed of a maximum of 40 alphanumeric characters (including spaces). This is the name that will be displayed in the desktop message lists and the reports.

3 - Enter the operator's **email** (optional).

4 - Enter the operator **Login name** . This is a descriptive name composed of 6 to 20 alphanumeric characters (including spaces).

> ***NOTE:*** *On login, operators must enter their login name followed by their password in order for the system to validate their access. The login name is displayed in the events details when operator events are generated (i.e. manual operation, login, logout, etc.).*

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

> ***NOTE:*** *The password is case-sensitive - make sure that all operators are aware of this.*

6 - 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.

7 - In the **Language** section, check the appropriate option for the display language for this operator. If you change the display language, it will be effective only when the operator logs out and logs in again. When an operator logs out and exits an application, the next operator who logs on the application will see the start up window in the language of the last operator.

8 - In the **Privileges** section:

- Select the **Auto acknowledge** option. If this option is selected, the **Manual** button is added to the Alarms desktop (see **Alarms Desktop**). The operator can decide to manually or automatically acknowledge events. This is an operator privilege.

- Select the **Override workstation workspace message** option, if applicable. When this field is selected, the basic workstation workspace configuration will be ignored and the operator will receive events from all workstations and gateways.

- Check the **Privileges** option if you want this operator to view hidden cameras. For camera definition: **Video** > **Camera** > **Show camera** option

- Automatic video display : this option tells the system to automatically display video clips on an alarm event for the operator who is logged on. If the Alarm desktop is configured and open, the video is automatically displayed. If the alarm desktop is not open, the system checks the video display settings for this workstation (**Devices** > **Messages 2 of 2** , **Disable auto display of video views** , if this option is not checked, the system checks the video view settings for this operator: **Operator** > **Automatic video display checkbox** .

NOTE: The Override workstation workspace message 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.

- If required, check **Allow login to EntraPass Web** from the operator. The EntraPass Web component must have been registered with the EntraPass Server in order to display the option.

- Check **Filter reports using workspace** for all requested **custom** and **In/Out** reports to be issued according to the operator's permissions as defined in his workspace.

*NOTE: In order to work properly, a selected component in Workspace must have its "parent" component selected as well, otherwise it will not be displayed in the report even if the **Filter reports using workspace** option is selected.*

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 log in 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 log in to different EntraPass applications or to the EntraPass Server select the field Allow login on application 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 components an operator has access to. A security level consists of menus through which an operator can modify the database, create components, view system components and events, etc.

NOTE: It is possible to define up to 250 custom security levels; EntraPass offers 3 built-in security levels (Installer, Administrator and Guard) on configuration. The default configuration for Installer permits access to all system components. The Installer must program other security levels to limit operator access to menu commands and/or options.

12 - From the **Workspace** pull-down menu, select a workspace that will determine which physical components (desktop display, card fields, etc.) the operator will be able to access for day to day operations.

NOTE: EntraPass offers 1 built-in Installer workspace when you install EntraPass for the first time.

13 - Access the **Security** section to edit the security features of the currently displayed operator profile:

- **Operator disabled** : use this feature if you want to temporarily suspend or limit an operator access to the system without using an expiry date. If you select an operator and then check this option, the selected operator will not be able to run the application.

- **Change password at next login** : use this feature if you want an operator to change his/her password at next login.

- **Disable operator on bad password** : use this feature to limit the number of retries on bad password. For example, if you set this number to three (3), the operator will be disable after three errors when entering his/her password.

- **Days before password is reset** : this feature allows to manage operators passwords. At the end of the number of the days specified in this field, the operator will be prompted to change his/her password.

- **Use expiration date** : this feature allows you also to manage operators password. When this feature is checked, you have to select an expiration date (Operator expiration date).

- **Operator expiration date** : used with the **Use expiration date feature** , the **Operator expiration date** allows you to disable an operator's access at a specified date.

- **Concurrent Logins** :

  - For concurrent logins into an EntraPass application, select **Enabled** .

  - For concurrent logins into an EntraPass application **and** through EntraPass WebStations, select **Enabled with concurrent logins from WebStations** .

14 - Select the **Web parameters** tab to configure EntraPass Web settings for an operator.

15 - Select the **Send an EntraPass Welcome E-mail** check box, to send a welcome e-mail to an operator. Select the links you want to include in the e-mail (EntraPass Web, EntraPass Go, and EntraPass Go Install). When the save button is pressed, the e-mail is sent.

*NOTE: To change the links that EntraPass sends in the welcome e-mail, click **Devices**, click **Application** and select your **SmartLink** from the **Application** list. Select the **Web Service** tab. Double-click the **EntraPass web link for welcome email** field to view and edit the EntraPass web path. Double-click the **Mobile link for welcome email** field to view and edit the path for EntraPass go, EntraPass go Install, and EntraPass go Pass.*
To facilitate multiple SmartLink connections, select, which mobile applications you want to connect to the selected SmartLink.

16 - Press the save icon.

NOTE: The EntraPass Web component must have been registered with the EntraPass Server in order to display the option.

Concurrent Logins

The EntraPass application allows simultaneous or concurrent EntraPass Web logins to the **same** EntraPass application. This should be planned in advance so when you are ready to install or update your application, you have all the option certificates that are required. Check **Table 1** for details.

Concurrent Logins

Part Numbers	Description	Maximum concurrent Logins (Connections)
EntraPass Corporate Edition		
E-COR-WEB-1	1 Web Connection	50
E-COR-WEB-3	3 Web Connections	
EntraPass Global Edition		
E-GLO-WEB-1	1 Web Connection	200
E-GLO-WEB-3	3 Web Connections	

NOTE: Changes to the currently displayed profile will take effect at the next login attempt.

1 - Click on the **Default value** tab to select a mandatory card type (optional).

2 - Check the **Mandatory field** option to enable it.

3 - Click on three-dot to select the card type.

Filtering Desktop Events

*NOTE: The filtering desktop events option is only available when the **Event Operator** mode has been enabled.*

You can select which type of event is displayed on the desktop for each operator. Events are grouped into 4 differnet selection groups. For each selection group you can edit the name (double-click on the tab name) and edit the events in the group. To filter events for an operator complete the following steps:

1 - Click on the **Desktop event selection** tab.

2 - Select the event group. Each group can have a workspace assigned to it.

- **Default**.
- **Invalid**.
- **Watchable**.
- **All**.

3 - Select or deselect events from the event group. Right-click on the window to open the **Extended selection box**.

4 - Click the save icon.

Under the **Default value** tab in the **Current selection** section, you can select which event group is assigned to which desktop.

*NOTE: Operators logged onto workstations with **Dedicated Event Desktop** enabled will default to the workstations event filter configuration.*

Database Structure Definition

Use the Database structure menu to browse the system database. It will display the entire structure of the database including:

- The physical components (EntraPass applications, gateways, sites, controllers, doors, relays, inputs and auxiliary outputs), and
- The logical components (cards, schedules, reports, instructions, groups, etc.).

Operators can edit or sort the system components from the Database structure window.

Viewing the Database Components

1 - From the **System** toolbar, click on the **Database structure** button.

NOTE: If the Video feature is enabled in EntraPass, its components will appear in the Database explorer.

2 - To display only the **Physical components** , select the physical components button. 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 button. When selected, logical components of the database will be displayed along with the physical components.

4 - You may use the **Refresh** button to refresh the display in order to obtain the most recent information saved in the server database.

5 - You may select the **Full Expand** button to fully expand the tree structure and view all sub-components of a selected component. For example, if you use this button on a controller, the system will display the controller components (doors, inputs, relays) on the right-hand side of the window.

6 - You may select the **Full 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 corresponding definition window so you can modify its parameters.

8 - To sort the component, right click the component, then select **Sorted by** from the contextual menu. Sort the components listed in the right-hand pane of the window for an easier find. You can sort by **component** 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**.*

Event Parameters Definition

*NOTE: The event parameters feature has been replaced by event operator. For more information click **here**.*

Defining event parameters is one of the most powerful features of the system. For each event, you can determine how it will be processed by the system. For example, you can:

- Direct events to output devices (such as Messages desktop and log printer),
- Send instructions to a SmartLink application,
- Define schedules that will allow, for example, to send alarms to an EntraPass application only at night,
- Send a specific event to a specific EntraPass application, etc.

There are more than 400 system events. The most common among them are:

- Access granted
- Input in alarm

- Card modified by operator, etc.

Events are associated with system components, such as doors, controllers, gateways, EntraPass applications, etc. Every event message is associated with a system component and output devices or group of devices. For example, an Access granted event can be defined for each individual door or by default it can be defined for all doors. This flexibility allows for different actions or responses on a door-by-door basis.

Defining Events Parameters

The **Event parameters** dialog allows you to customize your system events. In fact, you can specify events that will be printed automatically or acknowledged during a specific schedule. You can also send instructions to inform an operator of an alarm through other media (i.e.: email, pager, etc.) when alarms are generated. By default, all events are defined to be displayed on all the Message desktops of all EntraPass applications defined in the system . You can customize your system events by manually associating events and components. There are two types of associations: manual and default association.

- **Default associations:** Default associations are preset in the system. By default all events messages occur on all components associated with them and are displayed in Messages desktops. You may keep the default settings.

Default associations		Comments
Component	Workstation	
Default	Default	All events originating from all components are sent to all workstations
Default	(Specific) Work-station 2	All events originating from all components are sent to only Workstation 2
Specific (Door 1)	Default	Only events originating from Door 1 are sent to all workstations

- **Manual associations** : Manual associations are setup by administrator and allow to send messages to Message desktops for specific events. The following table shows the three types of manual associations:

Manual association		Example
Component	Workstation	
Specific	Specific	Events generated by Door 1 are sent to only Workstation 1.
Specific	Unspecified or default	Events generated by Door 1 are sent to all Workstations (default).
Unspecified or default	Specific	Events generated by any of the Doors (default) will be sent to Workstation 1 only.

NOTE: Manual associations take priority over default associations. When you define a manual association between an event message and a component, the default association is ignored. It can be restored by deleting the manual association. Manual associations should be used with caution. The most common use for this feature is the SmartLink application.

1 - From the **System** tab, click the **Event parameters** button.

2 - From the **Event category selection** drop-down list, choose a category between **Access control events** and **Intrusion events** .

3 - From the **Event** drop-down list, select an event for which you want to define settings.

NOTE: By default, all events are defined to be sent to the Messages desktop of all EntraPass workstations defined in the system with an always valid schedule. It is recommended to keep default settings especially when these settings apply to all events /components . However, you may decide to create manual associations if you want a specific event to generate a specific message or alarm. The selected event will appear on all doors and will be displayed on all EntraPass workstations.

4 - In the **Display settings** section, specify the display options: by default, all events are programmed to be displayed in the Messages desktop window of all the EntraPass workstations of the system , and are assigned an **Always valid** schedule.

NOTE: If you are running EntraPass SmartLink application, this schedule must remain to "Always valid" or otherwise messages/commands will not be forwarded to the application.

5 - From the **Print** pop-up menu, select a schedule to determine when the event will be printed. When this schedule is valid, the selected event will be printed on the printer defined on the workstation to which it is being sent.

6 - From the **colour** drop-down list, select the colour that will be used to display the event in the Message desktop. The default colours are set according to the following convention:

- **Red** for alarm events;
- **Green** for elements returning to a normal condition;
- **Yellow** for warnings and errors;
- **Blue** for other events.

7 - In the **Alarm Settings** section, specify:

- **Alarm (schedule**)—When this schedule is valid, the event will be sent to the Alarms Desktop of the selected workstations and will require an acknowledgement from the operator.
- **Instructions** —Select the instruction that will be sent to the Instruction desktop with the event to be acknowledged. Instructions will only be sent when the alarm schedule is valid.

NOTE: For the SmartLink application, the instruction does not require that the alarm schedule be valid. You can leave the Alarm schedule field blank, and the instruction will be sent anyway.

8 - Assign the **Priority** level to the event using the slider. This determines the sequence in which alarm messages will be displayed to the operator in the alarm queue. The priorities are preset to the most common values (0 = higher, 9 = lower).

9 - In the **SmartLink** section, click on the three-dot to select a **Task schedule** .

10 - Click on the three-dot to select a **Task Builder** .

Creating Associations

1 - In the **Event parameters** window, select an **Event category** and an **Event** from the drop-down lists. From the component pane (on the left) select a component and then select an EntraPass workstation to which the event message will be sent.

2 - Click the **Save** button to create the new association. In this case, All access - Door opened events that will occur on the selected door will be sent to the assigned workstation computer (selected on the right-hand side).

NOTE: The Save button is enabled only when the selected event/component becomes part of an association.

Viewing Default Parameters

1 - From the component pane (on the left) select a component and then select an EntraPass application to which the event message will be sent .

2 - Click on the **View default parameters** button in the toolbar to view the default parameters message box. It will show if the event parameters were set by default or manually.

3 - Click again on the **View default parameters** button to close the message box.

Deleting and Restoring Associations

You may decide, for example, that an event from a specific component should no longer be sent to the Message desktop of all workstations, or to a specific desktop. To do this, you have to delete the existing association. We recommend you use this feature with caution.

1 - In the **Event parameters** window, select the category and then the event you want to modify from the **Event** drop-down list.

2 - Click the **Delete** button in the toolbar.

3 - From the **Delete event parameters** window, make your choice:

- **Restore default** : this option will apply the default alarm and display settings.

- **Suppress messages** : if you select this option, the alarm and display settings fields will be left blank and ready for new information. Once you have deleted the settings, you must re-define them.

- **Cancel** : select this option if you want to cancel the delete operation.

Printing Event Parameters

EntraPass allows you to print events parameters (alarm and display settings) for the selected events.

1 - From the **Event parameters** window, select the **Printer** button.

2 - In the **Select events** pane, select the events to be included in your printout or click on the **Select all** button to select all the events from the displayed list.

3 - In the **Select workstations** pane select the EntraPass workstation (or workstations) to be included in your printout or click on the **Select all** button to select all the EntraPass workstations from the displayed list.

- **Print empty fields** : If selected, the system will print the fields that do not contain any information. Only the field title will be printed.

- **Print with default values** : 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 y), the report will be empty.

- **Print components reference** : If selected, the system will print the component physical address next to the component identification.

- Use the **Font** button to choose a different font (and font size) for your report.

- Select the **Preview** button before printing, if desired.

Instructions Definition

This menu is used to define instructions that must be assigned to events. When an alarm is generated, the instruction will display in the Instruction window (Desktop menu) for acknowledgement . Usually, each line contains a single directive; with the response instructions composed of several directives (lines). This allows for greater flexibility when modifications are required.

Defining an Instruction

1 - From the **Definition** main window, select the **Instruction** button.

> ***NOTE:*** *For EntraPass Special, when using* ***Event Operator****, the* ***Instructions*** *button is on the* ***System*** *tab. For EntraPass Corporate, Global, and hattrix, when using* ***Event Parameter****, the* ***Instructions*** *button is on the* ***Definition*** *tab.*

2 - To create a new instruction, click the **New** button. To modify an existing instruction, select one from the **Instruction** drop-down list.

3 - Enter the instruction name/identification in the language section.

4 - If the **Mandatory alarm comment** checkbox selected, the operator will have to add a comment in order to mark the alarm as “acknowledged”.

5 - 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.*

6 - To assign instructions to events, see Trigger and Alarm.

Message Filters Definition

The Message filter feature allows you to define filters for the Filtered Messages desktop. These filters are used to view a specific selection of events. There are many pre-defined filters such as: access events, controller events, etc. These filters can be accessed by all operators. You can select or create filters directly from the “Filtered Messages” desktop or from the Message Filters menu.

NOTE: For more information, see Filtered Messages Desktop.

Defining Event for a Message Filter

1 - In the System main window, select the **Message Filter** button. The Message filter window appears.

2 - From the **Message filter** drop-down list, select an event message type (for example: Door events or Relay events) for which you want to define a filter. You may also click the **New** button to create your own filter.

3 - From the **Event list** , select the events that must appear in the selected filter. You may check the **Select all events** option, if you do not want to select specific events. For example, for a Door events type filter, you may decide to include all events or select the **Access-denied** events.

4 - Select the **Door filters** tab to filter doors that will send messages to the Filtered messages desktop. Additionally, when "Access events" are filtered, the card holder's picture can be displayed with the event (if pictures are assigned to cardholders). You can select which doors will display the cardholder picture when the event for this door is generated.

5 - Check the **All doors** option or choose specific doors for which the cardholders picture will be displayed an door event.

6 - From the **Door filter type,** select the filter that will be used for filtering Door events:

- **Door filter** : Only events related to the selected doors will be sent to the Filtered Message desktop
- **Pictures filter** : Cardholders pictures related to cards presented to the selected doors will be sent to the Filtered Message desktop
- **Filters for doors and pictures** : Door events related to the selected doors as well as cardholders pictures that triggered door events on the selected doors will be sent to the Filtered Message desktop.

7 - Select the **EntraPass applications** tab to filter applications that will send messages to the Filtered Messages desktop.

8 - Check the **All EntraPass applications** option for the Filtered Messages desktop to receive all events originating from all EntraPass applications defined in the system. You may also choose to display events

from specific applications. To do this, select the EntraPass application from which you want to receive events.

9 - Select the **Gateway and connection** tab to filter gateways and sites events sent to the Filtered Messages desktop.

10 - Check the **All events** option to receive events originating from the components of the gateways or sites. You may select the gateway or the connection that will send events to be displayed.

NOTE: When you use filters, the system retrieves events that are already displayed in your Message desktop and sorts these events according to the settings of the selected filter. If 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.

11 - Select the **Special filter** tab to filter events according to their type.

- **Picture** : all events associated with a card holder's picture will be displayed in the Filtered Message desktop.

- **Fail-soft** : all events generated by a controller in stand-alone mode following a communication failure will be sent to the Filtered Message desktop. Fail-soft messages are identified with a + sign in the Filtered Message desktop (and Message Desktop) when this option is select when defining the Messages list properties (**Desktop** > **Message Desktop** > right-click an event > **Properties**).

- **Video** : all video record events will be sent to the Filtered Messages desktop.

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 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.

Operators Definition

Use the **Operator** menu to define system operators and to determine their security level and privileges. An operator is responsible for issuing cards, carrying out manual operations on system components,

requesting reports, arming the system, etc. For security reasons, each operator accessing the system database should have his/her profile defined to ensure that all the actions performed in the system will be traceable. You need to create at least one operator account or modify the pre-created accounts in order for the operator to use and operate EntraPass and to receive event messages.

There are three default operators created in the system. These are associated with three levels of access rights:

- Installer (login name and password are kantech): Full access to view, modify, delete, print components.
- Administrator (the login kantech1 and the password kantech): Medium access with limited access to system menus.
- Guard (login kantech2 and password are kantech): Limited access to system menus.

NOTE: You can define operators using the default operators or you can create new operators. For details about operators' security levels, see ***Security Level Definition*** .

NOTE: When the ***Active directory*** *application is active. A new default operator called* ***LDAP Interface*** *is created and available from the Operator drop-down list.*

Creating or Editing an Operator

1 - From the **System** tab, select the **Operator** button to open the Operator window.

NOTE: The upper right-hand corner shows the last EntraPass workstation where the operator logged on and the last login date.

2 - Enter the operator **Name** . The operator name is composed of a maximum of 40 alphanumeric characters (including spaces). This is the name that will be displayed in the desktop message lists and the reports.

3 - Enter the operator's **email** (optional).

4 - Enter the operator **Login name** . This is a descriptive name composed of 6 to 20 alphanumeric characters (including spaces).

NOTE: On login, operators must enter their login name followed by their password in order for the system to validate their access. The login name is displayed in the events details when operator events are generated (i.e. manual operation, login, logout, etc.).

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

NOTE: The password is case-sensitive - make sure that all operators are aware of this.

6 - 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.

7 - 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 on again. When an operator logs out and exits an application, the next operator who logs on the application will see the startup window in the language of the last operator.

8 - In the **Privileges** section:

- Select the **Auto acknowledge** option. If this option is selected, the **Manual** button is added to the Alarms desktop (see **Alarms Desktop**). The operator can decide to manually or automatically acknowledge events. This is an operator privilege.

- Select the **Override workstation workspace message** option, if applicable. When this field is selected, the basic workstation workspace configuration will be ignored and the operator will receive events from all workstations and gateways.

- Check the **Privileges** option if you want this operator to view hidden cameras. For camera definition: **Video** > **Camera** > **Show camera** option

- Automatic video display : this option tells the system to automatically display video clips on an alarm event for the operator who is logged on. If the Alarm desktop is configured and open, the video is automatically displayed. If the alarm desktop is not open, the system checks the video display settings for this workstation (**Devices** > **Messages 2 of 2** , **Disable autodisplay of video views** , if this option is not checked, the system checks the video view settings for this operator: **Operator** > **Automatic video display checkbox** .

NOTE: The Override workstation workspace message 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.

- If required, check **Allow login to EntraPass Web** from the operator. The EntraPass Web component must have been registered with the EntraPass Server in order to display the option.

- Check **Filter reports using workspace** for all requested **custom** and **In/Out** reports to be issued according to the operator's permissions as defined in his workspace.

*NOTE: In order to work properly, a selected component in Workspace must have its "parent" component selected as well, otherwise it will not be displayed in the report even if the **Filter reports using workspace** option is selected.*

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 log in 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 log in to different EntraPass applications or to the EntraPass Server select the field Allow login on application 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 components an operator has access to. A security level consists of menus through which an operator can modify the database, create components, view system components and events, etc.

NOTE: It is possible to define up to 250 custom security levels; EntraPass offers 3 built-in security levels (Installer, Administrator and Guard) on configuration. The default configuration for Installer permits access to all system components. The Installer must program other security levels to limit operator access to menu commands and/or options.

12 - From the **Workspace** pull-down menu, select a workspace that will determine which physical components (desktop display, card fields, etc.) the operator will be able to access for day to day operations.

NOTE: EntraPass offers one built-in Installer workspace when you install EntraPass for the first time.

13 - The **Active directory** label on the lower-left section of the screen is only visible on activation of the **Active directory application**. When you enter the **Profile** for an operator this profile is used as a template for that category of user.

After **synchronization** with Active directory the **Domain name** and the **Active directory** server that created the operator is displayed in the read-only fields underneath.

NOTE: Before synchronization, you must manually define the operator profile.The profile must exist in EntraPass and exactly match the sub-group underneath the LDAP base distinguishing name in Active directory. The Search icon in the toolbar permits Users to search by profile name, this search is case sensitive.

14 - If you select the **Disable synchronization** check box, **Single Sign On** is disabled and Active directory ceases to update any data. The operator still exists in EntraPass but will not be updated by the synchronization.

15 - Access the **Security** section to edit the security features of the currently displayed operator profile:

- **Operator disabled** : use this feature if you want to temporarily suspend or limit an operator access to the system without using an expiry date. If you select an operator and then check this option, the selected operator will not be able to run the application.

- **Change password at next login** : use this feature if you want an operator to change his/her password at next login.

- **Disable operator on bad password** : use this feature to limit the number of retries on bad password. For example, if you set this number to three (3), the operator will be disable after three errors when entering his/her password.

- **Days before password is reset** : this feature allows to manage operators' passwords. At the end of the number of the days specified in this field, the operator will be prompted to change his/her password.

- **Use expiration date** : this feature allows you also to manage operators' password. When this feature is checked, you have to select an expiration date (Operator expiration date).

- **Operator expiration date** : used with the **Use expiration date feature** , the **Operator expiration date** allows you to disable an operator's access at a specified date.

- **Concurrent Logins** :

  - For concurrent logins into an EntraPass application, select **Enabled** .

  - For concurrent logins into an EntraPass application **and** through EntraPass WebStations, select **Enabled with concurrent logins from WebStations** .

NOTE: The EntraPass Web component must have been registered with the EntraPass Server in order to display the option.

Concurrent Logins

The EntraPass application allows simultaneous or concurrent EntraPass Web logins to the **same** EntraPass application. This should be planned in advance so when you are ready to install or update your application, you have all the option certificates that are required. Check Table 1 for details.

Concurrent Logins

Part Numbers	Description	Maximum concurrent Logins (Connections)
EntraPass Corporate Edition		
E-COR-WEB-1	1 Web Connection	50
E-COR-WEB-3	3 Web Connections	
EntraPass Global Edition		

Part Numbers	Description	Maximum concurrent Logins (Connections)
EntraPass Corporate Edition		
E-GLO-WEB-1	1 Web Connection	200
E-GLO-WEB-3	3 Web Connections	

NOTE: Changes to the currently displayed profile will take effect at the next login attempt.

1 - Click on the **Default value** tab to select a mandatory card type (optional).

2 - Check the **Mandatory field** option to enable it.

3 - Click on three-dot to select the card type.

Defining a Login Message for a Single Operator

1 - From the **System** menu, select **Operator**.

2 - Select an operator from the drop-down list.

3 - Click the **Login message** tab.

4 - Set the recurrence:

- **None**.
- **Always**: The message will always pop up after login.
- **Only once**: The message will be displayed only once for each operator.
- **Until**: The message will be displayed until the selected date is reached.
- **Only once until**: The message will be displayed once until the selected date is reached or until the operator receives the message.

5 - Select **Disable all login messages** to stop the reception of login messages for the selected operator.

6 - Type a message in the boxes on the right (primary and secondary languages).

7 - Click the **Save** button.

Security Level Definition

Security level refers to the permissions granted to an operator to access EntraPass logical components (desktops, card information, etc.), as well as to perform some actions on those components.

NOTE: You have to program the appropriate security levels if you want to limit operator access to commands and/or options of the system menu.

It is possible to customize an operator security level; the system allows you to create up to 250 security levels. Each operator has a separate login name, password and a corresponding security level. The password is case-sensitive. There are three operators and security levels already configured in EntraPass. These are: Installer, Administrator and Guard.

- **Installer:**
  - **Login name and password** : kantech
  - **Security level** : By default, a user defined as Installer has full access to all the system menus. He/she can read and edit system components and has unrestricted access to the system.
- **Administrator:**
  - **Login name:** kantech2; password: kantech
  - **Security level** : Administrator. By default, a user defined as Administrator has limited access to a number of the system menus.
- **Guard:**
  - **Login name** : kantech2; password: kantech
  - **Security level** : Guard. By default, a user defined as Guard has limited access to the system menu.

Creating/Modifying an Operator Security Level

Assigning security levels is critical to the system. In fact, if a security level is given full access to a system menu, operators who are assigned this security level will be able to modify system parameters. Make sure that each operator is given the security level corresponding to his/her tasks.

Items in the Security Level window are presented in a root tree with all components available for selection. This structure makes it possible to target specific components when granting security level for manual operations. Each security level is identified by a colour: full access (green), read-only (yellow) and no access (red). The security manager or an operator with appropriate permissions can easily change or assign a component to a lower level security level by double clicking an item until it changes to the desired colour code.

NOTE: Operators will not be able to see items for which they have not been given access.

1 - Under the **System** tab, select the **Security level** button. The Security level window appears with the **Menu** tab enabled.

2 - From the drop-down list, select the **Security level** you want to modify.

- To create a new security level, click the **New** button and enter the necessary information in the language section.

3 - Select a system tab (**Workstation**, **EntraPass Web**, **EntraPass Go** or **Smartlink API**).

4 - Double-click an item until it reaches the desired status: **No access** (red) **, Read-only** (yellow) **or Full access** (green) **.** You can also check the appropriate items on the left to be more specific about the allowed rights.

NOTE: A user with Read-only rights will not be able to print components in EntraPass.

Defining Login Options for an Operator

The **Miscellaneous** tab allows you to define operator login and system display options:

- Operator login options: you can allow or restrict an operator to log in an EntraPass workstation or server.

- Active windows that can be kept on the desktop: EntraPass allows operators to keep five active windows on the desktop.

- Component display options: components can be displayed with our without their physical address. The physical address can appear on the left or right of the component name.

1 - Select the **Miscellaneous** tab to define parameters for the security level being defined.

2 - In the **Login restrictions** section, select the appropriate login options:

- Select **Allow login on server** to allow the operator to log in to the EntraPass server (Primary or Redundant).

- Select **Allow login on workstation** to allow the operator to log in to any application in the system.

3 - The **Keep on application desktop** section allows users to increase the number of active windows on the desktop. In fact, operators can open five windows at the same time: one configuration window and four windows from the other categories. EntraPass windows are classified in five categories:

- **Configuration screen** : this group includes all the menus that allow an operator to program the system. This group includes such menu items as: **User** menu (card, Badging, card access group, access level, visitor, card type; Definition menu; **Group** menu; **Devices** menu; **System** menu; Video menu; Custom and **In/Out reports** .

- **Operation screen** : this group includes all the Operation menu items and the Video playback option.

- Status screen : this group includes windows of the Status menu, Current recording menu and Report state menu.

- **Database screen** : The following menus are included in this category: Option menu (card format, authentication password, select languages, Printers options, Changes date and time, etc.); Items of the User menu (Daypass, batch operations and Import/Export CSV); View Report, Operation on In/Out, and View exported videos.

- **Report screen** : this group includes Quick Report, Custom and In/Out report requests and Video list windows.

NOTE: These options allow operators to keep more than one window active on the desktop. They can bring to front or send to back the window they want to display, simply by pressing [ALT-F6] .

4 - In the **Components physical address** section, specify how the component's physical address will be displayed. This will also affect how components will be sorted.

- **Display on left** —If selected, components will be sorted by their address (i.e. 01.01.01 Controller xyz).
- **Display on right** —If selected, components will be sorted by their component name (i.e. Controller xyz 01.01.01).
- **No display** —If selected, the address will not be displayed (i.e. Controller xyz) and components will be sorted by name.

5 - In the **Miscellaneous** section:

- Hide card holder pin content: If selected, it offers you the ability to hide the card holder pin content from the view.
- Hide Camera from video view: If you are using the Video feature, EntraPass enables you to deny viewing permission to a specified security level.

NOTE: Checking the Hide camera from video view option tells the system to verify access permission to cameras before loading a video view. For example, if the selected operator's security level has access to a video server but not to all cameras defined in the video server and has access to the selected video view, the system will hide the camera that has been un-selected when assigning permission to the video server. For details, see ***Video Server Configuration****.*

Hiding Card Information

EntraPass offers you the ability to hide card information fields from view. For example, you can decide that a certain security level (Guard for example) can view or modify card information field. To do so, select the security level, then under the **Card database fields** tab, check the box that corresponds to the fields you want to hide.

1 - Select the **Card database fields** tab to limit the number of card fields which are visible to the operator who is assigned this security level.

2 - Select the fields (either individually or in groups) that will be hidden to the selected security level. Click on a field box repeatedly to scroll through the different status (Normal, Hide or Read only).

Assigning Video Custom Buttons

EntraPass offers you the ability to customize five buttons for use in the Video interface. System installers and administrators can customize buttons for use by operators in the Video desktop. For example, a button customized for Playback with fixed delay with specific pre-record and record delays and assigned to a specific Security level will enable operators to trigger the actions related to the specific button. If you associate a custom button with a specific task (play back or generating video events, additional buttons are added to the Video desktop (**Desktops** > Desktop dedicated to video viewing)

1 - From the **Security level** drop-down list, select the security level you want to define/edit.

2 - Select the **Video custom button** tab to assign permission to this operator. The following permission can be granted:

- Playback with fixed delay
- Playback with custom delay
- Generate recording event with fixed parameters
- Generate recording event with custom parameters.

3 - Select the option you want to assign to the operator being modified.

NOTE: *Pressing the button associated with Playback with fixed delay will start a play back with the specified duration. This includes the pre-alarm recording time and the maximum recording time.*

Workspace Definition

Workspaces allow System Administrators to grant or deny operators access to system physical components such as gateways, sites, relays, etc. Workspaces are defined according to the type of tasks the operators will be allowed to perform in EntraPass; creating and editing items, viewing components, printing lists or reports, etc. Operators who are assigned a given workspace will not be able to see nor modify EntraPass components that are not selected in that workspace definition. Workspaces can also be used by operators to discriminate the information they want to view on screen. For example, a System Administrator who has access to all components of the EntraPass system may want to view only specific components. In that case, the System Administrator can define a specific workspace for that environment and work within those parameters.

NOTE: There is only one default Installer workspace created when you install EntraPass for the first time.

Workspace Filtering

- **Hierarchical filter** : items in a list will be displayed according to the item selected in the level above. For example, when selecting a specific site (parent), the system will automatically adjusts itself to display only the corresponding controllers (children). And if you select a specific controller (parent), the system will adjust itself to display only the corresponding doors (children), and so on.

NOTE: If a tab is empty, verify that you have selected components from it's parent.

- Once you have selected the **Hierarchical** filtering mode, it will remain activated under all tabs.

Selecting EntraPass Applications

This feature allows you to select the applications that will be available to an operator who is assigned this workspace. In the following example, the workspace (Administrator) will not view messages sent by the EntraPass SmartLink application because it is not assigned to their workspace.

1 - From the **Workspace** tab, select the workspace you want to define or edit.

NOTE: When an operator is allowed to use the "Network alarms message desktop (Desktops menu), only alarm events originating from the EntraPass applications and components of the applications that are selected in this window will be displayed. The workspace definition acts as a filter for the "Network alarms message desktop".

- Select **All EntraPass applications** if you want all the displayed applications to be available to the operator who is assigned the workspace

- You can also select individual EntraPass applications from the displayed list.

2 - Save your modifications.

Defining Gateways and Sites

1 - Move to the **Gateway and Site** tab to select the list of gateways and sites that will be available to an operator who is assigned the workspace.

- Select **All gateways and sites** if you want all the displayed gateways and sites to be available to the operator assigned to this workspace.
- You can also select individual gateways and sites from the displayed list.

2 - Save your modifications.

Defining Schedules

1 - Move to the **Schedule** tab to select the list of schedules that will be available to an operator.

- Select **All schedules** if you want all the displayed schedules to be available to the operator who is assigned this workspace.
- You can also select individual schedules from the displayed list.

2 - Save your modifications.

Defining Controllers

1 - Move to the **Controller** tab to select the list of controllers that will be available to an operator who is assigned the workspace.

- Select **All controllers** if you want all the displayed controllers to be available to the operator who is assigned this workspace.
- You can also select individual controllers from the displayed list.

2 - Save your modifications.

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 (Gateway and Site tab) 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.*

Defining Doors

1 - Move to the **Door** tab to select the list of doors that will be available to an operator who is assigned this workspace.

- Select **All doors** if you want all the displayed doors to be available to the operator who is assigned this workspace.
- You can also select individual doors from the displayed list.

2 - Save your modifications.

Defining Relays

1 - Move to the **Relay** tab to select the list of relays that will be available to an operator who is assigned the workspace.

- Select **All relays** if you want all the displayed doors to be available to the operator assigned this workspace.
- You can also select individual relays from the displayed list.

2 - Save your modifications.

Defining Inputs

1 - Move to the **Input** tab to select the list of inputs that will be available to an operator who is assigned the selected workspace.

- Select All inputs if you want all the displayed inputs to be available to the operator assigned this workspace.
- You can also select individual inputs from the displayed list.

2 - Save your modifications.

Defining Access Levels

Associating specific access levels to a workspace allows you to control the access levels that an operator can define or modify. For example, a security guard may have the right to issue cards that are valid for a given door or access level only.

1 - Move to the **Access level** tab to select the list of access levels that will be available to an operator who is assigned this workspace.

- Select **All access levels** if you want all the displayed access levels to be available to an operator who is assigned this workspace.
- You can also select individual access levels from the displayed list.

2 - Save your modifications.

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.

Defining Card Types

This feature restricts the operator action. In fact, card types that are not selected in this menu will not be available to an operator when creating or editing cards. For example, you may decide that an operator with the Guard workspace will not be able to issue a specific card type such as Security. To do this, select the Guard workspace, then uncheck Security when filtering card types for the Guard workspace.

1 - Move to the **Card type** tab to select the card types that will be available to an operator who is assigned the selected workspace.

- Select **All card types** if you want all the displayed card types to be available to the operator assigned this workspace.
- You can also select individual card types from the displayed list.

2 - Save your modifications.

Defining Card Access Group

This feature gives operators access to specific card access groups for batch operations according to their workspace.

1 - Move to the **Card access group** tab to select the list of card access groups that will be available to an operator who is assigned this workspace.

- Select **All Card access group** if you want all the displayed card access groups to be available to the operator who is assigned this workspace.
- You can also select individual card access groups from the displayed list.

2 - Save your modifications.

Defining Reports

This feature gives operators access to specific reports according to their workspace. For example, a System Administrator may have access to all the reports that can be generated whereas the Guards' Supervisor may only have access to all Guard Tour related reports. The reports will be generated from the **Archived Message list** on the workstation desktop. Once the reports have been assigned to workspaces, operators will only have access to reports that correspond to their workspace.

1 - Move to the **Report** tab to select the list of reports that will be available to an operator who is assigned this workspace.

- Select **All reports** if you want all the displayed reports to be available to the operator who is assigned this workspace.
- You can also select individual reports from the displayed list.

2 - Save your modifications.

Defining Graphics

1 - Move to the **Graphic** tab to select the list of graphics that will be available to an operator who is assigned the workspace.

- Select **All graphics** if you want all the displayed graphics to be available to the operator assigned this workspace.

- You can also select individual graphics from the displayed list.

2 - Save your modifications.

Defining Operators

For security reasons, an operator can see and change another operator's rights. Use the Operator tab to limit the possibility for an operator to see, edit or delete another operator.

1 - Move to the Operator tab to select the list of operators that will be available to an operator who is assigned the workspace.

- Select All operators or individual operators from the displayed list.

2 - Save your modifications.

Defining Badge Layouts

1 - Use the Badge Layout tab to determine which badge layout will be available for a given operator who is assigned the workspace.

2 - Move to the Badge Layout tab.

- Select All badge layout or individual badge layouts from the displayed list.

3 - Save your modifications.

Defining Workspaces

This feature gives operators access to information that pertains to specific workspaces according to other operators workspaces. For example, Guards in the system may have a workspace assigned to them according to the area they are patrolling and the type of information they can view and edit in EntraPass. The Guard's Supervisor, however, must have access the information available to all the Guards working in his department. In that case the list of workspaces for the Supervisor will contain all the Guards' workspaces defined in EntraPass.

1 - Move to the **Workspace** tab to select the list of workspaces that will be available to an operator who is assigned the selected workspace.

- Select **All workspaces** if you want all of them to be available to the operator who is assigned this workspace.
- You can also select individual workspaces from the displayed list.

2 - Save your modifications.

Specifying Security Level

The Security level tab in the workspace only limits the operators to select which security levels they can assign when creating/modifying operators.

1 - Move to the **Security level** tab to select the security level (s) that you want to assign that workspace. If you must create a new security level, see **Security Level Definition**.

- Select **All security levels** if you want to assign them all to that workspace.
- You can also select individual security level from the displayed list.

2 - **Save** your modifications.

Defining Video Servers

The video server list allows you to assign or limit operator access to specific video servers and cameras. For example, even if a workspace level allows access to a video server, you still have the ability to restrict access to a specific camera for that workspace. This feature makes it easier to define or modify permission for accessing a video server, a video view or other video menu items.

1 - Move to the **Video server** tab to select the list of video servers that will be available to an operator who is assigned the selected workspace.

- Select **All video servers** if you want all of them to be available to the operator who is assigned this workspace.
- You can also select individual video servers from the displayed list.

2 - Save your modifications.

NOTE: *To filter video views available to an operator, the operator's workspace must have access permission to the video server associated with this specific video view. For example, if operators are granted access permission to a video view but their workspace definition does not give them access to the video server where the video view is defined, the video view will not be available to operators with this workspace.*

Defining Cameras

1 - Go to the **Camera** tab to select the list of cameras available to an operator who is assigned the selected workspace.

- Select **All cameras** if you want all the cameras to be available to the operator who is assigned this workspace.
- You can also select specific cameras from the displayed list.

2 - Save your modifications.

Defining Video Views

1 - Move to the **Video views** tab to select the list of video views that will be available to an operator who is assigned the selected workspace.

- Select **All video views** if you want all of them to be available to the operator who is assigned this workspace.
- You can also select individual video views from the displayed list.

2 - Save your modifications.

Defining Tasks

Associating tasks to a workspace allows you to control the tasks that an operator can define or modify.

1 - Move to the **Task Builder** tab to select the list of tasks that will be available to an operator who is assigned this workspace.

- Select **All tasks** if you want all the tasks to be available to the operator assigned this workspace.
- You can also select individual tasks from the displayed list.

2 - Save your modifications.

Defining Panels

Associating panels to a workspace allows you to control the panels that an operator can define or modify.

1 - Move to the **Panel** tab to select the list of panels that will be available to an operator who is assigned this workspace.

- Select **All panels** if you want all the panels to be available to the operator assigned this workspace.
- You can also select individual panels from the displayed list.

2 - Save your modifications.

Defining Panel Components

Associating panel components to a workspace allows you to control the panel components that an operator can define or modify.

1 - Move to the **Panel Component** tab to select the list of panel components that will be available to an operator who is assigned this workspace.

- Select **All panel components** if you want all the panel components to be available to the operator assigned this workspace.
- You can also select individual panel components from the displayed list.

2 - Save your modifications.

Defining Events

*NOTE: If the **Event Operator** mode has been enabled, this feature is now available in Creating or Editing an Operator*

This feature is used to define the event messages that can be displayed to operators who are assigned the selected workspace.

1 - Move to the **Events** tab to select the list of events that will be displayed on an operator workstation.

- Select the events you want to display for the operator who is assigned this workspace.

2 - Save your modifications.

Operators in Workspace

1 - For security reasons, an operator can see and change another operator's rights. An additional tabulation was integrated under Workspace to limit the possibility for an operator to see, edit or delete another operator.

2 - From the **System** menu, select **Workspace**.

3 - Select an operator from the drop down list.

4 - Select the **Operator** tab. You will see a list of operators who can be seen by the selected operator in the **Workspace** drop down.

Audit

Use the **Audit** icon to view, which operator made changes, or deleted a component.

1 - To open the **Audit** window, click the **System** function, and click **Audit**.

2 - To select an operator, choose from the **Operator** list.

3 - To select a component, choose from one of the following options in the **Component** list.

- **All**
- **Create**
- **Modify**
- **Delete**

4 - In the **Start date and time** field, select a date and time to start the search.

5 - In the **End date and time** field, select a date and time to end the search. Click Search.

The search results populate two tables, the first table contains the following component information:

- **Color coded column**: indicates if the component was created, modified, or deleted.
  - Green: **Create**
  - Blue: **Modify**
  - Red: **Delete**
- **Date and time**: the date and time the card was created, modified, or deleted.
- **Type**: the menu that was changed.
- **Component Type**: the component that was changed.
- **Count**: the number of fields that were changed.

The second table contains the following component information:

- **Reference**: the item the change references.
- **Field name**: the name of the GUI field.
- **Old value**: the value before the change occurred.
- **New value**: the value when the system saved the change.
- **Field description**: description of the field name.

To access the following column options, click the Hamburger icon on the upper left table.

- **Data type**: the database data type:
  - **TimeStamp**
  - **Integer**
  - **Object**
  - **Components**
- **Table name**: the database table name.

NOTE: *Define the results based on the amount of records, or by date. For more information, see Server logs in System parameter.*

To access the context menu, select a table entry, and right-click. The following options are available:

- CSV export selected: export the selected entry of the card audit trail to a CSV format file.
- CSV export all: export the entire content of the card audit trail to a CSV format file.
- View old value: view a window with the value before the change.
- View old value parent: view a window of the parent of the selected component with the value before the change.

- View old value link: view a window representing a link to the component with the value before the change.
- View new value: view a window with the value after the change.
- View new value parent: view a window of the parent of the selected component with the value after change.
- View new value link: view a window representing a link to the component with the value after the change.

Archive Viewing

The Archive 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 Archive window. When you click "Preview", the system automatically launches the appropriate program to view the report.

Displaying a Report

1 - Under the **Report** toolbar, click the **Archive** button. The system displays the default destination folder. If the report was saved in a different folder, browse the disk, using the scroll-down arrow (bottom of the window) to the report you want to display.

2 - Select the report you want to view. If there is a printer installed, the **Preview** button is enabled. It is used to preview the report before printing it.

NOTE: You must have a printer installed on your computer in order to preview or print reports. To setup a printer, click on Start > Settings > Printers > Add Printer . For more information, consult your system administrator.

3 - Click the **Details** button to display information about the report. If you click the **Details** button, the Report details window appears, displaying information related to the selected report file such as the report file name, title, type, date, etc. The **Workspace as report filter** field indicates whether the report has been filtered according to the requester's workspace restrictions.

4 - Click the **Details** button again to close the Report details window.

5 - Click the **Preview** button to view the report in the system displays the Report preview window.

Previewing Reports

Report

Archive Viewing

1 - From the **Archive** window, select the report you want to view in the right-hand pane. If you select a report generated by Sybase, the Report Options window will display allowing you to customize your report before printing it.

> ***NOTE:*** *If you select a CSV type of report, the report will be generated in a WordPad window, in text format.*

2 - 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.

3 - Click on the **Preview button** , select a **printer** from the drop-down list and click **OK** . The system displays the result of the report. From that window, you can:

- Search text within the report
- Print a report
- Save a report in various formats such as PDF, RTF, HTML and TXT
- Load a report (in a.QRP format)

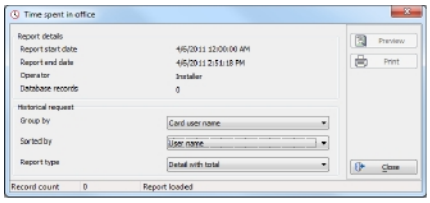
4 - Click **Properties** to access the Reports details window where detailed information is displayed:

- **Report file name** : 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 requested.
- **Delivered** : Displays the date and time at which the report was produced and printed.
- **Requested by** : Displays the name of the operator 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 In/Out Reports

1 - In the Archive window, select the report you want to view. If the selected report was defined as a "Display In/Out Report" and "Sybase Database" as the output format, the following window appears.



2 - Select the display options:

- Group by— Select this option for easier management. The report data may be grouped by card user names or by card numbers.
- Sort by—You may choose a sort order, by user names, or by card numbers.
- Report type—Select this option for easier management. You may choose to include details with or without total.

3 - Click Preview to display the result of the report. From that window, you can save the report (in.QRP format) or print the report.

Card Use Report

The card use report feature is used to create reports that will list cardholders who did, or did not, generate events for 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. 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)
- In/Out events (entry, exit)
- Other events

1 - In the **Card use report** window, select a report from the **Report** drop-down list. If you are creating a new report, click the **New** button in the toolbar, then enter the necessary information in the language section.

2 - 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 granted 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**s and **Access denied events** separately.

3 - 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** tab.

4 - Check the **Allow EntraPass Web Requests** for report requests through the EntraPass Web.

NOTE: The EntraPass Web component must have been registered with the EntraPass Server in order to display the checkbox.

5 - Specify the card use options (**Not used since or Used since**) and defined periods.

6 - To define the target period, click the **From** radio button and select a date. You may select a date in the calendar when you click the **drop-down arrow**. Alternatively, you may use the up/down controls or enter the **number of days back**, starting from today’s date.

7 - When you have finished defining the report, save it. You may request it using the **Report request** button in the **Report** toolbar.

Automatic Report Schedule

Select the **Automatic report schedule** tab to define automatic settings for your reports so they can be automatically generated when needed. Click ***here*** for more details.

Automatic Report Output

Select the **Automatic report output** tab to define automatic output settings for your reports. Click ***here*** for more details.

Custom Reports Definition

The Custom report definition feature allows users to define customized reports with their own automatic execution parameters. Reports that are defined with automatic settings are automatically generated at the specified time. However, they can be requested manually when needed.

Using the Default "All Events" Report

You can generate a default report that will include all events. The default report is an historical report type. EntraPass can send you an automatic report by email.

1 - Under the **Report** toolbar, click the **Custom report** button. The Custom report window appears.

2 - You can only edit the language section for the **All events** report.

Defining a Custom Report

General Parameters

1 - Under the **Report** toolbar, click the **Custom report** button. The Custom report window appears.

2 - To create a new report, click the **New** button (in the toolbar) and enter the necessary information in the language section. To modify an existing report, select it from the **report drop-down list**.

3 - You may **use the default All events** option or select a specific event type from the drop-down list (to select particular events, go to the next section **Events Selection**).

4 - Choose an **Events filter**:

- **Normal and abnormal events**: Select this option to include normal and abnormal events in the report.
- **Normal events**: Quick report can create reports based on normal events. In an access report, normal events would be events such as "access granted".
- **Abnormal events**: 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.

- **Watchable events**: These are preselected events that can be displayed on EntraPass Web Watchlist. It can be used to issue a report of events related to EntraPass Web.

5 - 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** tab.

6 - Check **Bypass operator workspace** to issue a report with no regards to the operator's workspace permissions (see **Creating or Editing an Operator** for more information).

7 - Check the **Allow EntraPass Web Request** for historical report request through the EntraPass Web. The EntraPass Web component must have been registered with the EntraPass Server in order to display the checkbox.

8 - **Origin Filter**: This filter is used to define a report of events coming from one (or more) of the selected sources only. If one or more sources (connection, gateway, site and application) are checked in the **Origin Filter**, an **Origin** tab will be added that will allow user to select one or more components related to selected source

9 - **Component filter**: Select a **Filter mode** for the components to be included. Use the checkbox to display deleted components.

10 - **Specific time frame**: Only events (event time) that are within this specific time frame will be included in your report.

Events Selection

1 - Select an event category from the drop-down list.

2 - Select **All events** or select each event to include in the report individually.

3 - If you have selected **Select all events**, you can also indicate which component status to display (New, Modify or Delete). In reports, events will be precessed by the following signs:

- **+** (New)
- **=** (Modify)
- **-** (Delete)

*NOTE: The checkboxes under **Specific Database Event** are displayed only when a database event is selected.*

*NOTE: The **Events selection** tab contains events based on the selected filters only.*

Origin

From this tab, you can select components from the origin(s) selected in the **General** tab with the **Origin filter**.

Components

If you have selected a **Filter mode**, the **Components** tab will appear **only when the corresponding events are checked**. You must specify the components that may affect the report.

1 - Move to the **Component** tab.

2 - Select a component type to display its items in the right-hand pane. If you select **Card type**, the right-hand pane displays all the card types defined in the system. If you select Doors, all the access system doors are displayed in the right-hand pane.

Cards

1 - In the Custom report window, move to the **Cards** 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. When you do this, the other fields are disabled. When you select the **Use card type as filter** option, you can add filters for your report. You can view the fields that are included/excluded as filters and specify a lower and upper boundaries for each selection.

3 - 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.

4 - Enter the value range in the **Lower/Upper boundary** fields according to the selection in the **Filter mode** field. These may be, for example, alphabet letters (if the filter index is by names; or numeric, if the filter index is by card number). You could, for instance, use the card user name and specify A to F in the **Lower/Upper boundary** as the lower and upper boundaries. As a result the system will include events in which the selected door is defined and events in which the defined card numbers appear but only for card holders whose names begin with A to F.

NOTE: Users can select more than one filter for the same report using the filter index. Events are filtered in times depending on how many filter indexes are defined for the report.

Automatic Report Schedules

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, and once.
- The time period covered .
- The output process: display, print, etc.
- The output type: Sybase, CSV, PDF.
- The language and the file name.

1 - In the Custom report window, move to 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 **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 the system will start executing the report.

4 - Specify the Scheduling parameters:

NOTE: These settings are ignored when the report is requested manually by an operator.

- **Start this many days back**: The report starts collecting events according to the number of days specified in this field. It is based on the present date.
- **Start at this time**: When 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 includes the specified number of days entered in this field. It is based on the present date.
- **Stop at this time**: Once you specify the number of days, specify the ending time (i.e.:5:00 pm), that is, the day on which the system will stop collecting data; you may also specify the time at which it will stop. For example, if you enter 7:00 and an event occurred at 8:00, then this event will not be included. To target events that occurred during a specific time frame, you must 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.*

Automatic Report Output

1 - Enter a **Report Name**. The default report name is YYY_MM_DD-HH_MM_SS, indicating the year_ month_day-hours, minutes_second. This name will also be used as the output file name. The default output directory is `\Users\Public\Documents\EntraPass`.

2 - From the **Database output type** , select the output format of the report. You may choose Sybase, CSV, PDF, Excel, RTF, or text formats by selecting the icon.

3 - From the **Database output process** drop-down list, select the report template. It will be used with the requested report. For details on the output format, see **Defining a Report Output Format**.

NOTE: *From the **Database output process*** drop-down *, you can select **Email custom report** if you want this report to be automatically sent to specified recipients. When you select the **Email custom report** the email options are displayed within the same page. EntraPass enables you to protect the report by a password before emailing it. When the email option is selected, the option to **use any smartlink available** is enabled. This option will use any available SmartLink to send the report email.*

The following table shows the difference between these database formats and their output file formats:

Database.	Description

Database.	Description
SyBase	The EntraPass database.
CSV	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.
Excel	Microsoft Excel file type.
PDF	**Portable Document Format** (**PDF**) is an open standard for document exchange. It can be opened with the free application Adobe Reader.
RTF	The **Rich Text Format** (**RTF**) is a proprietary document file format with published specification for cross-platform document interchange. Most word processors are able to read and write some versions of RTF.
text	A **text file** is a kind of file that is structured as a sequence of lines.Can be opened by a large number of editing tools.

4 - Select the report language.

Defining a Report Output Format

Historical and Card use reports

1 - If you select **Database only** (CSV and Sybase): 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 custom report - Display card last transaction report** (Sybase 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 Reports**.

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 (Sybase 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 (Sybase 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** (Sybase 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.

In/Out Reports

In/Out 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 "Archive" 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): 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 In/Out report (Sybase 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 In/Out Reports**.

4 - Two (2) databases with all data (Sybase): 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 (Sybase): 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 In/Out (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.

- File name—If you wish to overwrite the same report (for example—every week), you can enter a file name here and when the report will be executed according to specifications, the new report will replace the oldest report.

- Destination: this is where the report should be sent/printed automatically. You can also use the Overwrite existing output option to specify a different destination file.

- Report language—This field is used to include additional information in your report. Select from the displayed list.

Defining Automatic Report Schedules

Select 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 (Sybase, CSV, PDF)
- The destination (workstation)
- The language and the file name

1 - 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 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.

2 - Select the **Queue priority** level. A report with a priority of 1 will be processed before a report with a priority of 99.

3 - In the **Start report** field, enter the time at which the system will start executing the report.

4 - Specify the **Scheduling parameters**.

NOTE: These settings are ignored when the report is requested manually by an operator.

- **Start this many days back**: The report will start collecting events according to the number of days specified in this field. It is based on the present date.
- **Start at this time**: Once you specify the amount of days, specify the starting time (i.e.: 7:00am). For example, if you enter 7:00, events that occurred at 6:00 will not be included in the report.
- **Stop this many days back**: The report will include the specified number of days entered in this field. It is based on the present date.
- **Stop at this time**: Once you specify the number of days, specify the ending time (i.e.:5:00 pm), that is, the day on which the system will stop collecting data; you may also specify the time at which it will stop. For example, if you enter 7:00 and an event occurred at 8:00, then this event will not be included. To target events that occurred during a specific time frame, you have to use the Specific time frame option.

NOTE: The start and end time are only used for the first day and last day, for example if you start collecting events on Monday at 8:00 and end on Friday at 17:00 all events between 8:00 Monday and 17:00 Friday will be included. The system does not use the start and end time for each day but for the whole period.

Specifying Additional Options for an Automatic Report

1 - Click the **More** button to add more settings to the automatic scheduled report. When you click the **More** button, the **Automatic report output definition** window appears.

2 - From the **Database output type** drop-down list, select the output format of the report. You may choose Sybase, CSV, PDF, Excel, RTF, or text formats.

3 - Select the output process from the **Database output process** drop-down.

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
SyBase	The EntraPass database.
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.
Excel	Microsoft Excel file type.
PDF	**Portable Document Format** (**PDF**) is an open standard for document exchange. It can be opened with the free application Adobe Reader.
RTF	The **Rich Text Format** (**RTF**) is a proprietary document file format with published specification for cross-platform document interchange. Most word processors are able to read and write some versions of RTF.
text	A **text file** is a kind of file that is structured as a sequence of lines. Can be opened by a large number of editing tools.

4 - You may check the **Automatic file name (...)** option. The default file name is YYY_MM_DD-HH_MM_SS.X, indicating the year_ month_ day-hours, minutes_second.file extension.

5 - Select the report language. Please refer to **System Language Selection** for more information about the available languages.

6 - Select a destination.

In/Out Reports Definition

This feature is used to define customized In/Out 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 "In/Out report request" button. When requested manually, automatic settings are ignored .

Defining In/Out Reports

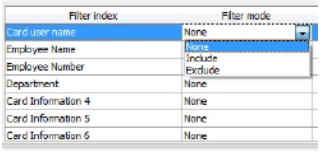
1 - Under the **Report** toolbar, click the **In/Out Report** button.

2 - If you select the **Doors** option, only the doors defined as "In/Out" doors (in the Door definition menu) are displayed. Check the **View deleted doors** to add deleted doors to the list. When you select the **Door group** option, the **View deleted doors** option is disabled. The system displays the door groups of your system; then you may select one.

3 - Check the **Overwrite existing output file** option if you want the system to replace the existing file. If you leave this option unchecked, the system will create another output file.

4 - Select **Display Hours and Minutes** to add them to the report.

5 - Select the **Card** tab to add other filters for the report.



*NOTE: The **Card type** tab appears when the Use card type as filter box is checked.*

6 - Select a filter index, then select a filter mode (**None** , **Include** , **Exclude**). If you have selected a filter index, select the filter mode and enter the value range in the **Upper/Lower boundary** fields. To include all the fields, leave the filter mode to **None** . For example, if you select Card number as the Filter index, leave the filter mode to **None** so that all events triggered by cards will appear in the report.

7 - To add information in the sort criteria, select an item from the **Additional information** drop-down list.

NOTE: Repeat these steps for all the card information fields that are listed in the filter index field. You could use the card user name and specify A to F in the Upper/Lower boundary fields for the system to include events in which the defined card numbers appear but only for card users whose names begin with A to F (G and up will not be included even if the card number is included in the range).

8 - Select the **Card type** tab if it is displayed, then specify the Card types that will be included in the report. This tab appears if you have checked the **Use card type filter** option.

9 - Select the **Automatic report schedule** tab to specify information for automatic reports. For details, see Defining Automatic Report Schedules.

10 - Select the **Automatic report output** tab to define automatic output settings for your reports. Click ***here*** for more details.

11 - Select the **Rules** tab to define the rules of In/Out 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.

- Select the **Keep only the first entry (first IN) and the last exit (last OUT)** option to get the time lapsed between the first reading of the card on an entry reader and the last reading of the card on an exit reader.

In/Out Reports Request

The Request In/Out reports feature is used to request the pre-defined In/Out reports that were created using the In/Out 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.

Requesting a In/Out Report Manually

1 - Under the **Report** toolbar, click the **In/Out Request** button. The In/Out Request report window appears.

2 - From the **Report list** display pane, select the In/Out report that you want to execute.

3 - Specify **Date and time** as well as the **Output parameters** .

4 - Select the **Queue priority** level. A report with a priority of 1 will be processed before a report with a priority of 99.

5 - Click **Execute** to trigger the report.

*NOTE: For the Sybase output type, the system displays a report preview window. For other output formats, you will have to retrieve the report manually since it is not printed or displayed. To view all the reports that have been generated, use the Archive button in the Report toolbar. For details on reports output formats, see **Defining a Report Output Format**.*

Operations on In/Out

Use the Operation on In/Out feature to manually insert, add or delete In/Out transactions in the database. This feature is useful for an organization using the In/Out feature for the payroll system, for instance.

Adding a Transaction in the In/Out Database

1 - Under the **Report** toolbar, click the **In/Out Adjustment** button.

2 - Enter the **Card number** for which you want to modify the In/Out transactions, then click the **Load** button. If you do not know the number, use the **Find** button.

NOTE: The card number field is mandatory to start loading.

3 - Select the **View deleted transactions** option if you want to view the transactions that were previously deleted. Deleted transactions are marked with an "X" in the **Delete** column.

4 - Check the **Find deleted cards** option if you want to find the deleted cards. This does not apply to entries that were added manually.

5 - Specify the **Start date** , the day on which the system will start to collect the events, by clicking the **Calendar** button 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 **Connection** drop-down list, select the appropriate connectionto view the In/Out 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 In/Out events that were generated for the selected doors will be displayed.

9 - Check the View deleted doors option so that even doors that are no longer defined as In/Out doors (but that have been defined as In/Out) will be displayed.

NOTE: Doors are mandatory to start loading.

10 - Enter the necessary information in the transaction table. The transaction table displays the transactions for the selected cardholder:

- The **Delete** column indicates transactions that have been deleted (if the **View deleted transactions** option is checked). These are identified by an X.
- The **Date** column indicates the date on which the transaction occurred. Use this field to specify the date when you manually insert a new transaction.
- The **Time** column indicates the time at which the cardholder entered or exited an area. Use this field to specify the time (entry or exit) when manually inserting a new transaction.
- The **Transaction** column indicates the transaction type. For every entry transaction, there should be an exit transaction.
  - **Entry** —indicates that this is an entry transaction generated when a cardholder presented his/her card at a door defined as entry.
  - **Exit** —Indicates that this is an exit transaction generated when a cardholder presented his/her card at a door defined as “Exit”.
  - **Manual entry** —Indicates that this is an entry transaction that was manually inserted or added in the system. When you manually insert a transaction, you have to specify if this transaction is an “Entry” transaction or an exit transaction. For every entry, there should be an exit.
  - **Manual exit** —Indicates that this is an “exit” transaction that was manually inserted or added in the system. When you manually insert a transaction, you have to specify if this transaction is an entry transaction or an exit transaction. For every entry, there should be an exit.
- The **Door** column indicates which door was accessed by this user. When you manually insert a transaction, you have to specify the door according to the transaction type (Entry or Exit).

NOTE: If you are inserting an entry transaction, only doors defined as "Entry doors" will be displayed in the list. If your are inserting an exit transaction, only doors defined as "Exit doors" will be displayed in the list.

11 - Click the **Load** button to load the transactions from the server for this cardholder. You have to enter the card number, select the gateway/connection and door(s), then click the **Load** button. The button is disabled once you have loaded the transactions.

12 - Click the **Add** button to add a transaction to the existing transaction list. The new transaction will be added at the end of the list.

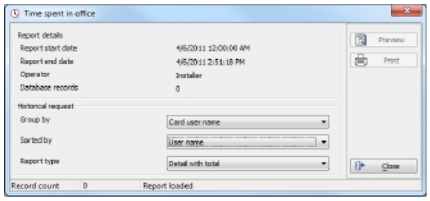
13 - Use the **Insert** button to insert a transaction between existing transactions or above any transaction.

14 - Click **Cancel** to cancel any insertion or modification that was made BEFORE saving.

NOTE: When you delete a transaction that was added manually, it is permanently deleted from the list; as opposed to transactions that were generated by controllers. When they are deleted, they are identified by an X in the Deleted column.

Previewing In/Out Reports

1 - In the Archive window, select the report you want to view. If the selected report was defined as a "Display In/Out Report" and "Sybase Database" as the output format, the following window appears.



2 - Select the display options:

- Group by— Select this option for easier management. The report data may be grouped by card user names or by card numbers.
- Sort by—You may choose a sort order, by user names, or by card numbers.
- Report type—Select this option for easier management. You may choose to include details with or without total.

3 - Click Preview to display the result of the report. From that window, you can save the report (in.QRP format) or print the report.

Previewing Reports

1 - From the **Archive** window, select the report you want to view in the right-hand pane. If you select a report generated by Sybase, the Report Options window will display allowing you to customize your report before printing it.

NOTE: *If you select a CSV type of report, the report will be generated in a WordPad window, in text format.*

2 - 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.

3 - Click on the **Preview button** , select a **printer** from the drop-down list and click **OK** . The system displays the result of the report. From that window, you can:

- Search text within the report
- Print a report
- Save a report in various formats such as PDF, RTF, HTML and TXT
- Load a report (in a.QRP format)

4 - Click **Properties** to access the Reports details window where detailed information is displayed:

- **Report file name** : 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 requested.
- **Delivered** : Displays the date and time at which the report was produced and printed.
- **Requested by** : Displays the name of the operator 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.

Quick Report Definition

Use the Quick report to quickly create reports for certain types of events. For example, you can 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.

Defining a Quick Report

1 - Under the **Report** toolbar, click the **Quick report request** button.

2 - From the **Event** drop-down list, select the event type for the current report (access, controller, door, relay, input, operator, manual operation events, and so on). If you have selected “access events”, the **Card** tab appears in the window.

3 - Among the **Event type** options, select the event type to be included in the report.

- **Normal and abnormal**—Select this option to include normal and abnormal events in the report.
- **Normal** —Use Quick report to 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.

- **Watchable events**—These are preselected events that can be displayed on EntraPass Web Watchlist. Use to issue a report of events related to EntraPass Web.

- **Custom events**—Select this option to include your own events. The **Custom** events become visible when the **Custom events** option is selected. This option allows the operator to select the components that have generated the selected events according to the setting in the "event" field.

NOTE: When you use the Event field, you have to specify which component(s) should be used or not used. When 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, that is the list of controllers to be included in the report.

4 - If **All Events** has been selected, **Specific Database Event** is displayed. You can choose to include **New (+)**, **Modify(=)**, and **Delete(-)** database events in the quick report.

5 - Select the **Card** tab to specify filter details about the report. The **Card** tab appears only if a card-related event is selected.

6 - In the **Card index** drop-down list, specify the information that will be used as the filter. For example, if you select "card number", only access events in which the defined card numbers appear will be selected.

NOTE: If you select Card number, the Lower and Upper boundary editable fields display the default numerical values to be replaced by card numbers. If you select Card user name , these fields are enabled to receive text data. For example, you can enter A in the Lower boundary field and F in the Upper boundary fields for the system to include events in which the selected door is defined and events in which the defined card numbers appear but only for card users whose names begin with A to F. If you select All , the editable fields are disabled.

7 - In the **Start/end date** field, enter the date and time on which the system will start to collect the events. For example, if you enter 7:00 and an event occurred at 6:00, this event will not be included. To target events that occurred during a specific time frame, use the **Time frame** field.

8 - In the **Time frame** field, check the Specific time frame option to include events that match the specified time frame. Enter the target time for the report.

9 - Define the output parameters:

- **Database output type** : Select the database output format by selecting the icon for Sybase, CSV, PDF, Excel, RTF, or text.

- **Report name** : The default is the current date and time. This can be edited.
  The report name is used to name to output file.
- Database output process —Select the appropriate output processes. A report template is associated with each output.
  - **Database only** : The report will be saved in the system database.
  - **Display (custom, detailed, summary or statistics) report:** The report appears on-screen.
  - **Report printed by (sequence, date & time or event)** : The report is printed according to the specified sort order.
  - **Email (custom, detailed, summary or statistics) report**: When email is selected a dedicated input box is launched to select which emails the report is sent to.

10 - Click on the **Execute** button to launch the report.

Report Log

The **Report Log** window allows you to view a detailed list of all history reports processed by the system.

1 - To view the Report log, select the Report **Log** button from the **Report** menu.

2 - Click the **Text filter** button to display the Text filter window. From that window, 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.

3 - Click the **Refresh** button to update the displayed data.

4 - Columns:

- **Date requested** : This is the normal incoming sequence, if you select another sorting mode, you interrupt the normal sequence.
- **Requested by** : When selected, all columns will be sorted according to the **Requested by** column in alphabetical order.

- **Report name** : When selected, all columns will be sorted according to the **Report name** column in alphabetical order.
- **Date from** : When selected, all columns will be sorted according to the **Date from** column in alphabetical order.
- **To (Date)** : When selected, all columns will be sorted according to the **To (Date)** column in alphabetical order.

5 - You may also clear the window. To do this, right-click in the window, then select **Delete All** from the shortcut menu.

6 - Fields:

- **Report Type** : Show the type of report (quick, custom…).
- **Process By** : Show which application executed the report.
- **Workspace applied** : Show whether a workspace was applied.
- **Destination** : Where the report was delivered.
- **Used Template** : Show the dll that was used for the report.
- **Items in report** : The number of items in the report.
- **Requested date** : When the report was requested (date and time).
- **Queued date** : Show when the report was added to the application queue that generated the report (Date and time and the total time elapsed).
- **Process date** : When the process was started (Date and time and the total time elapsed).
- **Delivery date** : Show when the report was delivered to destination (Date and time and the total time elapsed).
- **Completion date** : Show end date and time of report execution.
- **Completion State** : Show whether the report was completed successfully or aborted.

Report State

Use the **Report state** feature to display a list as well as the status of all requested reports that are still pending. From the **Report** tool bar, click on the **Report state** button:

Report state fields:

- **Priority** : Priority level for the treatment of messages (1 to 99). A a priority of 1 will be processed before a priority of 99.

- **CPU** : Level of CPU usage to be allowed to process the report (Lower, Normal, Higher).

- **Report** : Name of the report in process.
- **Destination** : Displays the workstation or SmartLink name to which the report will be sent to.
- **Progress** : When the report is processed, it displays the date in treatment, from the start to the end.
- **Count** : Indicate the number of records in the report.

Select a report then right click on it to display the contextual menu:

- **Next to be processed** : Indicates that this is the next report to proceed.
- **Promote** : Increases the priority level (above the next lower priority report).
- **CPU** : Allows you to change the CPU usage for the treatment of reports (Lower, Normal, Higher).
- **Help** : Click to see the related help topic.

Contextual menu for in process reports:

Select a report then right click on it to display the contextual menu:

- **Abort with data** : This function ends the process and the gathered informations are sent to the recipient.
- **Abort without data** : This function ends the process and the gathered informations are erased.
- **Priority** : Allows you to change the CPU usage for the treatment of reports (Lower, Normal, Higher).
- **Help** : Click to see the related help topic.

NOTE: A red dot indicates a pending report In/Out. A green one, a report in process.

Requesting Reports

With this feature operators can request pre-defined historical reports or Card use reports that were created using the Custom Report menu. Operators can also email the report to one or multiple recipients.

NOTE: If your report contain automatic settings, these will be ignored. You must indicate new settings.

1 - Under the **Report** toolbar, click the **Report Request** button. The Report request window appears.

2 - From one of the **report list** display pane (Custom reports on top or Card Use reports on bottom), select the report that you want to execute.

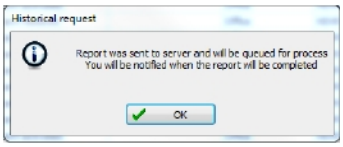
3 - Select the **Queue priority** level. A report with a priority of 1 will be processed before a report with a priority of 99.

4 - You may define **output parameters**, including the **database output type** format (Sybase, CSV, PDF, Excel, RTF or Text), the target folder, the output file name, etc. For more information on how to select an output format, see **Defining a Report Output Format**.

*NOTE: From the **Database output process**drop-down , you can select Email custom report if you want this report to be automatically sent to specified recipients. If you choose this option, t he email page is launched. EntraPass enables you to protect the report by a password before emailing it.*

NOTE: If a Card use report is selected, the "Date and time" section is disabled.

5 - Click **Execute** . A system message informs you that the report is being processed. The Report options window appears and is then minimized to the task bar.



6 - 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 colours, framing events, buttons in the reports, etc., or by sorting events in the report (by event ID number, alphabetical order or date and time).

7 - Enter the **description** in the **Search description** field. The report is updated in real-time when you enter a filter option.

8 - You may use **Preview** to preview the report or the **Properties** button to view details about the report. When you click the **Preview** button, the system will display the result of the report. From that window, you can save the report in various formats or print the report.

Roll Call Reports

The Roll call report is used to take a snapshot of who has swiped a card at a reader or a group of readers within a certain reset period. With the Roll call, one or many doors in EntraPass may be configured as entry points for a certain perimeter and upon criteria later defined in this document. Based on the last location a card holder has passed, operators will receive reports on who has entered this perimeter.

The roll call report is handled by the EntraPass Server. In order to operate properly, the server and the gateway must be running. This allows an accurate reading of the card holder location and for the system to react on a triggered input. The EntraPass Global, the Corporate Server and the Workstation may run as services on Windows. The Roll Call functionality is available in both application and services.

Functionalities

- A maximum of 8 roll call reports can be configured through EntraPass.
- Doors must be assigned to a report number (1-8) in order to be considered for the roll call report (see **Doors Configuration** *for more information*).
- At runtime, the Roll call report will list all individuals that have swiped a card at a pre-defined reader. No other card holder will be shown in the report than the ones who have entered a perimeter after the last perimeter reset.
- To create an “in-out” functionality, the operator must make sure that doors considered “out” of a building or connection have a different roll call number. Any door that doesn’t have a number assigned to it will have no effect on the location of the card holder for the roll call report.
- A configurable reset of the report is available and the default value is 12:00PM (midnight) every day. This function cleans the report. Reset can be performed for all reports in the roll call report window.
- Upon manual request in Report –> Roll Call Report or on trigger of a pre-configured input, a report can be generated up to 3 times to a pre-defined printer, workstation or email address.

Roll Call Report generation

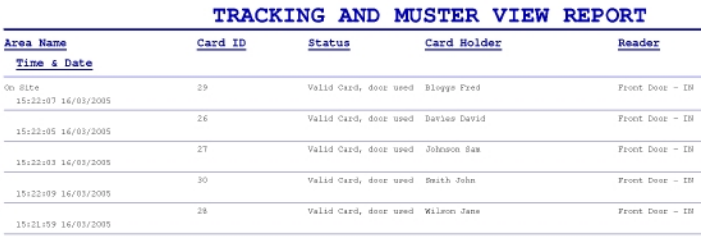
1 - Under the **Report** toolbar, click the **Roll call report** button:

2 - Select the roll call sector. If the roll call sector you wish to select is not listed, click on the button next to the drop-down arrow.

3 - Specify the report destinations:

- **Report Destination** : Select a destination using the three-dots button.
- **Output printer** : Select the printer (s) from the list.
- **E-mail recipient** : Enter the name (s) of the recipient (s) to email the report to.

Example of a Roll Call Report



TRACKING AND MUSTER VIEW REPORT

Area Name	Card ID	Status	Card Holder	Reader	Time & Date
On Site	29	Valid Card, door used	Bloggs Fred	Front Door - IN	15:22:07 16/03/2005
	26	Valid Card, door used	Davies David	Front Door - IN	15:22:05 16/03/2005
	27	Valid Card, door used	Johnson Sam	Front Door - IN	15:22:03 16/03/2005
	30	Valid Card, door used	Smith John	Front Door - IN	15:22:09 16/03/2005
	28	Valid Card, door used	Wilson Jane	Front Door - IN	15:21:59 16/03/2005

Specifying Additional Options for an Automatic Report

1 - Click the

button to add more settings to the automatic scheduled report. When you click this button, the **Automatic report output definition window** appears.

2 - From the **Database output type** drop-down list, select the output format of the report. You may choose Sybase, CSV, PDF, Excel, RTF or text formats.

3 - From the **Database output process** drop-down list, select the report template. It will be used with the requested report. For details on the output format, see **Defining a Report Output Format**.

*NOTE: From the **Database output process**drop-down , you can select Email custom report if you want this report to be automatically sent to specified recipients. If you choose this option, select the Email tab to enter the recipients' email address in the Send Email to field. EntraPass enables you to protect the report by a password before emailing it.*

The following table shows the difference between these database formats and their output file formats:

Database	Description
SyBase	The EntraPass database.
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.
Excel	Microsoft Excel file type.
PDF	**Portable Document Format** (**PDF**) is an open standard for document exchange. It can be opened with the free application Adobe Reader.
RTF	The **Rich Text Format** (**RTF**) is a proprietary document file format with published specification for cross-platform document interchange. Most word processors are able to read and write some versions of RTF.
text	A **text file** is a kind of file that is structured as a sequence of lines. Can be opened by a large number of editing tools.

4 - You may check the **Automatic file name (...)** option. The default file name is YYY_MM_DD-HH_MM_SS.X, indicating the year_ month_ day-hours, minutes_second.file extension.

5 - Select the report language and the destination.

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 Server application 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
  - the Mirror Database application, or
  - other third party software and hardware (the third party software is not recommended).

NOTE: *By default, when you backup or restore files, the Server databases will temporarily be disabled (not available). The Workstation s will not be able to modify the databases.*

The Backup Scheduler program is used to schedule automatic backups of your data, archives, and In/Out databases. Define the default settings and the system will do the rest.

Configuring the Backup when the EntraPass Server is Running as a Service

These steps are required when the EntraPass Server is running as a service and you must backup to another computer **within the same workgroup or domain**.

NOTE: You must have full administrator privileges to perform the following steps at the EntraPass Server. Please refer to the network administrator, if you don't have the privileges or you are not familiar with Windows Administrative Tools.

1 - From the EntraPass Server, go to Options > System Parameters > Server > Service Login Information.

2 - Fill-in all the mandatory fields: Domain name, Login name, Password and Password Confirmation.

NOTE: The Domain Name or the Workgroup must be the same for both, the EntraPass Server and the backup computer.

3 - Click OK.

Scheduling Automatic Backups of the System Database

1 - From the Options toolbar, select the Backup Scheduler button.

2 - Select the tab corresponding to the information you want to backup: Data, Archive, In/Out or Video event (In/Out).

NOTE: By default, the system will automatically backup your files every Sunday at 4:00 AM for all new installations. Setting this feature at 4:00AM has an added benefit of not interfering with the system processing time or other tasks scheduled around midnight.

3 - Select the **Automatic backup** option to enable the options displayed in the window. 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 In/Out (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:\Program files\Kantech\Server\Data or Archive or Time on video or V . 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.

- Under the **Data** tab only:
  - **Separate files** : will backup the databases one by one.
- Under the **Archive, In/Out** and **Video Event** tabs only:
  - **Separate files (full backup)** : will backup all databases.
  - **Separate files (incremental)** : will backup all databases. Only the information that was modified since the last backup will be saved.

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.

7 - Enter the time at which the backup will start (24:00 format).

8 - Select **Now** if you want to perform a backup immediately after saving the backup parameters.

*NOTE: This is not applicable to the **Configure Automatic backup** feature in the **Mirror Database and Redundant Server** application.*

9 - Repeat steps 1 to 8 for all the remaining tabs.

10 - Click **OK** to save.

Connection Password Modification

The connection password is used to authenticate EntraPass Workstations to the EntraPass Server. The connection password window is automatically displayed when the system has not yet been registered.

CAUTION:
Keep in mind that there is no way to reset the connection password if forgotten after its modification.

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 connection password is kantech, in lower case. Passwords are case sensitive.*

Changing the Connection Password

1 - From the **Options** main window, select the **Connection password** button.

2 - Enter the current connection password (case sensitive) in the **Old authentication password** field. The default authentication password is kantech, in lower case.

3 - Enter the new authentication password in **New authentication password** field (case sensitive).

4 - Enter the new authentication password in the **Verify authentication password** for confirmation. This field will verify that the new connection 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 authentication password** and in the **Verify authentication password** fields are identical (case sensitive).

NOTE: *The connection password is different from the operator password. The connection password is used to authenticate workstations, whereas the operator password is used to open a session.*

Credentials Parameters

Card

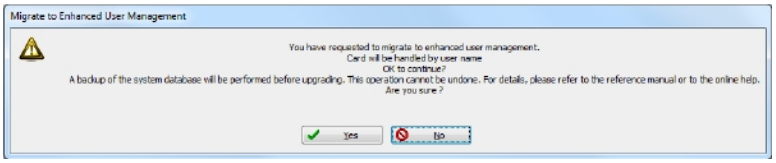
Under the **Card** tab, System Administrators will be able to migrate their EntraPass system to enhanced user management where users are managed by their user name as well as their card number (s) . Each card holder will be handled by user name and have up to 5 different numbers . This will allow for creating cards without assigning card number to the new cards, *see* **Issuing a New Card in Enhanced User Management Environment**

NOTE: *This option will be used with the EntraPass Web for card management.*

NOTE: *Enabling the migrate to enhanced user management is NOT REVERSIBLE through the software . However, when the system is migrating data, a backup is performed in EntraPass, so this can be restored to return to its previous action.*

- **Migrate to enhanced user management**: when checked, EntraPass will migrate to the enhanced user management *(see **Issuing a New Card in Enhanced User Management Environment** for more details)*.

After checking the box and clicking **OK**, a warning will popup on screen indicating that the action is irreversible before EntraPass performs a backup of your data.



Once the process has been completed, you will notice that the option is greyed out under the **Card** tab.

Enable access level exceptions: When checked, access level exceptions can be enabled by user for each door. On activation, the user will receive a warning message indicating that the controller reload process might slow down (to see how to link a specific schedule to a door, please refer to **Access Exception**).

Custom Messages

The Custom Messages option allows operators with proper security rights to define custom messages that can generate an event based on a schedule. Up to 10 custom messages can be programmed to trigger an

event at a preset time. And each custom message can be triggered when the schedule becomes valid, invalid, or both. In other words, you can trigger up to 20 custom events if you take into account the start and/or end of a schedule interval. Each custom events will be displayed in the Messages List on the Desktops.

Setting up Custom Messages

1 - From the **Options** toolbar, click **Custom Messages** .

2 - In the first tab, enter the first custom message you want to see display in the Messages List. Two fields are available for primary and secondary languages.

3 - Select a preset schedule that will determine when the custom event will be triggered.

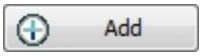
4 - Select if you want the custom event to be triggered when the schedule becomes **Valid** or **Invalid** , or both.

5 - Move to the second tab to enter a second custom message, and so on.

Dealer Information

About Box Details

To add dealer information in the **About** window, select **Display details in About box**.

1 - Fill the dealer information and add a picture logo if needed using the 

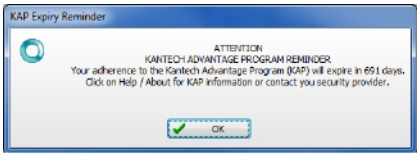
button.

2 - Fill the **Site information** data..

3 - Click **OK** once finished.

Kap Reminder

A message will be displayed reminding the user that the KAP period is ending. There are two different notifications: a pop-up on the screen or an email containing the following information:



Pop-up Message

A pop-up message is automatically generated by EntraPass to advise the user that his KAP is expiring:

- 60 days before expiration
- 30 days before expiration
- On expiration
- 30 days past expiration

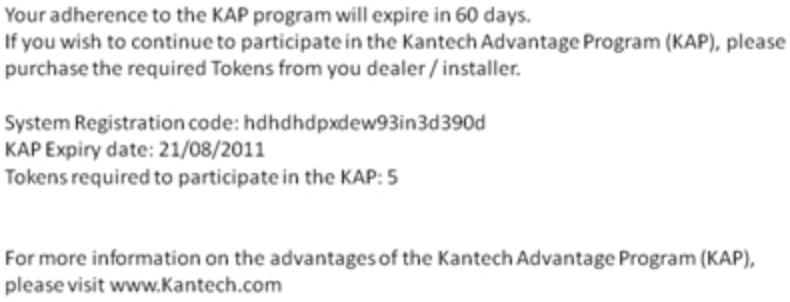
The reminder message has to be acknowledged by the user. It will be logged in the events database (displayed in the Message List) and will appear in reports.

Email

The Dealer Information window has been modified in order to configure the email reminder. Up to 4 recipients can be added. Clicking the Send reminder now button will save the information and send a reminder immediately.

A new event will also be logged in the desktop events list.

Each workstation will also receive a 60 second notification popup message.


Your adherence to the KAP program will expire in 60 days.
If you wish to continue to participate in the Kantech Advantage Program (KAP), please purchase the required Tokens from you dealer / installer.

System Registration code: hdhdhdpxdew93in3d390d
KAP Expiry date: 21/08/2011
Tokens required to participate in the KAP: 5

For more information on the advantages of the Kantech Advantage Program (KAP), please visit www.Kantech.com

NOTE: *The Kap Reminder feature can also be accessed from the About window.*

Defining a Card Display Format

The EntraPass system can accommodate various reader types. Depending on the reader type, the card display format may vary. The Display format dialog allows you to select the default format that is setup automatically when creating a new card.

1 - Under the **Options** toolbar, click the **Display format** button.

2 - From the **Card** list, s elect a display format for **Card #1** .

- **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.
- **FIPS** (Federal Information Processing Standard): This card format can use more than 32 bits of data.

3 - Check the **Use multiple card format** box if your environment contains multiple reader types and you would like to have the capability to select a different reader, that is not the default reader, when creating a new card.

4 - Select one of the **Duplicate PIN process** in the scrolling box. This feature can be used for example while loading cards in a batch. An operator may decide to set the PIN option to allow duplication. Later, if desired, the duplicate PINs can be changed to prevent confusion.

- **No duplication** : An error appears on the workstation; the PIN field will be reset to the default value (00000) and will be highlighted, inviting you to enter a new and valid PIN. Only PIN 00000 will be duplicated regardless of the PIN setting option.
- **Notify when duplication:** the server verifies if this PIN already exists. If the PIN exists, a message box appears, indicating that the PIN exists. A **Details** button will allow operators to view a list of cardholders who were issued this PIN.

- **Duplication:** no test will be processed, the PIN will be accepted even if it is a duplicate.

5 - **Number of PIN digits (KT-400 only):** This function allows using the **Keypad Pin Digit** option with the new KT400 firmware. You can choose to have 4, 5 or 6 digits (see **Card Options Definition** for more information).

NOTE: The PIN number must be set up once and kept that way in order to avoid any in duplication if truncated or filled by the system.

6 - When the Enhanced User Management option has been chosen, select an alternate default display format for **Card #2** . Repeat **Step 6** for **Card #3** , **Card #4** and **Card #5** .

7 - Under the Global display format for **KT-100** , **KT-300** and **KT-400** , select the appropriate option to coordinate with the selection in the upper section of the dialog.

- **24-bit Wiegand card, 5-digit PIN (KT-200 default)** : for up to 24-bit for KT-100, KT-200, KT-300 and KT-400.
- **32-bit card, 5-digit PIN** : for up to 32-bit for KT-100, KT-300 and KT-400.
- **24-bit Wiegand card, 6-digit PIN** : for up to 24-bit for KT-100, KT-300 and KT-400.
- **Up to 16 characters ABA card** , **6-digit PIN** : for up to 16 for KT-100, KT-300 and KT-400.

NOTE: KT-100, KT-300, and KT-400 controllers will do a hard reset on card format change. Avoid alternating between different card formats because this may result in lost card information.

Changing from a 24-bit to 32-bit Global Card Format

Changing from 24-bit to 32-bit global card format extends the amount of cards you can configure on EntraPass.

The ioProx 26-bit Wiegand reader does not support changing from a 24-bit to 32-bit global card format. If you have a combination of ioProx XSF and ioProx 26-bit Wiegand readers, do not manually change the format, or turn on the auto conversion feature. You first have to replace the 26-bit Wiegand readers with XSF readers.

To manually change from a 24-bit to 32-bit global card format, complete the following steps:

1 - Click the **Options** tab, and select **Display format** from the menu.

2 - In the **Global card format** area, choose the **32-bit card, 5-digit PIN** option.

3 - Click **OK**. If you made a change from a 24-bit Wiegand card, five or six digits, to a 32-bit card, five digit PIN, a prompt displays to ask if you require the cards converted to 32-bit family code.

- If you click **Yes**, enter the value of the extended facility code.
- If you click **No**, a prompt displays to enable the **Auto conversion** feature.

> ***NOTE:*** *The ability to change the global card format from 24-bit to 32-bit format is not available when running from a redundant server.*
> *EntraPass does not automatically backup data when you switch from 24-bit to 32-bit card format.*

In the workstation, EntraPass backs up the system prior to conversion.

After you change formats, the KT-100, KT-200, and KT-300 automatically do a hard reset. For the KT-1 and KT-400 the change is seamless.

Auto conversion

When you select the **Use Auto Conversion for legacy 24 bit cards** check box in the **Display Format** window, EntraPass automatically converts all cards to a 32-bit card format. The default value is cleared. To enable the check box, you must set the **Global Card Format** to the **32-bit card, 5 digit PIN** option.

When you select the auto conversion feature, and have not converted the cards to a 32-bit format, the system automatically modifies the card number and triggers a **Card definition modified** event. The events have to be non-fail soft events. The feature is available in the multi-site gateway, the global gateway, and the KT-NCC gateway.

> ***NOTE:*** *The Auto conversion feature is available when running the redundant server.*

Event Color and Priority

You can change the color and priority of any event.

1 - Under the **Options** toolbar, click on the **Event color and priority** button.

2 - Use the **Text filter** to search for events.

3 - Choose a custom **Color** and **Priority** level for an event. 0 is the highest priority and 9 is the lowest.

4 - Select **Abnormal** to make the event an abnormal event. Events such 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. This is later used in generating reports.

5 - Select **Watchable** to make the event watchable. These are preselected events that can be displayed on EntraPass Web Watchlist. It can be used to issue a report of events related to EntraPass Web.

Integration

The **Integration** tab allows the user to select third party hardware that has been integrated to EntraPass by Kantech.

- **DLL registration**: The available DLL in this menu will be used to specify which type of hardware the customer will connect to EntraPass.
    - Click on **Add** to integrate another DLL. For additional details, see Integrated Panel Configuration.

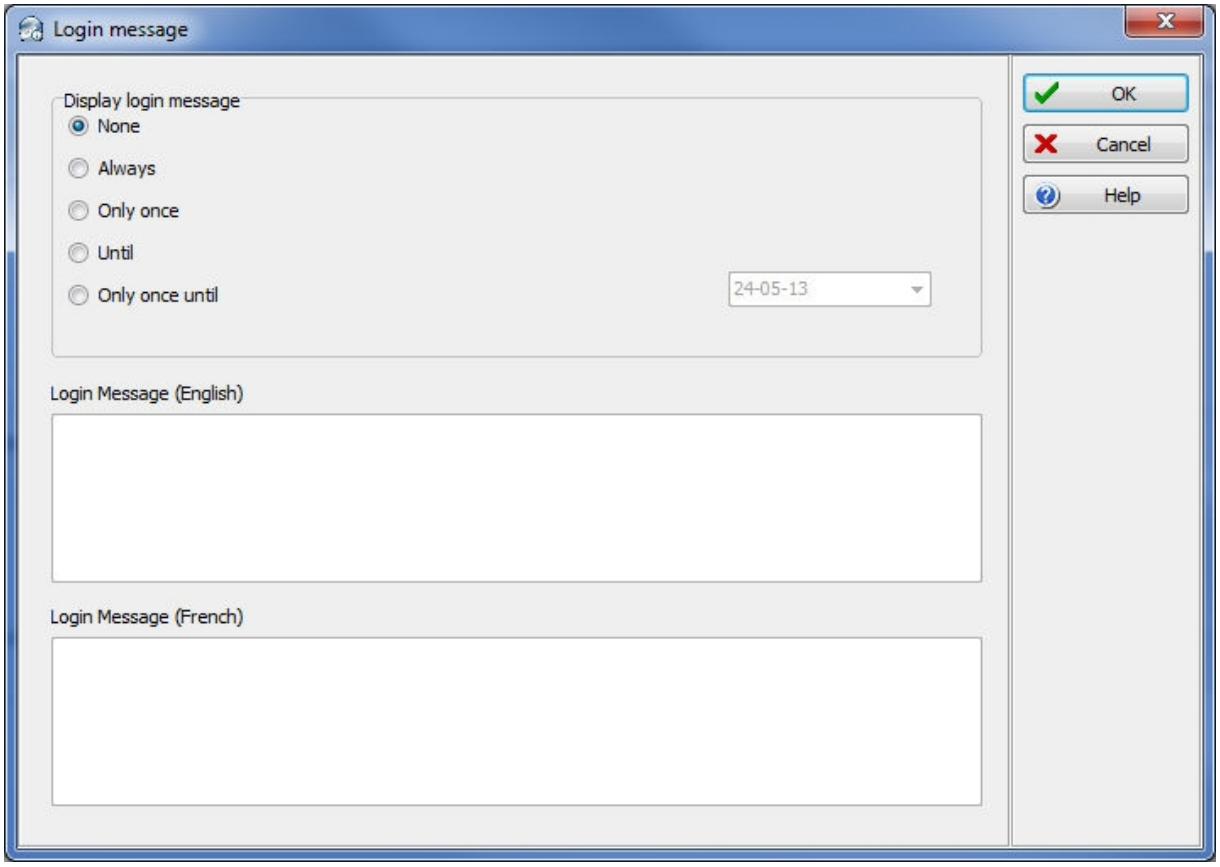
*NOTE: The DLL integration **must be done at the EntraPass Server** in order to communicate with the Multi-site Gateway where the third party hardware is physically connected and powered up.*

- **Virtual keypad**: The **Virtual keypad** tab allows the user to customize the virtual keypad screen display. Three different display modes can be selected: **Floating**, **Modal** or **Stay on top**.

Login Messages

This feature allows entering a text message that will be displayed to other operators when they log into any workstation.

1 - From the **Options** menu, select **Login message**:



2 - Set the recurrence:

- **None**.
- **Always**: The message will always pop-up after login.
- **Only once**: The message will be displayed only once for each operator.
- **Until**: The message will be displayed until the selected date is reached.
- **Only once until**: The message will be displayed once until the selected date is reached or until the operator got the message.

3 - Type a message in the boxes on the right (primary and secondary languages).

4 - Click the **OK** button.

Login/Email message display example:

Personalize the welcome e-mail message that EntraPass, and EntraPass go Pass sends to users and operators. Type a subject heading and choose to type your message in the primary or secondary operator language, or both languages. Complete the following steps:

1 - To write a message that operators see when they log in to any workstation, click the **Login/Email message** icon, and click the **Login message** tab.
2 - To write a welcome message for new EntraPass users, click the **Welcome message** tab.
3 - To write a welcome message for EntraPass go Pass users, click the **go Pass message** tab.
4 - To write a message to a user to explain why EntraPass is disabling their account, click the **Operator disable message** tab.

Multimedia Devices Configuration

The Multimedia devices utility allows you to set up your system multimedia objects:

- Alarm sound
- Video capture devices
- Signature capture devices
- Video feature devices

Selecting an Alarm Sound

1 - From the Options main window, select the **Multimedia devices** button.

2 - Check the **Assign alarm sound** option if you want an alarm sound notification.

3 - Select a sound from the displayed list.

4 - Select a **Priority** level for the selected sound so that it is played when an alarm defined with this priority is sounded.

NOTE: The Priority level refers to the order in which alarm messages are displayed in the Alarm desktop. In EntraPass, O is associated with the highest priority, and 9 to the lowest. For more information, see Options > Event color and priority.

5 - Click the **Play** button to listen to the selected sound. The system will play the selected sound.

6 - Click the **Add** button to add a new sound from your personal files. Clicking on this button displays a new window allowing you to add new alarm sounds.

*NOTE: The **Current** selection section displays the sound currently selected (in use). You can adjust the delay of the alarm sound in the Delay field.*

Defining Video Options

1 - From the Multimedia devices window, select the **Video capture** tab.

2 - Check the **Enable video capture** box to enable the video capture options in your system.

- **MCI device** : Standard Windows® capture drivers.
- **Twain device** : Twain capture drivers. (Recommended).
- **Use overlay** : Option activated for image capture devices.
- **Enable controls menu** : Activates options (such as zoom, pan and tilt) on image capture devices, if applicable.
- **MCI device number** : Select identification number of MCI device.
- **Portrait** : Enables portrait orientation of captured images.
- **Landscape** : Enables landscape orientation of captured images. (Default value).

3 - Click the **Test** button to verify if the video camera is functional.

Setting Up the Signature Capture Device

1 - From the Multimedia devices window, select the **Signature** tab.

2 - Check the **Enable Signature pad** option to enable the use of a signature pad device.

3 - From the displayed list of supported Signature pad devices, select the driver for the signature pad you want to use.

4 - Check the **Remote application** box if the signature device is setup as such.

5 - Select a **Pen width** .

6 - Use the **Test** button to check if the driver selected is functional. When you click the **Test** button, the **Signature Pad Test** window appears. This window appears whenever you choose the Signature pad option (Card, Visitor and Daypass definition windows).

7 - Select the **Video** tab to set video options for use with the Video Integration feature. This option allows you to choose between the windows or video format for Video playback (for Intellex only).

- **Disable DirectX** option: DirectX is a Windows® technology that enables higher performance in graphics and multimedia, including video and sound. By default, DirectX is enabled with the Video feature. However, you may want to disable it; if for example Video images are not correctly displayed or are not displayed at all, disabling DirectX can be useful. However, when DirectX is disabled, the system will use more system resources.

- The **Video bandwidth control** option allows you to reduce or increase the bandwidth required to stream live video without compromising video storage quality and computer performance. The range value is between 64 KB/s and 8192 KB/s.

*NOTE: The video bandwidth control value cannot **exceed** the EntraPass Server value (see page 476).*

Printers Selection and Configuration

The **Printer options** dialog that can be accessed under the **Options** toolbar allows users to select a log printer that will be used when printing events and to select a report or a badge printer.

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 an EntraPass application, a printer, or to activate a relay. Your decision may be based on, for instance, schedules that will send alarms to a remote terminal at a specific moment.

NOTE: You need to assign a "print" schedule to certain events to print them at a specified time.

1 - From **Printer options** dialog select the **Log printer** tab.

2 - Select a printing option in the **Printer type** section:

- **No log printer—** If you select this option, no event will be printed, even if a print schedule is defined for the events.
- **Use Network/Local Windows ® printer (page printer)** —If you select this option, all events sent to the printer will be buffered and printed when a full page is ready to be printed. Events will be printed on the network/local printer - not on a specific log printer.
- **Use local dot matrix printer** —If you select this option, all events sent to the printer will be printed one-by-one and one under the other, or it will print one event per page, depending on your printer type. Select the printer port that will be used in the "printer" field. Specify if messages and alarms will be printed on this printer.

3 - In the **Printer selection** section, specify whether you want to print message or alarms.

- **Print messages log** —If you select this option, all events that are assigned a "display" schedule in the events parameters menu will be printed.
- **Print alarms logs** —If you select this option, all events that are assigned an "alarm" schedule (and need to be acknowledged) in the events parameters menu will be printed.

4 - From the **Printer** drop-down list, select the specific printer that will be used as a log printer.

- If you have selected a **dot matrix printer** , select the **Port** on which the printer is connected to communicate with the computer. The **Port** field appears when a dot matrix printer is selected.

- If you are using a **network/local printer** , select the **Font** and the **Font size** . The font and font size influence the number of events that will be printed on one page. Using a smaller font increases the number of events printed on a page.

Selecting and Setting Up a Report Printer

The **Report printer** will be defined to print reports.

1 - From the **Printer options** window, select the **Report printer** tab.

Selecting and Setting Up a Badge Printer

The Badge printer will be defined to print badges that are created in EntraPass.

1 - From the Printer option window, select the **Badge printer** tab.

2 - Check the **Badge printer** option if a badge printer will be used; as a result, the Print badge and Preview badge button will be displayed in the Card, Visitor, and Day pass windows.

3 - From the **Select badge printer** drop-down list, select the appropriate badge printer.

4 - If you want the picture on the reverse side of the badge to be inverted, click the **Invert Reverse Side** box.

5 - Check the **Use bar code 39** as font when appropriate, and select the corresponding **Font** .

Registration

This menu is used to register new system components such as the KTES, Workstation, Gateway, SmartLink, etc. in order to register and use the system's database and to establish communication with the Server see **System Registration** .

Selecting and Setting Up a Badge Printer

The Badge printer will be defined to print badges that are created in EntraPass.

1 - From the Printer option window, select the **Badge printer** tab.

2 - Check the **Badge printer** option if a badge printer will be used; as a result, the Print badge and Preview badge button will be displayed in the Card, Visitor, and Day pass windows.

3 - From the **Select badge printer** drop-down list, select the appropriate badge printer.

4 - If you want the picture on the reverse side of the badge to be inverted, click the **Invert Reverse Side** box.

5 - Check the **Use bar code 39** as font when appropriate, and select the corresponding **Font** .

Service Login Information

The information entered here is required when the Server runs as a service and network resources need to be accessed from the Server. **Service Login Information** is required for the Backup Scheduler when using a network drive.

- You need to check the **Login Server Service Application** box to enable the feature.
- You **must** enter the server **Domain name or Computer name** , the **Login name** and the **Password** twice for confirmation.

*NOTE: When there is no domain name or workgroup configured, you must enter the **Computer Name** instead, in the **Domain Name** field.*

System Date & Time Modification

The **Change system** 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**).

1 - From the Option main window, select the **Date and Time** button.

2 - Enter the date in the **Date** field, or select a date from the calender. Connected components of this application will also receive the date change notification.

3 - Enter the time in the **Time** field. Connected components of this application will also receive the time change notification.

4 - Click **OK** to exit.

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* ***Time Parameters****.*

IMPORTANT : *You should not change the time using Windows®* ***settings. It is strongly recommended to change the system time through the server parameter settings.***

System Language Selection

EntraPass allows you to run the software in the language of your choice. The basic languages are English, French, Spanish, German and Italian. The Vocabulary Editor utility enable users to add other custom languages.

Changing the System Language

1 - From the EntraPass main window, select the **Options toolbar** , then click the **Select language** button.

NOTE: *When you modify the primary language, the database operation will be suspended during the operation and the changes will be effective only when you shutdown and then restart the system. The database language will be modified according the ascii values of the characters in the primary language. Accents and special characters of different languages may have an impact on your database.*

2 - From the **Select primary language** drop-down list, select the language you want to use as a primary language. From the **Select Secondary language** drop-down list, select the language you want to use as a secondary language.

3 - Log out of EntraPass and login again.

System Parameters Configuration

The System parameters dialog allows the System Administrator to modify parameters that define the EntraPass system.This dialog may be accessed from a workstation or a server. Parameters have been grouped together under different labels such asServer,Gateway, Firmware, Image, etc. If the Video Integration feature is enabled in your system,the corresponding parameters will appear under the Video label.

Server Parameters

Under the **Server** tab, you can defineserver logs capacity, diagnostic capabilities, security parameters, disk free space threshold, network alarms and button status.

E-mail Server

EntraPass offers users the ability to send reports using email capabilities. This function can also be used with SMTP servers asking for a user authentication.

NOTE: SSL secured connections are not supported.

1 - In the **Email server (SMTP or Exchange server)** field, enter the IP address of the Email server that will be used for sending emails.

2 - In the **Email Port** field, enter the number of the port that will be used for sending emails (usually 25).

3 - Select the encryption method.

- Unsecured (No SSL/TLS)
- Gmail(SSL/TLS)
- Secured (SSL/TLS)
- Office 365 (STARTTLS)

4 - Enter a valid Email address in the **Email sender** field. This email address will be used for authenticating the email server.

5 - Authentication: These options can be used to configure the authentication method.

- **No authentication** : No authentication will be applied.
- **SMTP authentication** : An authentication, sent on the SMTP port, must be validated before the message is released.

- **POP3 authentication** : An authentication, sent on the POP3 port, must be validated before the message is released.

6 - **Send to** : Recipient's address for the message to be sent.

7 - **Test** button: Send a test message with the selected parameters. According to the test results, different error or success messages could be displayed.

NOTE: The email port value is set to 25 by default. You may leave it as is or change this value to another available port on the network (between 0 and 65,535). For information about setting of the email server, contact the network administrator.

Operator auto-deactivate

Use the Operator auto-deactivate feature to automatically deactivate an operator if there is no activity on their account for a certain amount of days. The default is 90 days. When you install EntraPass for the first time or update from a previous version, this feature is turned off. When you turn on the Operator auto-deactivate feature, at midnight EntraPass checks the database for activated operators, and in the absence of activity, automatically sends an e-mail 10 days before the deactivation to notify the operator of their imminent disconnection.

NOTE: The Operator must complete their e-mail field to receive the notification e-mail. If their e-mail field is not complete, the deactivation occurs without the e-mail notification.
The auto-deactivate feature does not apply to LDAP operators, or the default EntraPass operators: administrator, installer, and operator.

To prevent deactivation the operator must log on to EntraPass using the workstation, web or mobile device before the deactivation date. If an Operator is deactivated, they have to manually enable the operator. To do this, click the **System** tab, and click **Operator** from the menu. Select the appropriate Operator and clear the **Operator disabled** check box.

In the event of a failure from the primary server, the feature continues to work fully on the redundant server. If the server and the redundant server are down on the day the notification e-mail is due to send, the notification e-mail is not sent but the Operator is deactivated as scheduled.

Setting the Operator auto-deactivate feature

To set the Operator auto-deactivate feature, complete the following steps:

1 - Click the **Options** tab, and click **System Parameters** from the menu.

2 - In the **System Parameters** window, click **Server**, and click the **Password rules** tab.

3 - Select the **Automatically deactivate operator** check box.

4 - In the **Days** field, click the arrows to select the amount of applicable days. Click **OK**. Thirty days is the minimum amount of days and 365 days is the maximum.

Server Logs

You can define the maximum number of records to store in the system logs and the system error logs (up to 100,000). Records include transactions such as: login to server, logout from server, disconnection, connection, stop or 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.

To make the **Audit** trail functionality available, select the **Audit trail** check box, and select one of the following data retention options:

- To define how many days to retain the audit data, select a number from the **Audit retention days** list. The default setting is 365 days, the minimum number is 30 days, and the maximum number is five years.
- To define how many records the system retains, select a number from 1 to 15 in the **Audit retention records** field. The default setting is five days.

In the **Audit trail selected component** area, select the components you want to appear in the **Audit trail** report. If you select the **Primary** check box, the component name is available in the audit trail. If you select the **Secondary** check box, the component list information is available in the audit trail.

Disk Space

The Disk Space feature has been developed as a protection against system failures that may be caused by the lack of disk space. This feature allows you to monitor the amount of free disk space for optimal system operation or for generating reports. In fact, EntraPass offers the ability to have the system abort the execution of a report if the free disk space has reached a specified threshold.

- **Disk free space threshold (MB)** : scroll-down list: specify a disk free space threshold that indicates when you want the system to send a message when the amount of free space falls below the value indicated. This value is in mega bytes. The range value is 2000 up to 99999 MB.
- **Time between notifications (hh:mm)** : enter the amount of time between notifications when the disk free space has reached the quota specified in the **Disk free space threshold** field. For example, if you enter 00:30 in the field, a system warning will be displayed every half hour. The time range value is 00:10 to 24:00.
- **Archival Path**: Enter the archival path. Saving historical data on a different drive will improve system performance.

Redundant Server

NOTE: The Redundant Server component will be available only if it has been previously registered.

You can define the **Auto-restart delay** (m:ss) for the Mirror Database and Redundant Server. The time range value is 1:00 to 9:59.

Quick synchronize: When this option is checked, the main server does not close the tables during the synchronization with the mirror database. Messages can still be received and the database viewed. A yellow button is then displayed on the left to indicate that the system is in read only mode.

*NOTE: The MS/SQL Interface program is not supported by the **Mirror Database and Redundant Server** . Even though the MS/SQL Interface cannot connect to the **Mirror Database and Redundant Server** , the MS/SQL Interface will buffer all the events.*

Logout and Idle

You will access this tab to specify the EntraPass applications behaviour when idle (when there is no action on the keyboard from the operator).

- **Automatic logout on idle** : the operator will have to re-inter his user name and password to enable the server application again. The maximum allowed delay is (mm:ss): 9 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.
- **Must login to close a Server application:** if checked, this option obliges operators to authenticate themselves by entering user name and password to close the Server application.
- **Notify last log out** : if checked, EntraPass will notify the last operator who is logging out.
- **Display Login List** : if checked, the five most recent operators to log into any EntraPass application will be displayed in the login dialog. This feature allows for easier system access for the operators who will simply select their user name and enter their password. It can also be used for administrative follow up where a System Administrator can view the list of operators who have recently logged on a specific application.

NOTE: Despite the advantages, it is recommended to disable the Display Login List whenever system security is at stake.

Schedule

The **Schedule** tab is where you will be able to upgrade to advanced schedule capability. In fact, EntraPass offers users more flexibility and ease of use by grouping schedules per gateway, connection or system logical components. This option is not automatically enabled upon installation of version 3.18 and higher of EntraPass.

NOTE: Make sure that you really need to upgrade to advance schedule before checking the box.

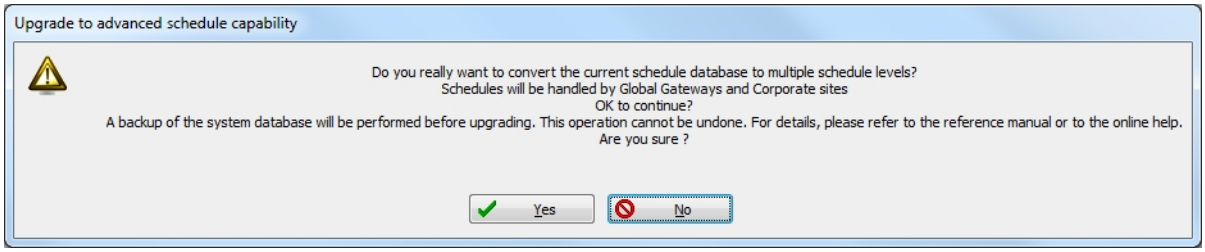
Schedules are grouped as follows:

- **System schedules** : System schedules are applicable to system logical components such as: operators login schedules, video triggers, etc. System schedules are not loaded in a particular controller; they are applicable to all the system. You can program an unlimited number of system schedules.

- Multi- site schedules : These are defined per connection. You can define 100 schedules per Multi-site for such purposes as power supervision (controllers), door unlocking, REX trigger (doors), activation mode (relay), input monitoring, etc.

- After checking the box and clicking **OK** , a warning will popup on screen indicating that the action is reversible but with consequences.

- We strongly suggest that you perform a backup of your data before activating this option.



- Once the process has been completed, you will notice that the **Schedule** tab will have disappeared from the System Parameter dialog.

- **Enable schedule to bypass Rex**: In order to enable the primary and secondary **Rex Bypass message schedule** options for doors, The **Enable schedule to bypass Rex** option must be selected. Please refer to **Door Configuration** for more details.

Icon Status

The **Status time out delay (m:ss)** parameter allows you to define a period of time before the workstation queries the server for the latest button statuses. The higher the delay, the lower the button refresh rate will be, therefore creating less traffic on the network. The maximum time out delay is 1 min. 30 seconds.

Service Login Information

The information entered here is required when the Server runs as a service and network resources need to be accessed from the Server. **Service Login Information** is required for the Backup Scheduler when using a network drive.

- You need to check the **Login Server Service Application** box to enable the feature.
- You **must** enter the server **Domain name or Computer name** , the **Login name** and the **Password** twice for confirmation.

NOTE: *When there is no domain name or workgroup configured, you must enter the* ***Computer Name*** *instead, in the* ***Domain Name*** *field.*

Password Rules

The purpose of this feature is to add more parameters to the actual operator's password.

1 - From the **Options** menu, select **System parameters**.

The password rules are :

- A minimum of 8 characters and a maximum of 20.
- A minimum of 0 and a maximum of 20 numerical characters.
- A minimum of 0 and a maximum of 20 special characters.
- A minimum of 0 and a maximum of 20 uppercase letters.

NOTE: *Once selected, all newly created or modified operators will need to comply to these new password rules.*

Firmware Parameters

This section contains all the information pertaining to controllers, gateways, and IP communication module, as well as the section to update you firmware.

*NOTE: The KTES tab will be available only if a KTES controller have been previously defined in the system. See **Kantech Telephone Entry System (KTES) Configuration** for more information.*

KT-100

The **KT-100** tab specifies the location of the folder containing the firmware for KT-100 controllers. The system will use this data to update the installed controllers (not available in EntraPass KTES Edition).

KT-300

The **KT-300** tab specifies the location of the folder containing the firmware for KT-300 controllers. The system will use this data to update the installed controllers (not available in EntraPass KTES Edition).

KT-400

The **KT-400** tab specifies the location of the folder containing the firmware for KT-400 controllers. The system will use this data to update the installed controllers .

- When checked, the **Enable TFTP KT-400 updater** option will allow operators to upgrade the KT-400 firmware from the **Update firmware** button from the **Operation** > **Site** dialog in EntraPass.

- Enable automatic firmware update: Select to make an update of each KT-400 with a different firmware version.

NOTE: The automatic firmware update function applies only to KT-400s that support it.

NOTE: The multi-site Gateway must be restarted in order to enable the TFTP KT-400 updater.

- For security reasons, you may decide, as a System Administrator to disable this option and not allow operators to update the firmware.

KT-1

The **KT-1** tab specifies the location of the folder containing the firmware for KT-1 controllers. The system will use this data to update the installed controllers.

- When checked, the **Enable TFTP KT-1 updater** option will allow operators to upgrade the KT-1 firmware from the **Update firmware** button from the **Operation** > **Site** dialog in EntraPass.

- **Enable automatic firmware update**: Select to make an update of each KT-1 with a different firmware version.

NOTE: The automatic firmware update function applies only to KT-1s that support it.

NOTE: The multi-site Gateway must be restarted in order to enable the TFTP KT-1 updater.

- For security reasons, you may decide, as a System Administrator to disable this option and not allow operators to update the firmware.
- Select the **Firmware flashing mode** to apply.

KTES

The **KTES** tab specifies the location of the folder containing the firmware for the KTES. The system will use this data to update the installed KTES.

Kantech IP Link

The **IP Link** tab specifies the location of the folder containing the firmware for the Kantech IP Link module . The system will use this data to update the installed firmware .

- When checked, the **Enable TFTP IP Link updater** option will allow operators to upgrade the IP Link firmware from the **Update firmware** button from the **Operation** > **Site** dialog in EntraPass.

NOTE: The Multi-site Gateway must be restarted in order to enable the TFTP IP Link updater.

- For security reasons, you may decide, as a System Administrator to disable this option and not allow operators to update the firmware.

ioSmart reader

- The **ioSmart reader** tab specifies the location of the folder containing the firmware for ioSmart readers. The system will use this data to update the installed readers.

ioModules

The **ioModule** tab specifies the location of the folder containing the firmware for the ioModules. The system uses this data to update the installed ioModules.

KT-401

The **KT-401** tab specifies the location of the folder containing the firmware for KT-401 controllers. The system will use this data to update the installed controllers .

- When checked, the **Enable TFTP KT-401 updater** option will allow operators to upgrade the KT-401 firmware from the **Update firmware** button from the **Operation** > **Site** dialog in EntraPass.

- Enable automatic firmware update: Select to make an update of each KT-401 with a different firmware version.

NOTE: The automatic firmware update function applies only to KT-401s that support it.

NOTE: The multi-site Gateway must be restarted in order to enable the TFTP KT-401 updater.

- For security reasons, you may decide, as a System Administrator to disable this option and not allow operators to update the firmware.

Image Parameters

The **Image** section is where you will define parameters for the badging features. You will define image quality for picture, signature and background images.

- If you are using the badging feature, it is recommended to leave the jpeg quality to default. Reducing the image quality may affect the quality of the pictures imported from badges.

- If you are not using the badging feature, you may reduce the jpeg quality of your images so that they will not occupy a large space in the database. You must take in consideration, however, that reducing the quality of the saved images may affect the quality of the photos imported into badges.

A parameter allows you to save cards and visitor card pictures, signatures and background graphics to a file instead of directly to the database. We are offering this option for sites that have large banks of pictures and graphics. The picture, signature and graphic database can currently contain up to 2 Gb of data each. The parameter will be used in instances where a site may need more space to save pictures, signatures and graphics.

Picture and Badging

The picture and badging feature allows you to adjust the image and signature quality for use with the Badging feature.

- Unchecking **Use JPEG format for pictures, signatures and badges** tells the system to save pictures (or signatures) in a tiff format.

NOTE: *Remember that this may affect the image quality. If you are not an advanced user, leave these values to default.*

- The **User picture, Signature, Badge background** and **Badge picture** indicate the quality of the image that will be saved. If you choose 10, the saved image quality will be poor; 100 indicates an excellent quality.

- Select the location of the **Picture (Signature) transparent colour position** for pictures and signature. Four choices are available (top-right, top-left, bottom-right and bottom-left). By default, the system chooses the bottom left-hand corner for the transparent background colour. EntraPass allows operators to choose a more suitable colour.

- When checking the **Save card pictures and signatures in a file** box, the system will create **Picture** and **Signature** directories under C:\Program Files\Kantech\Server_CE\Data where all pictures and signatures will be saved instead of directly in the database.

- When checking the **Save visitor pictures and signatures in a file** box, the system will create **Picture** and **Signature** directories under C:\Program Files\Kantech\Server_CE\Data where all visitor pictures and signatures will be saved instead of directly in the database.

NOTE: *When modifying an existing picture or signature, EntraPass will save it to the appropriate file and delete the corresponding entry in the database.*

Graphic

The graphic feature allows you to adjust the graphic quality for use with the EntraPass software.

- Unchecking **Use JPEG format for graphics** tells the system to save graphics in a tiff format.

NOTE: *Remember that this may affect the image quality. If you are not an advanced user, leave these values to default.*

- The JPEG quality value for **Graphic background** (**picture**) indicates the quality of the image that will be saved. If you choose 10, the saved image quality will be poor; 100 indicates an excellent quality.

- When checking the **Save graphics in a file** box, the system will create a **Graphic** directory under C:\Program Files\Kantech\Server_CE\Data where all graphics will be saved instead of directly in the database.

NOTE: When modifying an existing graphics, EntraPass will save it to the appropriate file and delete the corresponding entry in the database.

Report Parameters

The **Report** tab enables users to define the field separator for reports, disk free space threshold and user name format.

CSV

Under the **CSV** tab, you can define the field separator for your reports.

- By default, the system uses a comma (,) as the **Field separator** . You can modify the comma for another character. Other options are: Period, Equal, Semicolon, Colon, Space and tab.

- It is recommended to check the **Date and time on separate fields** option **.** When selected, CSV (comma separated values) as the output process for your reports, by default, the system includes the date and the time in a single field. When you select this option, the system will separate the date and the time fields.

Disk Space

This feature is a protection when for instance a huge report has been requested. In this case, the system will abort the execution of the report and displays an alert message indicating the reason of the cancellation.

- **Abort report if free space lower than (MB)**: scroll-down list allows you to specify the minimum amount of free disk space required for the execution of reports. The range value is 2000 to 999,999 MB.

- **Maximum event for email report** scroll-down list allows you to specify the maximum number of events that can be sent via an email report. The range value is 100 to 100,000 events.

- **Maximum event for standard report** scroll-down list allows you to specify the maximum number of events that can be sent in a report. The range value is 1000 to 500,000 events.
- **Simultaneous report process**: specify the maximum number of reports that can be generated simultaneously. Up to 10 reports can be executed simultaneously without affecting the performance of the system.

*NOTE: When the number of events for reports exceeds the maximum number, some events will not be included in the report. This will create the event **Report event quota exceeded**. This will be displayed in the desktop Messages and be added to the report.*

User Name Format

Specifying the user name format will tell the system how card holder's names will be displayed in EntraPass.

- **Parse user name** should be checked if you want to select a method of parsing the user's name in the system.

- **User name format** lets you select the parsing method. Options are: Begin with last name, Begin with first name.

- **Parse user name with** lets you select the character that will be used to parse the user name fields. Options are: Comma, Period, Equal, Semicolon, Colon, Space.

- **Strict search on card field** should be left empty unless you wish to keep the previous method (EntraPass Version 3.17 and lower) of strict searching a card field for reports.

NOTE: Prior to version 3.18 of EntraPass, the system used a strict search method that required Administrators to enter specific upper and lower boundaries to attain specific results. For example, for generating a report that included all users whose last name started with A, the lower boundary had to be A and the upper boundary had to be AZZZZZ. Now, the system will display all user names that start with an A just by entering A as a lower and upper boundary.

Video Parameters

The **Video** section will display only if the Video integration option is enabled in the EntraPass system. You will define the time synchronization, remote video process and JPEG format for video images.

Parameters

The **Parameters** tab allows you to define parameters for the video process.

- **Disable manual time synchronization** will keep the EntraPass server from updating the video server date and time following a manual modification of time. This feature is useful when, for example, you want to keep all recording events that occurred at the video server regardless of the actual time at the EntraPass server.

- The **Remote video process control parameters** section contains parameters that define remote management of video processes between the EntraPass Server and the video servers connected to EntraPass. It manages all the tasks (controls) related to: recordings, polls, events, and presets and patterns.

  - **Preset and pattern control application** field allows you to enter the number of applications that will be simultaneously launched for processing presets and patterns. The system is preset with a range value of 1 to 8 concurrent applications.

NOTE: *A Preset and Pattern Control application is launched each time a video recording is started following a trigger on a preset. If you set this number to 1 and if there are for instance more than 1 video servers with presets and patterns defined, the control application will process presets on all video servers. If you decide to increase the number of Preset and Pattern Control Applications, keep in mind that running many concurrent applications takes a great amount of system resources.*

- **Reset remote video process application** will allow the system to terminate and automatically restart the Remote Video Process application a few seconds later. This option may be used in instances when the video events are not being displayed.

- **Reset remote video process applications control** will allow the system to terminate the Control applications (recordings, polls, events and preset and patterns) and automatically restart the Remote Video Process application.

- Log Video process error will allow the system to keep a log of all video process errors in the EntraPass server files. Video process errors are logged in C:\Program files\Kantech\Server_CE\Bin\Log. Each Remote Video Process Control application generates a log file:

- RVP_LOG_00.txt (errors generated by RVP0.exe)
- RVPPoll_LOG_01.txt (errors generated by RVPPOLL1.exe)
- RVPEvent_LOG_02.txt (errors generated by RVEVENT3.exe)
- RVPRecord_LOG_03.txt (errors generated by RVPRECORD3.exe).
- RVPControl_LOG_04.txt (errors generated by RVPCONTROL4.exe).The system will generate as many log files as there are control applications running concurrently (RVPControl_LOG_05 to 08). The number of error log files will be equal to the number defined in the **Preset and pattern control application** field **.**

Snap:

The **Snap** option allows you to define the image quality that will display in the video thumbnails.

- The **Video image snap** indicates the quality of the image that will be saved as a thumbnail for each video. If you choose 10, the saved image quality will be poor; 100 indicates an excellent quality.

Intellex:

The **Intellex** options allow you to define the bandwidth allowed for the video process (for Intellex only).

- **Disable DirectX** will disable DirectX, a Windows® technology that enables higher performance when working or viewing graphics and other multimedia contents, including video and sound. By default, DirectX is enabled with the Video feature. You may sometimes need to disable it if, for example, video images are not correctly displayed or are not displayed at all.

NOTE: The system will use more system resources when DirectX is disabled

- **Limit video bandwidth** allows you to reduce or increase the bandwidth required to stream live video without compromising video storage quality and computer performance. The range value is between 64 KB/s to 8192 KB/s. The value will apply to all workstations including the EntraPass Server . However, for any specific workstation, this value can be reduced locally from the Options toolbar > Multimedia Devices > Video .
- **Video vault save delay** is used to indicate the time delay before the video vault recording can be played back.

*NOTE: The workstation value cannot **exceed** the EntraPass Server value.*

HDVR:

- **Video vault save delay** is used to indicate the time delay before the video vault recording can be played back.

TVR:

- **Video vault save delay** is used to indicate the time delay before the video vault recording can be played back.

Time Parameters

The **Time** section allows you to specify which gateway will be used to automatically adjust the time of all the computers connected to the EntraPass server. This feature is very useful when managing remote sites.

NOTE: The gateway polls the first controller on the first site at 5:47 am or 05:47, 1:47 pm or 13:47 and 7:47 pm or 19:47 to get the controller time.

- **No time adjustment** will disable the option.
- **By Gateway** will automatically synchronize the time of all computers with the Gateway selected in the scrolling list.
- **By Server** will automatically synchronize the time of all computers at regular intervals. You must also select the rate of **Hours between refreshes** in the adjacent selection box. The range value is 1 to 9999 hours.

Credentials Parameters

Card

Under the **Card** tab, System Administrators will be able to migrate their EntraPass system to enhanced user management where users are managed by their user name as well as their card number(s). Each card holder will be handled by user name and have up to 5 different numbers. This will allow for creating

cards without assigning card number to the new cards, *see* **Issuing a New Card in Enhanced User Management Environment**This option will be used with the EntraPass Web for card management. For more information on the EntraPass Web, please refer to the *EntraPass Web Help*.

NOTE: Enabling the migrate to enhanced user management is NOT REVERSIBLE through the software . However, when the system is migrating data, a backup is performed in EntraPass, so this can be restored to return to its previous action.

- **Migrate to enhanced user management**: The option is checked by default. EntraPass will migrate to the enhanced user management *(see **Issuing a New Card in Enhanced User Management Environment** for more details)*.

Workstation and Server

Toolbar Buttons

The toolbar buttons size can be increased up to 2.5 times the original size, in order to improve visibility of the text below the button. This is applicable to the EntraPass Server and the EntraPass Workstation. Logout and log back in to apply the change to the toolbar.

Assign a New Connection to a Site

*NOTE: Please refer to **Connection Configuration** for more details*

To enable or disable the feature, select an option:

- **Prompt**: System will prompt the user to specify the site to be connected to (optional) when creating a new connection.
- **Mandatory**: System will prompt the user to specify the site to be connected to (mandatory) when creating a new connection.
- **Disable** (default)

*NOTE: No reference will be made virtual sites unless at least one has been created previously (see **Site Configuration** for details).*

Integration

The **Integration** tab allows the user to select third party hardware that has been integrated to EntraPass by Kantech.

DLL registration: The available DLL in this menu will be used to specify which type of hardware the customer will connect to EntraPass.

- Click on **Add** to integrate another DLL. For additional details, see Integrated Panel Configuration.

*NOTE: The DLL integration **must be done at the EntraPass Server** in order to communicate with the Multi-site Gateway where the third party hardware is physically connected and powered up.*

Virtual keypad: The **Virtual keypad** tab allows the user to customize the virtual keypad screen display. Three different display modes can be selected: **Floating**, **Modal** or **Stay on top**.

Web Interface

Web tab

Use the **Web interface** button to configure EntraPass Web parameters.

- **Allow messages to EntraPass Web**: Select to allow the operator to see messages in EntraPass Web.
- **Maximum web messages**: Select a maximum from the counter.
- **Signature pad pen width**: Select a width value for the pen used with the signature pad.
- **Maximum request simultaneously by session**:Select the maximum number of report requests that can be done simultaneously.
- **Message filter for web messages**: From the drop-down list, select a filter for the messages to be displayed.
- **Badge image ratio for web**: Use the selector to increase the image printing quality (default value is 2). Note that increasing the ratio value will also increase the file size.

Web Customization tab

- **Custom color**: Click to change the color used in the interface (menus perimeter lines for example).
- **Page logo**: Click to insert (or change) a logo in the top left corner of the interface.

go Pass tab

If you register the go Pass mobile application, the **go Pass** tab appears. Use go Pass with a smartphone, or an Apple watch to lock or unlock a door. For convenience, you can control a door from a remote location. For a higher level of security use an ioSmart reader with the door, ioSmart readers use BLE technology. To cater for a range of security levels, select an option from the **Proximity Restriction** list.

1 - To display a cardholder's encrypted personal profile in the notification e-mails, select the **Display viable notification information** check box. Cardholders use their personal profile details or a link in the e-mail to gain access to the go Pass application.

2 - To resend all go Pass notification e-mails to all valid cardholders, click the **Resend go Pass notification for all valid cardholders** button.

3 - To control how and when SmartLink responds to invalid go Pass commands, define all three settings in the **Security** area:

a - To set how many invalid requests occur before SmartLink responds, enter a number in the **Notification debounce on wrong request** field.

a - To set the time to pass before SmartLink responds, enter a number in the **Debounce delay (ss)** field.

b - To prevent SmartLink responding to any go Pass request for a certain amount of time, enter a number in the **Disable go Pass when notification (m:ss)** field.

For example, # of invalid requests within # seconds = # seconds before SmartLink responds to go Pass request + event **Too many go Pass failed requests made** displays.

4 - Select one of the following options from the **Proximity Restriction** list:

- **None** - there is no restriction, the go Pass cardholder can lock, and unlock doors remotely, and at the door. EntraPass ignores BLE technology.
- **Strict (ioSmart BLE only)** – if the go Pass cardholder presents go Pass at an ioSmart reader, the go Pass cardholder has to be within range of the door.
- **Hybrid (BLE when available)** – use for go Pass cardholders who have access to ioSmart readers and non-ioSmart readers. If the go Pass cardholder is at an ioSmart door, the cardholder has to be within range, if it is a non-ioSmart door the cardholder can control the door remotely.

*NOTE: If you fail to select the **BLE** checkbox in the reader template that the controller uses, the **Proximity Restriction** selection is redundant.*

Time Parameters

The **Time** section allows you to specify which gateway will be used to automatically adjust the time of all the computers connected to the EntraPass server. This feature is very useful when managing remote sites.

NOTE: The gateway polls the first controller on the first connection at 5:47 am or 05:47, 1:47 pm or 13:47 and 7:47 pm or 19:47 to get the controller time.

- **No time adjustment** will disable the option.
- **By Gateway** will automatically synchronize the time of all computers with the Gateway selected in the scrolling list.

- **By Server** will automatically synchronize the time of all computers at regular intervals. You must also select the rate of **Hours between refreshes** in the adjacent selection box. The range value is 1 to 9999 hours.

User Name Format

Specifying the user name format will tell the system how card holder's names will be displayed in EntraPass .

- **Parse user name** should be checked if you want to select a method of parsing the user's name in the system.
- **User name format** lets you select the parsing method. Options are: Begin with last name, Begin with first name.
- **Parse user name with** lets you select the character that will be used to parse the user name fields. Options are: Comma, Period, Equal, Semicolon, Colon, Space.
- **Strict search on card field** should be left empty unless you wish to keep the previous method (EntraPass Version 3.17 and lower) of strict searching a card field for reports.

NOTE: *Prior to version 3.18 of EntraPass, the system used a strict search method that required Administrators to enter specific upper and lower boundaries to attain specific results. For example, for generating a report that included all users whose last name started with A, the lower boundary had to be A and the upper boundary had to be AZZZZZ. Now, the system will display all user names that start with an A just by entering A as a lower and upper boundary.*

General

Application

The **Application** menu allows operators to view various lists which show current operational status between the EntraPass server and the workstations connected to it

Viewing Applications Connected to the Server

Operators can view the status of all EntraPass applications from the Server user interface.

1 - In the EntraPass server application, click the **Application** button.

2 - Click the arrow sign next to each workstation to view details about a workstation (such as: registration codes, TCP/IP address, connections, messages buffered, etc.).

Error Log

The system errors are displayed with the date and time, the code number, the workstation name where the error originated from, the error code and its description.

1 - Select the **Error Log** button from the **Server** menu to view all the errors that occurred in the system.

2 - Click the **Text filter** button to display the Text filter window. From that window, 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.

3 - Columns:

- **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.
- **Code** : When selected, all columns will be sorted according to the **Code** column in alphabetical order.
- **Workstation** : When selected, all columns will be sorted according to the **Workstation** column in alphabetical order.
- **Error Code** : When selected, all columns will be sorted according to the **Error Code** column in alphabetical order.
- **Description** : When selected, all columns will be sorted according to the **Description** column in alphabetical order.

4 - You may also use the right-click menu to change the window background or to clear all the data displayed.

*NOTE: You can export the logs to a CSV file. To do this, right-click in the window, then select **CSV Export** from the shortcut menu.*

Log

The **Log** window 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 the log type. The Log window contains all the login and logout events for all workstations defined in the system.

1 - To view system logs, select the **Log** button from the **Server** menu.

2 - Click the **Text filter** button to display the Text filter window. From that window, 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.

3 - Columns:

- **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.
- **Workstation** : When selected, all columns will be sorted according to the **Workstation** column in alphabetical order.

- **Operator name** : When selected, all columns will be sorted according to the **Operator** name column in alphabetical order.
- **Transaction** : When selected, all columns will be sorted according to the **Transaction** column in alphabetical order.

4 - You may change the **background colour** . To do this, right-click on the window and select **Background colour** from the displayed shortcut list. Pick a color from the standard Windows dialog.

5 - You may also clear the window. To do this, right-click in the window, then select **Delete All** from the shortcut menu.

*NOTE: You can export the logs to a CSV file. To do this, right-click in the window, then select **CSV Export** from the shortcut menu.*

Registration

This menu is used to register new system components such as the KTES, Workstation, Gateway, SmartLink, etc. in order to register and use the system's database and to establish communication with the Server see **System Registration** .

Report Log

The **Report Log** window allows you to view a detailed list of all history reports processed by the system.

1 - To view the Report log, select the Report **Log** button from the **Report** menu.

2 - Click the **Text filter** button to display the Text filter window. From that window, 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.

3 - Click the **Refresh** button to update the displayed data.

4 - Columns:

- **Date requested** : This is the normal incoming sequence, if you select another sorting mode, you interrupt the normal sequence.
- **Requested by** : When selected, all columns will be sorted according to the **Requested by** column in alphabetical order.
- **Report name** : When selected, all columns will be sorted according to the **Report name** column in alphabetical order.
- **Date from** : When selected, all columns will be sorted according to the **Date from** column in alphabetical order.
- **To (Date)** : When selected, all columns will be sorted according to the **To (Date)** column in alphabetical order.

5 - You may also clear the window. To do this, right-click in the window, then select **Delete All** from the shortcut menu.

6 - Fields:

- **Report Type** : Show the type of report (quick, custom…).
- **Process By** : Show which application executed the report.
- **Workspace applied** : Show whether a workspace was applied.
- **Destination** : Where the report was delivered.
- **Used Template** : Show the dll that was used for the report.
- **Items in report** : The number of items in the report.
- **Requested date** : When the report was requested (date and time).
- **Queued date** : Show when the report was added to the application queue that generated the report (Date and time and the total time elapsed).
- **Process date** : When the process was started (Date and time and the total time elapsed).
- **Delivery date** : Show when the report was delivered to destination (Date and time and the total time elapsed).
- **Completion date** : Show end date and time of report execution.
- **Completion State** : Show whether the report was completed successfully or aborted.

Backup

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 computer system fails, you may restore a backup copy onto another computer, on which the EntraPass server has been installed .

The EntraPass **Backup** tab allows operators to perform manual backups of the system data (D), archive (A), In/Out (T) and video (V) 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 database will temporarily be disabled. In the EntraPass application main window, you will notice that the second coloured square at the bottom left of the screen turns red when the database is unavailable. Modifications made on the workstations will not be applied to the database until the database is available again.*

All the system data can be found under the following path: C:\Program Files\Kantech\ Server_CE\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).

Creating Backups of Type D, A, T and V

By default, the name of the sub-directory in which the data/archive/In-Out/Video 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, T for In/Out, V for video). The following steps explain how to backup data. The same steps apply also when you backup archives or In/Out data.

1 - Select the item you want to backup:

- **Backup Data**
- **Backup Archive**
- **Backup In/Out**
- **Backup Video Events**

EntraPass suggests a location and a file name for the backup choose to keep the default settings, or select a new location and file name.

NOTE: *By default, EntraPass backs up all the information originating from the following directory: C:\Program Files\Kantech\Server_CE\Data or Archive or* In/Out *to C:\ProgramFiles\Kantech\Server_CE\Backup\ X_YYYY_MM_DD-h_mm_ss, where X is the data type. The data type is followed by the year, month and day information as well as the time of the backup.*

2 - Select the Backup type:

- **Separate file** : The system will back up the databases one by one (standard). This backup type includes the Regdata.ini file containing the following identification data: software used to create the backup, backup type (data, archive, In/Out), operator who requested the backup, date and time of the backup as well as the software version.

3 - From the **Drives** drop-down list, select the drive on which the backup will be performed. A list of choices is available according to your computer settings. To save as default, leave as is.

4 - You may click the **New folder** button if you want to specify a new destination folder.

5 - Click **OK** to launch the backup procedure. The backup process can be viewed on the bottom part of the window.

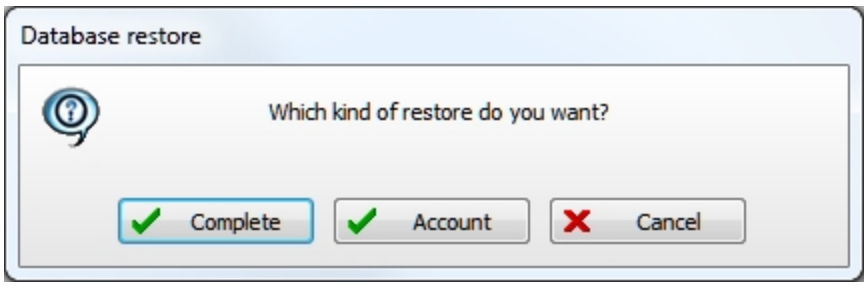
*NOTE: You can use the "Backup Scheduler" to schedule or plan automatic backups. To schedule automatic backups see **Backup Scheduler**. When you backup or restore files, the Server databases are temporarily disabled. You cannot modify the databases when a backup is in process.*

Restores

If you are restoring data, it is strongly recommended to perform a backup before you do so. 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 **Backup** tab, select the desired Restore button (Data, Archive, In/Out, Video). The system displays the Restore data window. 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.



3 - If you click on the **Complete** button, the system will restore all the information from the selected directory.

*NOTE: If the EntraPass version the operator is restoring is different to the version currently stored in **Restores**, the system displays a message instructing the operator to ensure the versions match. This affects only **Backup Data.***

NOTE: By default, the system restores all the information originating from the following directory: C:\ProgramFiles\Kantech\Server_CE\Backup\ X_YYYY_MM_DD-h_mm_ss to C:\Program Files\Kantech\Server_CE\Data or Archive or In/Out *.*

NOTE: It is recommended to reload the Gateway after restoring the data (Operation > Reload data).

Options

Defining a Card Display Format

The EntraPass system can accommodate various reader types. Depending on the reader type, the card display format may vary. The Display format dialog allows you to select the default format that is setup automatically when creating a new card.

1 - Under the **Options** toolbar, click the **Display format** button.

2 - From the **Card** list, s elect a display format for **Card #1** .

- **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.

- **FIPS** (Federal Information Processing Standard): This card format can use more than 32 bits of data.

3 - Check the **Use multiple card format** box if your environment contains multiple reader types and you would like to have the capability to select a different reader, that is not the default reader, when creating a new card.

4 - Select one of the **Duplicate PIN process** in the scrolling box. This feature can be used for example while loading cards in a batch. An operator may decide to set the PIN option to allow duplication. Later, if desired, the duplicate PINs can be changed to prevent confusion.

- **No duplication** : An error appears on the workstation; the PIN field will be reset to the default value (00000) and will be highlighted, inviting you to enter a new and valid PIN. Only PIN 00000 will be duplicated regardless of the PIN setting option.

- **Notify when duplication:** the server verifies if this PIN already exists. If the PIN exists, a message box appears, indicating that the PIN exists. A **Details** button will allow operators to view a list of cardholders who were issued this PIN.

- **Duplication:** no test will be processed, the PIN will be accepted even if it is a duplicate.

5 - **Number of PIN digits (KT-400 only):** This function allows using the **Keypad Pin Digit** option with the new KT400 firmware. You can choose to have 4, 5 or 6 digits (see **Card Options Definition** for more information).

NOTE: The PIN number must be set up once and kept that way in order to avoid any in duplication if truncated or filled by the system.

6 - When the Enhanced User Management option has been chosen, select an alternate default display format for **Card #2** . Repeat **Step 6** for **Card #3** , **Card #4** and **Card #5** .

7 - Under the Global display format for **KT-100** , **KT-300** and **KT-400** , select the appropriate option to coordinate with the selection in the upper section of the dialog.

- **24-bit Wiegand card, 5-digit PIN (KT-200 default)** : for up to 24-bit for KT-100, KT-200, KT-300 and KT-400.

- **32-bit card, 5-digit PIN** : for up to 32-bit for KT-100, KT-300 and KT-400.

- **24-bit Wiegand card, 6-digit PIN** : for up to 24-bit for KT-100, KT-300 and KT-400.

- **Up to 16 characters ABA card** , **6-digit PIN** : for up to 16 for KT-100, KT-300 and KT-400.

NOTE: KT-100, KT-300, and KT-400 controllers will do a hard reset on card format change. Avoid alternating between different card formats because this may result in lost card information.

Changing from a 24-bit to 32-bit Global Card Format

Changing from 24-bit to 32-bit global card format extends the amount of cards you can configure on EntraPass.

The ioProx 26-bit Wiegand reader does not support changing from a 24-bit to 32-bit global card format. If you have a combination of ioProx XSF and ioProx 26-bit Wiegand readers, do not manually change the format, or turn on the auto conversion feature. You first have to replace the 26-bit Wiegand readers with XSF readers.

To manually change from a 24-bit to 32-bit global card format, complete the following steps:

1 - Click the **Options** tab, and select **Display format** from the menu.
2 - In the **Global card format** area, choose the **32-bit card, 5-digit PIN** option.
3 - Click **OK**. If you made a change from a 24-bit Wiegand card, five or six digits, to a 32-bit card, five digit PIN, a prompt displays to ask if you require the cards converted to 32-bit family code.
   - If you click **Yes**, enter the value of the extended facility code.
   - If you click **No**, a prompt displays to enable the **Auto conversion** feature.

NOTE: The ability to change the global card format from 24-bit to 32-bit format is not available when running from a redundant server.
EntraPass does not automatically backup data when you switch from 24-bit to 32-bit card format.

In the workstation, EntraPass backs up the system prior to conversion.

After you change formats, the KT-100, KT-200, and KT-300 automatically do a hard reset. For the KT-1 and KT-400 the change is seamless.

Auto conversion

When you select the **Use Auto Conversion for legacy 24 bit cards** check box in the **Display Format** window, EntraPass automatically converts all cards to a 32-bit card format. The default value is cleared. To enable the check box, you must set the **Global Card Format** to the **32-bit card, 5 digit PIN** option.

When you select the auto conversion feature, and have not converted the cards to a 32-bit format, the system automatically modifies the card number and triggers a **Card definition modified** event. The events have to be non-fail soft events. The feature is available in the multi-site gateway, the global gateway, and the KT-NCC gateway.

NOTE: The Auto conversion feature is available when running the redundant server.

Connection Password Modification

The connection password is used to authenticate EntraPass Workstations to the EntraPass Server. The connection password window is automatically displayed when the system has not yet been registered.

CAUTION:
Keep in mind that there is no way to reset the connection password if forgotten after its modification.

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 connection password is kantech, in lower case. Passwords are case sensitive.*

Changing the Connection Password

1 - From the **Options** main window, select the **Connection password** button.

2 - Enter the current connection password (case sensitive) in the **Old authentication password** field. The default authentication password is kantech, in lower case.

3 - Enter the new authentication password in **New authentication password** field (case sensitive).

4 - Enter the new authentication password in the **Verify authentication password** for confirmation. This field will verify that the new connection 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 authentication password** and in the **Verify authentication password** fields are identical (case sensitive).

NOTE: *The connection password is different from the operator password. The connection password is used to authenticate workstations, whereas the operator password is used to open a session.*

System Language Selection

EntraPass allows you to run the software in the language of your choice. The basic languages are English, French, Spanish, German and Italian. The Vocabulary Editor utility enable users to add other custom languages.

Changing the System Language

1 - From the EntraPass main window, select the **Options toolbar** , then click the **Select language** button.

NOTE: When you modify the primary language, the database operation will be suspended during the operation and the changes will be effective only when you shutdown and then restart the system. The database language will be modified according the ascii values of the characters in the primary language. Accents and special characters of different languages may have an impact on your database.

2 - From the **Select primary language** drop-down list, select the language you want to use as a primary language. From the **Select Secondary language** drop-down list, select the language you want to use as a secondary language.

3 - Log out of EntraPass and login again.

System Date & Time Modification

The **Change system** 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**).

1 - From the Option main window, select the **Date and Time** button.

2 - Enter the date in the **Date** field, or select a date from the calender. Connected components of this application will also receive the date change notification.

3 - Enter the time in the **Time** field. Connected components of this application will also receive the time change notification.

4 - Click **OK** to exit.

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 ***Time Parameters****.*

IMPORTANT : *You should not change the time using Windows®* ***settings. It is strongly recommended to change the system time through the server parameter settings.***

System Parameters Configuration

The System parameters dialog allows the System Administrator to modify parameters that define the EntraPass system.This dialog may be accessed from a workstation or a server. Parameters have been grouped together under different labels such asServer,Gateway, Firmware, Image, etc. If the Video Integration feature is enabled in your system,the corresponding parameters will appear under the Video label.

Server Parameters

Under the **Server** tab, you can defineserver logs capacity, diagnostic capabilities, security parameters, disk free space threshold, network alarms and button status.

E-mail Server

EntraPass offers users the ability to send reports using email capabilities. This function can also be used with SMTP servers asking for a user authentication.

NOTE: *SSL secured connections are not supported.*

1 - In the **Email server (SMTP or Exchange server)** field, enter the IP address of the Email server that will be used for sending emails.
2 - In the **Email Port** field, enter the number of the port that will be used for sending emails (usually 25).
3 - Select the encryption method.
- Unsecured (No SSL/TLS)
- Gmail(SSL/TLS)
- Secured (SSL/TLS)
- Office 365 (STARTTLS)

4 - Enter a valid Email address in the **Email sender** field. This email address will be used for authenticating the email server.
5 - Authentication: These options can be used to configure the authentication method.
- **No authentication** : No authentication will be applied.
- **SMTP authentication** : An authentication, sent on the SMTP port, must be validated before the message is released.

- **POP3 authentication** : An authentication, sent on the POP3 port, must be validated before the message is released.

6 - **Send to** : Recipient's address for the message to be sent.

7 - **Test** button: Send a test message with the selected parameters. According to the test results, different error or success messages could be displayed.

NOTE: The email port value is set to 25 by default. You may leave it as is or change this value to another available port on the network (between 0 and 65,535). For information about setting of the email server, contact the network administrator.

Operator auto-deactivate

Use the Operator auto-deactivate feature to automatically deactivate an operator if there is no activity on their account for a certain amount of days. The default is 90 days. When you install EntraPass for the first time or update from a previous version, this feature is turned off. When you turn on the Operator auto-deactivate feature, at midnight EntraPass checks the database for activated operators, and in the absence of activity, automatically sends an e-mail 10 days before the deactivation to notify the operator of their imminent disconnection.

NOTE: The Operator must complete their e-mail field to receive the notification e-mail. If their e-mail field is not complete, the deactivation occurs without the e-mail notification.
The auto-deactivate feature does not apply to LDAP operators, or the default EntraPass operators: administrator, installer, and operator.

To prevent deactivation the operator must log on to EntraPass using the workstation, web or mobile device before the deactivation date. If an Operator is deactivated, they have to manually enable the operator. To do this, click the **System** tab, and click **Operator** from the menu. Select the appropriate Operator and clear the **Operator disabled** check box.

In the event of a failure from the primary server, the feature continues to work fully on the redundant server. If the server and the redundant server are down on the day the notification e-mail is due to send, the notification e-mail is not sent but the Operator is deactivated as scheduled.

Setting the Operator auto-deactivate feature

To set the Operator auto-deactivate feature, complete the following steps:

1 - Click the **Options** tab, and click **System Parameters** from the menu.
2 - In the **System Parameters** window, click **Server**, and click the **Password rules** tab.
3 - Select the **Automatically deactivate operator** check box.
4 - In the **Days** field, click the arrows to select the amount of applicable days. Click **OK**. Thirty days is the minimum amount of days and 365 days is the maximum.

Server Logs

You can define the maximum number of records to store in the system logs and the system error logs (up to 100,000). Records include transactions such as: login to server, logout from server, disconnection, connection, stop or 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.

To make the **Audit** trail functionality available, select the **Audit trail** check box, and select one of the following data retention options:

- To define how many days to retain the audit data, select a number from the **Audit retention days** list. The default setting is 365 days, the minimum number is 30 days, and the maximum number is five years.
- To define how many records the system retains, select a number from 1 to 15 in the **Audit retention records** field. The default setting is five days.

In the **Audit trail selected component** area, select the components you want to appear in the **Audit trail** report. If you select the **Primary** check box, the component name is available in the audit trail. If you select the **Secondary** check box, the component list information is available in the audit trail.

Disk Space

The Disk Space feature has been developed as a protection against system failures that may be caused by the lack of disk space. This feature allows you to monitor the amount of free disk space for optimal system operation or for generating reports. In fact, EntraPass offers the ability to have the system abort the execution of a report if the free disk space has reached a specified threshold.

- **Disk free space threshold (MB)** : scroll-down list: specify a disk free space threshold that indicates when you want the system to send a message when the amount of free space falls below the value indicated. This value is in mega bytes. The range value is 2000 up to 99999 MB.
- **Time between notifications (hh:mm)** : enter the amount of time between notifications when the disk free space has reached the quota specified in the **Disk free space threshold** field. For example, if you enter 00:30 in the field, a system warning will be displayed every half hour. The time range value is 00:10 to 24:00.
- **Archival Path**: Enter the archival path. Saving historical data on a different drive will improve system performance.

Redundant Server

NOTE: The Redundant Server component will be available only if it has been previously registered.

You can define the **Auto-restart delay** (m:ss) for the Mirror Database and Redundant Server. The time range value is 1:00 to 9:59.

Quick synchronize: When this option is checked, the main server does not close the tables during the synchronization with the mirror database. Messages can still be received and the database viewed. A yellow button is then displayed on the left to indicate that the system is in read only mode.

*NOTE: The MS/SQL Interface program is not supported by the **Mirror Database and Redundant Server** . Even though the MS/SQL Interface cannot connect to the **Mirror Database and Redundant Server** , the MS/SQL Interface will buffer all the events.*

Logout and Idle

You will access this tab to specify the EntraPass applications behaviour when idle (when there is no action on the keyboard from the operator).

- **Automatic logout on idle** : the operator will have to re-inter his user name and password to enable the server application again. The maximum allowed delay is (mm:ss): 9 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.
- **Must login to close a Server application:** if checked, this option obliges operators to authenticate themselves by entering user name and password to close the Server application.
- **Notify last log out** : if checked, EntraPass will notify the last operator who is logging out.
- **Display Login List** : if checked, the five most recent operators to log into any EntraPass application will be displayed in the login dialog. This feature allows for easier system access for the operators who will simply select their user name and enter their password. It can also be used for administrative follow up where a System Administrator can view the list of operators who have recently logged on a specific application.

NOTE: Despite the advantages, it is recommended to disable the Display Login List whenever system security is at stake.

Schedule

The **Schedule** tab is where you will be able to upgrade to advanced schedule capability. In fact, EntraPass offers users more flexibility and ease of use by grouping schedules per gateway, connection or system logical components. This option is not automatically enabled upon installation of version 3.18 and higher of EntraPass.

NOTE: Make sure that you really need to upgrade to advance schedule before checking the box.

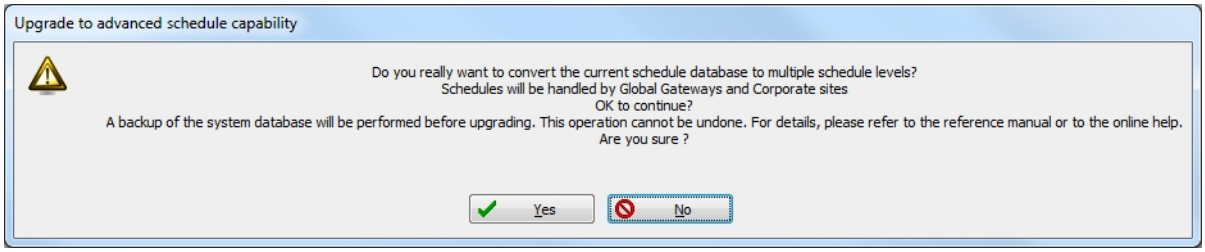
Schedules are grouped as follows:

- **System schedules** : System schedules are applicable to system logical components such as: operators login schedules, video triggers, etc. System schedules are not loaded in a particular controller; they are applicable to all the system. You can program an unlimited number of system schedules.

- Multi- site schedules : These are defined per connection. You can define 100 schedules per Multi-site for such purposes as power supervision (controllers), door unlocking, REX trigger (doors), activation mode (relay), input monitoring, etc.

- After checking the box and clicking **OK** , a warning will popup on screen indicating that the action is reversible but with consequences.

- We strongly suggest that you perform a backup of your data before activating this option.



- Once the process has been completed, you will notice that the **Schedule** tab will have disappeared from the System Parameter dialog.

- **Enable schedule to bypass Rex**: In order to enable the primary and secondary **Rex Bypass message schedule** options for doors, The **Enable schedule to bypass Rex** option must be selected. Please refer to **Door Configuration** for more details.

Icon Status

The **Status time out delay (m:ss)** parameter allows you to define a period of time before the workstation queries the server for the latest button statuses. The higher the delay, the lower the button refresh rate will be, therefore creating less traffic on the network. The maximum time out delay is 1 min. 30 seconds.

Service Login Information

The information entered here is required when the Server runs as a service and network resources need to be accessed from the Server. **Service Login Information** is required for the Backup Scheduler when using a network drive.

- You need to check the **Login Server Service Application** box to enable the feature.
- You **must** enter the server **Domain name or Computer name** , the **Login name** and the **Password** twice for confirmation.

*NOTE: When there is no domain name or workgroup configured, you must enter the **Computer Name** instead, in the **Domain Name** field.*

Password Rules

The purpose of this feature is to add more parameters to the actual operator's password.

1 - From the **Options** menu, select **System parameters**.

The password rules are :

- A minimum of 8 characters and a maximum of 20.
- A minimum of 0 and a maximum of 20 numerical characters.
- A minimum of 0 and a maximum of 20 special characters.
- A minimum of 0 and a maximum of 20 uppercase letters.

NOTE: Once selected, all newly created or modified operators will need to comply to these new password rules.

Firmware Parameters

This section contains all the information pertaining to controllers, gateways, and IP communication module, as well as the section to update you firmware.

*NOTE: The KTES tab will be available only if a KTES controller have been previously defined in the system. See **Kantech Telephone Entry System (KTES) Configuration** for more information.*

KT-100

The **KT-100** tab specifies the location of the folder containing the firmware for KT-100 controllers. The system will use this data to update the installed controllers (not available in EntraPass KTES Edition).

KT-300

The **KT-300** tab specifies the location of the folder containing the firmware for KT-300 controllers. The system will use this data to update the installed controllers (not available in EntraPass KTES Edition).

KT-400

The **KT-400** tab specifies the location of the folder containing the firmware for KT-400 controllers. The system will use this data to update the installed controllers .

- When checked, the **Enable TFTP KT-400 updater** option will allow operators to upgrade the KT-400 firmware from the **Update firmware** button from the **Operation** > **Site** dialog in EntraPass.

- Enable automatic firmware update: Select to make an update of each KT-400 with a different firmware version.

NOTE: The automatic firmware update function applies only to KT-400s that support it.

NOTE: The multi-site Gateway must be restarted in order to enable the TFTP KT-400 updater.

- For security reasons, you may decide, as a System Administrator to disable this option and not allow operators to update the firmware.

KT-1

The **KT-1** tab specifies the location of the folder containing the firmware for KT-1 controllers. The system will use this data to update the installed controllers.

- When checked, the **Enable TFTP KT-1 updater** option will allow operators to upgrade the KT-1 firmware from the **Update firmware** button from the **Operation** > **Site** dialog in EntraPass.

- **Enable automatic firmware update**: Select to make an update of each KT-1 with a different firmware version.

NOTE: The automatic firmware update function applies only to KT-1s that support it.

NOTE: The multi-site Gateway must be restarted in order to enable the TFTP KT-1 updater.

- For security reasons, you may decide, as a System Administrator to disable this option and not allow operators to update the firmware.
- Select the **Firmware flashing mode** to apply.

KTES

The **KTES** tab specifies the location of the folder containing the firmware for the KTES. The system will use this data to update the installed KTES.

Kantech IP Link

The **IP Link** tab specifies the location of the folder containing the firmware for the Kantech IP Link module . The system will use this data to update the installed firmware .

- When checked, the **Enable TFTP IP Link updater** option will allow operators to upgrade the IP Link firmware from the **Update firmware** button from the **Operation** > **Site** dialog in EntraPass.

NOTE: The Multi-site Gateway must be restarted in order to enable the TFTP IP Link updater.

- For security reasons, you may decide, as a System Administrator to disable this option and not allow operators to update the firmware.

ioSmart reader

- The **ioSmart reader** tab specifies the location of the folder containing the firmware for ioSmart readers. The system will use this data to update the installed readers.

ioModules

The **ioModule** tab specifies the location of the folder containing the firmware for the ioModules. The system uses this data to update the installed ioModules.

KT-401

The **KT-401** tab specifies the location of the folder containing the firmware for KT-401 controllers. The system will use this data to update the installed controllers .

- When checked, the **Enable TFTP KT-401 updater** option will allow operators to upgrade the KT-401 firmware from the **Update firmware** button from the **Operation** > **Site** dialog in EntraPass.

- Enable automatic firmware update: Select to make an update of each KT-401 with a different firmware version.

NOTE: The automatic firmware update function applies only to KT-401s that support it.

NOTE: The multi-site Gateway must be restarted in order to enable the TFTP KT-401 updater.

- For security reasons, you may decide, as a System Administrator to disable this option and not allow operators to update the firmware.

Image Parameters

The **Image** section is where you will define parameters for the badging features. You will define image quality for picture, signature and background images.

- If you are using the badging feature, it is recommended to leave the jpeg quality to default. Reducing the image quality may affect the quality of the pictures imported from badges.

- If you are not using the badging feature, you may reduce the jpeg quality of your images so that they will not occupy a large space in the database. You must take in consideration, however, that reducing the quality of the saved images may affect the quality of the photos imported into badges.

A parameter allows you to save cards and visitor card pictures, signatures and background graphics to a file instead of directly to the database. We are offering this option for sites that have large banks of pictures and graphics. The picture, signature and graphic database can currently contain up to 2 Gb of data each. The parameter will be used in instances where a site may need more space to save pictures, signatures and graphics.

Picture and Badging

The picture and badging feature allows you to adjust the image and signature quality for use with the Badging feature.

- Unchecking **Use JPEG format for pictures, signatures and badges** tells the system to save pictures (or signatures) in a tiff format.

NOTE: *Remember that this may affect the image quality. If you are not an advanced user, leave these values to default.*

- The **User picture, Signature, Badge background** and **Badge picture** indicate the quality of the image that will be saved. If you choose 10, the saved image quality will be poor; 100 indicates an excellent quality.

- Select the location of the **Picture (Signature) transparent colour position** for pictures and signature. Four choices are available (top-right, top-left, bottom-right and bottom-left). By default, the system chooses the bottom left-hand corner for the transparent background colour. EntraPass allows operators to choose a more suitable colour.

- When checking the **Save card pictures and signatures in a file** box, the system will create **Picture** and **Signature** directories under C:\Program Files\Kantech\Server_CE\Data where all pictures and signatures will be saved instead of directly in the database.

- When checking the **Save visitor pictures and signatures in a file** box, the system will create **Picture** and **Signature** directories under C:\Program Files\Kantech\Server_CE\Data where all visitor pictures and signatures will be saved instead of directly in the database.

NOTE: *When modifying an existing picture or signature, EntraPass will save it to the appropriate file and delete the corresponding entry in the database.*

Graphic

The graphic feature allows you to adjust the graphic quality for use with the EntraPass software.

- Unchecking **Use JPEG format for graphics** tells the system to save graphics in a tiff format.

NOTE: *Remember that this may affect the image quality. If you are not an advanced user, leave these values to default.*

- The JPEG quality value for **Graphic background** (**picture**) indicates the quality of the image that will be saved. If you choose 10, the saved image quality will be poor; 100 indicates an excellent quality.

- When checking the **Save graphics in a file** box, the system will create a **Graphic** directory under C:\Program Files\Kantech\Server_CE\Data where all graphics will be saved instead of directly in the database.

NOTE: When modifying an existing graphics, EntraPass will save it to the appropriate file and delete the corresponding entry in the database.

Report Parameters

The **Report** tab enables users to define the field separator for reports, disk free space threshold and user name format.

CSV

Under the **CSV** tab, you can define the field separator for your reports.

- By default, the system uses a comma (,) as the **Field separator** . You can modify the comma for another character. Other options are: Period, Equal, Semicolon, Colon, Space and tab.

- It is recommended to check the **Date and time on separate fields** option **.** When selected, CSV (comma separated values) as the output process for your reports, by default, the system includes the date and the time in a single field. When you select this option, the system will separate the date and the time fields.

Disk Space

This feature is a protection when for instance a huge report has been requested. In this case, the system will abort the execution of the report and displays an alert message indicating the reason of the cancellation.

- **Abort report if free space lower than (MB)**: scroll-down list allows you to specify the minimum amount of free disk space required for the execution of reports. The range value is 2000 to 999,999 MB.

- **Maximum event for email report** scroll-down list allows you to specify the maximum number of events that can be sent via an email report. The range value is 100 to 100,000 events.

- **Maximum event for standard report** scroll-down list allows you to specify the maximum number of events that can be sent in a report. The range value is 1000 to 500,000 events.
- **Simultaneous report process**: specify the maximum number of reports that can be generated simultaneously. Up to 10 reports can be executed simultaneously without affecting the performance of the system.

*NOTE: When the number of events for reports exceeds the maximum number, some events will not be included in the report. This will create the event **Report event quota exceeded**. This will be displayed in the desktop Messages and be added to the report.*

User Name Format

Specifying the user name format will tell the system how card holder's names will be displayed in EntraPass.

- **Parse user name** should be checked if you want to select a method of parsing the user's name in the system.

- **User name format** lets you select the parsing method. Options are: Begin with last name, Begin with first name.

- **Parse user name with** lets you select the character that will be used to parse the user name fields. Options are: Comma, Period, Equal, Semicolon, Colon, Space.

- **Strict search on card field** should be left empty unless you wish to keep the previous method (EntraPass Version 3.17 and lower) of strict searching a card field for reports.

NOTE: Prior to version 3.18 of EntraPass, the system used a strict search method that required Administrators to enter specific upper and lower boundaries to attain specific results. For example, for generating a report that included all users whose last name started with A, the lower boundary had to be A and the upper boundary had to be AZZZZZ. Now, the system will display all user names that start with an A just by entering A as a lower and upper boundary.

Video Parameters

The **Video** section will display only if the Video integration option is enabled in the EntraPass system. You will define the time synchronization, remote video process and JPEG format for video images.

Parameters

The **Parameters** tab allows you to define parameters for the video process.

- **Disable manual time synchronization** will keep the EntraPass server from updating the video server date and time following a manual modification of time. This feature is useful when, for example, you want to keep all recording events that occurred at the video server regardless of the actual time at the EntraPass server.

- The **Remote video process control parameters** section contains parameters that define remote management of video processes between the EntraPass Server and the video servers connected to EntraPass. It manages all the tasks (controls) related to: recordings, polls, events, and presets and patterns.

  - **Preset and pattern control application** field allows you to enter the number of applications that will be simultaneously launched for processing presets and patterns. The system is preset with a range value of 1 to 8 concurrent applications.

NOTE: A Preset and Pattern Control application is launched each time a video recording is started following a trigger on a preset. If you set this number to 1 and if there are for instance more than 1 video servers with presets and patterns defined, the control application will process presets on all video servers. If you decide to increase the number of Preset and Pattern Control Applications, keep in mind that running many concurrent applications takes a great amount of system resources.

- **Reset remote video process application** will allow the system to terminate and automatically restart the Remote Video Process application a few seconds later. This option may be used in instances when the video events are not being displayed.

- **Reset remote video process applications control** will allow the system to terminate the Control applications (recordings, polls, events and preset and patterns) and automatically restart the Remote Video Process application.

- Log Video process error will allow the system to keep a log of all video process errors in the EntraPass server files. Video process errors are logged in C:\Program files\Kantech\Server_CE\Bin\Log. Each Remote Video Process Control application generates a log file:

- RVP_LOG_00.txt (errors generated by RVP0.exe)
- RVPPoll_LOG_01.txt (errors generated by RVPPOLL1.exe)
- RVPEvent_LOG_02.txt (errors generated by RVEVENT3.exe)
- RVPRecord_LOG_03.txt (errors generated by RVPRECORD3.exe).
- RVPControl_LOG_04.txt (errors generated by RVPCONTROL4.exe).The system will generate as many log files as there are control applications running concurrently (RVPControl_LOG_05 to 08). The number of error log files will be equal to the number defined in the **Preset and pattern control application** field **.**

Snap:

The **Snap** option allows you to define the image quality that will display in the video thumbnails.

- The **Video image snap** indicates the quality of the image that will be saved as a thumbnail for each video. If you choose 10, the saved image quality will be poor; 100 indicates an excellent quality.

Intellex:

The **Intellex** options allow you to define the bandwidth allowed for the video process (for Intellex only).

- **Disable DirectX** will disable DirectX, a Windows® technology that enables higher performance when working or viewing graphics and other multimedia contents, including video and sound. By default, DirectX is enabled with the Video feature. You may sometimes need to disable it if, for example, video images are not correctly displayed or are not displayed at all.

NOTE: The system will use more system resources when DirectX is disabled

- **Limit video bandwidth** allows you to reduce or increase the bandwidth required to stream live video without compromising video storage quality and computer performance. The range value is between 64 KB/s to 8192 KB/s. The value will apply to all workstations including the EntraPass Server . However, for any specific workstation, this value can be reduced locally from the Options toolbar > Multimedia Devices > Video .
- **Video vault save delay** is used to indicate the time delay before the video vault recording can be played back.

*NOTE: The workstation value cannot **exceed** the EntraPass Server value.*

HDVR:

- **Video vault save delay** is used to indicate the time delay before the video vault recording can be played back.

TVR:

- **Video vault save delay** is used to indicate the time delay before the video vault recording can be played back.

Time Parameters

The **Time** section allows you to specify which gateway will be used to automatically adjust the time of all the computers connected to the EntraPass server. This feature is very useful when managing remote sites.

NOTE: The gateway polls the first controller on the first site at 5:47 am or 05:47, 1:47 pm or 13:47 and 7:47 pm or 19:47 to get the controller time.

- **No time adjustment** will disable the option.
- **By Gateway** will automatically synchronize the time of all computers with the Gateway selected in the scrolling list.
- **By Server** will automatically synchronize the time of all computers at regular intervals. You must also select the rate of **Hours between refreshes** in the adjacent selection box. The range value is 1 to 9999 hours.

Credentials Parameters

Card

Under the **Card** tab, System Administrators will be able to migrate their EntraPass system to enhanced user management where users are managed by their user name as well as their card number(s). Each card holder will be handled by user name and have up to 5 different numbers. This will allow for creating

cards without assigning card number to the new cards, *see* **Issuing a New Card in Enhanced User Management Environment**This option will be used with the EntraPass Web for card management. For more information on the EntraPass Web, please refer to the *EntraPass Web Help*.

NOTE: Enabling the migrate to enhanced user management is NOT REVERSIBLE through the software . However, when the system is migrating data, a backup is performed in EntraPass, so this can be restored to return to its previous action.

- **Migrate to enhanced user management**: The option is checked by default. EntraPass will migrate to the enhanced user management *(see **Issuing a New Card in Enhanced User Management Environment** for more details)*.

Workstation and Server

Toolbar Buttons

The toolbar buttons size can be increased up to 2.5 times the original size, in order to improve visibility of the text below the button. This is applicable to the EntraPass Server and the EntraPass Workstation. Logout and log back in to apply the change to the toolbar.

Assign a New Connection to a Site

*NOTE: Please refer to **Connection Configuration** for more details*

To enable or disable the feature, select an option:

- **Prompt**: System will prompt the user to specify the site to be connected to (optional) when creating a new connection.
- **Mandatory**: System will prompt the user to specify the site to be connected to (mandatory) when creating a new connection.
- **Disable** (default)

*NOTE: No reference will be made virtual sites unless at least one has been created previously (see **Site Configuration** for details).*

Integration

The **Integration** tab allows the user to select third party hardware that has been integrated to EntraPass by Kantech.

DLL registration: The available DLL in this menu will be used to specify which type of hardware the customer will connect to EntraPass.

- Click on **Add** to integrate another DLL. For additional details, see Integrated Panel Configuration.

*NOTE: The DLL integration **must be done at the EntraPass Server** in order to communicate with the Multi-site Gateway where the third party hardware is physically connected and powered up.*

Virtual keypad: The **Virtual keypad** tab allows the user to customize the virtual keypad screen display. Three different display modes can be selected: **Floating**, **Modal** or **Stay on top**.

Web Interface

Web tab

Use the **Web interface** button to configure EntraPass Web parameters.

- **Allow messages to EntraPass Web**: Select to allow the operator to see messages in EntraPass Web.
- **Maximum web messages**: Select a maximum from the counter.
- **Signature pad pen width**: Select a width value for the pen used with the signature pad.
- **Maximum request simultaneously by session**:Select the maximum number of report requests that can be done simultaneously.
- **Message filter for web messages**: From the drop-down list, select a filter for the messages to be displayed.
- **Badge image ratio for web**: Use the selector to increase the image printing quality (default value is 2). Note that increasing the ratio value will also increase the file size.

Web Customization tab

- **Custom color**: Click to change the color used in the interface (menus perimeter lines for example).
- **Page logo**: Click to insert (or change) a logo in the top left corner of the interface.

go Pass tab

If you register the go Pass mobile application, the **go Pass** tab appears. Use go Pass with a smartphone, or an Apple watch to lock or unlock a door. For convenience, you can control a door from a remote location. For a higher level of security use an ioSmart reader with the door, ioSmart readers use BLE technology. To cater for a range of security levels, select an option from the **Proximity Restriction** list.

1 - To display a cardholder's encrypted personal profile in the notification e-mails, select the **Display viable notification information** check box. Cardholders use their personal profile details or a link in the e-mail to gain access to the go Pass application.

2 - To resend all go Pass notification e-mails to all valid cardholders, click the **Resend go Pass notification for all valid cardholders** button.

3 - To control how and when SmartLink responds to invalid go Pass commands, define all three settings in the **Security** area:

a - To set how many invalid requests occur before SmartLink responds, enter a number in the **Notification debounce on wrong request** field.

a - To set the time to pass before SmartLink responds, enter a number in the **Debounce delay (ss)** field.

b - To prevent SmartLink responding to any go Pass request for a certain amount of time, enter a number in the **Disable go Pass when notification (m:ss)** field.

For example, # of invalid requests within # seconds = # seconds before SmartLink responds to go Pass request + event **Too many go Pass failed requests made** displays.

4 - Select one of the following options from the **Proximity Restriction** list:

- **None** - there is no restriction, the go Pass cardholder can lock, and unlock doors remotely, and at the door. EntraPass ignores BLE technology.
- **Strict (ioSmart BLE only)** – if the go Pass cardholder presents go Pass at an ioSmart reader, the go Pass cardholder has to be within range of the door.
- **Hybrid (BLE when available)** – use for go Pass cardholders who have access to ioSmart readers and non-ioSmart readers. If the go Pass cardholder is at an ioSmart door, the cardholder has to be within range, if it is a non-ioSmart door the cardholder can control the door remotely.

*NOTE: If you fail to select the **BLE** checkbox in the reader template that the controller uses, the **Proximity Restriction** selection is redundant.*

Dealer Information

About Box Details

To add dealer information in the **About** window, select **Display details in About box**.

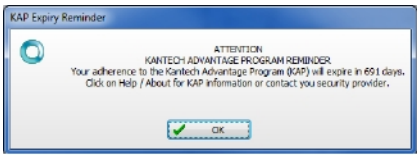
1 - Fill the dealer information and add a picture logo if needed using the Add button.

2 - Fill the **Site information** data..

3 - Click **OK** once finished.

Kap Reminder

A message will be displayed reminding the user that the KAP period is ending. There are two different notifications: a pop-up on the screen or an email containing the following information:



Pop-up Message

A pop-up message is automatically generated by EntraPass to advise the user that his KAP is expiring:

- 60 days before expiration
- 30 days before expiration
- On expiration
- 30 days past expiration

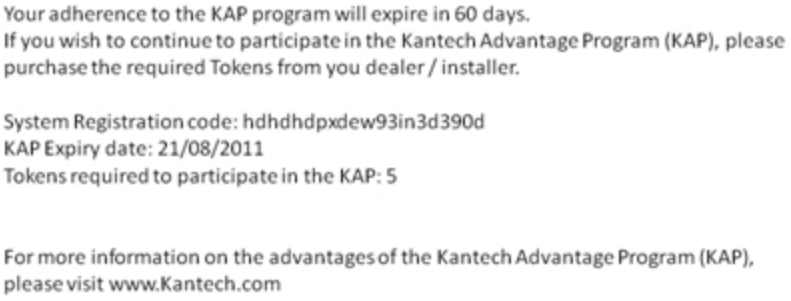
The reminder message has to be acknowledged by the user. It will be logged in the events database (displayed in the Message List) and will appear in reports.

Email

The Dealer Information window has been modified in order to configure the email reminder. Up to 4 recipients can be added. Clicking the Send reminder now button will save the information and send a reminder immediately.

A new event will also be logged in the desktop events list.

Each workstation will also receive a 60 second notification popup message.


Your adherence to the KAP program will expire in 60 days.
If you wish to continue to participate in the Kantech Advantage Program (KAP), please purchase the required Tokens from you dealer / installer.

System Registration code: hdhdhdpxdew93in3d390d
KAP Expiry date: 21/08/2011
Tokens required to participate in the KAP: 5

For more information on the advantages of the Kantech Advantage Program (KAP), please visit www.Kantech.com

NOTE: The Kap Reminder feature can also be accessed from the About window.

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 Server application 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
  - the Mirror Database application, or
  - other third party software and hardware (the third party software is not recommended).

NOTE: By default, when you backup or restore files, the Server databases will temporarily be disabled (not available). The Workstation s will not be able to modify the databases.

The Backup Scheduler program is used to schedule automatic backups of your data, archives, and In/Out databases. Define the default settings and the system will do the rest.

Configuring the Backup when the EntraPass Server is Running as a Service

These steps are required when the EntraPass Server is running as a service and you must backup to another computer **within the same workgroup or domain**.

NOTE: You must have full administrator privileges to perform the following steps at the EntraPass Server. Please refer to the network administrator, if you don't have the privileges or you are not familiar with Windows Administrative Tools.

1 - From the EntraPass Server, go to Options > System Parameters > Server > Service Login Information.

2 - Fill-in all the mandatory fields: Domain name, Login name, Password and Password Confirmation.

NOTE: The Domain Name or the Workgroup must be the same for both, the EntraPass Server and the backup computer.

3 - Click OK.

Scheduling Automatic Backups of the System Database

1 - From the Options toolbar, select the Backup Scheduler button.

2 - Select the tab corresponding to the information you want to backup: Data, Archive, In/Out or Video event (In/Out).

NOTE: By default, the system will automatically backup your files every Sunday at 4:00 AM for all new installations. Setting this feature at 4:00AM has an added benefit of not interfering with the system processing time or other tasks scheduled around midnight.

3 - Select the **Automatic backup** option to enable the options displayed in the window. 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 In/Out (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:\Program files\Kantech\Server\Data or Archive or Time on video or V . 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.

- Under the **Data** tab only:
  - **Separate files** : will backup the databases one by one.
- Under the **Archive, In/Out** and **Video Event** tabs only:
  - **Separate files (full backup)** : will backup all databases.
  - **Separate files (incremental)** : will backup all databases. Only the information that was modified since the last backup will be saved.

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.

7 - Enter the time at which the backup will start (24:00 format).

8 - Select **Now** if you want to perform a backup immediately after saving the backup parameters.

*NOTE: This is not applicable to the **Configure Automatic backup** feature in the **Mirror Database and Redundant Server** application.*

9 - Repeat steps 1 to 8 for all the remaining tabs.

10 - Click **OK** to save.

Custom Messages

The Custom Messages option allows operators with proper security rights to define custom messages that can generate an event based on a schedule. Up to 10 custom messages can be programmed to trigger an event at a preset time. And each custom message can be triggered when the schedule becomes valid, invalid, or both. In other words, you can trigger up to 20 custom events if you take into account the start and/or end of a schedule interval. Each custom events will be displayed in the Messages List on the Desktops.

Setting up Custom Messages

1 - From the **Options** toolbar, click **Custom Messages** .

2 - In the first tab, enter the first custom message you want to see display in the Messages List. Two fields are available for primary and secondary languages.

3 - Select a preset schedule that will determine when the custom event will be triggered.

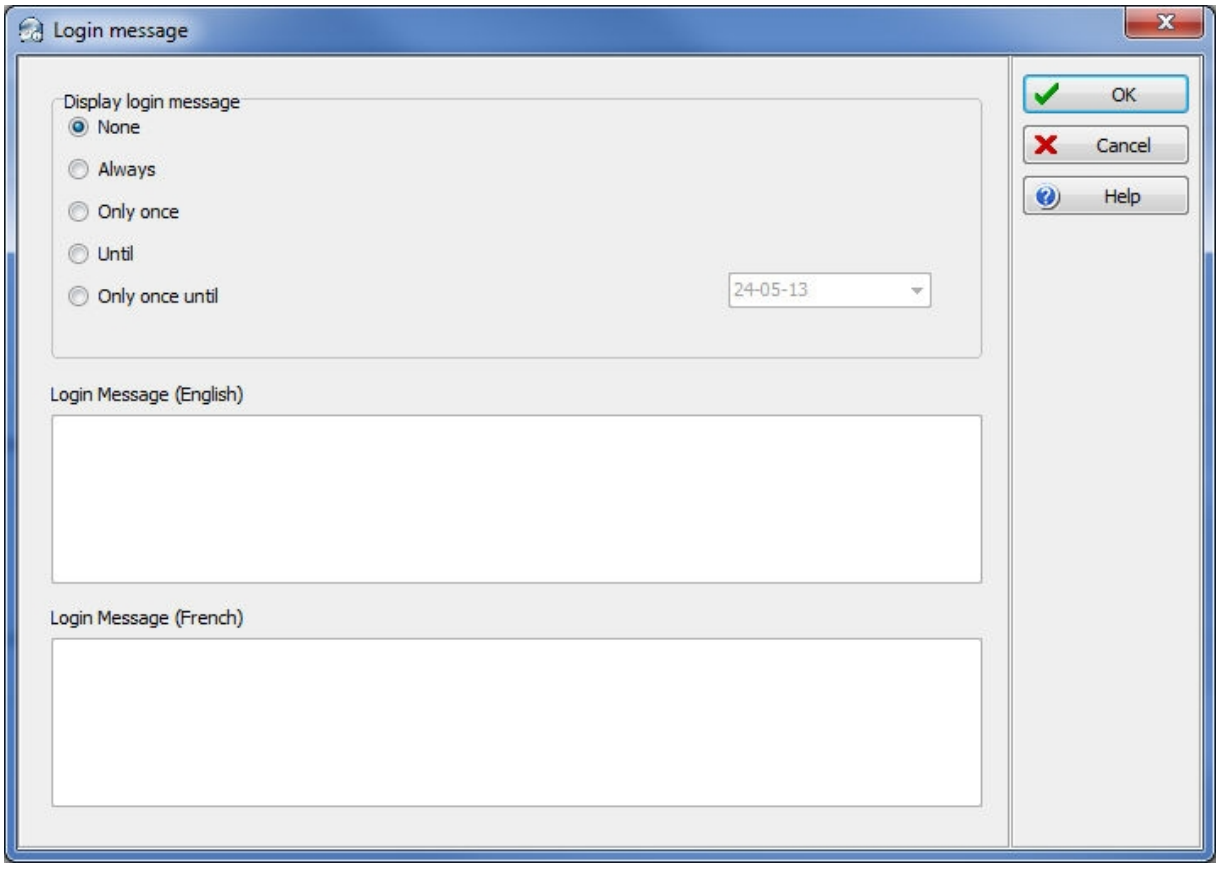
4 - Select if you want the custom event to be triggered when the schedule becomes **Valid** or **Invalid** , or both.

5 - Move to the second tab to enter a second custom message, and so on.

Login Messages

This feature allows entering a text message that will be displayed to other operators when they log into any workstation.

1 - From the **Options** menu, select **Login message**:



2 - Set the recurrence:

- **None**.
- **Always**: The message will always pop-up after login.
- **Only once**: The message will be displayed only once for each operator.
- **Until**: The message will be displayed until the selected date is reached.

- **Only once until**: The message will be displayed once until the selected date is reached or until the operator got the message.

3 - Type a message in the boxes on the right (primary and secondary languages).

4 - Click the **OK** button.

Login/Email message display example:

Personalize the welcome e-mail message that EntraPass, and EntraPass go Pass sends to users and operators. Type a subject heading and choose to type your message in the primary or secondary operator language, or both languages. Complete the following steps:

1 - To write a message that operators see when they log in to any workstation, click the **Login/Email message** icon, and click the **Login message** tab.

2 - To write a welcome message for new EntraPass users, click the **Welcome message** tab.

3 - To write a welcome message for EntraPass go Pass users, click the **go Pass message** tab.

4 - To write a message to a user to explain why EntraPass is disabling their account, click the **Operator disable message** tab.

Configuring a KTES Using Express Setup

When you select a connection type to a **new connection** and immediately **save**, the system prompts you to use the **Express Setup** tool to define the device. You may also launch this tool by selecting a KTES and clicking the **Express Setup** (rabbit button) in the **KTES** dialog.

1 - From the **Site** window, click on **New** to define a new site. Assign it a name for both languages.

2 - Under the **General** tab, select the **Controller type** : **Secure IP (KTES)** .

3 - Click on **Save** , a message box should display: Do you want to use the **Express Setup** program to configure the associated devices. Click **Yes** to continue with the **Express Setup** .

- If you click on **No** , you can always return to the **Express Setup** by clicking on the button.

4 - Check the **Door contact** and the **REX contact** options.

5 - Check the **Postal lock** option, if applicable.

6 - Click the **Advanced** button to define the other devices, such as doors, inputs, relays and outputs.

NOTE: *Components are listed in the left-hand pane. The related tabs are displayed in the middle of the window. When you select a component, its default name, number and default settings are displayed in the language section. Select a component to enable its tab. Components that are assigned are gray and cannot be modified at this stage. However, you may later modify any component description in* ***KTES*** *dialog menu (Devices >* ***Kantech Telephone Entry System*** *).*

Defining Relays

You may configure relays to define their operation mode, activation and deactivation schedules. If you want to assign a name to the relay, you have to select it. When you use the Select All button, the default names are kept.

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** .

3 - In the **Automatic activation schedule** drop-down list, choose the appropriate activation schedule.

4 - In the **Disable relay action** drop-down list, choose the appropriate action.

Defining Inputs

By default, the response time for a REX is 250 ms; it is 500 ms for other input zones. The alarm restore time is 500 ms 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 - Choose the **Input normal state** option.

3 - 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 in the **Definition > Schedule** .

Defining Auxiliary Outputs (LED and Buzzer)

If you want to change their assignment, you may do so while defining a controller or a KTES and in the **Devices > Output.**

1 - Select the first undefined output (its checkbox is not gray). Check its box to enable the language fields, then assign names to it.

2 - Choose the **Operating mode** option.

3 - Assign a door to the output from the **Selected doors** drop-down lists.

The following table summarizes how output zones are used by the system.

Auxiliary output	Use	Controllers

Auxiliary output	Use	Controllers
1	LED (Door 1)	KT-100, KT-200, KT-300 and KTES
2	Buzzer (Door 1)	
3	LED (Door 2)	KT-200 & KT-300
4	Buzzer (Door 2)	
3	LED (Door 1)	KT-400
4	Buzzer (Door 1)	
7	LED (Door 2)	
8	Buzzer (Door 2)	
11	LED (Door 3)	
12	Buzzer (Door 3)	
15	LED (Door 4)	
16	Buzzer (Door 4)	

Database Utility

The Database utility program verifies the integrity of the database tables that are used to store events, alarms, network alarms, and graphics. Basically, the system scans all the system database tables and corrects errors (when they are found). 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 used since the system database is not available during operations on the databases. Some verifications such as re-indexing the archive files, updating database fields, verifying archive files, or swapping database languages require that the EntraPass applications be shutdown. Once all the EntraPass applications that are running on the EntraPass Server computer are closed, you can start the Database utility. When an operation that requires the application to be shutdown is launched, the operator is warned that the database access will be suspended during the operation.

NOTE: The EntraPass Server must be shutdown before you run the database utility.

Running the Database Utility

1 - You can use the buttons under the **Utility** tab in the EntraPass server application, or launch the Database Utility from the Windows® **Start** > **All Programs** > **EntraPass Corporate Edition** > **Workstation** > **Database Utility** .

NOTE: When you select the File > Workstation menu, the system displays only two buttons, the Verify database integrity and the Update database fields buttons. The File > Server menu offers more choices.

Verifying Database Integrity

1 - Click the **Verify database integrity** button in the toolbar. You have the choice to perform a **quick** or a **complete** check.

- **Quick check** : The system scans through the database tables, but does not display a detailed report afterwards.

- **Complete check** : The system scans through the database tables and a detailed report is displayed.

Updating Database Fields

This function is automatically executed when you perform a software is updated. If an operator performs a database restore (**Server** , **Options** toolbar, **Restore**), the database fields are automatically updated when the information is restored. Even when an operator performs a database restore outside the Server (copies the databases from a third party backup program), this function is automatically carried out when the Server is started up again.

1 - From the EntraPass Database utility window, select the **Update database field** button.

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.

Verifying Database Index

The **Verify database Index** program allows to entirely rebuild the database 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.

Verifying 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.

Verifying Database Hierarchy

In EntraPass, the database is set up in a hierarchical way, which means that all components have a parent and can have children 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 connection 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 cannot be fixed, this could mean that the database is too damaged to be fixed. It will be necessary to restore the database.

verifying 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.

Verifying In/Out Files

This function is used to verify In/Out database files. It assigns a new unique sequential value to all primary indexes of In/Out database files.

Verifying Video Event Files

This function is used to verify video event files. It assigns a new unique sequential value to all primary indexes of video event files. Depending on the number of video event files you have, start with the **quick check of the database**, if you get errors then do the **complete check of the database**.

Swapping Descriptions

This function is used to interchange or to swap the database descriptions.

Cleaning the 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.

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.

Rebuilding Card Last Transaction Files

This function is used to rebuild the card last transaction files.

EntraPass Video Vault

The EntraPass Video Vault application addresses the need for optimal video data storage and archive management. This application offers an easy way for collecting important video data for future reference. In fact, video recordings have a limited life span depending on the video server setting and capability. Moreover, since video recordings require a great amount of disk space, using an archive management tool such as EntraPass Video Vault enables organizations to better manage and easily retrieve video contents. EntraPass Video Vault enables EntraPass users to:

- View the status of video archiving requests
- Monitor the status of video servers associated with the active EntraPass Video Vault application
- Monitor video download logs
- Archive video segments
- Use the video vault as a video server gateway.
- Receive event triggers. EntraPass sends an automatic e-mail that contains four thumbnails: one before, one during, and two after the event.

The EntraPass Video Vault application will process the following video segment types:

- Video segments that were triggered by an automated trigger
- Video segments triggered by a manual operation
- Video segments recorded following video server triggers
- Exported video segments tagged for archiving

NOTE: *The EntraPass Video Vault application requires an additional license. It is possible to install more than one EntraPass Video Vault application with EntraPass. Each EntraPass Video Vault must be configured for use with EntraPass (* ***Devices > EntraPass Applications*** *).*

Installing the EntraPass Video Vault

An Option Certificate is required to install EntraPass Video Vault. For details about installing EntraPass advanced options, see **Adding System Components**.

Launching the EntraPass Video Vault

At startup, the EntraPass Video Vault application tries to connect to the EntraPass server. If you are launching the application for the first time, you may need the EntraPass Server's IP address. Also, make sure to launch the EntraPass Server before attempting to run EntraPass Video Vault.

1 - From the shortcut menu on the desktop, or from the Windows® **Start** menu, launch the EntraPass Video Vault application.

- Video Vault root directory: indicates the default folder where video segments are stored. The EntraPass Video Vault root directory is determined when configuring EntraPass Video Vault from the EntraPass environment (**EntraPass workstation application > Devices > EntraPass Applications > EntraPass Video Vault**). The default EntraPass Video Vault root directory is C:\Kantech Video Vault.

- **Current process** : indicates the number of video segments that are being retrieved for archival purposes.

- **(KVI, KVA, AVI, IMG) files archived** : shows the number of video segment files retrieved by EntraPass Video Vault.

- **Default video file format** : the default format for archiving files. This format is defined while configuring video archiving parameters for the EntraPass Video Vault: **EntraPass workstation application > Video > Video server > Video Vault Parameters** tab.

- **Registered Video Server(s)** : indicates the number of video servers associated with he active EntraPass Video Vault application. An EntraPass Video Vault application is associated with a video server when defining the Video Server (**EntraPass workstations application > Video > Video server > Video Vault Parameters** tab).

- **Processing error count** : indicates the number of unsuccessful video archiving processes. To learn why the archiving process was not completed, login to **Video Vault > Action** menu item **> Video Server List** . The **Action** menu item appears only when you have entered a valid operator user name and password. EntraPass enables you to retry retrieving unsuccessful archiving processes from the Video Events List window: **EntraPass workstation application > Video > Video Events List** .

Managing Archived Video Segments

1 - From the EntraPass Video Vault main window, select **System > Login** to launch EntraPass Video Vault and login.

2 - Enter the **User name** and **Password** for EntraPass Video Vault, then click **OK** to close the Operator login window. You cannot log in two EntraPass applications simultaneously using the same user name and password. Since you must run EntraPass Video Vault and the EntraPass server at the same time, make sure to use a different user name for EntraPass Video Vault.

NOTE: To view detailed information about the numerical values displayed on the main window, login to EntraPass Video Vault.

3 - To view the list of Video servers associated with the EntraPass Video Vault application and the status of the archiving process, select the **View Video server** menu item.

- Video server on line, archive period valid : During this period, the EntraPass Server retrieves video segments from the Video server and queues them for archiving by EntraPass Vault. All video segments originating from video triggers (automatic or manual) and segments tagged to be archived in the Video Events List are archived in the EntraPass Video Vault.

- **Video server offline, archive period valid** : This status is tagged with a red flag. It indicates that the EntraPass server cannot retrieve video segments from the Video server for various reasons. Video segments recorded during that period will not be available for EntraPass Video Vault.

- **Video server online, archive period not valid**

- **Video server offline, archive period not valid**

4 - To view the list of drive on which video data have been archived, select the **View drive list** menu item. The Drive list window shows the status of all the files retrieved by EntraPass Video Vault from the Video server.

- Disk ready

- Disk space lower than 100 MB

- Network drive not available

- Cannot access this drive

5 - Select Transaction log to view the list of transaction errors.

NOTE: The transaction log window shows all the transactions that have occurred in the software since the last time it was run. The Filters fields enable users to select the type of transactions to be displayed.

Express Setup Program

The Express Setup program offers a quick and simple way to configure all the components of a system gateway : type of readers used, number of connections, connection name, number of controllers on a connection, etc. For example, it enables users to modify a door's name by automatically applying default settings to all relays and inputs of controllers connected to the selected door.

Configuring a Multi-site Gateway connection Using Express Setup

1 - From Windows® Start menu: Start > **All Programs** > **EntraPass Corporate Edition** > **Workstation/Server** > **Express Setup**. You may also launch Express Setup by clicking the Express Setup button from the registration window or gateway definition window.

2 - From Windows® Start menu: Start > **All Programs** > **EntraPass Global Edition** > **Workstation/Server** > **Express Setup**. You may also launch Express Setup by clicking the Express Setup button from the registration window or gateway definition window.

NOTE: The Operator login window 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 connection, then click the **New connection** button.

5 - Enter the connection name in the **connection description** field, then select the reader type.

6 - Select the **Controller type** for this connection.

NOTE: The KTES option is available for a Multi-site Gateway only.

*NOTE: There is no **reader type** or **number of controllers** to select when the controller type is a KTES.*

7 - Select the **Reader type** .

8 - Set the **Number of controllers** .

9 - Specify the **Connection type** . This indicates how the connection communicates with the gateway computer. The connection types available will follow the controller type selection.

- Select **Direct (RS-232 or USB)** , if the connection 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 connection baud rate (usually set at either 9600 or 19200). The default value is 19200.

- Select **Ethernet (polling)** if the connection communicates with the gateway through a terminal server device (Lantronix) using a port number. Then you have to specify the terminal server's IP Address and Port number . To configure the terminal server, follow the manufacturer's instructions or refer to the terminal server documentation.

- Select **Dial-up (RS-232) modem** if applicable.

- Select **Secure IP (KT-400)** if applicable. Complete the associated tabs.

- Select **Secure IP (KTES)** if applicable. Complete the associated tabs.

- Select **Secure IP (IP Link)** if applicable. Complete the associated tabs.

10 - Click **OK** .

11 - Specify the minimum configuration for the controllers or KTES defined in the site. This includes assigning a name to the controller/KTES, specifying the passback option, and entering the serial number.

*NOTE: The **serial number** column appears only for the KT-100, KT-300, KT-400 controllers and the KTES. The **passback type** column only appears for the KT-300 and the KT-400. 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.*

12 - For a new site with a **KTES** , go to **Step 14** .

13 - Check the **Same door 1 and 2** and **Same door 3 and 4** option if a reader is installed on each side of the door. The **Same door 3 and 4** boxes are available only when you are using KT-400.

14 - Select the appropriate **Passback type** (none, soft or hard). If a door is defined as an access door, there is no anti-passback defined for this door. An entry or an exit door can be assigned a passback option.

15 - Go to **Step 16** .

16 - Check the **Door contact** option.

17 - Check the **Postal lock** option, if applicable, for a KTES only.

18 - Enter the **Serial number** , if this column is displayed. The serial number (**S/N**) is on a sticker and generally starts with **Axxxxxxx** .

19 - Click **OK** . The components associated with the controller and to the site are created in the server database. By default, the KT-200 and KT-300 are assigned two doors except for the KT-400 which is assigned four 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 program.

Controller or KTES	Door	Relay	Input zone	Auxiliary output
KT-100	1	4	4	2
KT-200	2	2	16	4
KT-300	2	2	8	4
KT-400	4	4	16	16
KTES	1	3	4	2
KT-1	1	2	5	5

The following tables summarize how input zones are used by the system for controllers.

Input zone	System use	Controllers
1	Door 1 contact	KT-100, KT-200, KT-300, KT400 and KT-1
2	Door 1 Rex	
3	Door 2 contact	KT-300
4	Door 2 Rex	
5	Door 2 contact	KT-400
6	Door 2 Rex	
9	Door 2 contact	KT-200
10	Door 2 Rex	
9	Door 3 contact	KT-400
10	Door 3 Rex	
13	Door 4 contact	
14	Door 4 Rex	

The following tables summarize how input zones are used by the system for the KTES.

Input zone	System use	Kantech Telephone Entry System
1	Door Contact	KTES
2	Postal Lock	
3	Door Rex	
4	Future	

The following table summarizes how output zones are used by the system.

Auxiliary output	Use	Controllers
1	LED (Door 1)	KT-100, KT-200, KT-300 and KTES
2	Buzzer (Door 1)	
3	LED (Door 2)	KT-200 and KT-300
4	Buzzer (Door 2)	
1	OUT1 (Door 1)	KT-400
2	OUT2 (Door 1)	
3	LED (Door 1)	
4	Buzzer (Door 1)	
5	OUT1 (Door 2)	
6	OUT2 (Door 2)	
7	LED (Door 2)	
8	Buzzer (Door 2)	
9	OUT1 (Door 3)	
10	OUT2 (Door 3)	
11	LED (Door 3)	
12	Buzzer (Door 3)	
13	OUT1 (Door 4)	
14	OUT2 (Door 4)	
15	LED (Door 4)	
16	Buzzer (Door 4)	

Auxiliary output	Use	Controllers
1	OUT1 (Door 1)	KT-1
2	OUT2 (Door 1)	
3	LED (Door 1)	
4	Buzzer (Door 1)	
5	Unassignable	

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 XSF Format,
- The power supervision schedule is always valid,
- The failsoft delay is enabled for 45 seconds,
- The resistor type is **none** (KT-100, KT-300, KT-400 and KTES),
- The wait for second card delay is 30 seconds.

Configuring a Controller Using Express Setup

When you select a connection type to a **new site** and immediately **save** , the system prompts you to use the **Express Setup** tool to define the device. You may also launch this tool by selecting a controller and clicking the **Express Setup** in the **Controller** dialog.

1 - From the **Controller** window, select an undefined controller.

2 - Under the **General** tab, select the **Controller type** .

3 - Click on **Save** , a message box should display: Do you want to use the **Express Setup** program to configure the associated devices. Click **Yes** to continue with the **Express Setup** .

- If you click on **No** , you can always return to the **Express Setup** by clicking on the button.

NOTE: Please note that the KT-300 is a 2-door system while a KT-400 is a four-door system.

4 - Specify if **Both readers are installed on the same door,** if applicable (not for a KTES). When two readers are installed on the same door, the REX contact option is disabled.

5 - Click the **Advanced** button to define the other devices, such as doors, inputs, relays and outputs.

*NOTE: Components are listed in the left-hand pane. The related tabs are displayed in the middle of the window. When you select a component, its default name, number and default settings are displayed in the language section. Select a component to enable its tab. Components that are assigned are gray and cannot be modified at this stage. However, you may later modify any component description in its definition menu (Devices > **Controller/Door/** Relay / Input / Output).*

Configuring a KTES Using Express Setup

When you select a connection type to a **new site** and immediately **save**, the system prompts you to use the **Express Setup** tool to define the device. You may also launch this tool by selecting a KTES and clicking the **Express Setup** (rabbit button) in the **KTES** dialog.

1 - From the **Site** window, click on **New** to define a new site. Assign it a name for both languages.

2 - Under the **General** tab, select the **Controller type** : **Secure IP (KTES)** .

3 - Click on **Save** , a message box should display: Do you want to use the **Express Setup** program to configure the associated devices. Click **Yes** to continue with the **Express Setup** .

- If you click on **No** , you can always return to the **Express Setup** by clicking on the button.

4 - Check the **Door contact** and the **REX contact** options.

5 - Check the **Postal lock** option, if applicable.

6 - Click the **Advanced** button to define the other devices, such as doors, inputs, relays and outputs.

NOTE: Components are listed in the left-hand pane. The related tabs are displayed in the middle of the window. When you select a component, its default name, number and default settings are displayed in the language section. Select a component to enable its tab. Components that are assigned are gray and cannot be modified at this stage. However, you may later modify any component description in ***KTES*** *dialog menu (Devices >* ***Kantech Telephone Entry System*** *).*

Defining Relays

You may configure relays to define their operation mode, activation and deactivation schedules. If you want to assign a name to the relay, you have to select it. When you use the Select All button, the default names are kept.

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** .

3 - In the **Automatic activation schedule** drop-down list, choose the appropriate activation schedule.

4 - In the **Disable relay action** drop-down list, choose the appropriate action.

Defining Inputs

By default, the response time for a REX is 250 ms; it is 500 ms for other input zones. The alarm restore time is 500 ms 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 - Choose the **Input normal state** option.

3 - 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 in the **Definition > Schedule** .

Defining Auxiliary Outputs (LED and Buzzer)

If you want to change their assignment, you may do so while defining a controller or a KTES and in the **Devices > Output.**

1 - Select the first undefined output (its checkbox is not gray). Check its box to enable the language fields, then assign names to it.

2 - Choose the **Operating mode** option.

3 - Assign a door to the output from the **Selected doors** drop-down lists.

The following table summarizes how output zones are used by the system.

Auxiliary output	Use	Controllers
1	LED (Door 1)	KT-100, KT-200, KT-300 and KTES
2	Buzzer (Door 1)	
3	LED (Door 2)	KT-200 & KT-300
4	Buzzer (Door 2)	
3	LED (Door 1)	KT-400
4	Buzzer (Door 1)	
7	LED (Door 2)	
8	Buzzer (Door 2)	
11	LED (Door 3)	
12	Buzzer (Door 3)	
15	LED (Door 4)	
16	Buzzer (Door 4)	

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 ***Server Utilities****.*

1 - From the Windows® Start menu, click Start > **All Programs** > **EntraPass Corporate Edition** > **Workstation/Server > PING Diagnostic** .

2 - From the scrolling list, select the application you want to monitor (Server, Workstation, Gateway, etc.).

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 your 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)

Quick Report Viewer

The **Quick Report Viewer** program allows operators to view previously saved reports without having to start EntraPass. It is used to view / display / load reports that were previously saved (in a.QRP format) during a print preview or Quick reports. For details on requesting and generating reports, see **Requesting Reports**. This program is useful when EntraPass is off-line and when a report must be displayed for specific purposes.

1 - From the Windows® task bar, click Start > All Programs > EntraPass > Server > Quick Report **Viewer** .

2 - Click the **Open** button to open a report. The system displays the **Open** window:

3 - By default, when a report is saved in a QRP format, the system automatically saves it in "My Documents" folder. If you have saved the report in another folder you have to browse to the folder to select the report.

4 - Click **Open** to preview the report. Once you have selected the requested report, the system will display your report:

5 - Use the toolbar buttons to preview the report:

Icon	Description
	Use the Zoom out button to zoom out the report view.
	Use the Zoom In button to display details (view closer).
	Use Previous Page and Next Page buttons to change pages.
	Use the Open button to open a report located in any folder on your computer.
	Use the Print button to print the report. There will be no printer setup dialog box, the report will automatically print, to cancel the printing, click Cancel.
	Use the Quit button to quit the application.

The SmartLink Interface

The SmartLink interface allow a user to define a message and format type that may be sent on the second COM port or to a disk file. The following pages explain how to build a character string that can be sent through the SmartLink. Using the SmartLink feature, you can interface to just about any intelligent device such as video matrix switchers, paging systems, etc. To do this, a RS-232 link is cabled between one of the EntraPass Workstation and the external device. The necessary command strings and protocols can be easily edited on connection to fit just about any job.

The SmartLink simplifies the interfacing to "alien" intelligent devices because it provides the system installer all the tools necessary to build and maintain the actual interface without having to purchase "special" drivers from Kantech. In communications, a link is a line or channel over which data is

transmitted. The transmission of data from one computer to another, or from one device to another. A communications device, therefore, is any machine that assists data transmission. For example, modems, cables, and ports are all communications devices.

Required Material

- A computer that meets the same requirements as an EntraPass Workstation (see **Minimum System Requirements**).
- Installation CD-ROM for the SmartLink application including the serial number.

Installation

1 - Create the new application in the Workstation Registration menu, see **Minimum System Requirements** for more information on how to create new applications,

2 - Install the SmartLink application on the computer (see **System Installation**).

*NOTE: EntraPass Web will be installed automatically with **SmartLink**.*

3 - Once the SmartLink application is installed, you need to configure the SmartLink application,

4 - If you are using the Message Mode, you will need to create tasks. For more information on how to create tasks with the Task Builder, see **Task Builder Definition**.

Configuring the SmartLink Application

The configuration is done on an ordinary EntraPass workstation or any EntraPass Workstation for configuration (found on the same computer as the Server software). Depending on the modes that will be used for the SmartLink (Messages or Commands), you must program the workstation accordingly.

Starting the SmartLink Application

1 - From the computer where the SmartLink application is installed, click on the Windows® task bar and select **Start > All Programs > EntraPass > SmartLink > SmartLink** . The SmartLink application will be started. Refer to the *SmartLink Reference Manual DN1327* for more information on the SmartLink Application.

2 - The application user interface includes status information about the Smartlink application.This information allows installers to quickly identify any issues with the system.

NOTE: *Limited support is provided on the SmartLink interface.*

Vocabulary Editor

The Vocabulary Editor allows users to translate the display text of the software in the language of their choice. EntraPass offers you the possibility of adding up to 99 languages for the purpose of changing the text language in the graphic user interface. However, you can only run the software in two languages at a time, a primary and a secondary language. If you want to use the software in a language other than English, French, German, Italian or Spanish, you can have the database dictionary translated in the language of your choice. You will then have to integrate the translated dictionary in the software. The creation of a new display language is carried out in three stages:

- Translating the source text,
- Integrating the newly created language to the EntraPass dictionary in the Server,
- Distributing the new custom language to all EntraPass application.

NOTE: *In order to be able to run a new language, your operating system (Windows ®) must support the desired language. For example, your keyboard (characters) and window (display) must support the specific characters of the desired language. The computers where EntraPass applications are running must also support the language. For more information on language support, refer to your system administrator.*

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 just have to select it in the Setup window. For more information, see* ***System Installation****.*

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 Italian or German.

1 - Start the Vocabulary editor from the Windows® **Start** menu: click Start > **All Programs** > **EntraPass Corporate Edition** > **Vocabulary Editor** > **Vocabulary Editor** .

2 - Select one of the **available languages** and click on **New** . The system displays the **Select language** window.

3 - 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.

4 - Click on the new **Custom Language** and then on the **Edit custom language** 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\"Application type"\CustomDictionary\files.xxx.0

The table below shows the value of the Vocabulary Editor colour codes.

VOCABULARY EDITOR colour CODES	VALUE
Green	Valid text string.
Blue/Green	New text string.
Red	Obsolete text string.

- The "Source language" column contains text based on the basic language that was selected during the creation of the vocabulary. This column will serve as a "source" for the translation. Software language columns cannot be modified by the user.

- Use the right-click to enable a contextual sub-menu or use the **Language editor** toolbar. A hint appears when you position the mouse over a button.

Integrating the 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. The table below describes the buttons action in the vocabulary editor dialog. These options can also be selected from the **Actions** menu.

Icon	Description
	Apply changes to operational dictionary : this option is useful when you want to test your changes before you update other workstations.
	Restore 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.
	Create self-extracting file for update: If you decide to implement the new vocabulary. The system creates an **Updatedictionary.exe** file, and prompts you to select a destination folder for the file.

1 - Start the Vocabulary Editor. The Vocabulary Editor window toolbar displays five buttons.

NOTE: The Graphic User Interface will only appear in one of five languages: English, French, German, Italian 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 Redundant 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 Redundant server, then start the Mirror database.

Updating the System Vocabulary

1 - Exit all EntraPass programs.

2 - Start **Windows Explorer ®** > **Kantech** > (**EntraPass application**), then copy the **Updatedictionary.exe** on the server.

3 - Double-click **Updatedictionary.exe.** The system displays the EntraPass applications that are installed on the computer.

4 - Select each application, then click the **Update dictionary** button.

5 - You have to copy **Updatedictionary.exe** on every computer where EntraPass is installed, and then double-click it in order to launch the language update. To do so, you have first to exit all EntraPass applications before you run the self-extracting file.

6 - Select the application you want to update (one at a time) and click **Update dictionary** button. The system will automatically copy the vocabulary to the **Custom Dictionary** directory then merge the custom directory with the application dictionary.

*NOTE: You **MUST** update all the applications in the system.*

NOTE: *To restore the dictionary back to original default values, follow the same procedures as for updating the dictionary.*

7 - Once you have finished updating the dictionary database for the Primary Server, the Mirror Database and the Redundant Server, start the Primary server.

8 - Select the **Options** toolbar, then select the **Select language** button.

9 - In the **Select the language** window, select the primary language and the secondary language. The newly integrated language is displayed in the list. It is important to select the language at this stage, otherwise the operators of the system will not be able to use it.

NOTE: *For example, if your primary language is "English" and your secondary language is "French": if you select your new language (i.e. Russian) as primary, all operators who have "English" as their display language in the Operator menu will be modified to "Russian". On the other hand, if you change the secondary language to "Russian" and operators are using "English", you will have to manually select "Russian" in the Operator definition menu". To assign the desired language to an operator, use the System definition menu, then select the Operator definition menu.*

10 - Before you update all the applications, 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.*

EntraPass Icons

Animated icons indicate the status of physical or logical components in the windows of EntraPass software. They represent the component status in real time and simulate a movement by displaying a series of pictures associated with the component. If a particular component status is difficult to identify, use this section to identify it.

Alarm Systems

Alarm system icons indicate the status of an alarm system within the Graphic desktop (Desktop > Graphic desktop) or in the “Operation” window.

Alarm system is in alarm

This animated icon appears when the alarm system is in alarm. It is displayed in:

- the Alarm message box when an acknowledgement is required.
- the “Operation” window
- the Desktop > Graphic desktop.

Alarm system is armed

This animated icon appears when the alarm system is armed. It is displayed in:

- the Operation window
- the Desktop > Graphic desktop.

Alarm system is armed with input in alarm (forced arming)

This animated icon appears when arming the alarm system while a surveillance area is in alarm. The system will allow you to arm the system (forced armed) and the icons will display the input in alarm in:

- the Operation window
- the Desktop > Graphic desktop.

Alarm system is in arming request delay

This animated icon appears when the alarm system in the “arming request” delay (waiting for confirmation with the arming request input button). It is displayed in:

- the “Operation” window
- the Desktop > Graphic desktop.

Alarm system is disarmed

This animated icon appears when the alarm system is disarmed. It is displayed in:

- the “Operation” window.
- the Desktop > Graphic desktop.

Alarm system is in entry delay

This animated icon appears when the alarm system is in “entry” delay. It is displayed in:

- the “Operation” window.
- the Desktop > Graphic desktop.

Alarm system is in “Exit” delay

This animated icon appears when the alarm system is in “exit” delay. It is displayed in:

- the “Manual Operation” window.
- the Desktop > Graphic desktop.

EntraPass Icons

Alarm system status is not yet known

This animated icon appears when the status of the alarm system is unknown. It is displayed in:

- the “Graphic” window (the Desktop > Graphic desktop) when the status of the alarm system is unknown.

Alarm system is in “Postpone” mode

This animated icon appears when the alarm system is in “postpone” mode. Once this delay is over, the system will initiate the exit delay and arm again (if the “no disarm” schedule is still valid). It is displayed in:

- the Operation window.
- the “Graphic” window (the Desktop > Graphic desktop).

Controllers

Controller animated icons indicate the status of a door controller in the graphic window (Desktop > Graphic desktop) or in the “Operation” window.

Status unknown

Appears when the EntraPass application has not received the component status after four (4) attempts. It is displayed in:

- the Operation window (alarms, areas, guard tours, door, elevator door, relay, input, reload data)
- or the Desktop > Graphic desktop.

Controller AC failure

Appears when the controller is in AC failure. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset

Controller Polling Malfunction

Appears when the controller polling function is malfunctioning. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller

Controller AC failure and Tamper Switch in “alarm”

Appears when the controller is in AC failure and the tamper switch is in alarm. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset

Controller is not communicating

Appears when the controller is not communicating. It is displayed in:

- the “Operation” — “Area”, “Guard Tour” and “Controller Reset” windows. “Controller Reset” windows. “Controller Reset” windows.
- the Desktop > Graphic desktop.

Controller communication is regular (no problem)

Appears when the controller is communicating and the communication is regular. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset.

Controller is in “Reset” and AC failure

Appears when the controller is in “reset mode” and in “AC failure”. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset.

Controller is in “Reset”, “AC failure” and “Tamper in alarm”

Appears when the controller is in “reset mode”, in “AC failure” and the tamper is in alarm. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset

Controller is in reset and tamper in alarm

Appears when the controller is in “reset mode” and the tamper is in alarm. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset.

Controller tamper in alarm

Appears when the controller tamper is in alarm. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset when the controller tamper is in alarm.

Controller reloading firmware

Appears when the controller is reloading firmware. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset.

KT-400 controller trouble

Appears when there is a KT-400 controller trouble. It is displayed in:

- the Desktop > Graphic desktop
- the Operation > Controller.

Doors

Icons representing a door state indicate the status of door within the graphic window (from the desktop) or within the “Operation” window.

Door forced open

This animated icon appears when the door is opened and that no access granted nor request to exit was permitted. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door, Elevator Door

Door forced open (reader disabled)

This animated icon appears when the door is opened and that no access granted nor request to exit was permitted and the reader is disabled. it is displayed in:

- the “Graphic” window (desktop—graphic)
- the Operation > Door, Elevator Door

Door closed and locked

This animated icon appears when the door is closed and locked. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door

Door closed and locked (reader disabled)

This animated icon appears when the door closed and locked and that the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door.

Door open too long

This animated icon appears when the door is opened more than the permitted delay set in “open time”. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door, Elevator door.

Door open too long (reader disabled)

This animated icon appears when the door is opened more than the permitted delay set in “open time” and that the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door, Elevator door.

Door open and unlocked manually

This animated icon appears when the door is opened and it was unlocked by an operator. it is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door.

Door open and unlocked manually (reader disabled)

This animated icon appears when the door is opened and it was unlocked by an operator and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)

- the Operation > Door > Elevator door.

Door is opened and unlocked by schedule

This animated icon appears when the door is opened and it was unlocked by a schedule. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door.

Door is opened and unlocked by schedule (reader disabled)

This animated icon appears when the door is opened, and it was unlocked by a schedule and the reader is disable. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door.

Door pre-alarm on open too long

This animated icon appears when the door is opened more than half the time permitted delay set in “open time”. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door.

Door pre-alarm on open too long (reader disabled)

This animated icon appears when the door is opened more than half the time permitted delay set in “open time” and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door.

Door still opened schedule invalid

This animated icon appears when the door is opened and the unlock schedule is invalid. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door.

Door still opened schedule invalid (reader disabled)

This animated icon appears when the door is opened and the unlock schedule is invalid and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/ Elevator door.

Door unlocked by an operator

This animated icon appears when the door is unlocked by an operator (manually). It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door.

Door unlocked by an operator (reader disabled)

This animated icon appears when the door is unlocked by an operator (manually) and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door.

Door unlocked by a schedule

This animated icon appears when the door is unlocked by a schedule. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door.

Door unlocked by a schedule (reader disabled)

This animated icon appears when the door is unlocked by a schedule and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door.

Elevator door unlocked and closed

This animated icon appears when the elevator door is closed and unlocked. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door.

Wireless Lock Connected

This icon appears when the wireless lock is connected. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)

- the Operation > Integrated Panel/Wireless Lock.

Wireless Lock Error

This icon appears when the wireless lock has an error associated with it. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Integrated Panel/Wireless Lock.

Relays

Relays icons indicate the status of a relay within the graphic window (from the desktop) or within the "Operation" window.

Relay activated by an event

This animated icon appears in:

- the "Graphic" window (desktop—graphic) when the relay is triggered by an event.
- the Operation > Relay when the relay is triggered by an event.

Relay temporarily activated by an event

This animated icon appears in:

- the "Graphic" window (desktop—graphic) when the relay is temporarily activated by an event.
- the Operation > Relay when the relay is temporarily activated by an event.

Relay activated by an input

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is triggered by an input.
- the Operation > Relay when the relay is triggered by an input.

Relay temporarily activated by an input

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is temporarily activated by an input.
- the Operation > Relay when the relay is temporarily activated by an input.

Relay activated by an operator

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is activated by an operator.
- the Operation > Relay when the relay is activated by an operator.

Relay temporarily activated by an operator

This animated icon appears in:

- the “Graphic” window (desktop—graphic) for a relay temporarily activated by an operator.
- the Operation > Relay when the relay is temporarily activated by an operator.

Relay temporarily activated by a schedule

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is activated by a schedule.
- the Operation > Relay when the relay is activated by a schedule.

Relay deactivated

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the relay is not activated.
- the Operation > Relay when the relay is not activated.

Inputs

This section is used to indicate the status of an input within the graphic window (from the desktop) or within the “Operation” window.

Input activated—Not supervised

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is activated and the monitoring schedule is invalid.
- the Operation > Input when the input is activated and the monitoring schedule is invalid.

Input activated—Supervised

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is activated and the monitoring schedule is valid.
- the Operation > Input when the input is activated and the monitoring schedule is valid.

Input activated—Not supervised manual operation

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is activated, manually operated and the monitoring schedule is invalid.
- the Operation > Input when the input is activated, manually operated and the monitoring schedule is invalid.

Input activated—Supervised manual operation

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is activated, manually operated and the monitoring schedule is valid.
- the Operation > Input when the input is activated, manually operated and the monitoring schedule is valid.

Input activated—Supervised temporarily manual operation

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is activated, manually operated and the monitoring schedule is temporarily valid.
- the Operation > Input when the input is activated, manually operated and the monitoring schedule is temporarily valid.

Input in alarm—Not supervised

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in alarm and the monitoring schedule is invalid.
- the Operation > Input when the input is in alarm and the monitoring schedule is invalid.

Input in alarm—Shunted by operator

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in alarm and it is shunted by an operator.
- the Operation > Input when the input is in alarm and it is shunted by an operator.

Input in alarm—Supervised

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in alarm and the monitoring schedule is valid.
- the Operation > Input when the input is in alarm and the monitoring schedule is valid.

Input in alarm—Supervised by operator

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in alarm and it is supervised by an operator (continuous supervision).
- the Operation > Input when the input is in alarm and it is supervised by an operator (continuous supervision).

Input OK—Not supervised

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in normal condition and the monitoring schedule is invalid.
- the Operation > Input when the input is in normal condition and the monitoring schedule is invalid.

Input OK—Shunted by operator

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in normal condition and it is shunted by an operator.
- the Operation > Input when the input is in normal condition and it is shunted by an operator.

Input OK—Supervised

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in normal condition and the monitoring schedule is valid.
- the Operation > Input when the input is in normal condition and the monitoring schedule is valid.

Input OK—Supervised by operator

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the input is in normal condition and it is supervised by an operator (continuous supervision).
- the Operation > Input when the input is in normal condition and it is supervised by an operator (continuous supervision).

Controller connection

These icons indicate the status of a connection, or gateway within the graphic window (from the desktop) or within the “Operation” window.

Connection status is not yet known

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the status of the controller connection is not yet known.

Controller connection connected

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the connection is connected and communication is OK.
- the Operation > Reload data when the connection is connected and communication is OK.

Controller connection connected and in “Reload Data”

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the connection is connected and is in “reload data” state.
- the Operation > Reload data when the connection is connected and is in “reload data” state.

Controller connection—Communication Failure

This animated icon appears in:

- the “Graphic” window (Desktop—graphic) when the connection is disconnected and there is a communication failure.

- the Operation > Reload data when the connection is disconnected and there is a communication failure.

Gateways

Gateway—Communication Failure

This animated icon appears in:

- the “Operation” (door, elevator door, relay, input, reload gateway) window when the gateway is in communication failure.
- the “Graphic” window (desktop—graphic) when the gateway is in communication failure.

Gateway in “Reload Data”

This animated icon appears in:

- the “Graphic” window (Desktop—graphic) when the gateway is being reloaded.
- the Operation > (door, elevator door, relay, input, reload gateway) when the gateway is being reloaded.

Gateway—Communication Failure during Reload Data

This animated icon appears in:

- the “Operation” (reload data gateway) window when the gateway loses communication during a reload data operation.
- the “Graphic” window (desktop—graphic) when the gateway loses communication during a reload data operation.

Gateway communication is regular (no problem)

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the gateway is communicating and the communication is regular.
- the Operation > Reload data gateway, communication is regular.

Gateway Trouble

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the gateway is not communicating.
- the Operation > Reload data gateway, the gateway is not communicating.

Gateway Trouble when Reloading

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the gateway is not communicating.
- the Operation > Reload data gateway is not communicating with the gateway during a reload data operation.

Gateway (Gateway Software Interface):

Gateway OK—communicating

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the gateway is communicating.
- the Operation > Reload data when the gateway is communicating.

Gateway in “Reload Data”

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the gateway is being reloaded.
- the Operation > Reload data when the gateway is being reloaded.

Gateway—Communication Failure

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when gateway is not communicating.
- the Operation > Reload data when the gateway is not communicating.

EntraPass Application

Application status is not yet known

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the status of the application is not yet known.

Application attempts communication

This animated icon appears in:

- the start-up window when the workstation attempts to communicate with the server.

Application—Communication Failure

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the workstation is in communication failure.
- the “Operation” window (alarm, area, guard tour, door, elevator door, relay, input, reload gateway) when the workstation is in communication failure.

Others

Database Initialization

This animated icon appears in:

- the start-up window when the workstation initializes the database.

Data not available

This animated icon is used to indicate a transient stage. This could indicate that the requested information is not currently available.

No status available

This animated icon is used to indicate a transient stage. This could indicate that the requested component status is not currently available.

Output status is not yet known

This animated icon appears in:

- the “Graphic” window (desktop—graphic) when the status of the output is not yet known.

Status unknown

This animated icon appears in:

- the “Operation” (alarms, areas, guard tours, door, elevator door, relay, input, reload) window when the workstation has not received the component status after four (4) attempts.
- the “Graphic” window (desktop—graphic) when the workstation has not received the component status after four (4) attempts.

Error in process

This animated icon appears in:

- the “Operation” (alarms, areas, guard tours, door, elevator door, relay, input, reload data) window when a specific error is detected.
- the “Graphic” window (desktop—graphic) when a specific error is detected.

Undefined Component

This animated icon appears in:

- the “Operation” window (alarm, areas, guard tour, door, elevator door, relay, input, reload data gateway) when the component does not exist.
- the “Graphic” window (desktop—graphic) when the component does not exist.

© 2019 Tyco Security Products. All rights reserved.