

EntraPass Global Edition Administration Guide



Building Technologies & Solutions

www.kantech.com

2024-02-01

A16382C604-A

8.71



A16382C604-A

Contents

EntraPass Global Edition.....	21
Privacy notice.....	22
Copyright.....	22
Release Notes 8.71.....	23
New features.....	23
Technical support.....	24
How to.....	26
How to create a backup.....	26
How to create a badge.....	26
How to create a card.....	26
How to create a schedule.....	27
How to create a simple report.....	27
How to create an access level.....	27
How to print a list of cards.....	27
How to print a list of access levels.....	28
How to print a list of doors.....	28
How to set up desktops.....	28
How to use shortcut keys.....	28
How to personalize the web logon window.....	29
How to deactivate connections and controllers.....	29
How to enable go Pass for a user.....	29
How to migrate from event parameter to event operator mode.....	30
How to set the database to read-only mode manually.....	31
How to schedule a technician appointment.....	32
How to enable EntraPass maintenance mode.....	32
How to set up the ioSmart.....	33
How to configure an ioSmart reader on the operation tab.....	33
FAQ.....	34
Introduction.....	38
What is EntraPass?.....	38
Kantech Advantage Program (KAP).....	38
SmartLink.....	39
Mirror database and redundant server.....	39
KT-NCC controller and gateway.....	39
Dual gateways option.....	39
Redundant gateway.....	39
Wireless door license.....	39
Kantech IP Link.....	40
KT-100, KT-200, KT-300, KT-1, KT-2, and KT-400 controllers.....	40
KT-400 controller.....	40
Expansion modules for the KT-400.....	40

Kantech ioSmart card reader.....	40
Kantech Telephone Entry System.....	40
Express setup.....	41
hatrix for managed access control.....	41
Elevator control capability.....	41
Integrated badging.....	41
Interactive floor plans.....	41
Configurable desktops by operator.....	41
Interfacing with external alarm panels.....	41
Partitioning alarm system.....	41
In/Out feature.....	41
Muster reporting for parking and emergency management.....	42
Visual diagnostics.....	42
Enhanced video integration.....	42
EntraPass video vault.....	42
Vocabulary editor.....	42
Intrusion integration.....	42
Installation.....	43
Minimum system requirements.....	43
Operating system compatibility.....	43
Web Server.....	43
hatrix.....	43
Workstation and Gateway applications with NCC.....	44
DOS application ONLY.....	45
Additional requirements.....	45
Security hardening guide.....	45
System installation.....	45
System registration.....	47
Registering the system.....	47
Adding system components.....	49
Windows services.....	50
System components edition.....	51
Assigning a descriptive name to an application.....	51
Getting started.....	52
Accessing an account under hatrix.....	52
Switching account and security level.....	52
Basic functions.....	52
Finding components.....	52
Using the extended selection box.....	54
Selecting components.....	54
Printing a list or report.....	55
Viewing component links.....	55
Floating windows.....	56

System tree view.....	56
Using the comment field as a notepad.....	57
Deleting an item.....	58
Viewing component links.....	58
EntraPass toolbar.....	58
Express setup.....	59
Session Start and End.....	60
Starting the EntraPass server.....	60
Starting the Gateway Program.....	61
Starting the EntraPass workstation.....	62
Accessing an account under hattrix.....	62
Switch Account and Security Level.....	62
Accessing Information on the Server Workstation Connection Status.....	62
Modifying your Work Area Properties.....	63
Retrieving hidden windows on the desktop.....	63
Using the extended selection box.....	63
Desktops.....	64
Alarms Desktop.....	64
Defining an Alarms Desktop.....	64
Viewing System Alarm Messages.....	65
Displaying Alarm Desktops Automatically.....	66
Acknowledging Alarms/Events.....	67
Automatic Acknowledgement.....	67
To Acknowledge an Alarm Message.....	67
To Acknowledge Alarms from the Alarms Desktop.....	68
Mandatory Alarm Comment.....	68
Changing desktop events.....	68
Changing the Display Properties.....	68
Custom report desktop.....	69
Configuring a custom reports desktop.....	69
Comment entry and display.....	70
Playing archived video recordings from a desktop message list.....	70
Customizing event display in the message desktops.....	70
Defining a system search desktop.....	71
Filtered Messages Desktop.....	72
Configuring a Filtered Messages Desktop.....	72
Graphic desktop.....	72
Viewing Graphics in the Graphic Desktop.....	73
Area graphic.....	75
Area empty.....	75
Area card list.....	75
Monitoring an Area Group for Muster Reporting.....	77
Message List Desktop.....	77

Viewing and Sorting System Events.....	77
Customizing event display in the message desktops.....	78
Performing Tasks on System Messages.....	79
Add, Modify, or Delete Tagged Events.....	80
Picture Desktop.....	81
Modifying Pictures Display Options.....	81
Specific desktop customizing.....	82
Customizing a desktop for a “full access” operator.....	82
Customizing a desktop for a “read-only” operator.....	83
hatrix additional search capability.....	83
Transferring a customized desktop.....	84
Desktop colors.....	84
Status.....	85
Application Status.....	85
Database status.....	86
Graphic Status.....	87
Viewing a Controller Status.....	87
Numerical Status.....	88
Server State.....	89
Logins.....	90
Text Status.....	90
Displaying a Component Status.....	90
Video server status.....	91
Viewing the video server's full status.....	91
Operations.....	93
Manual operations on alarm systems.....	93
Performing Manual Operations on an Alarm System.....	93
Arming an Alarm System Manually.....	94
Disarming an Alarm System Manually.....	94
Modifying the alarm system postponement delay manually.....	94
Manual operations on areas.....	94
Card location.....	95
Manual operations on controllers.....	95
Selecting a controller.....	96
Performing a controller soft reset.....	97
Performing a controller hard reset.....	97
Reloading a controller manually.....	97
Manually reloading controller firmware.....	97
Manually clearing buffered events.....	97
Manually unlocking a reader keypad.....	97
Manually resetting a reader power.....	98
Resetting Cards In and Cards Out counters or all controller local areas.....	98
Calculating the number of Cards In and Cards Out.....	98

Card location.....	98
Requesting unassigned modules.....	98
Full status.....	99
Module status.....	99
Edit.....	99
Manual operations on doors.....	99
Selecting a Door or a Door Group.....	100
Manually locking a door.....	100
Manually unlocking a door.....	100
Temporarily unlocking a door.....	100
Resetting a door schedule.....	101
Enabling a door reader.....	101
Disabling a door reader.....	101
Modifying access level schedules.....	101
Manual operations on elevator doors.....	101
Selecting an elevator door.....	103
Locking floors or floor groups from elevator doors.....	103
Unlocking floors or floor groups from elevator doors.....	103
Temporarily unlocking floors or floor groups from elevator doors.....	104
Unlocking a floor or floor group for one-time access.....	104
Resetting an elevator door schedule.....	104
Enabling an elevator floor.....	105
Disabling an elevator floor.....	105
Manual operations on gateway.....	105
Selecting a gateway.....	106
Viewing gateway statistics.....	106
Updating physical components.....	106
Performing a hard reset.....	106
Reloading gateway data.....	106
Broadcasting.....	107
Forcing a firmware reload.....	107
Redundant gateway operations.....	107
Manual operations on guard tours.....	107
Starting a Guard Tour.....	108
Manual operations on inputs.....	109
Performing Manual Operations on Inputs.....	109
Returning an Input to Its Normal State Manually.....	110
Setting Up Continuous Input Supervision.....	110
Stopping Monitoring an Input.....	110
Stopping Input Supervision (Shunt) Temporarily.....	110
Manual operations on integrated panels.....	110
Manual operations on action scheduler.....	111
Programming the Action scheduler.....	111
The KT-NCC, Global Gateway and the Action scheduler.....	113

Programming the Action scheduler from the Door or Relay windows.....	113
Printing the Action scheduler calendar.....	113
Manual operations on relays.....	113
Selecting relays.....	114
Deactivating a relay manually.....	114
Activating a relay manually.....	114
Activating a relay temporarily.....	114
Resetting a relay schedule.....	115
Manual operations on sites.....	115
Performing manual operations on a site/connection.....	116
Communication status messages available in the list.....	116
Manual operations on view roll call.....	116
Users.....	118
Access exception.....	118
Access levels definition.....	118
Badge designing.....	119
Creating a badge template.....	119
Badge Sample in hattrix Credential.....	125
Printing badges.....	125
Batch Operations on Cards.....	126
Performing Operations on a Group of Cards.....	126
Card access groups definition.....	127
Card Filter Definition.....	128
Card Printing.....	128
Card Type Definition.....	130
Creating a New Card Type.....	130
Adding Comments to a Card.....	130
Limiting Card Usage.....	130
Cards definition.....	130
Issuing a new card.....	131
Issuing a new card in enhanced user management environment.....	132
Card audit trail.....	134
Quick Access to Door List per Card.....	135
Creating New Cards Using the "Save As" Feature.....	135
Issuing cards using the "Batch Load" feature.....	135
Viewing and verifying PINs.....	136
Card handling.....	136
Finding a card using the toolbar search.....	136
Finding a card using the card search window.....	136
Editing a card.....	137
Deleting a card.....	137
Customizing Card Information Fields.....	137
Cardholder Access Levels Assignment.....	138

Access exception.....	139
Card options definition.....	139
Adding Comments to a Card.....	140
Limiting Card Usage.....	140
Assigning pictures and signatures.....	141
Assigning a Picture from a File.....	141
Assigning a Picture Using a Video Camera.....	141
Importing a signature from a file.....	142
Adding a Signature from a Signature Capture Device.....	142
Working with Photos and Signatures.....	142
CSV Files Import and Export.....	143
Using a predefined pattern.....	143
Creating a New Import/Export Pattern.....	144
Exporting cards.....	144
Importing cards.....	145
Correcting import or export errors.....	145
Customizing Card Information Fields.....	146
Issuing a new card in enhanced user management environment.....	146
Last Transactions Display.....	148
Viewing the last transaction.....	148
Quick Access to Door List per Card.....	149
Tenants List.....	149
Creating a New Tenants List.....	150
Adding new tenants to the list.....	150
Importing a tenant list.....	151
Exporting a tenant list.....	152
Validating card access.....	153
Definition.....	154
Alarm Systems Definition (Global/KT-NCC).....	154
Example of an alarm partition.....	154
Operation.....	154
Arming, Postponing and Disarming.....	154
Alarm System Capabilities.....	155
Common Inputs.....	155
Perimeter and Volumetric Detection.....	155
Arming Procedure.....	156
Disarming Procedure.....	156
Disarming when “No Disarm” Schedule is Valid Procedure.....	157
Postponing arming procedure.....	157
Area Definition (Global/KT-NCC Gateways Only).....	161
Card location.....	163
Designing the background for the graphic window.....	164
Assigning system components to graphic icons.....	164

Printing system components and graphics.....	165
Event Relays Definition (Global/KT-NCC Gateways).....	165
Defining Event Relays.....	165
Printing Event Relay.....	165
Trigger and Alarm (previously Event Trigger).....	166
Creating a new trigger.....	166
Disable a Trigger.....	166
Create a new Alarm notification.....	166
Receiving notification e-mails for video triggers.....	167
Floors Definition.....	168
Graphics Definition.....	168
Defining Components of a Graphic.....	168
Designing the Background for the Graphic Window.....	169
Assigning System Components to Graphic Icons.....	170
Printing System Components and Graphics.....	170
Guard Tour Definition (Global/KT-NCC Gateways Only).....	170
Holiday Definition.....	171
Schedules Definition.....	172
Defining a schedule.....	173
Task builder definition.....	174
Minimum requirements.....	174
Using the task builder.....	174
Task building examples.....	178
Groups.....	181
Access level groups grouping.....	181
Area group creation.....	181
Trigger group creation.....	181
Controller group creation.....	182
Door group creation.....	182
Floor group creation.....	182
Input group creation.....	183
Relay group creation.....	183
Devices.....	184
Application Configuration.....	184
Configuring an application.....	185
Configuring an Oracle/MS-SQL Interface (CardGateway).....	190
Creating Server Databases Manually.....	192
Creating an operator manually in the Oracle/MS-SQL Server.....	192
Creating a Kantech operator for an MS-SQL Server.....	192
Creating a Kantech operator for an Oracle Server.....	192
Configuring the mirror database and redundant server.....	192
Configuring the SmartLink application.....	194
Configuring the EntraPass Video Vault Application.....	197

Change site labels.....	200
Comment field.....	200
Trigger and alarm tab.....	202
Connection configuration.....	202
Setting up communication timing.....	204
Configuring a direct RS-232 connection type.....	204
Configuring an IP device connection type.....	204
Configuring an Ethernet polling connection type.....	206
Configuring a dial-up (RS-232) modem connection type.....	206
Migrating KT-Standalone backup data to an EntraPass server.....	208
Configuring controllers.....	209
Unassigned modules.....	210
Configuring general parameters for Kantech controllers.....	210
Changing controller type.....	212
Configuring specific controller parameters.....	213
Configuring the status relay activations (multi-site Gateway only).....	214
Configuring licensed wireless doors.....	214
Defining controller options.....	216
Supervision Schedule.....	217
KT-200.....	217
KT-300.....	219
KT-400.....	220
KT-1/KT-2.....	225
Enabling exit readers.....	226
Video gateway or video vault enrollment.....	227
Adding an ioSmart reader.....	228
Controller event buffer overflow message.....	228
Expansion modules setup.....	229
Configuring doors.....	230
Defining general parameters for a door.....	230
Defining Door Keypad Options.....	232
Defining door contact options.....	233
Defining REX (Request to Exit) options.....	234
Card multi-swipe.....	235
Defining interlock options (mantrap).....	236
Defining elevator doors.....	237
Defining a door under a Global/KT-NCC Gateway.....	238
Configuring door events (multi-site gateway only).....	239
Defining door options for controllers and the KTES (multi-site gateway only).....	239
Configuring external alarm system interfaces (multi-site Gateway only).....	240
Managing door access levels.....	241
Reader Templates.....	242
EntraPass Gateways configuration.....	242
Configuring a Gateway Application.....	243

Configuring a Multi-site Gateway.....	244
Configuring a Global Gateway.....	246
Configuring a redundant gateway.....	247
Configuring a KT-NCC Gateway.....	248
Input configuration.....	250
Defining Input.....	251
Defining relays and inputs.....	252
Defining Tamper and Trouble.....	253
Defining an Input for an Elevator Door.....	253
Enabling remote event reporting (multi-site Gateway only).....	254
Defining an Input for a Group of Doors.....	254
Integrated component configuration.....	255
Integrated panel configuration.....	256
Intrusion panel integration within the global gateway and KT-NCC.....	257
General tab.....	257
Panel component tab (Bentel, DSC Maxsys, PowerSeries Neo and Pro).....	260
RS-232 tab.....	262
Kantech Telephone Entry System (KTES) Configuration.....	262
Defining general parameters for the KTES.....	262
Defining the Kantech Telephone Entry System parameters.....	263
Defining the Language and Welcome Message parameters.....	265
Defining the Options parameters.....	266
Defining the status relay parameters.....	266
Defining the Pager options.....	267
Configuring Tenant Administration Level parameters.....	269
Output device configuration.....	269
Defining General Options for an Output.....	269
Associating Events with Auxiliary Outputs.....	270
Relay configuration.....	270
Defining relays.....	270
Site configuration.....	271
Video.....	272
Camera definition.....	272
Defining a Camera.....	272
Associating a camera with an icon.....	273
Defining Presets and Patterns.....	273
Defining events recorded by a camera.....	273
Current recording.....	274
Viewing the current recordings.....	274
EntraPass Video Vault Browsing.....	275
Viewing Video Segments Archived in the EntraPass Video Vault.....	275
Viewing exported videos.....	275
Exporting video files.....	275

Finding video events.....	276
Recording parameters.....	278
Setting Up Recording Parameters.....	278
Setting Up Stop Recording Trigger Parameters.....	279
Video desktop.....	279
Displaying a video view.....	279
Video event list.....	280
Using the video event list.....	280
Finding video events.....	280
Playing Video Segments.....	281
Linking Video Clips with Key Frames.....	281
Exporting Video Files.....	282
Protecting a Video with a Password.....	282
Video playback.....	282
Viewing a Video Playback.....	283
Video server configuration.....	283
Defining the video server communication settings.....	283
Enhancing the Security of Video Servers.....	286
Remote Video Connection.....	286
Defining the EntraPass Video Vault.....	286
Programming the Exacq DVR using EntraPass.....	288
Programming the Exacq DVR to connect to EntraPass.....	288
Defining exacq DVRs.....	288
Activating the Video Gateway for hattrix license.....	288
Video triggers.....	289
Defining video triggers.....	289
Video Views Creation and Modification.....	290
Modifying a Video View.....	290
Video views definition.....	291
Defining video view general parameters.....	291
Accounts.....	294
Account configuration.....	294
Customizing account information fields.....	294
Miscellaneous.....	294
Badging credential.....	294
Adding a shipping address.....	295
Importing gateways, sites or connections.....	295
Comment.....	295
Login message.....	295
Account manager.....	296
Customizing account manager information fields.....	296
Account settings.....	297
Account statistics.....	297

Enabling the account statistics feature.....	297
Account management.....	298
Accounts tab.....	299
Account configuration.....	300
Account status.....	301
Account type and status.....	302
Configuring an account.....	303
Configuring the default state for a new account.....	303
Viewing account statistics.....	304
Viewing accounts status.....	304
Switching an account.....	304
Badging credential.....	304
Card credentials.....	304
Switching accounts and logon.....	305
System.....	306
Active Directory.....	306
Associations.....	324
Commissioning.....	324
Configuring the security level in EntraPass Web.....	325
Creating or editing a field technician.....	325
Credential E-mail Notification.....	325
Filtering Desktop Events.....	325
Database Structure Definition.....	326
Viewing the Database Components.....	326
Defining Alarm Systems.....	327
Defining Card Filters.....	327
Event Parameters Definition.....	327
Defining events parameters.....	328
Creating Associations.....	329
Viewing Default Parameters.....	330
Deleting and Restoring Associations.....	330
Printing Event Parameters.....	330
Instructions definition.....	331
Defining an Instruction.....	331
Message Filters Definition.....	331
Defining Event for a Message Filter.....	331
Operators definition.....	333
Creating or editing an operator.....	333
Concurrent Logins.....	336
Defining a Login Message for a Single Operator.....	336
Security level definition.....	336
Creating and modifying operator security levels.....	337
Defining Login Options for an Operator.....	337

Hiding Card Information.....	338
Assigning Video Custom Buttons.....	339
Workspace definition.....	339
Workspace filtering.....	340
Selecting accounts.....	340
Selecting an account manager.....	340
Selecting EntraPass applications.....	340
Defining gateways and sites.....	341
Defining schedules.....	341
Defining controllers.....	341
Defining doors.....	341
Defining relays.....	341
Defining inputs.....	342
Defining access levels.....	342
Defining alarm systems.....	342
Defining areas.....	342
Defining guard tours.....	342
Defining card types.....	343
Defining card filters.....	343
Defining card access group.....	343
Defining reports.....	343
Defining graphics.....	344
Defining operators.....	344
Defining badge layouts.....	344
Defining workspaces.....	344
Specifying security level.....	345
Defining video servers.....	345
Defining cameras.....	345
Defining video views.....	345
Defining tasks.....	346
Defining panels.....	346
Defining panel components.....	346
Defining events.....	346
Operators in workspace.....	347
Audit.....	347
Reports.....	349
Archive viewing.....	349
Displaying a Report.....	349
Previewing Reports.....	349
Card Use Report.....	350
Automatic Report Schedule.....	351
Automatic Report Output.....	351
Custom reports definition.....	351
Using the default “all events” report.....	351

Defining a Custom Report.....	351
Defining a Report Output Format.....	355
Historical and card use reports.....	355
In/Out reports.....	355
Defining automatic report schedules.....	356
Specifying additional options for automatic reports.....	357
In/Out reports definition.....	358
Defining In/Out Reports.....	358
In/Out reports request.....	359
Requesting a In/Out Report Manually.....	359
Muster reports.....	359
Muster reports for emergency management.....	360
Muster reports for parking management.....	361
Muster report generation.....	361
Operations on In/Out.....	362
Adding a Transaction in the In/Out Database.....	362
Previewing In/Out Reports.....	364
Previewing Reports.....	364
Quick report definition.....	365
Defining a Quick report.....	365
Report Log.....	366
Report state.....	367
Report state fields.....	367
Contextual menu of in process reports.....	368
Requesting Reports.....	368
Roll Call Reports.....	369
Functionalities.....	369
Roll Call Report generation.....	369
Specifying additional options for automatic reports.....	370
Options.....	371
Alarm Management.....	372
Compatible mode.....	372
Notification based on event priority.....	372
Notification based on the operator acknowledgement level.....	372
Notification based on the workstation acknowledgement level.....	372
Notification based on the workstation and on the operator acknowledgement level.....	372
Backup Scheduler.....	373
Configuring the Backup when the EntraPass Server is Running as a Service.....	373
Scheduling Automatic Backups of the System Database.....	374
Badge Printer.....	375
Connection password modification.....	375
Changing the connection password.....	376
Credentials Parameters.....	376

Card.....	376
Badge Printer.....	377
Custom messages.....	377
Setting up custom messages.....	377
Dealer Information.....	377
About box details.....	377
KAP reminder.....	377
Defining a card display format.....	378
Changing from a 24-bit to 32-bit global card format.....	380
Auto conversion.....	380
Event color and priority.....	380
Integration.....	381
Login messages.....	381
Login message example.....	382
Configuring multimedia devices.....	382
Selecting an alarm sound.....	382
Defining video options.....	383
Setting up the signature capture device.....	383
Configuring and selecting printers.....	384
Selecting and setting up a log printer.....	384
Selecting and setting up a report printer.....	384
Registration.....	384
Service Login Information.....	385
System date and time modification.....	385
System language selection.....	385
Changing the system language.....	385
Changing the system language for an operator.....	386
System parameters configuration.....	386
Server parameters.....	386
Gateway parameters.....	391
Firmware parameters.....	391
Image parameters.....	393
Report parameters.....	394
Video parameters.....	395
Time parameters.....	397
Credentials Parameters.....	397
Workstation and Server.....	398
Integration.....	398
Web Interface.....	399
EntraPass Server.....	403
General.....	403
Application.....	403
Error Log.....	403

Log.....	404
Registration.....	404
Report Log.....	404
Backup.....	405
Backups.....	405
Restores.....	406
Options.....	407
Connection password modification.....	407
System language selection.....	408
System date and time modification.....	408
Backup Scheduler.....	408
Utilities.....	411
Database utility.....	411
Running the Database Utility.....	411
EntraPass Video Vault.....	413
Installing the EntraPass Video Vault.....	414
Launching the EntraPass Video Vault.....	414
Managing archived video segments.....	414
Express setup program.....	415
Configuring a global connection using Express Setup.....	415
Configuring a multi-site gateway connection using express setup.....	416
Configuring a controller using Express Setup.....	420
Configuring a KTES using Express Setup.....	420
Defining relays.....	420
Defining Inputs.....	421
Defining auxiliary outputs (LED and buzzer).....	421
PING Diagnostic.....	422
Quick report viewer.....	422
The SmartLink interface.....	423
Required material.....	423
Installing the SmartLink application.....	423
Configuring the SmartLink application.....	423
Starting the SmartLink application.....	423
Vocabulary editor.....	424
Installing the Vocabulary Editor.....	424
Translating the system language.....	424
Integrating the custom language in EntraPass.....	425
Distributing the New System Vocabulary.....	426
Updating the system vocabulary.....	426
Upgrading the System Vocabulary.....	427
EntraPass icons.....	428
Alarm systems.....	428
Alarm system is in alarm.....	428

Alarm system is armed.....	428
Alarm system is armed with input in alarm (forced arming).....	428
Alarm system is in arming request delay.....	428
Alarm system is disarmed.....	429
Alarm system is in entry delay.....	429
Alarm system is in “exit” delay.....	429
Alarm system status is not yet known.....	429
Alarm system is in “postpone” mode.....	429
Controllers.....	430
Status unknown.....	430
Controller is in AC failure.....	430
Controller polling malfunction.....	430
Controller is in AC failure and Tamper Switch in alarm.....	430
Controller is not communicating.....	431
Controller communication is regular (no problem).....	431
Controller is in Reset and AC failure.....	431
Controller is in Reset, AC failure, and Tamper Switch is in alarm.....	431
Controller is in Reset and Tamper Switch in alarm.....	432
Controller tamper switch in alarm.....	432
Controller reloading firmware.....	432
KT-400 controller trouble.....	432
Doors.....	432
Relays.....	437
Relay activated by alarm system in alarm.....	437
Relay activated by alarm system function.....	437
Relay activated by alarm system delay.....	438
Relay activated by an event.....	438
Relay temporarily activated by an event.....	438
Relay activated by an input.....	438
Relay temporarily activated by an input.....	438
Relay activated by an operator.....	439
Relay temporarily activated by an operator.....	439
Relay temporarily activated by a schedule.....	439
Relay deactivated.....	439
Inputs.....	439
Input activated—Not supervised.....	439
Input activated—Supervised.....	440
Input activated—Not supervised manual operation.....	440
Input activated—Supervised manual operation.....	440
Input activated—Supervised temporarily manual operation.....	440
Input in alarm—Not supervised.....	441
Input in alarm—Shunted by operator.....	441
Input in alarm—Supervised.....	441
Input in alarm—Supervised by operator.....	441

Input OK—Not supervised.....	442
Input OK—Shunted by operator.....	442
Input OK—Supervised.....	442
Input OK—Supervised by operator.....	442
Controller connection.....	443
Connection status is not yet known.....	443
Controller connection connected.....	443
Controller connection connected and in “Reload Data”.....	443
Controller connection—Communication failure.....	443
Gateways.....	444
Gateway—communication failure.....	444
Gateway—communication failure during reload data.....	444
Gateway communication is regular (no problem).....	444
Gateway trouble.....	444
Gateway trouble when reloading.....	444
Gateway OK—communicating.....	445
Gateway in “reload data”.....	445
Gateway—communication failure.....	445
Gateway—reload KT-NCC firmware.....	445
EntraPass Application.....	446
Application status is not yet known.....	446
Application attempts communication.....	446
Application—Communication Failure.....	446
Others.....	446
Database Initialization.....	446
Data not available.....	446
No status available.....	447
Output status is not yet known.....	447
Status unknown.....	447
Error in process.....	447
Undefined Component.....	447
End-User License Agreement.....	448

EntraPass Global Edition



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.

Copyright

© 2024 Johnson Controls. All rights reserved. JOHNSON CONTROLS and KANTECH are trademarks of Johnson Controls.

Release Notes 8.71

See the following list of new features for this release.

New features

EntraPass

- Multi-language feature:
 - In a system with hattrix, you can now change the user interface language for accounts and operators. This user interface language can be different from the primary and secondary languages defined for the database. For more information, see [Changing the system language](#) and [Changing the system language for an operator](#).
 - When requesting a report, quick report, In/Out report, or custom scheduled report, you can now select the database language and a user interface language to execute the report in. In the report, the descriptions display in the selected database language, and the labels display in the selected user interface language. For more information, see [Requesting Reports](#), [Defining a Quick report](#), [Requesting a In/Out Report Manually](#), and [Defining automatic report schedules](#).
 - OSDP communications standard implemented:
 - ioSmart Gen 1 readers and ioSmart Gen 2 readers support Open Supervised Device Protocol (OSDP).
 - Kantech KT-400, KT-4, and KT-1 controllers support Open Supervised Device Protocol (OSDP) communication with third party readers.
For more information about configuring OSDP readers connected to KT-400, KT-4, or KT-1 controllers, see [Configuring an OSDP reader to a KT-400 or KT-4 controller](#) and [Configuring an OSDP reader to a KT-1 controller](#)
- ❗ **Note:** For optimal communication and performance between a KT-controller and ioSmart, use the encrypted Kantech RS-485 protocol.
- KT-4 four-door controller support: You can now add a KT-4 controller as a sub-type of the KT-400 controller. For more information, see [Configuring a KT-4 controller](#).

Limitations

- Integration DLL on KT-4 and KT-NCC Gen 2: No integration panel works with the KT-4 or KT-NCC Gen 2 for this release
- Microsoft Visual C++ 2005 and 2008 are removed because Microsoft no longer provides support. Customers can still manually install it to support the Panasonic integration.

Technical support

If you cannot find the answer to your question in this manual, contact your installer. Your installer is familiar with your system configuration and may be able to answer your questions. If you are an installer, contact your system operator.

If you require additional information, email access-support@jci.com, or go to: https://www.kantech.com/Support/Contact_Technical_Support_Advanced.aspx.

See the following table for the technical support opening hours and phone numbers in your region.

Table 1: Technical support contact details

North America	Number type	08:00 to 20:00 GMT -05:00
USA and Canada	Toll free	+1 888 222 1560
USA and Canada	Direct	+1 450 444 2030

Latin America	Number type	08:00 to 20:00 GMT -03:00
Argentina, Buenos Aires	Direct	+54 11 5199 3104
Brazil, Sao Paulo	Direct	+55 11 3181 7377
Chile, Santiago	Direct	+56 2 3210 9662
Colombia, Bogota	Direct	+57 1 344 1422
Colombia, Cali	Direct	+57 2 891 2476
Colombia, Medellin	Direct	+57 4 204 0519
Costa Rica, National	Direct	+506 4 000 1655
Dominican Republic, Santo Domingo	Direct	+1 829 235 3047
El Salvador, 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	Number type	09:00 to 17:00 GMT +08:00
Asia Pacific	Toll free	+800 2255 8926
China	Direct	+86 21 6163 8644
India	Direct	+91 80 4199 0994
Australia	Direct	+1 800 580 946
Oceania and New Zealand	Direct	+64 9942 4004

EMEA	Number type	08:00 to 18:00 GMT +01:00
Europe, Middle East, and Africa	Toll free	+800 2255 8926
Europe, Middle East, and Africa	Direct	+31 475 352 722
United Kingdom	Direct	+44 330 777 1300
Israel	Direct	+972 77 220 1350

EMEA	Number type	08:00 to 18:00 GMT +01:00
Spain	Direct	+900 99 31 61
Denmark	Direct	+45 4494 9001
France	Direct	+0800 90 79 72
Germany	Direct	+0800 1806 757
Italy	Direct	+39 02 3051 0112
Belgium	Direct	+0800 76 452
Ireland	Direct	+1800 94 3570
Nordic Countries	Direct	04494 9001
Greece	Direct	00800 3122 9453
South Africa	Direct	+27 10 100 3292
Russia	Direct	+81 0800 2052 1031
Turkey	Direct	+00800 3192 3007
United Arab Emirates	Direct	(0)800 0310 7123
Bahrain	Direct	(0)800 04127
Kuwait	Direct	(0)22062915
Qatar	Direct	(00) 800100841
Egypt	Direct	(0) 8000009697
Oman	Direct	(00) 8007 4364
Lebanon	Direct	01 426 801, new dial tone and then dial 8552343677
Kingdom of Saudi Arabia	Direct	+96 6800 8500 509

How to

Use this section to find quick solutions to common tasks in EntraPass.

How to create a backup

1. On the EntraPass server, click the **Options** tab.
2. Click **Backup Scheduler**.
3. To choose the type of data that you want to back up, click one of the following tabs: **Data**, **Archive**, **In/Out** or **Video Event**.
4. Select the **Automatic backup** check box.
5. In the **Backup folder** pane, choose where to save the backup.
6. In the **Backup frequency** pane, choose how often you want to back up the system.
7. To start a backup immediately, select the **Now** check box.

Result

For more information about configuring backups, see [Backups](#).

How to create a badge

1. On the EntraPass workstation, click the **Users** tab.
2. Click **Badge**.
3. In the **Badge** window, click the **New** icon.
4. In the **Badge properties** window, choose the badge properties and click **OK**.
5. In the **English** and **French** fields, enter a name for the badge.
6. In the lower center of the window, click **Click here to modify the badge layout**.
7. In the **Badge design** window, choose the elements that you want to include in the badge.
8. To save your badge design choices, from the menu, click **Layout** and click **Exit**.
9. Click **Save**.

Result

For more information about configuring badges, see [Badge Designing](#).

How to create a card

About this task:

- **Important:** A gateway must exist prior to creating a new card in EntraPass. For more information, see [EntraPass Gateways Configuration](#).

An access level must exist prior to creating a new card in EntraPass. For more information, see [How to create an access level](#).

1. On the EntraPass workstation, click the **Users** tab.
2. Click **Card**.
3. In the **Card** window, click the **New** icon.
4. On the **Card number** tab, in the **Card # 1** field, enter the card number and press **Enter**.
5. In the **Card user name** field, enter the card user name.
6. Click the **Access level** tab.
7. From the **Access level** list, select an access level.
8. Click **Save**.

Result

For more information about creating cards, see [Cards Definition](#).

- ❗ **Note:** If you activated enhanced user management, see [Issuing a new card in enhanced user management environment](#).

How to create a schedule

1. On the EntraPass workstation, click the **Definition** tab.
2. Click **Schedule**.
3. In the **Schedule** window, click the **New** icon.
4. In the **English** and **French** fields, enter a name for the new schedule.
5. Click **Save**.
6. In the **Start time** and **End time** columns, enter start and end times for the schedule.
7. Select the days of the week to apply to the schedule.
8. Select up to a maximum of four holidays to apply to the schedule.

Result

For more information about defining holiday, see [Holiday Definition](#).

How to create a simple report

1. On the EntraPass workstation, click the **Report** tab.
 2. Click **Quick Report**.
 3. In the **Quick report** window, from the **Event** list, select which events to include in the report.
 4. In the right pane of the window, in **Report name** field, enter a name for the report.
 5. Click **Execute**.
- For more information about creating reports, see [Quick Report Definition](#).

How to create an access level

About this task:

- **Important:** A Gateway must exist prior to creating a new access level in EntraPass. For more information, see [EntraPass Gateways Configuration](#).

1. On the EntraPass workstation, click the **Users** tab.
 2. Click **Access level**.
 3. In the **Access level** window, from the **Connection** list, select a gateway or connection.
 4. Click the **New** icon. The **Card number** field is enabled.
 5. In the **English** and **French** fields, enter a name for the access level.
 6. Click **Save**.
- For more information about creating cards, see [Access Level Definition](#).

How to print a list of cards

1. On the EntraPass workstation, click the **Users** tab.
2. Click **Card**.
3. In the **Card** window, click the **Print** icon.
4. From the **Card index** list, select the card type.
5. **Optional:** You can specify a card number range and filters, and select the card fields to be printed. For more information, see [Card Printing](#).

6. Click **Print**.
7. From the list, select a printer, and click **OK**.

How to print a list of access levels

1. On the EntraPass workstation, click the **Users** tab.
2. Click **Access level**.
3. In the **Access level** window, click the **Print** icon.
4. From the **Select Site/Connection/Gateway** list, select a site, connection, or gateway.
5. In the **Access level** pane, select the access levels to print.
6. Click **Print**.
7. From the list, select a printer, and click **OK**.

How to print a list of doors

1. On the EntraPass workstation, click the **Devices** tab and click **Door**.
2. In the **Door** window, click the **Print** icon.
3. From the **Site/Connection/Gateway** list, select a site, connection, or gateway.
4. In the **Door** pane, select the doors to print.
5. Click **Print**.
6. From the list, select a printer, and click **OK**.

How to set up desktops

1. On the EntraPass workstation, click the **Desktops** tab.
 2. Right click on one of the desktop buttons and click **Properties**.
 3. In the **Desktop name** field, enter a name for the desktop.
 4. Select the desktops to display.
 5. To save your changes, click **OK and GO**.
- For more information about configuring desktops, see [Desktops](#).

How to use shortcut keys

About this task:

Use shortcut keys for faster operation. The following table lists the EntraPass shortcut keys.

Table 2: EntraPass 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 a drop-down list	Open list
F5	Where available	Refresh
F8	Anywhere	Global search
F10	Anywhere	Log on/Log off
F11	Anywhere	Workspace
F12	Anywhere	Switch account

How to personalize the web logon window

About this task:

You can customize the default logon welcome message and icon for EntraPass Web.

To customize the logon window, complete the following steps:

1. Go to **C: > inetpub > wwwroot > EntrapassWeb**, and open the `web.cfg` file in a text editor.
2. Find the key entry `<add key = "WelcomeMessage" value="EntraPass Web"/>`.
3. Replace `EntraPass Web` with your customized message. Use a maximum of 30 characters to ensure that the message displays 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. EntraPass web supports JPG and PNG file formats.
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 that the entire image is visible.

How to deactivate connections and controllers

1. On the EntraPass workstation, click the **Devices** tab.
2. Click **Connection** or **Controller**.
3. From the list, select the connection or the controller that you want to deactivate.
4. Select the **Deactivated** check box and click **Save**.

Result

All settings and events are saved for the deactivated connection or controller.

The billing report includes deactivated connections or controllers. This does not affect doors that are connected to other connections or controllers.

How to enable go Pass for a user

About this task:

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. For more information, see [Adding system components](#). You must also enable go Pass for the Smartlink application.

To enable go Pass for the Smartlink application, complete the following steps:

1. On the EntraPass workstation, click the **Devices** tab.
2. Click the **Application** button.
3. Select the Smartlink to use for your go Pass application.
4. Click the **Web Service** tab and select **Allow Go Pass**.
5. Ensure the **Connection name**, **IP address / Domain name**, and **port** numbers, are present for the Smartlink connection.
6. Click the **SmartLink e-mail** tab.
7. Ensure the **E-mail Server parameters** are present for the connection.

To enable go Pass for your hattrix system, complete the following steps:

1. On the EntraPass workstation, click the **Accounts** tab.
2. Click the **Account**
3. Click the **Miscellaneous** tab.
4. Select **Allow go Pass**.

To enable go Pass for a user and send credentials, complete the following steps: button, and select the account you want to enable the go Pass feature for.

1. On the EntraPass workstation, click the **Users** tab.
2. Click **Card**.
3. From the **Card user name** list, select an existing user, or click the **New** icon to create a new one.
4. Select the **Enable go Pass** check box. For new users, the card number automatically generates in the **Card #1** field. For existing users with an access card, the card number is already in the **Card #1** field. The **Key Cycle** default value is 12 hours, and the **Key Lifespan** default value is 24 hours. For more information about Key Cycle and Key Lifespan, see [go Pass tab](#).
5. Enter the user's email address. The user receives go Pass instructions at this email address.
6. Select the **Notify** button, and select the check box to send the instruction email.
7. Select the language of the user.
8. Click **Save**.

The user receives an automated email which contains details on how to download the go Pass application to their smartphone. The user's credentials are automatically entered into the application. If the user cannot open the activation link, they can copy the activation key from the email and paste it into the manual activation field of the go Pass application.

Troubleshooting

If the Smartlink port or address changes, you lose access to go Pass. To get access to go Pass access, you must update the credentials. To send the updated credentials to all go Pass users, complete the following steps:

1. On the EntraPass workstation, click the **Options** tab.
2. Click **System Parameters**.
3. From the menu, select **EntraPass Web** and select **Resend to all go Pass users**.

Result

Users receive updated credentials by email.

- ① **Note:** To use go Pass, you must have a valid KAP. For more information, see [Kantech Advantage Program \(KAP\)](#).

How to migrate from event parameter to event operator mode

About this task:

Event operator mode replaces the event parameter mode for managing events. By default, new installations use event operator mode. Upgraded systems must enable the mode.

To enable event operator mode and to transfer existing event parameters to triggered alarm notifications, complete the following steps:

1. On the EntraPass server or workstation, click the **Options** tab.
 2. Click **System Parameters**.
 3. Click the **Server** icon.
 4. Click the **Alarm Management** tab.
 5. Select **To enable event operator mode and to transfer existing event parameters to triggeredMigrate from Event Parameters to Event Operator**.
 6. Click **OK** to begin the migration.
 7. Click **OK** to confirm the operation. To ensure safety, an automatic backup is performed and the database sets to **locked**.
 8. During migration, events display in the operator's default desktop.
 - If the **Override workstation workspace message** option is selected, events display in the selected workspace. To select a workspace, see Step 12 of [Creating or editing an operator](#).
 - If the **Override workstation workspace message** option is not selected, events display in the default desktop.
 - If the operator has never logged on to the workstation or if the operator's last logon was not to the workstation, the operator sees all events
 - If the operator's last logon was to the workstation and **Apply Workstation workspace and event parameters** is selected, the operator sees events in the workspace defined in the **When Logged In** option and from the schedule defined in **Event Parameters** from that workstation.
 - If the operator's last logon was to the workstation and **Apply Workstation workspace and event parameters** is not selected, the operator sees events with the display schedule defined in **Event Parameters** from that workstation.
 9. Existing event parameters merge into single triggers and alarms based on their type (Application, Door, Input, etc), their alarm schedule, and their instruction. Task Builder tasks that are defined in **Event Parameters** also migrate.
 10. The alarm management model transfers to each trigger and alarm. **Compatible** and **Event Priority** modes transfer to **Acknowledge for all connected workstations**.
 11. After the migration, to view the changes, log out and then log on again to all active workstations.
- ❗ **Note:** The migration from event parameter mode to event operator mode cannot be reversed.

How to set the database to read-only mode manually

About this task:

If you enable the database read-only mode, you cannot modify the database. Messages, alarms and manual operations continue to work as normal.

To set your EntraPass database to read-only mode, complete the following steps:

1. On the EntraPass server or workstation, right-click anywhere in the main window.
2. Click **Database read-only**.
3. Click **Yes** to confirm the action.
4. Click **OK** to close the confirmation box. The network database state indicator, in the lower right of the window, turns from green to black.

5. To restore your database to normal mode, right-click anywhere in the main window and click **Database read-only**. The network database status indicator, in the lower right of the window, turns from black to green.
- ❗ **Note:** The database remains in read-only mode until an operator disables it or until the server is restarted.

How to schedule a technician appointment

1. On to the EntraPass workstation, right-click anywhere in the main window and click **Global Search <F8>**, or press F8.
 2. In the **Global Search** window, click the **Technician appointment** tab.
 3. Right-click in the window and click **Add an appointment**.
 4. In the **Text filter** field, search for the user name or the email address of the field technician. For more information, see [Creating or editing a field technician](#).
 5. From the **Account** list, add the account.
 6. From the **Workspace** list, add a workspace. For more information, see [Workspace](#).
 7. From the **Message Filter** list, add a message filter. For more information, see [Message Filter](#).
 8. In the **Start date** and **End date** fields, enter start and end dates.
 9. To send an email to the selected field technician, select the **Send email notification** check box.
 10. To save the appointment, click **OK**.
 11. To delete or modify the appointment, right-click on the list of appointments and click **Modify an appointment** or **Delete an appointment**.
 12. To search for an existing technician appointment, in the **Text filter** field, enter the name, login name, company name, or email address of the technician, and click **Search**.
- ❗ **Note:** A technician can have multiple appointments at the same time for different accounts. This allows the technician to test account-specific features. The technician must select the required account during login.

How to enable EntraPass maintenance mode

About this task:

If you enable EntraPass maintenance mode, all alarm notifications are bypassed. This includes all alarm acknowledge popup messages and emails sent from an **Event Trigger**. This mode does not affect reports sent by email, billing report emails, and KAP reminder emails.

To enable maintenance mode, complete the following steps:

1. On the EntraPass server or workstation, right-click anywhere in the main window.
 2. Click **Maintenance mode**.
 3. Click **Yes** to confirm the action.
 4. Click **OK** to close the confirmation box. When maintenance mode is enabled, a **Maintenance mode** message displays at the bottom of the window.
 5. To disable maintenance mode, right-click anywhere in the main window and click **Maintenance mode**.
- ❗ **Note:** Maintenance mode remains active until an operator disables it or until the server is restarted.

How to set up the ioSmart

About this task:

Connect the Kantech ioSmart card reader to a supporting KT-400, KT-1, or KT-2 controller. The ioSmart supports both Wiegand and RS-485 connections to the controller.

If you connect the ioSmart using a Wiegand connection, use the Express Setup Program to configure the reader. For more information, see [Express setup](#).

If you connect the ioSmart using an RS-485 connection, complete the following steps:

1. On the EntraPass workstation, click the **Devices** tab, and click **Controller**.
2. From the **Controller** list, select a controller, and click on the **ioSmart** tab.
3. Click **+Add** to add an ioSmart reader to the controller.
4. In the **Serial number** field, enter the ioSmart reader's serial number.
5. From the **Door** list, select the associated door.
6. If the ioSmart reader includes a keypad, select the **Keypad** check box.
7. Click **Terminals** to configure the ioSmart reader's inputs and outputs.
8. In the **Setup terminals** window, in the **I1** and **I20** panes, select the terminal functions.
 - **Disabled**
 - **Single input**
 - **Dual input**
 - **Lock output**
 - **Relay**
- ① **Note:** You can configure I1 and I2O for a maximum of four inputs, using both I1 and I2O in dual inputs mode, or for two inputs and one output, a lock output or a relay.
9. Click the **KT-1/KT-2** or the **KT-400** tab, and, from the **RS-485 baud rate** list, select the appropriate baud rate for your system.
10. In the **Reader template** field, click the **Three dot** icon, and select a reader template.
11. To configure the reader template, on the EntraPass workstation, click the **Devices** tab, and click **Reader template**.

How to configure an ioSmart reader on the operation tab

You can also configure the ioSmart reader on the operation tab.

1. On the EntraPass workstation, click **Operation**.
2. Click **Controller**.
3. In the **Connection** pane, select the appropriate device.
4. In the **Controller** pane, right-click the controller, and click **Request unassigned modules**.
5. Right-click a controller and click **Unassigned Module**. This creates a **Controller unassigned module requested by operator** event on the desktop.
6. Right-click the event to assign the ioSmart reader. The serial number of the ioSmart reader is automatically filled on the **Configuration** tab.
7. **Optional:** To view the status of the configured ioSmart reader, on the EntraPass workstation, click **Operation**, and click **Door**. In the **Door** pane, right-click the appropriate door.
8. **Optional:** To view the status of all configured ioSmart readers that are connected to a controller, on the EntraPass workstation, click **Operation**, and click **Controller**.

FAQ

Use this section for quick answers to frequently asked questions about the EntraPass system.

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.

Does the KT-NCC connect to the EntraPass server?

Yes, as the KT-NCC is a gateway, it communicates with the EntraPass server using Ethernet.

How many secondary access levels can be stored on the KT-400 in stand-alone mode?

12 secondary access levels can be stored. This option is available only in EntraPass Global Edition.

How is a muster report different from roll call report?

The muster report is available only with EntraPass Global Edition. Use a muster report for a snapshot of who is inside an area group at a specific time. You can print or email the report in any of the following formats: CSV, XLS, PDF, RFT, TXT.

The roll call report is available with all EntraPass editions. Use a roll call report for a list of cards that use specific doors in a roll call sector during a specific time. You can print or email the report in a CSV format.

Is it possible to import access levels?

Access levels cannot be imported.

What are the communication ports for the following EntraPass products: Server, Workstation, 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 options to disarm a virtual alarm system?

This can be achieved by using software manual disarm and disarming at a door reader using a card.

What are the options to arm a virtual alarm system?

Virtual alarm system options are only available in EntraPass Global Edition. There are three methods to arm a virtual alarm system:

- With a card swipe
- With a card and an arming input
- With only an arming input

What are the options available in batch operation?

The batch operation allows the user to make changes to the card database with one 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.

What do we use event relays for, and what options are there for the relays?

This function is only available for specific events in EntraPass Global Edition. We can set each relay to activated temporarily, activate or deactivate according to the relay schedule.

What happens when we save card pictures on a hard drive instead of the server database?

A parameter allows you to save cards, 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 can be used in instances where a connection may need more space to save pictures, signatures and graphics.

What is a Global Gateway?

A Global Gateway is either a KT-NCC or a Global Windows Gateway. The Global Gateway allows for all global functions such as anti-passback, area (people) tracking, muster reporting, virtual alarm system, guard tours, secondary access levels, global I/O and other functions.

What are the differences between Global, KT-NCC and Multi-Site Gateways?

Use the Global and KT-NCC gateways for global functionality through the gateway. For example, if an input triggers an alarm on a specific controller, it can activate a relay on a separate controller residing on the same gateway.

The KT-NCC can support 128 controllers: three loops of 32 controllers, and four IP loops of eight controllers each, using a Lantronix UDS1100. It can support the KT-1, KT-2, and KT-400 in IP mode.

Use the multi-site gateway for local functionality for each controller. It can also support the KT-IP and KTES in IP mode.

What is the difference between anti-passback on a Global, KT-NCC, or Multi-Site Gateway?

Multi-site gateway: Anti-passback is local to the controller.

Global gateway and KT-NCC: Anti-passback on the Global gateway and KT-NCC are global functions which can be implemented with the areas. There are various levels of anti-passback that can be programmed on the Global and KT-NCC gateway, such as Normal Supervisor, or Normal and Supervisor.

What happens to global functions if someone disconnects the controllers from the Global Gateway?

The controllers will revert to a 'Corporate' mode. The controllers will keep their card and schedule programming. Functions such as virtual alarm panels, areas, dual custody, guard tours and others will work only when the controllers are connected to the KT-NCC.

What is the difference between one time access and temporary unlock door for the KT-100, KT-200, KT-300, KT-1, KT-2, and KT-400?

One time access on the KT-100, KT-200, KT-300, KT-1, KT-2, and KT-400

Perform this command using the operation door menu and it will follow the unlock time of the door. If the door stays open longer than the unlock time, it will generate an event pre alarm door open too long, and if it is not closed at the end of the open time it will generate door open too long.

Temporary unlock on the KT-100, KT-200, KT-300

Perform this command using the operation door menu and it will follow the unlock time of the door. If the door stays open longer than the unlock time, it will generate an event pre alarm door open too long, and if it is not closed at the end of the open time it will generate door open too long.

Temporary unlock on the KT-1, KT-2, and KT-400

Perform this command using the operation door menu. After 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 are the differences between the three unlock conditions for inputs: latch, follow, and access?

Latch: Unlocks and stays unlocked if the input goes into alarm mode.

Follow: Follows the condition of the input. When the input goes into alarm mode, it unlocks the door or the group. When the input is restored, the door or group is locked.

Access: When the input goes into alarm mode, it unlocks the door or group for the defined unlock time for each door.

① **Note:** These conditions are only available in EntraPass Global Edition.

What is the purpose of custom messages?

The custom messages option allows operators, with the appropriate 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.

What is the purpose of a secondary access level?

The secondary access levels are used to assign 12 additional access levels to the cardholder for each KT-NCC and Global gateway. The secondary access levels are created to fulfill a specific access purpose and then assigned to the cardholder. Those secondary access levels allow for more flexibility and management of the card's access rights.

Where can I synchronize operators with Active Directory?

You can launch synchronization from a number of locations, including the following:

- **System/Active Directory:** Click **Sync Now** to manually start synchronization with the selected Active Directory server.
- **Status/Application:** Right-click **SmartLink** to see two sync options:
 - **LDAP force synchronize all** synchronizes all Active Directory servers.
 - **LDAP force synchronize** synchronizes only one particular Active Directory server.
- **LDAP service control:** Right-click the **Active Directory** icon in the Windows notification area to see the **Sync Now** option. This option synchronizes all Active Directory servers on the selected SmartLink.

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.

Introduction

Use this section for an overview of what EntraPass does, its main features, and the applications associated with it. For global contact details, see [Technical support](#). The main features include the following:

- [Kantech Advantage Program \(KAP\)](#)
- [SmartLink](#)
- [Mirror database and redundant server](#)
- [KT-NCC controller and gateway](#)
- [Dual gateways option](#)
- [Redundant gateway](#)
- [Wireless door license](#)
- [Kantech IP Link](#)
- [KT-100, KT-200, KT-300, KT-1, KT-2, and KT-400 controllers](#)
- [Kantech ioSmart card reader](#)
- [Kantech Telephone Entry System](#)
- [Express setup](#)
- [hatrix for managed access control](#)
- [Elevator control capability](#)
- [Integrated badging](#)
- [Interactive floor plans](#)
- [Configurable desktops by operator](#)
- [Interfacing with external alarm panels](#)
- [Partitioning alarm system](#)
- [In/Out feature](#)
- [Muster reporting for parking and emergency management](#)
- [Visual diagnostics](#)
- [Enhanced video integration](#)
- [EntraPass video vault](#)
- [Vocabulary editor](#)
- [Intrusion integration](#)

What is EntraPass?

EntraPass is a comprehensive menu-driven access control software package. The access control system includes components such as door readers, exit detectors, and motion detectors that are professionally installed and electronically controlled. Use system workstations to perform operations such as acknowledging alarms, modifying the system database, and receiving event messages. A supporting advantage of access control is that all system events are carefully archived and can be retrieved easily for inspection purposes.

Kantech Advantage Program (KAP)

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

SmartLink

EntraPass enables organizations to interface to most intelligent devices including CCTV multiplexers, alphanumeric pager systems, automated emails, HVAC systems, LCD panels, and video matrix switchers, using an RS-232 or network connection between one of the EntraPass SmartLink workstations and remote EntraPass WebStations. For advanced system integration, use the bi-directional SmartLink to communicate with software applications including In/Out systems, Badging systems, Human Resource Management systems, and Student Registration systems, 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 redundant server which supports all the features and functionality of the primary server, except the card gateway program. After the primary server returns online, all archives are merged and the entire database is copied or merged from the redundant server.

- ❗ **Note:** The card gateway is not compatible with Windows Server 2008 64 bits. You must install client 32 bits.

KT-NCC controller and gateway

EntraPass is compatible with the KT-NCC Network Communications Controller. Using the KT-NCC allows for access control in a widely-dispersed environment without running extensive amounts of cable from each remotely-located controller back to the server. When combined with the powerful EntraPass Global Edition software, the KT-NCC allows customers to more effectively utilize critical global security features for unsurpassed security.

Dual gateways option

Each global gateway application includes one multi-site gateway when the dual gateways option is enabled. This option does not require any additional license.

Redundant gateway

If the gateway fails, connectivity to controllers is lost. This results in controllers reverting to a mode where controllers keep their card and schedule programming but are not updated. A redundant gateway is up-to-date with the primary gateway but remains dormant until the primary gateway fails. When the primary gateway fails, the controllers automatically switch to the redundant gateway without having to reload. This ensures the system remains fully operational. You must manually reinstate the primary gateway when it is back online.

- ❗ **Note:** The redundant gateway is available only for multi-site gateways.
- ❗ **Note:** The redundant gateway feature is not compatible with DSC PowerSeries Neo or PowerSeries Pro panels.

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:** You must purchase a door license for each wireless door.

Kantech IP Link

EntraPass is compatible with the Kantech IP Link which provides an Ethernet connection that serves as a polling device that controls 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, KT-1, KT-2, and KT-400 controllers

EntraPass is compatible with Kantech KT-100, KT-200, KT-300, KT-1, KT-2, 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 customer's needs and budget.

KT-400 controller

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

Expansion modules for the KT-400

Connect expansion modules to the KT-400 controller to add outputs such as 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 for each KT-400 controller.

- **KT-MOD-REL8:** This 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 for each KT-400 controller.
- **KT-MOD-INP16:** This 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 for each KT-400. Adding the 16 onboard inputs of the KT-400 gives a total of 256 inputs for each KT-400.
- **KT-MOD-OUT16:** This is an open drain to 12 VDC 16-output module. You can use it for elevator access control (which 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 for each KT-400.

Kantech ioSmart card reader

The Kantech ioSmart card reader provides card access for users through a KT-400, KT-1, or KT-2 door controller. The ioSmart supports the transmission of card numbers using Wiegand protocol. Supported formats include the standard 32-bit format, the standard 26-bit format, and other Kantech proprietary formats like eXtended Security Format (XSF) and Smartcard Security Format (SSF). To provide an easy upgrade path to customers, some imodels support both the smart card technology and the Kantech ioProx proximity technology.

Kantech Telephone Entry System

Using the Kantech Telephone Entry System (KTES), users can grant visitors access to a building using their own land telephone or cellular telephone. Using an integrated modem, this telephone line can also serve as a programming link or a monitoring link. The KTES functions as a stand-alone unit or as a part of a complete access control system such as EntraPass 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 KT-100, KT-300, KT-1, KT-2, and KT-400 controllers, and any controller that supports a Wiegand interface port. To simplify the process of importing and exporting tenant lists, an automated procedure has been implemented to guide you through the various steps. For information about the installation and the local programming of the KTES, refer to the *KTES Installation Manual*, DN1769, and the *KTES Programming Manual*, DN1770.

Express setup

Installers can use the express setup program to automatically define and configure 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.

hatrix for managed access control

The hatrix functionality allows a central station to manage several clients. In this type of environment, under a multi-site gateway, a central station can handle several workstations where each client can access their account information on an individual basis. For more information, see the Accounts section.

Elevator control capability

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

Integrated badging

The integrated badging feature in EntraPass allows 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

In EntraPass, you can import and display high-resolution graphics that have been created on CAD-type systems and converted to .jpg or .bmp file types. Using this feature, you can design a graphic-based system that operators can use with minimal training. You can add interactive buttons to floor plans to display component status and allow full manual operation of the component in real-time.

Configurable desktops by operator

In EntraPass, you can assign each operator up to 8 configurable desktops. These desktops display selected windows featuring message events, user photos, filtered events, high-resolution graphics and videos, global alarms and alarm instructions. Desktops can contain any combination of windows.

Interfacing with external alarm panels

KT-100, KT-300, KT-1, KT-2, and KT-400 controllers allow users to arm, disarm, and postpone the arming of an external alarm panel through a multi-site gateway. This allows EntraPass to easily integrate with an external alarm system.

Partitioning alarm system

In EntraPass Global Edition, a site can be divided into 100 alarm system partitions. You can configure each alarm partition with any number of readers, door contacts, motion detectors, sirens, user access rights and arming schedules.

In/Out feature

Operators can use the In/Out feature to print or download time sheets in a CSV format to a payroll system.

Muster reporting for parking and emergency management

In EntraPass, muster reporting allows for roll call reporting which is often used in emergency situations where the location of all personnel is required at once. Muster reports listing all the people belonging to an area can be printed automatically or upon request when an alarm is triggered. Graphics also pop up on screen as soon as an area is vacated. Muster reporting can also be used for parking management where preset parameters can be defined to trigger an action, for example lock a gate, when an area has reached its maximum capacity.

Visual diagnostics

In EntraPass, you can see a visual representation of the system devices, with conditions updated in real-time, including high resolution floor plans that you can import and display. You can add interactive system buttons to the graphic to display component statuses in real-time. You can perform manual operations from the real-time system graphic.

Enhanced video integration

EntraPass integrates with American Dynamics' Intellex® digital video management system through the powerful Intellex Application Programming Interface (API) to provide real-time video monitoring as well as video playback. You can link video to real-time video monitoring as well as video playback. You can link video to access events and you can record video 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. To view a camera directly from a floor plan, double-click the camera or dome button. Operators can configure viewing parameters for digital video applications in EntraPass.

EntraPass video vault

The EntraPass video vault automatically stores all video clips from an Intellex alarm or an EntraPass video alarm 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. You can connect each EntraPass video vault to as many Intellex units as defined within the EntraPass software. You can save video in up to 24 pre-programmed hard drive locations. You can automatically associate a .bmp image with each video clip, and you can automatically create a thumbnail image of the first frame of the video clip.

Vocabulary editor

Use the vocabulary editor to translate the EntraPass software into up to 99 languages. By default, EntraPass is available in English, French, Spanish, German, Italian, Portuguese, Dutch, Turkish, Simplified Chinese, Finnish, Czech, Slovak, Danish, Swedish, and Haitian Creole.

Intrusion integration

You have full access to the panel virtual keypad attached to a KT-400. 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 fetches the data directly from the hardware panel to optimize the provisioning process.

Installation


Use this section to find out what the minimum software and hardware system requirements are for optimum EntraPass performance. Follow the recommendations in the [Security hardening guide](#) for best security practices. For instructions on how to install the system, see [System installation](#). After you complete the system registration, you can add different components. For more information about adding components, see [Adding system components](#).

Minimum system requirements

Operating system compatibility

EntraPass is compatible with the following operating systems:

- Windows Server 2008 R2 Standard/Enterprise
- Windows Server 2012 R2 Standard/Datacenter x64
- Windows Server 2016 Standard and Windows Server 2016 Datacenter
- Windows Server 2019 Standard/Datacenter x64
- Windows Server 2022 Standard and Windows Server 2022 Datacenter
- Windows 7 Pro/Enterprise/Ultimate, all in 32-bit and 64-bit versions
- Windows 10 Enterprise x86/Windows 10 Enterprise x64
- Windows 11 Pro and Enterprise

 **Note:** Ensure that all operating systems have their latest service packs and updates.

 **Note:** Perform software installations with administrator rights.

Ensure that you install the EntraPass software on a computer that meets the following minimum requirements:

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

Web Server

- Dual Core processor
- 4GB RAM
- PCI Express 8X graphics card with 64 MB memory and DirectX 9.0 support
- Microsoft Internet Information Services (IIS) version 7 or later with the latest security updates

hatrix

Install each EntraPass application on its own dedicated server class computer that meets the minimum specifications.

Table 3: EntraPass application specifications

EntraPass application	Server class computer specification	Optional	Dedicated computer
EntraPass Server	Specification 1	No	Yes
EntraPass Corporate Gateway	Specification 2	No	Yes

Table 3: EntraPass application specifications

EntraPass application	Server class computer specification	Optional	Dedicated computer
EntraPass Redundant Server	Specification 1	No	Yes
EntraPass Web	Specification 2	Yes	Yes
EntraPass Workstations	Specification 3	Yes	No

Specification 1

- Pentium Dual Core processor, 2.0 GHz or better
- 500-watt power unit (Preferably a Dual power supply)
- 4 GB RAM.
- 300GB hard disk drive space (preferably RAID 1 or 5)
- CD / DVD ROM drive
- 100/1000 Base-T network adapter (recommended Dual-NIC)
- Appropriate UPS

Specification 2

- Pentium Dual Core processor, 2.0 GHz or better
- 500-watt power unit (Preferably a Dual power supply)
- 4 GB RAM.
- 300GB hard disk drive space (preferably RAID 1 or 5)
- CD / DVD ROM drive
- 100/1000 Base-T network adapter (recommend Dual-NIC)
- Appropriate UPS

Specification 3

- Pentium Dual Core processor, 2.0 GHz or better
- 500-watt power unit
- 4 GB RAM.
- 300GB hard disk drive space
- CD / DVD ROM drive
- (optional) High end video card if doing remote video monitoring
- 100/1000 Base-T network adapter (recommend Dual-NIC)

Virtual environment supported

- VMware Workstation Version 7 and higher

Workstation and Gateway applications with NCC

- Windows® 98 Operating System ONLY (DOS is required for NCC program and is not available with other Operating Systems)
- Pentium III processor at 450 MHz (minimum)
- 64 MB RAM (128 MB recommended)
- 2 GB HDD minimum
- 17 inch screen (1024 x 768 minimal resolution)

- 4 MB Graphic adapter card
- 10/100 MBPS Ethernet TCP/IP Network card

DOS application ONLY

- DOS Version 6.22 or higher Operating System (DOS is required for the Global Gateway program and is not in Windows®)
- Pentium III processor at 450 MHz (minimum)
- 64 MB RAM (128 MB recommended)
- 2 GB HDD minimum
- Requires EMS memory

Additional requirements

For several applications, you can use the following devices:

- **Video capture card:** to capture user images for card identification
- **Sound card:** to use warning sounds when an alarm is reported
- **Badge printer:** to print badges (Badging)
- **Signature capture device:** to capture signatures (Badging)
- **Log printer:** (dot-matrix or laser) to print events (messages and alarms)
- **Report printer:** (laser) to print reports

Security hardening guide

To ensure the highest level of security for EntraPass, use the following setup, configuration, and installation measures.

⚠ CAUTION: Failure to comply with the following security configuration may result in a weakened operational state with related security vulnerabilities.

To comply with 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. For information about how to implement SSL in internet information services (IIS), refer to the Microsoft website: <https://support.microsoft.com/en-nz/help/299875/how-to-implement-ssl-in-iis>

📘 Note: This link is only for reference; contact Microsoft for support on how to implement SSL.
3. Change default passwords during installation.
4. To improve system performance, use a load balancer with your routers in front of the EntraPass server. For information about how to set up the load balancer, refer to the product manufacturer's installation guide.
5. To isolate EntraPass servers, use a firewall. In the firewall, only open ports that you require to use EntraPass. Block all other internet traffic. For a list of default ports used with EntraPass, see [Communication ports](#).
6. To protect your information, store data backups in a secure location.

System installation

1. Before you begin the installation, close all EntraPass applications.

2. Insert the software USB flash drive into a USB port, or the CD-ROM into the CD-ROM drive. If your computer is configured to autorun, the installation program starts automatically. If the installation program does not start automatically, click **Start**, click **Run**, and, in the field, enter `D:\Setup.exe` (D: is the CD-ROM drive).
3. From the **Choose setup language** list, select a language. English is selected by default.
 - ① **Note:** You cannot change the setup (InstallShield) language if you need to perform an EntraPass update or install system components with a different language. To change the setup language, you must remove and re-install the software.

The system and database language depends on the language you select when installing the software. For example, if you select **English**, it is the system default language at start up. You can change the system and database language in the EntraPass Server and EntraPass Workstation.
4. Click **OK**. The **Welcome** window displays.
 - See the software version you are about to install in the upper left of the window.
 - To verify or modify parameters you have set up, navigate between the installation windows by clicking **Back** or **Next**.
 - You can cancel the installation at any time.
5. Click **Next** to continue the installation.
6. In the **Setup Start** window, select the operations you want to perform. The first set of options are for new installs and the last option is for updates. During the first installation, you can select only one of the install options. We suggest that you select the first install option on the list.
 - **Install Server, Database and Workstation :** Select this option to install the EntraPass Global Edition system. It is greyed out if the application is already installed on the machine.
 - **Install Additional Workstation:** Select this option to install an additional workstation. It is greyed out if a server or a workstation is already installed on the machine.
 - **Install EntraPass System Components:** Select this option to install optional or additional EntraPass system components such as Gateways, WebStations, SmartLink, Video Vault, Oracle/MS-SQL Interface and Mirror Database and Redundant Server. The option is greyed out if the component is already installed on the computer.
 - ① **Note:** Install the redundant gateway using the Gateway option. The serial used for registration distinguishes it as a redundant gateway.
 - **Install EntraPass System Tools :** Select this option to install EntraPass System utilities such as vocabulary editor, report viewer, and video viewer. The option is greyed out if the utility is already installed on the machine.
 - **Update Installed Applications:** This option is greyed out if the system has not been installed previously. To update your EntraPass system, see *Updating EntraPass*.
7. Click **Next**.
8. In the **Serial Number** window, enter the serial number for the EntraPass Global Server or Software. The information is located in the CD-ROM pocket. Make sure to enter the correct digits. The **Next** button activates only if the serial number is valid.
9. Click **Next**.
10. Review the End-User License Agreement (EULA). If you understand and agree with the conditions that are described in the EULA, click **I accept**, or, to cancel the installation, click **I do not accept**.

① **Note:** You cannot complete the installation if you do not accept the EULA.

11. Click **Next**.
12. In the **Customer Information** window, enter the user name and the company name.
13. From the **User Type** list, select one of the following options:
 - Anyone who will use this computer
 - Only the person currently logged in and registered in the system
14. Click **Next**.
15. In the **Choose Destination Location** window, you can keep the selected directory and click **Next**, or select another directory.
 - To change the directory, click **Change**. In the **Choose Folder** window, select the new installation directory.
 - Type the destination directory or double-click the directory structure to find the destination directory, and click **OK**. In the **Choose Destination Location** window, the path to the directory updates.
16. Click **Next**.
17. In the **Ready to Install the Program** window, review the parameters that you set up. If everything is ready for the installation, click **Next**, or if you want to change a parameter, click **Back**.
18. In the **Installation setup** window, select the primary and secondary languages, and click **OK**. This defines the language that is used to build the database and the languages that are used to run EntraPass, and click **OK**.
19. During the installation process, you are prompted to install the Intellex API. If you require the Intellex API, click **Yes**, and follow the instructions.
20. You can select to install the applications as Windows services. Applications that run as Windows services automatically restart after a system shut down even if it is accidental.
21. You can select to restart your computer at this time or do it later.
22. Remove the USB flash drive or the CD-ROM.
23. Click **Finish** to complete the installation.

① **Note:** You must restart the computer after the installation.

System registration

Register the system as soon as possible so that users can install additional options and can use the access system without restrictions. Before the system is registered, it is functional but it is limited to only 10 cards, and operators are logged out after one hour of idle time and they must re-enter the randomly-generated 20-character password to log on.

Registering the system

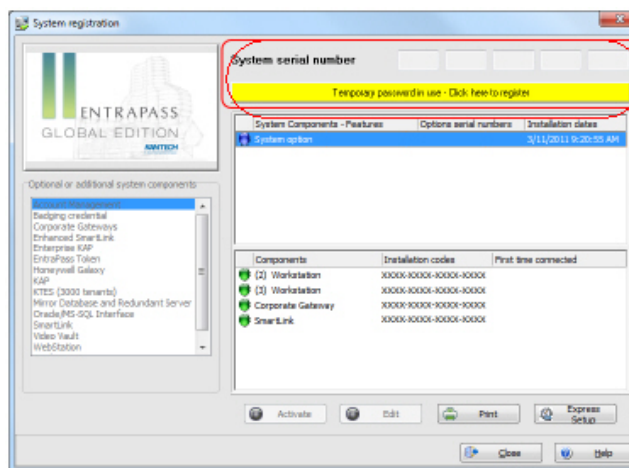
1. To start the EntraPass Server, click the **Server** icon on the computer desktop, or go to:
Start > EntraPass Global Edition > Server > Server .
2. Click the **Login/Logout** icon.

Figure 1: Operator login window



3. In the **Operator login** window, in the **User name** field, enter `kantech`. The field is not case sensitive.
4. In the **Password** field, enter the temporary 20-character password that displays at the bottom of the **Operator login** window. The temporary password displays only in new installations and is highlighted in yellow.
 - ① **Note:** After you complete the system registration, you must change all default usernames and passwords.

Figure 2: System registration window



5. In the **System registration** window, click **Temporary password in use - Click here to register**. This button appears only on new installations.
 - ① **Note:** To register a new system, you need a registration confirmation code. You can get the code online at www.kantech.com, or you can contact your local technical support.
6. Log on to the Kantech website at <http://www.kantech.com>.
 - ① **Note:** If you do not have logon details for the Kantech website, click **Register**, complete the **Site Registration** form, and click **Submit**. You will receive your membership confirmation by email within 1 to 2 business days.
7. Click the **Support** tab, click **Kantech Registration**, and click **Kantech EntraPass Software Registration**.

8. On the **EntraPass Software Registration** page, in the **Serial Number** field, enter the system serial number, and complete the registration steps to get the registration confirmation code.
9. In EntraPass, in the **System Registration** window, in the **Registration Confirmation Code** field, enter the registration confirmation code, and click **OK**. The **OK** button activates only when the registration confirmation code is valid.

❗ **Note:** If you exit the Server main window without registering the system, the **Change Authentication Password** window displays. It does not display after the system is registered.

Adding system components

About this task:

After you register the Server, you can install additional system components, including EntraPass applications and other utilities such as the EntraPass Video Vault application. Before you install system components, ensure that the designated computer meets the minimum requirements.

❗ **Note:** 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. On the EntraPass Server, click **Connection**, or on the EntraPass workstation, click **Options**, and click **System Registration**.

❗ **Note:** The EntraPass Server has five workstation applications and one Global Gateway application. One workstation application installs automatically 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 four additional workstation applications. Ensure that the computer you are installing them on meets the minimum requirements. For information about the minimum requirements, see [Operating system compatibility](#).

2. To print the installation codes, click **Print**. Use the codes when you install the workstation or gateway applications. To avoid errors, do not copy the codes onto 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. In the **System registration** window, in the **Optional or additional system components** pane, select the component that you want to install, and click **Click here to install component**.

4. In the **Component registration (Name of component)** window, in the **Option serial number** field, enter the option serial number. The serial number is located on the option certificate.

❗ **Note:** To register a new component, you need a registration confirmation code. You can get the code online at www.kantech.com, or you can contact your local technical support.

5. Log on to the Kantech website at www.kantech.com.

❗ **Note:** If you do not have logon details for the Kantech website, click **Register**, complete the **Site Registration** form, and click **Submit**. You will receive your membership confirmation by email within 1 to 2 business days.

6. Click the **Support** tab, click **Kantech Registration**, and click **Kantech EntraPass Software Registration**.

7. On the **EntraPass Software Registration** page, in the **System Serial Number** field, enter the system serial number, and complete the registration steps to get the registration confirmation code.
8. In EntraPass, in the **Component registration (Name of component)** window, in the **Registration confirmation code** field, enter the registration confirmation code you receive, and click **OK**. The **OK** button activates only when both codes are valid.
 - ① **Note:** After you enter the registration confirmation code, the system generates an **Installation Code** in the **System registration** window. Blue flags identify components that have been created but that are not activated. Green flags indicate components that are activated. You need the installation code when you are ready to install the component with the EntraPass CD-ROM.

Figure 3: Installation codes

Component Name	Status Flag	Registration Code
(4) Workstation	Blue flag	XXXX-XXXX-XXXX-XXXX
Corporate Gateway	Blue flag	XXXX-XXXX-XXXX-XXXX
Smartlink	Blue flag	XXXX-XXXX-XXXX-XXXX
Video Vault	Blue flag	XXXX-XXXX-XXXX-XXXX
Mirror Database and Redu...	Blue flag	XXXX-XXXX-XXXX-XXXX
(4) Workstation	Blue flag	XXXX-XXXX-XXXX-XXXX
(5) Workstation	Blue flag	XXXX-XXXX-XXXX-XXXX

9. Repeat Steps 3 to 8 for each system component.
 - ① **Note:** You need to establish communication between the EntraPass Server and the computer where the new component or option is installed, if applicable. Perform this step only if you have installed the component or option on a different computer to where the EntraPass workstation application is installed.

Windows services

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

Table 4: Windows system tray icons

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

Right-click the **Active directory** icon to access the following options:

- **Start:** starts the service.
- **Stop:** stops the service.
- **Restart:** stops and then restarts the service.
- **Sync NOW:** pushes the active directory changes to EntraPass immediately.
- **View LOG:** opens the folder where the `log.txt` file is located.

On the **About** menu, see general information about the application, such as the version installed, technical support contact details, and copyright.

System components edition

In EntraPass, users can assign custom names to applications for easy identification in system events. You can also modify the component names in the definition menu. To access the definition menu, click **Devices** and click **Application**.

Assigning a descriptive name to an application

1. In the **Registration** window, select an application, and click **Edit**.

Figure 4: Edit a component window

2. In the **Edit a component** window, in the **Description** fields, enter a descriptive name for the application. If EntraPass runs in two languages, enter two names, the first in the primary language and the second in the secondary language.
 3. Select any of the following options that apply to the application:
 - **Workstation locked:** select this option if the application will be installed on a computer and will be used only for receiving system events.
 - **Locked for authentication:** select this option if you do not want the computer where you have installed the EntraPass application to send its authentication data to the server.
 - **Use specific password for authentication:** select this option if you want to assign a specific password to this workstation. If you select this option, in the **Authentication password** field, enter the password.
- ① **Note:** The **Application type** field displays which type of application the selected EntraPass application is. For example, if the application is a Multi-site Gateway application, it displays **Multi-site Gateway**. The application type also displays in the EntraPass application definition window.
- ① **Note:** In hattrix, the **Edit a component** window only displays the **Description** fields so that you can set up a name for your master account.

Getting started

Use this section to learn how to perform [Basic functions](#), including how to start the system and how to find and manage components. The [EntraPass toolbar](#) section provides a table with an image and description of all the toolbar icons. If you want to minimize the time for defining system components, go to the [Express setup](#) section. To view a component in a hierarchy list, see the [System tree view](#) and the [Using the extended selection box](#).

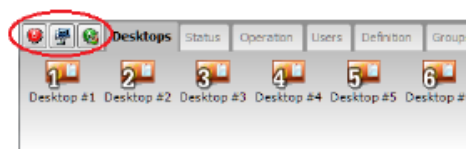
Accessing an account under hattrix

The hattrix option is available only after you register the hattrix feature using an option serial number. For more information about registering additional components, see [Adding system components](#).

After you register hattrix, you can become an account operator or an account manager, depending on your operator level.

- As an account operator, you have access only to an account that a system administrator has assigned to you. Your logon name and password take you directly to that account in the EntraPass main window.
- As an account manager, you can access several accounts. When you log on to EntraPass, a **Switch account** icon displays next to the **Login/Logout** icon.

Figure 5: Switch account icon



Switching account and security level

1. To access an account, select the account manager.
2. From the **Account** list, select an account.
3. Select a workspace.
After you switch account managers, system requests are adjusted accordingly. Events can be restricted based on the selected account or account manager.

Basic functions

Use this section to find information about the following basic system operations:

- Finding components
- Using the extended selection box
- Selecting components, a specific folder, a connection or a gateway
- Printing lists or reports
- Viewing links between components
- Calling the system tree view

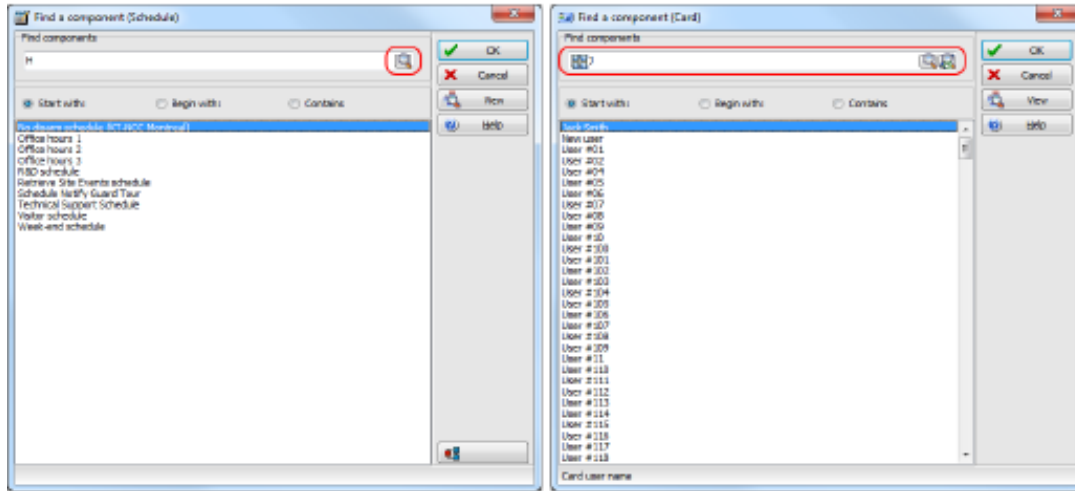
Finding components

About this task:

To search for a component or a card in the system database, use the find a component search function.

There are two types of find a component window: access one type on any EntraPass window toolbar, and access the other type on the toolbars on any of the windows that relate to users.

Figure 6: Find a component windows



The following table lists the find a component search icons and their functions.

Table 5: Search icons

Icon	Description
	Click the Find icon to search for components or cards.
	Click the Details icon to search for the picture that corresponds to the card you search for.
	Click the Index icon to select which criteria you want to search, for example, card number, email or card information fields.

To search for a component or a card, complete the following steps:

1. On the window toolbar, click the **Find** icon.
2. In the **Find a component** window, in the **Search** field, enter a keyword.
3. To narrow the search results, click one of the following buttons:
 - **Start with:** the list of results includes all of the components that start with the keyword you enter, in alphabetical order, and includes all other components in the database.
 - **Begin with:** the list of results includes only components that start with the keyword you enter.
 - **Contains:** the list of results includes all of the components that contain the keyword you enter.
4. **Optional:** When you search for cards, the default search criteria is card user name. To change the search criteria, on the left of the **Search** field, click the **Index** icon and select which criteria you want to search, for example, card number or email.
5. **Optional:** When you search for cards, to search for the picture that corresponds to the card you select, click the **Details** icon.
6. Click the **Find** icon.
7. From the list of search results, select the component that you want to display.

8. Click **OK**. The component that you select displays in the window where you initiate the search.

Using the extended selection box

Use the extended selection box to view and search all of the components of a drop-down list. This option is available for components such as applications, controllers, and doors. If the option is available, when you place the cursor over the list, a tooltip displays the following message: **Right-click to load the extended selection box**.

1. To view the **Extended selection box** window, right-click the list.
2. To filter the list, in the **Text filter** field, enter a search term. In the **Filters type** area, select from the following filter options:
 - Contains
 - Starts with
 - Ends with
 - Exact words
 - Selected
3. Select the **Filter on enter** or **Suppress address** check boxes, as required.
4. In the **Columns** field, select the number of columns you want the list to display.

Selecting components

About this task:

Operators can use the component selection function to select one or more system components.

1. In the active window, click the **Select Components** button.
2. Select the options that are displayed or click **Select All** to select all of the displayed options. To view components that are not grouped, click **Single**, or to view existing groups, click **Group**.
3. From the list, select the component or group that you want to display.
4. To display the components associated with the selected component, click **View**.
5. Click **Select all** to select all of the components, if available, or click **Clear all** to remove the check marks from the selected components.
6. Click **Cancel** to return to the previous window without making any selections or changes.
7. In the **Extended selection box** window, in the **Columns** field, select the number of columns that you require to display all of the components. For more information, see [Using the extended selection box](#).
8. To apply your changes and return to the previous window, click **OK**.

Selecting a specific folder

About this task:

To locate a specific folder on your network or hard drive for a backup or other functions, complete the following steps:

1. In the active window, click the **Select** button. It is identified by "...".
2. In the lower part of the window, browse through the **Drives** list. To ensure that the displayed list is up-to-date, click **Refresh drive**.
3. When you locate the folder you require, select it, and click **OK**.

Selecting a specific connection or gateway

About this task:

You can associate a specific component with a specific gateway/connection. For example, you can define a specific holiday for a specific connection or gateway.

1. In an active window, click the **New** icon.
2. In the selected gateway/connection window, double-click a gateway/connection from the displayed list, and click **OK**.
3. Enter a meaningful name for the component that you are defining.
4. Follow the steps to complete the task.

Printing a list or report

About this task:

Operators can use the print function to complete the following tasks:

- Print a list of cards
 - Print event-relay association
 - Set up a report for printing
1. In any EntraPass window, click the **Print** icon.
 2. Select the components that you want to include in the list or report. If available, click **Select all** to include all the displayed components in the list or report.
 3. Select **Print empty fields** and **Print component reference**, if available, to include the titles of the fields even if they are empty.
 4. Click **Font**, and in the **Font** window, select the font type, style, size, and color for your list or report. Click **OK**.
 5. Click **Preview** to preview the list or report and access the following options:
 - Define the printer setup.
 - Print a hard copy of the list or report.
 - Save the list or report for later use using the **Quick Viewer** program, or load an existing report. For more information, see [Quick Report Viewer](#).
 6. Click **Print**.
- ❗ **Note:** If there is no printer configured for the computer, an error message appears.

Viewing component links

About this task:

Use the view component links feature to view all instances of an item within other menus. You can view all links an item has with other items. Before you delete a component from the database, click the **View links** icon to find out which menus are affected by the deletion.

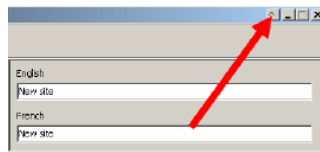
1. In any EntraPass window, select a component and click the **View links** icon. All the components that are associated with the selected component display. For example, on the EntraPass workstation, click **Definition** and click **Schedule**. From the **Schedule** list, select **Always valid**, and click the **View links** icon. The system displays 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 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.

2. To view the links of the selected door with other components of the system, select the door and click the **View links** icon again. All system components that are associated with the selected door appear. In this example, the door is used in the administrator access level; users that are granted this access level are allowed to access the selected door.
3. To print the list of links for the selected component, click **Print**.

Floating windows

Use the **Floating window** button to move a window outside of the workstation. The **Floating window** button is located to the left of the **Minimize** button on windows that support the floating window function. To return the window to the workstation, close it and reopen it. No information about the window's position is kept by the system.

Figure 7: Floating window button



System tree view

Use the system tree view function to view list of components in a hierarchical format. You can select or deselect the components that are displayed in the system tree view. Access the system tree view in any of the following ways:

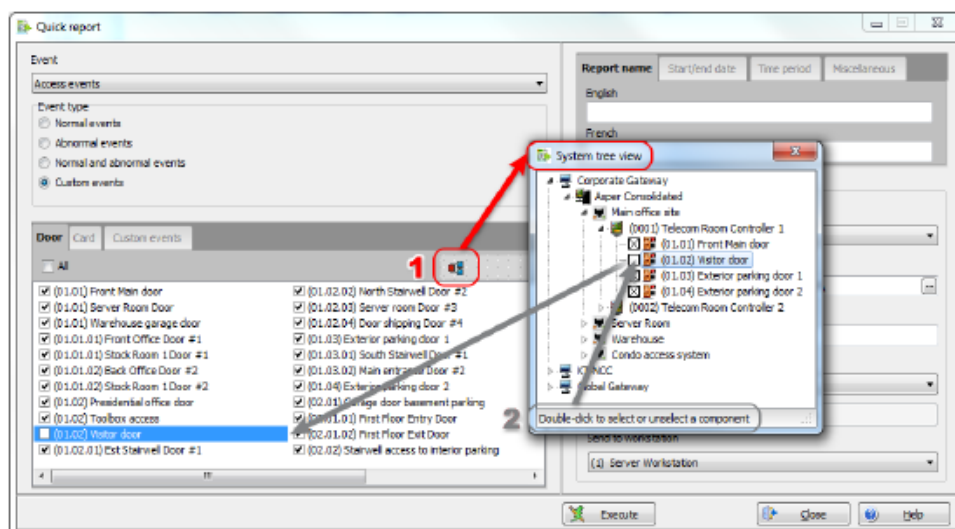
Accessing the system tree view in a window

About this task:

You can access the system tree view in some windows.

1. On the EntraPass workstation, click the **Reports** tab, click **Quick report**, and click the **System tree view** icon.
2. In the **System tree view** window, double-click to select or deselect a component. The changes automatically update on the corresponding tab.

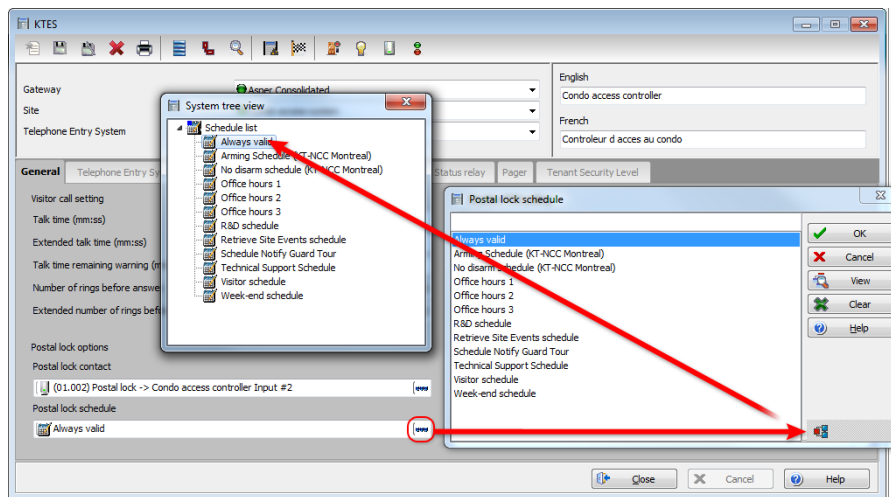
Figure 8: System tree view in quick report window



Accessing the system tree view using the more options icon

- In a given data field, click the **More options (⋮)** icon, and then click the **System tree view** icon.

Figure 9: Accessing the system tree view using the more options icon

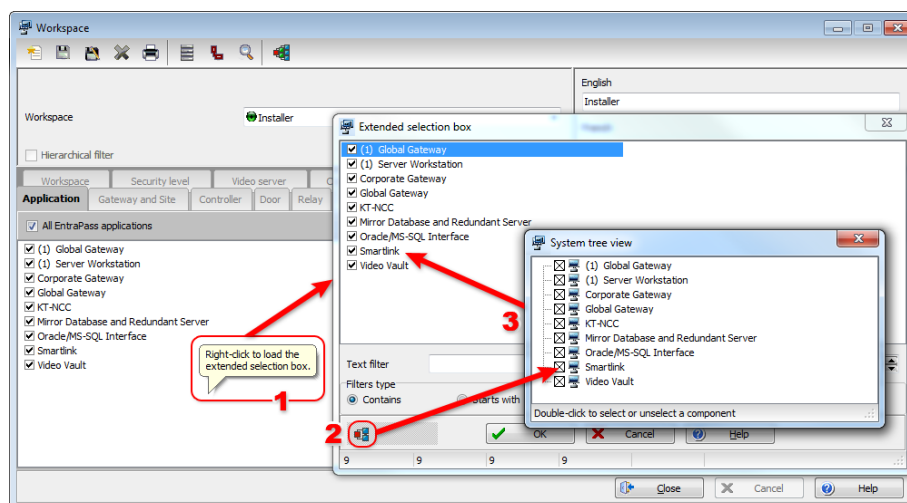


Accessing the system tree view using the extended selection box

1. On the EntraPass workstation, click the **System** tab, click **Workspace**, click the **Application** tab, and right-click.
2. In the **Extended selection box** window, click the **System tree view** icon.
3. In the **System tree view** window, double-click to select or deselect a component. The changes automatically update in the **Extended selection box** window.

Example:

Figure 10: Accessing the system tree view using the extended selection box



Using the comment field as a notepad

In the **Card**, **Account**, and **Device** windows, click the **Comment** tab and enter your comments. Alternatively, double-click anywhere in the blank section of the window. In the **Notepad** window, enter your comments. Click **Save**. The text you enter displays in the **Comment** tab.

Deleting an item

To delete the currently selected record, click the **Delete** icon. To protect against accidental deletion, a warning displays and you must confirm that you want to delete the item.

In the **Delete details** window, view the estimated server processing time for the deletion operation, and the number of:

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

When a component is deleted, all links with other items are deleted. However, the archived records are kept in the database after an item is deleted.

Viewing component links

- For information about how to view links between components, see [Viewing component links](#).

EntraPass toolbar

EntraPass windows display a selection of the following toolbar icons to provide quick access to system functions.

Table 6: EntraPass toolbar icons











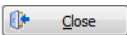
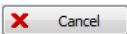







Icon	Description
	Click the New icon to add new items, such as connections, schedules and controllers, to the system database.
	Click the Save icon to save all of the information you have entered since the last save. Information saves directly in the system.
	Click the Save As icon to save all of the information of an existing component under a new name without affecting the original component. If you use this option while issuing a card, you can create a new card or save under a new card number without having to modify the information of the original card.
	Click the Delete icon to delete the currently selected record. To protect against accidental deletion, a warning displays and you must confirm that you want to delete the item. When a component is deleted, all links with other items are deleted. However, the archived records are kept in the database after an item is deleted.
	Click the Print icon to print information. Depending on which window you are working in, you can print items such as reports or card lists.
	Click the Parent icon to display your search in a hierarchy or, according to the menu you are in, to divide searches by gateways, connection, and controller. This icon is useful when the system database increases in size as you can find a specific item by selecting its parent items.
	Click the View links icon to view all instances of an item in other menus. For more information, see Viewing component links .
	Click the Find icon to search for a specific item or component in the system database. For more information, see Finding components .
	Installers and system administrators can click the Express Setup icon to configure system devices by assigning default settings.

Table 6: EntraPass toolbar icons

Icon	Description
	Click the System tree view icon to display the components list in a hierarchy. You can select or deselect the components displayed in this window.
	Click the Close button to close a window. If you forget to save information before closing a window, the system prompts you to confirm the save operation.
	Click the Cancel button to cancel all modifications that were made since the last time a valid save was performed. The system prompts you to confirm the operation.
	Click the Help icon to view the help content about the EntraPass window you are in.
	Click the OK button to save and accept the modifications, additions or deletions made to a record in the system database.
	Click the Select all icon is to select all of the items or components that are displayed in a list.
	Click the Remove all icon to deselect all of the items or components that were previously selected in a list.
	In several system windows, operators can access graphic and animation icons. Use these icons to display the status of a component before performing an operation on that component. In the Status and Operations windows, click the Enable graphic icon to display the image related to the selected component, for example, a door, and to display the associated components, for example, a reader. To display components in real time, use this icon with the Enable animation icon.
	If you click the Enable animation icon to activate it, the Enable graphic icon is also activated. If you click this icon, the status of the selected component displays in real time. For example, when you lock a door which was previously unlocked, the image of the reader is modified; the green dot changes to red.
	Click the Audit trail button to open the Audit trail window. View the date and time of changes, and the operator who made the changes to a component or a card. This feature is available in any window where you can edit a card or a component. For more information, see Card audit trail .
Right-click	Right-click to access a shortcut menu and select specific commands depending on which window is open.

 **Note:** Toolbar icons for features that are not activated are automatically hidden from view.

Express setup

Use the express setup to configure system components, such as sites and controllers, and 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.

Use the express setup to configure a connection or to define controllers associated with a connection. When used to configure a connection, installers can associate the connection with a gateway. Installers can configure the connection rapidly, giving minimum configuration information about the controllers connected to it.

When used to configure a controller, operators can assign default values to a controller and to its associated devices, such as input, relays, and output. In this case, it is launched from a system message window or from a controller definition menu.

There are two versions of the express setup program: Express Setup NCC only configures global gateways and Express Setup only configures multi-site gateways.

To start **Express Setup**, go to: **Start > All Programs > EntraPass Global Edition > Server > Express Setup** or, in any appropriate EntraPass window, click the **Express Setup** icon.

- ① **Note:** You must log on to the server when you start **Express Setup**. As the program allows you to modify the system devices configuration, you must authenticate yourself before proceeding with any modification.

Session Start and End

1. 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.
2. 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.

① **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

Use the EntraPass server for the following functions:

- Displaying all the applications connected to the server, the system event and system error logs
 - Registering new connections including workstation applications, gateway applications, client applications such as SmartLink, Video Vault, and Report Viewer
 - Performing backups of data, archives, and in/out databases
 - Restoring data, archive, and in/out databases
 - Verifying database integrity
 - Changing the database language
1. From the **Start** menu or by clicking the desktop icon, start the EntraPass server. The **Server start up** window displays a progress bar and information related to the server start up process. When the process is complete, the logon window displays.
 2. Click the **Login/Logout** button.
 3. In the **EntraPass Operator** logon window, enter your **User name** and **Password**. The default user name is `kantech`. It is not case sensitive. Create a new password. For information about creating passwords, see [Password rules](#).

① **Note:** To allow an operator to log on to the server, the system administrator must click **System > Security Level**, and select the option **Allow login on server**. For more information, see [Security Level Definition](#).

The system stores the last five user names, allowing operators to select their user name from the list. To delete a user name from the list, select the user name and press Delete

on the keyboard. By default, the **Display Login List** parameter is disabled. You must enable it in the **EntraPass Application** window.

4. After you enter the correct logon information, the EntraPass server main window displays with the toolbars activated. Select the desired toolbar to perform an operation or to display system information.
 - ❶ **Note:** The color of the status bar indicates the communication status: green indicates that communication is working and red indicates communication problems.
5. Hover over the status flag to see a tooltip which describes 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 may 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

About this task:

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.
 - ❶ **Note:** The Gateway type field indicates the gateway that is running. It may be a Multi-site Gateway or a Global Gateway.
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.
 - ❶ **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.

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 is installed. Operators use the workstation to access and program the system database and components.

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

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

- ① **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, just start the server.

1. From the **Start** menu or by clicking the desktop icon, start the EntraPass workstation.

- ① **Note:** When the server is offline, the first status flag on the left (coloured rectangles of the status bar) turns red; the **Login/Logout** icon is disabled. If this happens, launch the server and the EntraPass workstation resumes its operation.

2. Click the **Login/logout** icon.

3. Enter your **User name** and **Password**. The default user name is `kantech`. It is not case sensitive. If you have not already done so, create a new password. For information about creating passwords, see [Password rules](#).

- ① **Note:** If you cannot log on, check if the Caps Lock key on your keyboard is activated. When you log on successfully, the system menu, toolbar, and status bar are enabled.

By default, operators are not allowed to log on to more than one EntraPass workstation at a time. If required, an operator can have concurrent logons. For more information, see [Creating or editing an operator](#). An operator can log on to the EntraPass server and the EntraPass workstation at the same time.

Accessing an account under hattrix

For information about accessing an account under hattrix, see [Accessing an account under hattrix](#).

Switch Account and Security Level

1. To access an account, select the account manager:
2. Select an account from the **Account** drop down list.
3. Select a **Workspace**

Result

After switching account managers, system requests will be adjusted accordingly. Events can be restricted based on the selected account or account manager.

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.
- ① **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

About this task:

In EntraPass, you can open multiple windows in the desktop area. When a window is minimized or sent to the background, it completely disappears from the screen. Use a command in the workstation contextual menu to retrieve the windows.

- If the window is minimized, the command in the menu brings it to the front of the screen where you can maximize it.
- If the window is sent to the background, the command in the menu brings 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.
2. In the contextual menu, view the list of open windows. Select the window that you want to view. For example, select **Status screen** to bring it back to the foreground.

Using the extended selection box

About this task:

For information about how to use the extended selection box, see [Using the extended selection box](#). For information about how to use the extended selection box to access the system tree view, see [Accessing the system tree view using the extended selection box](#).

Desktops

Use this section to view events that have alarms defined to them, ensure you first define the alarm and associated schedule and [Creating a new trigger](#) in the definition section. You can also view the [Custom report desktop](#) to view pre-defined reports, their generation status, and when available video recordings.

Use the [Graphic desktop](#) to view the exact location of a component on a connection, and obtain a status update. The [Picture Desktop](#) displays the cardholder's picture with access events notifications. An operator with the correct permissions can use the [Specific desktop customizing](#) feature to transfer or customize a desktop for an operator with read-only permissions.

Follow the steps in the [Changing the Display Properties](#) procedure to change the appearance of your desktop, and follow the steps in [Customizing event display in the message desktops](#) to define how you want you organise the events view.

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).

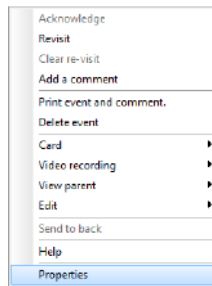
Defining an Alarms Desktop

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](#).

- ① **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.
- **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.

Viewing System Alarm Messages

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

About this task:

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.
 - ① **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.

- ① **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.

- ① **Note:** When an alarm message is acknowledged by an operator, the notification is acknowledged or removed at all workstations.

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**.

- ① **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**).

- ① **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.

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.
- ① **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.

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

About this task:

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).

① **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.

① **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).

① **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 an event group to display the events from that group. Select none to block all messages.

For more information about event groups, see [Filtering Desktop Events](#).

See the following list of options available on this menu:

- 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.

① **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 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**.

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 is 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 changes from green to blue to indicate a custom report is being generated. It turns green again when the data transfer is completed and the data is 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 customreport state in real-time

About this task:

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 appears.
2. Select **Report State** . The **Report State** dialog opens displaying report generation information.
3. When the report is generated in the **Desktop** window, the information in the **Report State** dialog disappears. Click **Close** .

Comment entry and display

A comment can be added to any type of event. In the fifth column from the left, a '-' sign indicates that a comment has been added by the system while a '+' sign indicates 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 want to play and right-click to access the contextual menu.
2. If the video is stored in the EntraPass Video Vault, the **Play from Vault** option is enabled. When you click on it, the **Video Playback** window opens 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). 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.
- ① **Note:** To change the font colour of system messages: **Options > Event color and priority**.

Defining a system search desktop

About this task:

Use this feature to search for a card globally across all the different accounts. The operator can view or edit the cards resulting from that search.

1. On the **Desktop** tab, right-click a desktop.
2. In the **Desktop properties** window, in the **Desktop name** field, assign a name to the new desktop.
3. Select the window type for this desktop.
4. Select the **System Search** option.

- ① **Note:** For more information about activating the system search option, see [Creating and modifying operator security levels](#)

Result

After it is activated, the operator can access the desktop. By entering a user name or part of it, the system displays information related to the cards associated with that user.

If permitted by the operator's security level, you can view or edit a card or account by right-clicking on the selected card. The operator can also grant a one-time access on a door.

The screenshot shows a web-based interface for managing access control. On the left, there is a search section titled 'Card user name' with a text input field containing 'mike' and a 'Search' button with a magnifying glass icon. To the right of the search section is a table with two columns: 'Card user name' and 'Card number'. The table contains one row with the values 'Mike' and '46:54650'. Below the search section is another table with two columns: 'Gateway or Site' and 'Door'. The 'Gateway or Site' column lists five entries, all starting with '01 - Global Gateway'. The 'Door' column lists five entries: 'Controller #1 Door #1', 'Controller #1 Door #2', 'Controller #2 Door #1', 'Controller #3 Door #1', and 'Controller #3 Door #2'. A blue button labeled 'One-time access door' is positioned over the second row of the 'Gateway or Site' table.

Card user name	Card number
Mike	46:54650

Gateway or Site	Door
01 - Global Gateway	Controller #1 Door #1
01 - Global Gateway	Controller #1 Door #2
01 - Global Gateway	Controller #2 Door #1
01 - Global Gateway	Controller #3 Door #1
01 - Global Gateway	Controller #3 Door #2

Filtered Messages Desktop

The **Filtered Messages** desktop allows operators to display specific events. For example, you can create filters to display events that are related to a specific controller and from a particular gateway of the system. If this is the case, those events will be displayed in the **Filtered Message** desktop. Filtered messages are defined in the **Message filters** menu: **System > Message filters**.

- ① **Note:** When you use filters, the system retrieves events that are already displayed in the **Messages** desktop and filters these events according to the selected filters.

Configuring a Filtered Messages Desktop

1. From the Desktop main window, select the desktop you want to configure as a **Filtered messages desktop**.
2. Assign a meaningful name to the **Filtered message desktop**; then define the desktop type (Message window, Picture window or both).
3. You can change the **Text filter**, to display specific events. For information about the **Filtered messages** desktop, see [Message List Desktop](#).






Graphic desktop

Use the Graphic desktop to display the graphical location of an alarm occurrence. To enable this function, you must define the graphic in the system. For more information, see [Graphics Definition](#). 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](#).

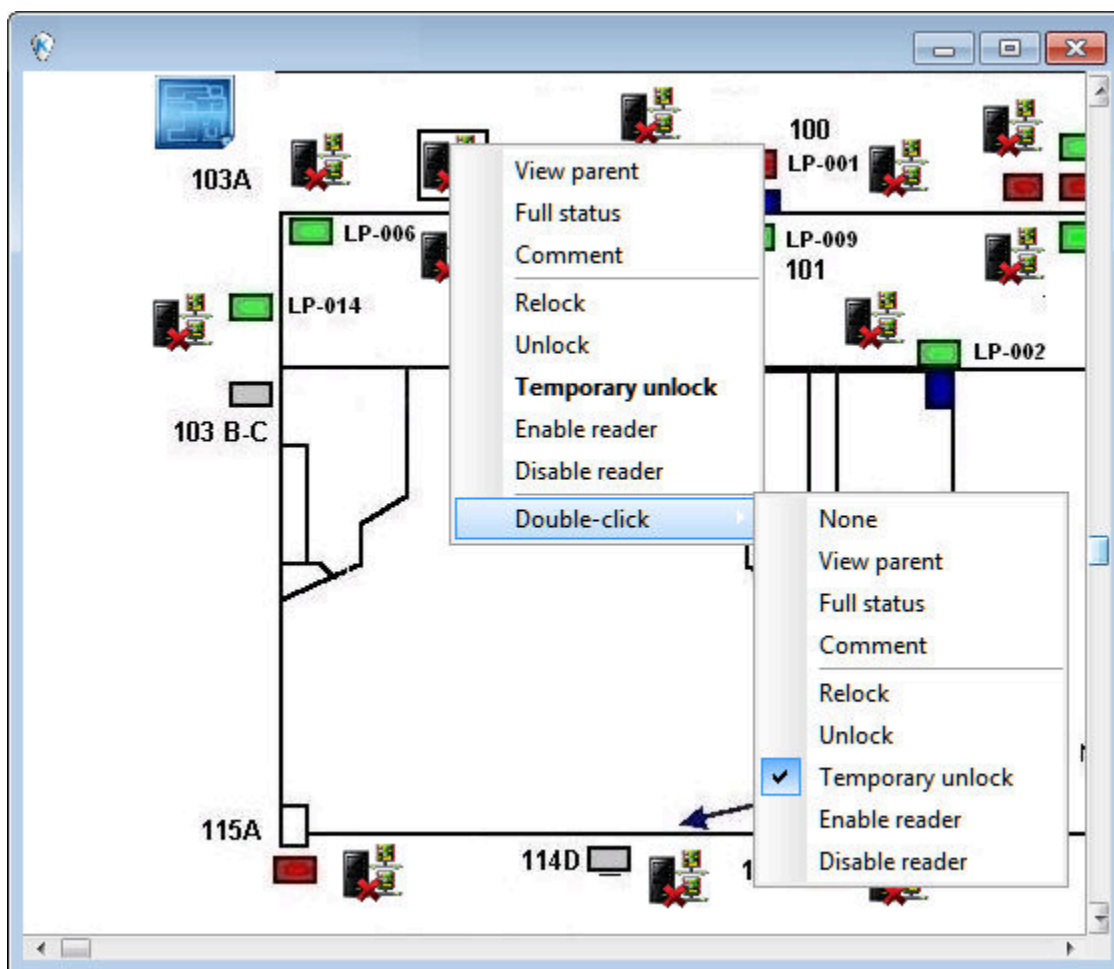
The following table describes the icons that display on the graphic.

Table 7: Graphic icons

Icon	Description
	Area group is active: cardholders are in one or several areas of the area group.
	Area group is empty: all cardholders have vacated the areas within the area group.
	Area is active: cardholders are in the area.
	Area is empty: all cardholders have vacated the area.
	Area is full: an operator has applied a cardholder limit to the area, and the area has reached its limit.

Viewing Graphics in the Graphic Desktop

1. Select the desktop button you want to assign to graphic, name the desktop (Graphics, for example), then define the window type (**Floating** or **Desktop**).
2. Click **OK and Go** to display the **Graphics** desktop.
3. Right-click anywhere in the **Graphic** desktop then, from the shortcut menu, select the graphic you want to display.
 - ① **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 will have to manually request the results for the component by using **Show result**.
5. Right-click a component in abnormal condition to enable a sub menu.



① **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, for more information see the [Comment Field](#).
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.

① **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](#).

Area graphic

The area graphic represents an area or an area group that you want to monitor. The graphic automatically updates every five seconds. To use additional functions, right-click a component icon to display the shortcut menu:

- **View parent**
- **Full status**
- **Comment**
- **Area empty**
- **Get card in area**
- **Search and locate user**

Area empty

About this task:

Use area empty to move all cards from one area into another area. For graphic icon descriptions, see [Monitoring an Area Group](#). The area graphic changes to reflect the move, and the area report indicates the move in the last reader swiped and date and time columns.

To move all cards from one area into another area, complete the following steps:

1. Click **Area empty** to open the **Area** window. A list of all areas appears in the left pane.
2. In the left pane, select the area that you want to move the cards into. The right pane populates with all the components that you have moved. The area graphic changes to reflect the move, and the area report indicates the move in the date and time column.

Area card list

1. To open an area card list, or an area group card list, click the component icon.
2. Right-click and click **Get card in area**. The area card list appears. You can open a maximum of three area card lists at one time. If you open a fourth list, the first list closes. When you open new windows, and close them correctly, EntraPass saves the last position and size of each window.

The following tables describes the columns in an area card list.

Result

Table 8: Area card list columns

Column	Description
Card number	Cardholder's card number.
Card user name	Cardholder's name.
Supervisor	An x in the supervisor column indicates that the cardholder has a high supervisor level, the level column indicates, which level. A + in the supervisor column indicates the cardholder has privileged status.
Level	The level of the supervisor.
Invalid	Displays cards for the following possible reasons: <ul style="list-style-type: none">• Cards in an area outside of their scheduled time.• An operator manually moved the card into the invalid area.
Last reader swiped	Records the last reader swiped.

Table 8: Area card list columns

Column	Description
Date and time	Displays the date and time of the last transaction, the transaction type may be a card swipe or a manual move. If the transaction is a card swipe, the time recorded depends on the door-timing configuration.
Optional: Card information	To access an optional Card information field , right-click in the card list for the shortcut menu and select the appropriate field. For more information, see User Definable Field in the next table. Click Refresh to pull any modifications made on the cards. If you select another Card information field , EntraPass automatically refreshes. Note: If you have a large amount of cards, a progress bar indicates the task, and disappears when loaded.

To use the following functions on a card, select the card from the area card list, and right-click to access the shortcut menu.

Table 9: Card shortcut menu functions

Menu option	Action
Report type	Select one of the following reports: <ul style="list-style-type: none"> • Cards in area • Supervisor cards in area • Invalid cards in area
User Definable Field	Right-click in the card list for the shortcut menu: <ul style="list-style-type: none"> • Select Card information field, to add or change a card information field. • Select None, to hide the field. The system automatically refreshes when you add or change a user definable field. You can add only one card information field.
Search and Locate User	<ol style="list-style-type: none"> 1. In the Search and Locate User window, type user in the Search field to populate a list. 2. Select a user from the list to open The locate and move user window. 3. Optional: Click the Move to button, to select a new location.
Move card to another area	Select a new area from the list.

Click **Print** to open a printer window. The output includes the following columns:

- **Card number**
- **Card user name**
- **Supervisor level**
- **Invalid**

On the lower left of the status bar, see the following statistics:

Column	Description
1	Number of cards in the area.
2	Number of supervisor cards in the area.
3	Number of invalid cards in the area.

Monitoring an Area Group for Muster Reporting

About this task:

Use muster reports to monitor specific areas when an emergency occurs. Muster reports list cardholders and their location at the time of the emergency. When an input triggers a muster event, the muster event automatically populates an area group card list associated with the muster report. EntraPass populates the Area Group card list with all the cardholders in the defined area of the muster report. For details for the muster report details, see [Area Card List](#) for details of the muster report details.

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

About this task:

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.

- ① **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.
 - ① **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.
 - ① **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). 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.
- ① **Note:** To change the font colour of system messages: **Options > Event color and priority**.

Performing Tasks on System Messages

About this task:

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

① **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](#).

Result

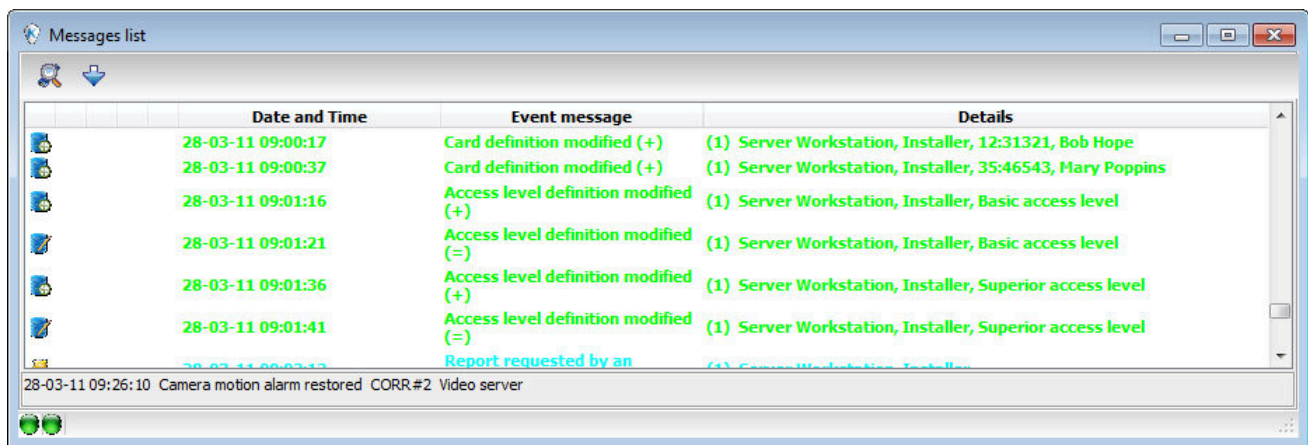
Also, in order to reduce the quantity of data retrieved, a filter can be added to the user name or to the card information fields (1 to 10) when searching for a card. Enter a name for the filter and click the button on the left side of the field to display the contextual menu.

- **Video recording:** This menu item 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.
 - ① **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 a 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 preceeded 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

About this task:

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

About this task:

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

1. Log on using the user name and password of the operator with ‘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.

① **Note:** A **Permit button** appears when the operator who is logged on has ‘read-only’ access permission. The permission acquired during this session is valid until the operator logs out. Click the **Permit** button. The operator logon window appears. Enter your user name and password, and click, **OK**. The temporary permission is granted.

hatrix additional search capability

This new feature was created to answer to two different situations:

- A user has lost his card and calls the hatrix central to have a door unlocked. The central operator needs to locate the user within the database to confirm he has access to the door.
- A user cannot log into EntraPass Web and calls the hatrix central. The central operator has to edit the operator’s data or reset his password.

Functionality

About this task:

A **Global Search** function is already available for users under hatrix. However, a new feature allows filtering the displayed results using any of the card information fields (1040).

- You can right-click on the user name to show more information. A pop-up window opens to display more information containing the following:
 - A table with the connection, access level, doors and user’s access rights for the corresponding schedule.
 - The card status.
 - The user’s rights to edit a card.
 - The user’s rights to unlock a door.
- The user’s rights to switch directly into this account (this way the operator can see the doors to which the user does not have access to. Logging into a user’s account allows the operator to perform any operations).
- The doors to which this user has access (that can be unlocked).
 1. From the **Desktops** menu, right click on a desktop button.
 2. Select **Properties**.
 3. From the **Desktop properties** window, select **Global Search**.

Result

The **Global Search** window will be displayed besides the **Message list**.

In a **Global Search**, there is now an extra tabulation so you can search through operators. The searchable operator fields are :

- The operator’s name
- The login name

From the results, you can:

- Edit the operator

- Reset the operator password (use the operator's e-mail address as the recipient).

Transferring a customized desktop

About this task:

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 select the appropriate check box. You can select operators one by one, or you can use the **Select all** button.

Desktop colors

About this task:

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.

Status

Use this section to view the status of applications and components in text and graphical representations from different system perspectives. You can use [Application Status](#) to view the status of applications, including EntraPass Workstations, and peripheral applications, the status items of each application depends on the connection type.

You can use the [Text Status](#) to view the status of a particular component in text form. To view how many sites or gateways are in a “not normal” state, use the [Numerical Status](#). You can hover over a component of a door controller in the graphic status to view its status in the component list.

You can use the [Database status](#) to view all applications defined in the gateway and controller sites, and view the communication status of each application. The [Video server status](#) lists all the parameters of the video servers connected to the Video Vault. To view detailed information on the server including system information, system global memory, system process memory and system disk space, use [Server State](#). To view how many operators are logged in to the system for each application, use [Logins](#).

Application Status

About this task:

The **Application Status** displays details about a selected application, for example: 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.
 - A 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.
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 to the application. The operator name is used for many purposes, for example to identify who performed a modification to a card, and 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 resets 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 was operational. If the Server is shutdown, this number resets.
- ① **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](#)).
- ① **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.

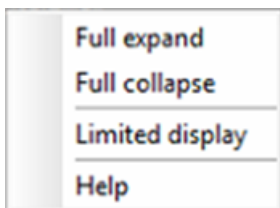
Database status

About this task:

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

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

1. Click the **Status** tab and click the **Database** button.
- ① **Note:** The button identifies the type of component.
2. In the **Database** window, select the application you want to view the database. In the lower pane, the status and full name of the selected component display.
 3. Select a component to modify its definition. For example, if you select a door, right-click the door to display a shortcut menu.
 4. Select a command in the shortcut menu.



- ① **Note:** The command list varies according to the selected component.
5. The shortcut menu offers the following options:
 - **Full expand:** Click to expand the tree status and view all components. Only applications that are connected to the server display a + sign.
 - **Full collapse:** Click to collapse the tree status and hide all components of the root component.

- **Edit:** When you select an assigned component (input) and click edit, the system edits the definition window so that 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. If you select **Limited display**, the system erases the previous status and displays the status of the next selected component.
- ① **Note:** The icons on the left side of the components indicate the component type.

Graphic Status

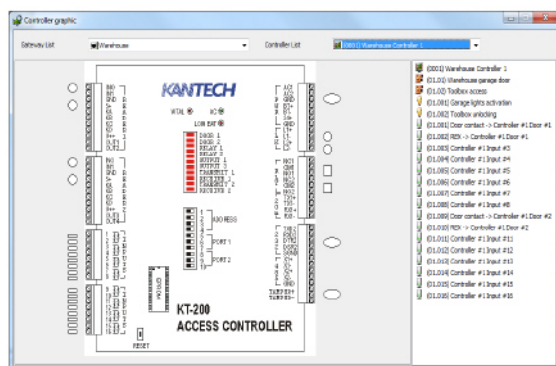
This feature is used to display a graphical status of a door controller, including the status of all its components (outputs, inputs, power supply status, communication status, etc.) represented by coloured shapes (circle, square, etc.).

- 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).

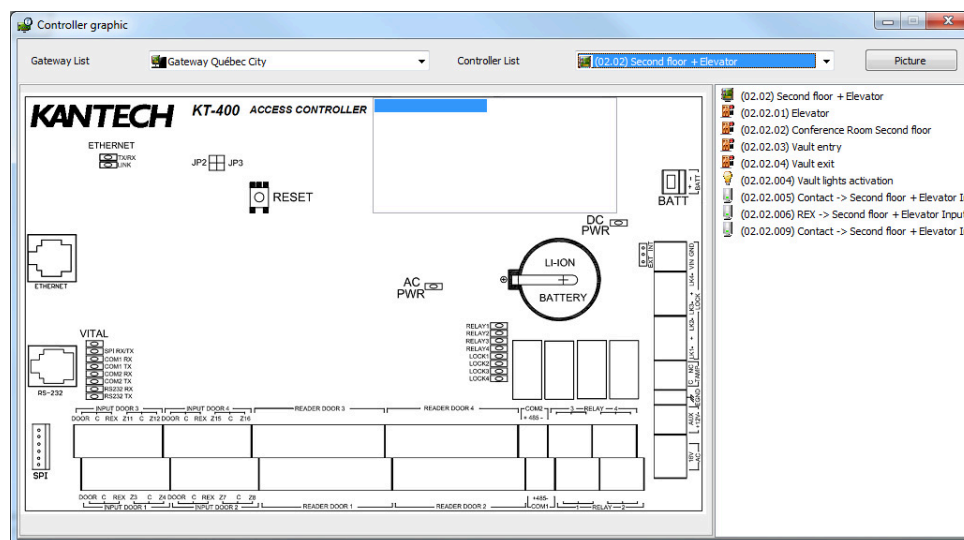
Viewing a Controller Status

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



① **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).

① **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.

Numerical Status

About this task:

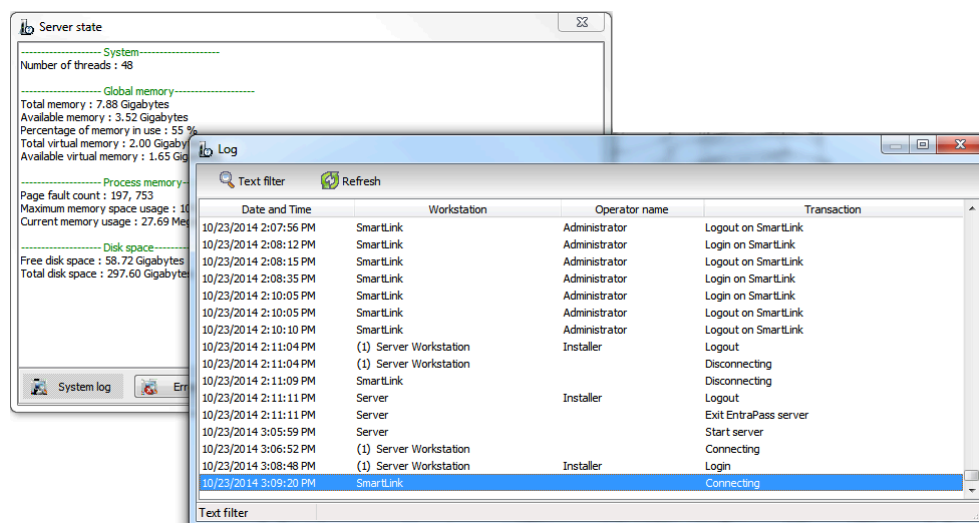
This menu allows an operator to view the number of components in a “not normal” state for a selected gateway.

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.

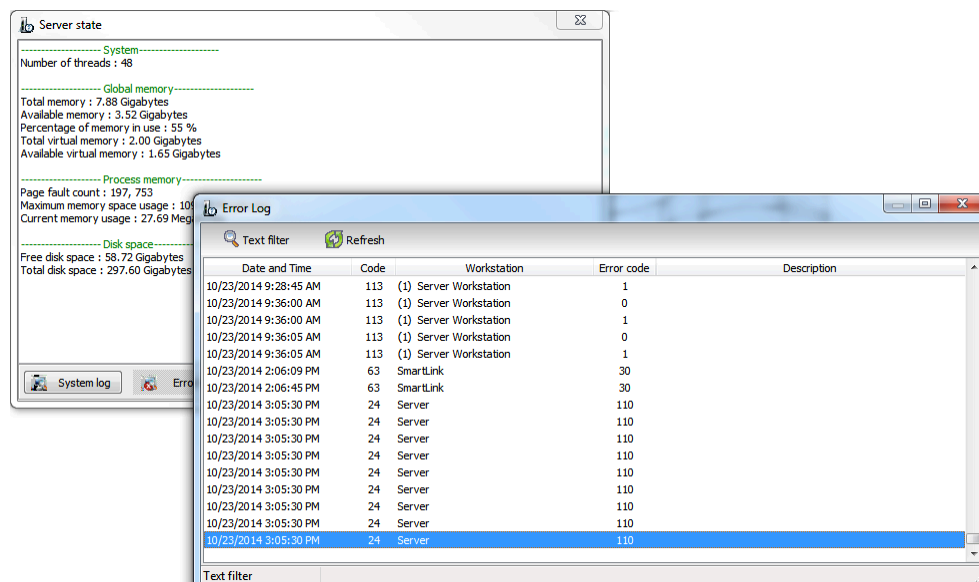
Server State

The **Server state** window 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.
- **Account** : The account to 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.

- ① **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.

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

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.

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

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**

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 eight buttons represent system devices (Workstation, Gateway, Connection, Controller, Door, Input and Output). When a button representing a system device is selected, all the components defined in the system are displayed for selection.
- 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.

Video server status

In EntraPass, you can display the parameters of the video devices that are connected to the video server. For example, operators can view information related to network data transfer such as images and digital sounds.

- ❗ **Note:** Installing and using the video feature may take a large amount of your company's network bandwidth (LAN or WAN). The network administrator may control the use of the network bandwidth for video transfer.

Viewing the video server's full status

1. On the Graphic desktop window, right-click the **Video server** icon to display a shortcut menu.
2. On the shortcut menu, click **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.

Result

The following table provides descriptions of the displayed fields.

Table 10: Video server full status window

Item	Description
Unit name	The network name of the remote DVMS system. For example, Intellex. The unit name is followed by the DVR IP address
Unit type	The type of unit. For example, Intellex or Iris (network client).
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), or Custom (a custom schedule has been set by the operator).

Table 10: Video server full status window

Item	Description
Recording in progress	The active record statue of the remote DVMS unit. Values can be: True (is recording) or False (stopped recording).
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.
Record mode	The record mode can be linear or circular. If you select Linear , the recording continues uninterrupted until the available space is finished; if you select Circular , the DVR notifies the operators before the recording space is completely filled. The operator can 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.

Operations




Use this section to perform manual operations on system applications and components. You must have the applications and components configured and defined. Each section describes the icons available, and a full description of their functionality. Operations range from reloading a controller database, locking or unlocking doors, to monitoring a selected input. See the following list of applications and components:

- [Manual operations on alarm systems](#)
- [Manual operations on areas](#)
- [Manual operations on controllers](#)
- [Manual operations on doors](#)
- [Manual operations on elevator doors](#)
- [Manual operations on gateway](#)
- [Manual operations on guard tours](#)
- [Manual operations on inputs](#)
- [Manual operations on integrated panels](#)
- [Manual operations on action scheduler](#)
- [Manual operations on relays](#)
- [Manual operations on sites](#)
- [Manual operations on view roll call](#)

Manual operations on alarm systems

This menu allows you to manually change the state of an alarm system. You can arm, disarm or modify the postponement delay time of an alarm partition. The Alarm systems menu is only used under Global Gateways.

Table 11: Alarm system state icons

Icon	Definition
	Arm alarm: automatically arm an alarm system when the arming delay is over.
	Disarm alarm: automatically disarm the selected alarm system.
	Alarm postpone: automatically postpone the delay time of an alarm system while the alarm system is in postpone mode.

You can also visualize the remaining time for the entry, exit, arm request or arm postponement delays, under way for any of the alarm partitions.

Note: It is not possible to postpone an alarm partition in this window, it can only be done at a reader using a card.

Performing Manual Operations on an Alarm System

1. From the **Operation** window, select the **Alarm system** button.
2. Click the **Enable animation** button to view a real-time display of the alarm system status.
 - The left-hand pane displays the list of all system gateways. You may select All or select an individual gateway.

- The individual alarm system associated with the gateway selected on the left are displayed in the right pane. If you select All on the left, all alarm systems will be listed on the right. You can select one, several or all alarm system.

Arming an Alarm System Manually

About this task:

This option is used to automatically arm the alarm system when the arming delay is over. For more information on arming alarm systems, see [Alarm Systems Definition \(Global/KT-NCC\)](#).

1. Select a gateway or an alarm system.
2. Click the **Arm alarm** button. The selected alarm system will automatically be armed.

Disarming an Alarm System Manually

About this task:

This option is used to disarm the selected alarm system. The system will disarm automatically. For more information on disarming alarm systems, see [Alarm Systems Definition \(Global/KT-NCC\)](#).

1. Select a gateway or an alarm system.
 2. Click the **Disarm alarm** button. The selected alarm system will automatically be disarmed.
- ① **Note:** If a “no disarm” schedule is effective and an operator disarms the system, the alarm system’s exit delay will activate before the partition arms automatically. After the exit delay, the alarm system will arm again if there is no postpone and if the “no disarm” schedule is still valid.

Modifying the alarm system postponement delay manually

About this task:

This option is used to modify the postponement delay time of an alarm system while the alarm system is in “postpone mode”.

1. Select gateway or an alarm system.
2. Click the **Alarm postpone**. The Change delay on action dialog appears.
3. Enter the **New time** delay (m:ss) and click **OK**. The selected alarm system postponement delay is modified. **Maximum allowed:** 16 hours.




① **Note:** This operation does not “decrement” the postpone count allowed.

Manual operations on areas

About this task:

This feature is used to empty cards that are in an area to the unknown area and/or move selected cards to a specific area. The **Area** dialog can only be used with Global Gateways.

Table 12: Area icons

Icon	Definition
	Get card list: list all of the cards in the selected area, after the filter and sorting criteria have been defined.
	Empty area: move the cards in the selected area into the unknown area.
	Move only selected card: move the selected cards to a specific area.


You can also display supervisor cards, invalid cards or all the cards located in a specific area.

1. From the **Gateway** list, select a gateway to view an area.
2. Select an area from the left-hand pane (for example, Cards in area), the system will automatically display:
 - The number of cards that are currently located in the selected area (all cards, supervisors and invalid).
 - The number of supervisor cards that are currently located in the selected area (assigned with a supervisor level).
 - The number of invalid cards that are currently located in the selected area. A card is invalid because the schedule assigned to the cardholder's access level does not authorize the cardholder to remain inside the selected area.
3. From the **Filter** drop down list select an item, then click the **Refresh** button to display detailed information on the selected item.
 - **Cards in Area** : If selected, the system will display all the cards located in the selected area. The card total will be displayed under the "gateway list" field.
 - **Supervisor Cards in Areas** : If selected, the system will display all the supervisor cards (assigned with a supervisor level) located in the selected area. The card total will be displayed under the "gateway list" field.
 - **Invalid Cards in Area** : If selected, the system will display all the cards located in the selected area. The card total will be displayed on the top left-hand of the window (all cards, supervisors and invalid). When a card is invalid, it means that the card access level is no longer good. If for example, a user remains in an area longer than the period of time he is allowed, his card will become invalid and he will no longer be able to exit the area.

Card location

About this task:

This function allows finding where area a user card is located.

1. Select a Gateway from the list.
2. Click the  button to display the **Find a component** dialog or select **Search and locate user** from the contextual menu.
 - ① **Note:** The button is only available when a specific gateway is selected from the list.
3. From the **Find a component** dialog, double click on a user card or click **OK**.












Result

The **Locate and Move user** dialog is displayed. Now you can see the area in which the user card is located and also move it to another location.

Manual operations on controllers

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

Table 13: Controller icons

Icon	Definition
	Soft reset: does 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: erases the existing controller database and reloads it with new information in the controller database. Execute reset commands with caution. Before you carry out a controller reset operation, contact Technical Support. For more information, see Technical Support .
	Reload: reload the controller database; if for example a controller database is not reloaded correctly due to an erratic operation.
	Reload controller firmware: reloads the firmware of the controller.
	Clear buffered events: offline controllers buffer events until they reconnect to the server. This operation discards saved events on the controller. This operation is only available for KT-400, KT -1, and KT-2 controllers.
	Unlock reader keypad: unlocks the reader keypad for KT-100, KT-300, KT-400, KT-1, and KT-2 controllers.
	Reset reader power: resets the controller reader power. You can perform this operation on KT-300, KT-400, KT-1, KT-2, and KTES controllers.
	Forgive: resets 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 for each local area, obtain a card list in local area controllers, move cards (when you have a KT-1, KT-2, or KT-400 system) and allows you to get position a card. This feature is used only for a 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: reloads the firmware of the ioSmart module.

- ① **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 are 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).

- ① **Note:** If only one site or gateway one site is defined in the system, the Site Controller or Gateway list pane the Site Controller 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

About this task:


A soft reset refreshes the data in the controller.

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

Performing a controller hard reset

About this task:

A hard reset deletes 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 the controller or controller group.
2. Click the **Hard reset** button in the toolbar. This command sends new information to the controller to update its physical components (relays, inputs, doors and outputs).

Reloading a controller manually

About this task:

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 controller or controller group.
2. Click the **Reload** button in the toolbar. The controller's database is reloaded.

Manually reloading controller firmware

About this task:

You can use EntraPass to reload the firmware for KT-100, KT-NCC, KTES, KT-300, KT-400, KT-1, and KT-2 controllers. Perform a firmware reload after a system or firmware upgrade.

1. In the **Controller** dialog, select the controller or controller group.
2. On the toolbar, click **Reload controller firmware**.

Manually clearing buffered events

About this task:

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. On the toolbar, click the **Clear buffered events** button.

Result

This option is also available when you right-click the controller you want. This operation is only available for KT-400, KT -1, and KT-2 controllers.

Manually unlocking a reader keypad

About this task:

EntraPass allows you to unlock the reader keypad for KT-100 and KT-300 controllers from a workstation.

1. In the **Controller** dialog, select the controller or controller group.
2. Click the **Unlock reader keypad** button in the toolbar.

Manually resetting a reader power

About this task:

EntraPass Global Edition allows you to reset a KT-300 controller reader power.

1. In the **Controller** dialog, select controller or controller group.
2. Click the **Reset reader power** button in the toolbar.

Resetting Cards In and Cards Out counters or all controller local areas

About this task:

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

1. In the **Controller** dialog, select the controller or controller group.
2. Click the **Forgive** button in the toolbar. Card holders are considered inside or outside until the next use of their card at an entry or exit reader.

Calculating the number of Cards In and Cards Out

About this task:

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 the 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.

① **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**.

Requesting unassigned modules

This feature provides the serial numbers of all ioSmart readers and ioModules connected 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.

- ① **Note:** If you want to view 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 a group of doors.

Operators can manually lock or unlock a door, temporary lock or unlock a door or a group of doors, and enable or disable readers on selected doors.

Table 14: Door icons

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
	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.

- ① **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.

① **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.

① **Note:** The **Door Group** bottom panel is available only to the selected site or to a selected connection not linked to a site.

Manually locking a door

1. In the **Door** dialog, select door or door group.
2. Click the **Lock-door** button in the toolbar.

Manually unlocking a door

1. In the **Door** dialog, select doors or door group.
2. Click the **Unlock-door** button in the tool bar. The selected doors are manually unlocked. The system prompts for operator confirmation. A door defined with an automatic unlocking schedule remains unlocked until:
 - The next valid change of the unlocking schedule, or
 - An operator manually locks the door.

Temporarily unlocking a door

About this task:

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.

- ① **Note:** The maximum unlock time: 4:15 (255 seconds).

1. Click the **Temporarily unlock** button. The **Change delay on action** dialog displays.

2. Enter the **New time delay (m:ss)** and click **OK** . The selected door is temporarily unlocked by an operator.

① **Note:** If a door contact is installed, the door re-locks as soon the system sees a “door open-door closed” transition. There is no “Animation” for this type of operation.

Resetting a door schedule

About this task:

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

1. In the **Door** dialog, select the doors or door group.
2. Click the **Return to Schedule** button. This option resets the schedule for the selected components.

Enabling a door reader

1. In the **Door** dialog, select the doors 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 the doors 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 schedules

About this task:

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.

Result

For more information about access levels, click [here](#).

Manual operations on elevator doors

In the **Elevator** window, authorized operators can complete the following manual operations:

- Lock or unlock elevator floors or floor groups
- Temporarily unlock elevator floors or floor groups
- Reset elevator door schedules for floors or floor groups
- Enable or disable elevator floors or floor groups
- Enable or disable elevator door readers

When operators configure manual operations, the following process occurs with cardholders:

- The cardholder pushes the **up/down** button and the elevator door opens.
- The cardholder presents the card to the reader, usually inside the cab.

- The system confirms that the schedule assigned to the elevator door is valid, and then confirms which floor group is associated to this elevator door.
- The system verifies each floor of the floor group in the floor group menu and confirms if the schedule associated to each floor of the group is valid or invalid.
- Users can select floors that have valid schedules from the elevator panel.

Table 15: Elevator door icons

















Icon	Definition
	Lock all floors: The first instance of this icon manually locks the selected elevator floor group.
	Unlock floor group: The first instance of this icon manually unlocks the selected elevator floor group. This floor group remains unlocked until the next valid change of the unlocking schedule, or until an operator manually locks the floor group.
	Unlock elevator floors temporarily: The first instance of this icon temporarily unlocks the selected elevator floor group for a pre-set delay. When the delay expires, the elevator floor group automatically locks.
	One-time access elevator door: The first instance of this icon manually unlocks the selected elevator floor group for one-time access in a pre-set time. When the time expires, the elevator floor group automatically locks.
	Elevator return to schedule: The first instance of this icon applies the locking schedule to the selected elevator floor group.
	Enable elevator reader: This icon enables a previously disabled reader.
	Disable elevator reader: This icon disables a reader and users cannot access any elevator floors even if they have access rights.
	Enable all floors: The first instance of this icon enables a previously disabled elevator floor group.
	Disable floor group: The first instance of this icon disables the selected elevator floor group. Users cannot access the elevator floors in the group, even if they have access rights.
	Lock elevator door (individual floors): The second instance of this icon manually locks the selected elevator floors.
	Unlock elevator door (individual floors): The second instance of this icon manually unlocks the selected elevator floors. These floors remain unlocked until the next valid change of the unlocking schedule, or until an operator manually locks the floors.
	Temporarily unlock elevator door (individual floors): The second instance of this icon temporarily unlocks the selected elevator floors for a pre-set delay. When the delay expires, the elevator floors automatically lock.
	One-time access to elevator door: The second instance of this icon manually unlocks the selected elevator floors for one-time access in a pre-set time. When the time expires, the elevator floors automatically lock.
	Elevator door return to schedule (individual floors): The second instance of this icon applies the locking schedule to the selected elevator floors.

Table 15: Elevator door icons

Icon	Definition
	Enable floors (individual floors): The second instance of this icon enables a previously disabled elevator floor.
	Disable floors (individual floors): The second instance of this icon disables the selected elevator floors. Users cannot access the elevator floors, even if they have access rights.

- ❗ **Note:** When you hover your cursor over an icon, a description displays the operation you can perform, as listed in the previous **Elevator door icons** table. Use this description to differentiate between buttons that appear the same but have different functions, such as **Disable floor group** and **Disable floors (individual floors)**.

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 pane displays the list of all **Sites/Gateways**. You can select all or select one connection/gateway.
 - The individual elevator doors associated with the connection/gateway selected on the left are displayed in the upper-right side of the pane. If you select **All** on the left, then all elevator doors in the system are 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 lower right of the pane. If you select **All** on the left, all elevator door groups are listed at the lower right. You can select one, 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 or floor groups from elevator doors

1. Select an elevator door or a group of elevator doors.
 2. To lock a previously unlocked floor group or floors, use the following options:
 - a. For a floor group, click the **Lock all floors** button in the toolbar and select the required floor group to lock.
 - b. For individual floors, click the **Lock elevator door (individual floors)** button in the toolbar and select the required floors to lock.
 3. Click **OK**.
- ❗ **Note:** You can only lock a door defined without an unlocking schedule 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 or floor groups from elevator doors

1. Select an elevator door or a group of elevator doors.
2. To unlock a previously locked floor group or floors, use the following options:
 - a. For a floor group, click the **Unlock floor group** button in the toolbar and select the required floor group.
 - b. For individual floors, click the **Unlock elevator door (individual floors)** button in the toolbar and select the required floors.

3. Click **OK**, then click **Yes**.

- ① **Note:** These steps only enable the elevator floors or floor group that are defined with an X in the column of the **Floor group definition** menu. For a door defined with an automatic unlocking schedule, the floors remain unlocked until the next valid change of the unlocking schedule, or an operator manually locks the door.

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

When a manual unlocking operation finishes, only floors that are defined with an X in the field of the **Floor group definition** menu are available for selection. If the system loses communication and the controllers are working in stand-alone mode, then you can only select the floors marked with an X and the access schedule is ignored.

Temporarily unlocking floors or floor groups from elevator doors

About this task:

You can temporarily unlock a floor or floor group from an elevator door for a preset delay. When the delay expires, the elevator door re-locks automatically. The maximum unlock time: 4:15 (255 seconds).

1. For a floor group, click the **Unlock elevator floors temporarily** button. For individual floors, click the **Temporarily unlock elevator door (individual floors)** button. The **Change delay on action** dialog displays.
2. Enter the **New time delay (m:ss)** and click **OK**. The selected elevator floor is temporarily unlocked by an operator.

- ① **Note:** This command temporarily enables the elevator floor group or floors that are defined with an X in the column of the **Floor group definition** menu.

An Animation is not available for this type of operation. To temporarily unlock all floors, use the **temporarily unlock door** option in the **manual operation on doors** menu.

Unlocking a floor or floor group for one-time access

1. Select an elevator door or a group of elevator doors.
2. To unlock a floor or floor group for one-time access, use the following options:
 - a. For a floor group, click the **Unlock floor group** button in the toolbar and select the required floor group.
 - b. For individual floors, click the **Unlock elevator door (individual floors)** button in the toolbar and select the required floors.
3. Click **OK**

Resetting an elevator door schedule

About this task:

You can reset an elevator door schedule after a manual operation is performed on a component.

1. In the **Elevator** dialog, select the elevator door or door group.
2. To reset the schedule for floors or floor groups, use the following options:
 - a. For floor groups, click the **Elevator return to schedule** button and select the required floor groups.
 - b. For individual floors, click the **Elevator door return to schedule (individual floors)** button and select the required floors.
3. Click **OK**.

Enabling an elevator floor

1. In the **Elevator floor** dialog, select the floor or floor group.
2. To enable previously disabled floors or floor groups, use the following options:
 - a. For floor groups, click the **Enable all floors** button and select the required floor groups.
 - b. For individual floors, click the **Enable floors (individual floors)** button and select the required floors.
3. Click **OK**.








Disabling an elevator floor

1. In the **Elevator door** dialog, select the floor or floor group.
2. To disable previously enabled floors or floor groups, use the following options:
 - a. For floor groups, click the **Disable floor group** button and select the required floor groups.
 - b. For individual floors, click the **Disable floors (individual floors)** button and select the required floors.
3. Click **OK**. Users cannot access the selected floors or floor groups, even if they have access rights.

Manual operations on gateway

Manual operations on the gateway feature allows operators to communicate with the gateways , to refresh data, perform different types of resets and force firmware reloads through the gateways .

Table 16: Gateway icons

Icon	Definition
	Soft reset: does not affect the database. This command sends new information to a gateway to update its physical components (relays, inputs, doors and outputs). Soft reset is available on the KT-NCC gateway only.
	Hard reset: deletes the existing gateway database and reloads it with new information. Execute reset commands with caution. Before you carry out a gateway reset operation, we recommend you contact our Technical Support. Hard reset is available on the KT-NCC gateway only. For more information, see Technical Support .
	Broadcast: sends a signal to the selected component manually. Broadcast is available on the KT-NCC gateway only.
	Forced reload firmware: forces a reload of the selected firmware. Forced reload firmware is available on the KT-NCC gateway only.
	Reset interlock group: clears all interlocks.
	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**

- ① **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.

Updating physical components

1. Select the gateway that you want to perform a soft reset for.
2. Click the **Soft reset** button. This command sends new information to the gateway to update its physical components (relays, inputs, doors and outputs).

Performing a hard reset

About this task:

- ① **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 that you want to perform a hard reset for.
 2. Click the **Hard reset** button. This command erases the existing gateway database and reloads it with new information.

Reloading gateway data

About this task:

EntraPass allows operators to reload data in order to refresh system parameters with new data from the system database. When must 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 that you want to reload the data for.
2. Click the **Reload data** button, and the gateway data is updated.

Broadcasting

1. Select the gateway that you want to send a broadcast to.
2. Click the **Broadcast** button. This command sends a manual broadcast to the gateway.

Forcing a firmware reload

1. Select the KT-NCC that you want to force a firmware reload on.
2. Click the **Forced reload firmware** button. This command forces the KT-NCC firmware to reload.

Note: Before reloading any firmware, EntraPass ensures that a reload is not currently in progress, and then reloads uncompressed applications.

If you select a component other than the KT-NCC, the **Forced reload firmware** button is unavailable.

Redundant gateway operations

About this task:

If a redundant server is used in a number of ways, it becomes active following the failure of the primary gateway. You can also manually switch to it and use it during primary gateway maintenance. If a redundant gateway is automatically switched to the primary gateway, the primary gateway can only be reinstated manually.

1. From the EntraPass workstation main window, select the **Operation** tab and click the **Gateway** button to open the **Gateway** dialog where all the gateways connected to your system are listed.
2. Select your multi-site gateway to see the status of all gateways.
3. Right-click on a gateway to view options.
4. **Select as online gateway** to reinstate primary gateway.

Result



A green square highlights the active gateway. A yellow square highlights non-active gateways.

Note: Gateways can be reloaded individually or together. To reload a gateway individually right-click the gateway and select **Reload**. To reload the gateways together right-click the multi-site gateway and select **Reload**. This reloads all associated gateways.

Manual operations on guard tours

This dialog allows the operator to initiate, modify the delay allowed between stations, modify the next station and end a guard tour. The **Guard tour** dialog can only be used with Global Gateways.

Table 17: Gaurd tour icons

Icon	Definition
	Start guard tour: must be clicked to start the guard tour.
	End guard tour must be clicked after the last station of the tour has been visited by the guard.

Guard tours are used to allow guards to perform tours while being monitored by the system. Events will be generated at each visited stations.

These tours consist of different stations that must be triggered within a certain time, otherwise the system will give an alarm event. These stations can either be readers or inputs.

① **Note:** Guard Tours can only be initiated and ended from the manual operations of the system.

Starting a Guard Tour

1. From the **Gateway List** drop-down menu, select the gateway where the guard tour is defined.
2. Select the guard tour you want to start from the **Guard tours** list. Once you have selected the guard tour, click on the “Start Guard Tour” button. The system will display a card-selection window:
3. Select the cardholder who will be responsible for the guard tour. A card has to be chosen in order to initiate the guard tour. If doors are defined in the guard tour definition, then a card will have to be presented at the defined reader(s) and this cardholder must also have access to the doors. Once you have selected a cardholder and clicked **OK**, the system will display the **Guard tour** window.

① **Note:** Please remember the following:





- During a tour, using the “modify” button will reset the time allowed between two stations.
 - Only one (1) guard tour can be run at a time per gateway.
 - A tour must always be completed with the command “End guard tour” entered by the operator after the system displays the “Last station in guard tour” message.
 - During a tour, if the delay is almost expired, using the “modify” button will reset the time allowed between two stations.
4. Click **More** to display extended information on the selected guard tour. The system will display the stations to be visited as well as the delays from stations to stations. This button can be used only when a guard tour has been started.
 5. Click the **Start guard tour** button to start the guard tour sequence. Guard tours can only be initiated from this window. You can also assign a schedule that will generate the event “Guard Tour Scheduled” to warn operators or remind them that the guard tour must be started.
 6. Click the **End guard tour** button to end the guard tour sequence. When the last station has been visited, the system will generate the event “Last station in guard tour”, then the “end guard tour” button must be used. Once you end a guard tour, the system generates the event “Ending of a guard tour”.
 7. Click the **End guard tour** button will also cancel a guard tour that has started.

8. The following buttons are displayed in the right-hand. They provide additional information on the guard tour:
 - **Previous station** : Provides information (text and picture) concerning the previous station (door or input) that the guard triggered.
 - **Next station** : Provides information (text and picture) concerning the next station (door or input) to be triggered.
 - **Delay to next station** : Indicates the time remaining for the guard to reach the next station. If this time expires, a warning will be displayed.
 - **State** : Displays the guard tour state. The possible states are:
 - **Normal** : When the guard tour is normal.
 - **Pre-alarm** : For example, if the delay programmed for a specific station is set to 2:00 minutes, and this delay expires, the system will generate the event "Guard tour station late", then the system will initiate the pre-alarm delay. After this delay expires, the system will then generate the "Guard tour alarm" event and the status will change to alarm.
 - **Alarm** : When the pre-alarm delay is over and the guard tour is in alarm.
 - **Modify next station** : This option allows the operator to modify the next station, for the guard tour currently in progress. When you modify the next station, the system will generate the event "Guard tour sequence modified".
 - **Modify delay to next station** : This option allows the operator to modify the time remaining for the guard in order to reach the next station. This modification only affects the guard tour currently in progress.
- ① **Note:** When you modify the next station, the system will generate the "Guard tour late time delay modified" event.

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.

Table 18: Input icons

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.
	Input with no supervision will terminate the input monitoring, regard-less 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.

- ① **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**. You may select **All** or select one connection/gateway.
 - The individual input 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 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

About this task:

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.

Setting Up Continuous Input Supervision

About this task:

You will use this feature to monitor an input at all times. This option can only be setup manually.

1. Select an input or a group of inputs.
2. Click the **Input continuous supervision** button.

Stopping Monitoring an Input

About this task:

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

About this task:

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 integrated panels

1. On the EntraPass workstation, click **Operations** and click **Integrated Panel**.

2. If required, select a specific component from the **All components** list.
3. In the left column, right-click a **panel**.
4. Click **Full status** to view the panel status details.
5. Click **Virtual Alarm Panel** to view the virtual keypad.
6. Right-click a **partition**.
7. Click **Arm partition** or **Disarm partition** as required.
8. Right-click a **zone**.
9. Click **Zone bypass** or **Zone unbypass** as required. When the panel is next disarmed, the zone returns 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**.

Table 19: Action scheduler icon

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

About this task:

The following table outlines the controller compatibility and firmware requirements for this feature.

Table 20: Controller and firmware compatibility

Controller	V3 Assa-Abloy firmware compatibility	Gateways	Fail-soft mode
KT-2, all firmware versions	Yes	Multi-site, Global, KT-NCC	Yes
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

Table 20: Controller and firmware compatibility

Controller	V3 Assa-Abloy firmware compatibility	Gateways	Fail-soft mode
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

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**.
 - ① **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.
 - ① **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.
 - ① **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.
 - ① **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, or KT-2.
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-2, KT-400, or KT-400 rev 1 is used in stand-alone mode and loses connection with the KT-NCC, the controller 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

About this task:

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

About this task:

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

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.

Table 21: Relay icons

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

- ① **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**. 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.
- ① **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.
- ① **Note:** If you manually deactivate a relay that is usually activated according to a schedule, it remains 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, you must reactivate it again for the remaining scheduled time. One relay can be defined for various components of the system, and its activation or deactivation relates 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 is 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, 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 appears on the screen.
3. Enter the **New time delay (m:ss)** and click **OK** . The selected relay is temporarily activated by an operator.

Note: The selected relay is temporarily activated. This is useful for an operator who wants to activate temporarily a relay that 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 is deactivated automatically.

Resetting a relay schedule

About this task:










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 the relay or relay group.
2. Click the **Return to Schedule** button. This option resets the schedule for the selected components.

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.

Table 22: Site icons

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 controller.

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 KT-NCC, Global and multi-site Gateways.

Table 23: KT-NCC and Global Gateways

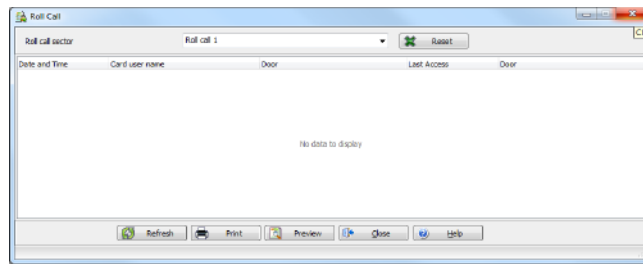
Message	Description
Connection Communication OK	All controllers on the connection communicate with the gateway.
Connection Communication Trouble	At least one controller on the connection is not communicating with the gateway.
Connection Communication Failure	None of the controllers on the connection can communicate with the gateway.
Connection Communication Cannot be Opened	The gateway cannot open the communication port.

Table 24: 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 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:



For more information, see [Roll Call Report](#).



Users

Users contains information on how to add, import, define, and export a user's card details. Cardholder features include the following: access levels, usage restrictions, audit trail, privileges, managing groups, tenants, badges, and personal information.

Access exception

About this task:

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 are saved.

⚠ **WARNING:** User list report does not take Access Exception into account.

Result

To enable the **Access level exception** feature, see [Credentials Parameters](#).

Access levels definition

About this task:

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 and per gateway (Global/KT-NCC Gateways). To assign an access level to a card, you have to:

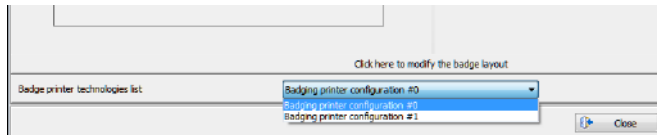
- Create schedules that correspond to the time the user has access to the desired doors.
 - Assign the created schedule to the desired doors (in the Access level definition menu).
 - Assign the access level to a card.
1. The default access level is Always valid, all doors : cardholders assigned this 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. Click **New** and 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 add comments to the current access level. You can double-click in the blank space to display the edition window.

Badge designing

EntraPass contains a badge layout editor for 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.
2. To associate a specific printer configuration to a badge, on the lower section of the window, select from the drop-down options.



- Note:** The printer configuration description must be first entered from the **System Parameters/Credentials** menu. For more information, see [Badging Printer](#).

The **Badge printer technologies list** is displayed only when the **Badging Credential** option is enabled.

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.

3. 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, such as adding background colour or graphics, or modifying the font.

- Note:** When you move the cursor over the badge design objects, a hint explaining each object appears. 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.
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

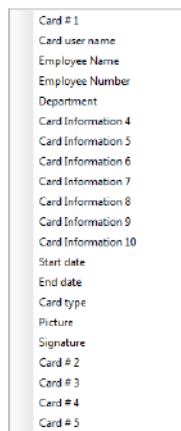
By a simple click and drop feature, the Badging utility permits you to incorporate objects into the badge template:

- 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

- ① **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.



- 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.

❶ **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](#).

- 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.

❶ **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 are "snapped" to the nearest grid mark.
- **Grid settings:** allows you to specify the horizontal (Height) and vertical (Width) grid spacing (in pixels).

❶ **Note:** To disable the grid deselect **Show grid line** in the Align menu.

To modify card fields properties

About this task:

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

- From the Badge design template, right-click the object you have inserted (in this example, Card information fields).
- From the shortcut menu, select **Card fields properties**.

❶ **Note:** The Properties menu item depends on the selected item. For example, it changes 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).
- ① **Note:** The Set as default checkbox allows you to apply all the characteristic to all text objects that will be incorporated in the template.

When Text Orientation is set to “Other” it is not possible to re-size the field.

To modify picture properties

About this task:

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

About this task:

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 required 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. The Preview section shows the result of the changes you apply to the text.

To add bar codes

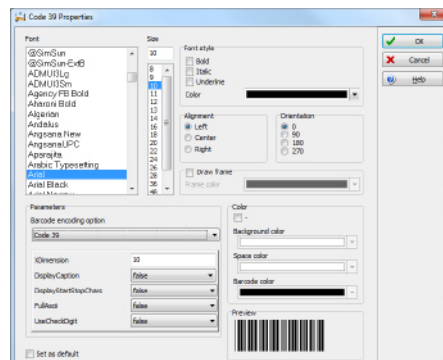
About this task:

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.



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

About this task:

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.

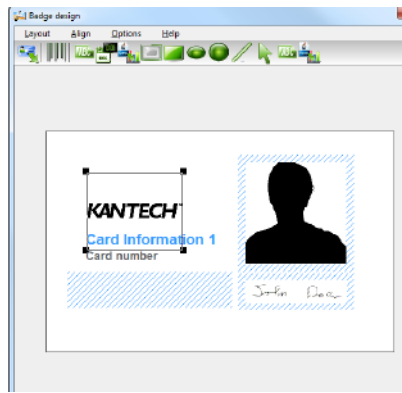
1. From the Badge Design template, select the **Current date** button, then click in the Badge design work area.
2. Right-click the current date to display the shortcut menu.
3. To align the current date, see To Align Objects in the Template Layout.
4. Select **Current date properties** from the shortcut menu.
5. From the Current date properties window, you can:
 - Select the date format at the top of the window
 - Change the text properties: font, colour, justification, orientation

Adding an image

About this task:

You can import background images from any directory. You can incorporate scanned images, photos taken with a digital camera and artwork created in any illustration design program into the badge design.

1. In the **Badge design** window, click the **Picture** icon.
 - ❗ **Note:** The Badging feature supports most available image formats: BMP, JPG, EMF, WMF, GIF, PNG, PCD, and TIF.
2. Drag the **Picture** icon to the template work area. The Image properties window appears.
3. In the **Image properties** window, click the **Select image from file** button.
4. In the **Open** window, browse to the desired image, and 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 in the figure.

5. Using the sizing handles, adjust the image to the required 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 more information, see [To modify picture properties](#).

To place other design objects

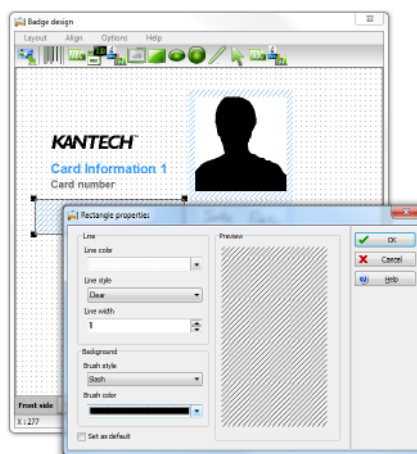
About this task:

Use the Badging feature to 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).

Badge Sample in hattrib Credential

This feature is used to print the word SAMPLE across the badge so it is not included in the Badging Credential count. The hattrib manager can send this sample for approval before printing all other badges.

Functionality

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.

Result

The badge sample feature displays the word SAMPLE across the credential (see below) of the newly created badge

Note: If the badge is 2-sided, the word Sample will be printed on both sides.

Printing badges

You may print badges 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 the Card window.
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

About this task:

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 window, click the **Preview badge** button.

- ① **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.
- **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.

Batch Operations on Cards

Use this menu to modify a specific card type group. For example, you could modify the end date of all the cards that are assigned the “administrator” card type. Individual fields appear only when the appropriate check box is selected.

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.

① **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.
 - **Supervisor level:** If supervisor level is selected, the system will set levels according to according to the values defined in the system.
 - **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.

Table 25: 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

About this task:

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.

- ① **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** list. To create a new group, click 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** list, select the primary access level that will determine the access to the doors of the selected connection.
 4. To select a secondary access level for a Gateway/connection, click the square button next to the **Access level** column, for the Gateway/connection you want to configure.

① **Note:** When a KT-400, KT-1, or KT-2 controller is operating in stand-alone mode, the **primary** and **secondary** access levels remain valid.

When a KT-100, KT-200, or KT-300 controller is operating in stand-alone mode, the secondary access levels are no longer valid, only the **primary** access level remains valid.
 5. Select the **Access level** in the scroll list.
 6. If you need to set up an expiration date for the secondary access level, click the **Use date** option and click the **Expiration date scroll list button** where a calendar appears.

① **Note:** The **Access level** button displays a green indicator when secondary access levels are assigned.

Card Filter Definition

About this task:

The **Card Filter** feature is used to bring more flexibility to the operators in regards to the cards' treatment rights.

1. From the **Users** toolbar, click the **Card Filter** button. The **Card Filter** dialog appears.

① **Note:** You can select a card filter for a given card user from the **Card** dialog. See [Cards Definition](#) for more information.

① **Note:** The card filter field is added on the card printout and in the list of fields that you can choose from during a card importation. See [Creating a New Import/Export Pattern](#) for more information.

① **Note:** The **Card Filter** feature is only available with the hattrix option enabled.

Card Printing

About this task:

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.

- ① **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.

- ① **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.

① **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 file 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.

① **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.

- ① **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](#).

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

About this task:

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.
- ① **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.


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](#).

Table 26: Activity report icon

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. Click the **Users** tab, and click **Card**.

① **Note:** If you activated the enhanced user management, see [Issuing a new card in enhanced user management environment](#).

2. In the **Card** window, click the **New** icon. The Card number field is enabled.
3. In the **Card number** field, enter the number printed on the card and 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. In the **Card user name** field, enter the cardholder's name. You can enter up to 50 characters.
5. Click **Card type** 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 tasks such as modifying an existing card group or creating reports. For more information on how to create or modify card types, see [Card Type Definition](#).

① **Note:** In the **Card type** window, you can right-click the **Card type** field and click **New** to create a new card type, click **Select** to pick an existing card type, or click **Edit** to edit an existing card type.

The system automatically displays the creation date, the modification date and the modification count information in the upper right of the card window.

6. Click **Card filter** to access the **Card filter** menu. Select the card filter for the new card. The card filter gives more flexibility to the operators in regard to the cards' treatment rights. For more information on how to create or modify card filters, see [Card Filter Definition](#).

① **Note:**

In the **Card type** window, you can right-click the **Card type** field and click **New** to create a new card type, click **Select** to pick an existing card type, or click **Edit** to edit an existing card type.

The system automatically displays the creation date, the modification date and the modification count information in the upper right of the card window.

7. Fill out the **Card Information 1 to 40** 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. Later, card information fields will be used to index reports, customize cardholder lists, etc.

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

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. Click the **Users** tab, and click **Card**.
2. In the **Card** window, click the **New** icon. In the **Card user name** field, enter the card holder's name. You can enter up to 50 characters.
3. Click **Save**.
4. Double-click 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 actions such as, modifying an existing card group and creating reports. For more information about how to create or modify card types, see [Card Type Definition](#).

Note: In the **Card type** field, you can right-click the **Card type** field, and select **New** to create a new card type, select **Select** to choose an existing card type, or select **Edit** to edit an existing card type.
5. Click the **Card number** tab, and double-click **Card #1** if you want to change the label.
6. In the **Card number**, 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** applies to the user which means all 5 cards.
 - When the **Multiple Card Format** is selected, a list of all card formats is displayed when you right-click the **Card number** field.
 - When a card format is defined by the system administrator, the card format in use has a check mark next to its description.

The screenshot shows the 'All Card' application window. The top section displays card details for 'Jack Smith', including card type 'Regular employee' and creation/modification dates. Below this is a table of card numbers. Card #1 is selected, and a dropdown menu is open, showing a list of card types and their corresponding card numbers. The card numbers are displayed in a hexadecimal format (e.g., HHHHHH, HH1D0000, etc.).

Card number	General	Access level	Miscellaneous	Comment	Usage	Picture	Intrusion
Card #1	HHHHHH (Hexadecimal 24 bits)						
Card #2	HH1D0000 (Hexadecimal and decimal 24 bits)						
Card #3	00000000 (Octal 24 bits)						
Card #4	00000000 (Octal 24 bits)						
Card #5	00000000 (Decimal 32 bits)						

Card #1 dropdown menu options:

- HHHHHH (Hexadecimal 24 bits)
- HH1D0000 (Hexadecimal and decimal 24 bits)
- 00000000 (Octal 24 bits)
- 00000000 (Octal 24 bits)
- 00000000 (Decimal 32 bits)
- HHHHHHHH (Hexadecimal and decimal 32 bits)
- HHHHHHHHHH (Hexadecimal and decimal 32 bits)
- 00000000 (Decimal ABA, 7 digits)
- 00000000 (Decimal ABA, 8 digits)
- 00000000 (Decimal ABA, 9 digits)
- 000000000 (Decimal ABA, 10 digits)
- 0000000000 (Decimal ABA, 11 digits)
- 00000000000 (Decimal ABA, 12 digits)
- 000000000000 (Decimal ABA, 13 digits)
- 0000000000000 (Decimal ABA, 14 digits)
- 00000000000000 (Decimal ABA, 15 digits)
- 000000000000000 (Decimal ABA, 16 digits)
- 0000000000000000 (Decimal ABA, 17 digits)
- 0000000000 (Corporate 1000)
- 0000000000000000 (RPS)

- ## Result

Card

Card user name: Mike

Card type: Administrator

Card filter:

Creation date: 15-08-11
Modification date: 08-11-11
Modification count: 7
☐ Copy to visitor card

Card number | General | Access level | Miscellaneous | Picture | Usage | Comment

Card number	Display card number	Use expiration date	Expiration date	Trace	Stolen/lost	Deactivated
Card number #1	12-21112	<input checked="" type="checkbox"/>	05-08-11	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Card number #2	12-13215	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Card number #3	00-76546	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Card number #4	15-04684	<input checked="" type="checkbox"/>	30-11-11	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Card number #5	16-00001	<input checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Sodex request state : Request to print Requested by : 15-08-11 10:15:11, Installer

Close Cancel Help

- EntraPass Global Edition Administration Guide

Card audit trail

About this task:

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 definition](#).

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.

- **Date 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 the 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

About this task:

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:

Result



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

About this task:

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

About this task:

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

- ① **Note:** When this option is selected, the first card presented to the door reader is only saved 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.
- ① **Note:** If an operator clicks the **Close** button without saving (when the **Save** button is still enabled), a system prompt asks to save the last information.

Viewing and verifying PINs

You can view and validate each configured cardholders' PINs in the Card window.

Viewing cards assigned the same PIN

1. From the **Card** window, click the **List of PIN owners** button.
 2. Enter the PIN number to validate and click **OK**. A list containing all operators that have a PIN number displays on the screen.
- ① **Note:** If the system is set to PIN duplication (Options > System Parameters), and if the PIN is used by more than one cardholder, the system displays a list of cardholders who are using the PIN. This feature is useful when 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

Finding a card using the toolbar search

1. On the EntraPass workstation, click **Users** and click **Card**.
2. In the **Card** window, on the toolbar, click the **Find** icon.
3. In the **Find a component (Card)** window, in the **Search** field, enter a keyword.
4. To narrow the search results, click one of the following buttons:
 - **Start with:** the list of results includes all of the components that start with the keyword you enter, in alphabetical order, and includes all other components that are in the database.
 - **Begin with:** the list of results includes only components that start with the keyword you enter.
 - **Contains:** the list of results includes all of the components that contain the keyword you enter.
5. **Optional:** The default search criteria is card user name. To change the search criteria, on the left of the **Search** field, click the **Index** icon and select which criteria you want to search, for example, card number or email.
6. **Optional:** To search for the picture that corresponds to the card that you select, click the **Details** icon.
7. Click the **Find** icon.
8. From the list of search results, select the card that you want to display.
9. Click **OK**. The card that you select displays in the **Card** window.

Alternatively, in the **Card** window, in the **Card user name** field, enter a user name. Existing user names display as you enter a value in this field. Select the card that you want to display.

For more information about searching in EntraPass, see [Finding components](#).

Finding a card using the card search window

1. On the EntraPass workstation, click **Users** and click **Card**.

2. In the upper left of the **Card** window, click the **Expand arrow** button.
3. In the **Find a component (Card)** window, in the **Search** field, enter a keyword.
4. To narrow the search results, click one of the following buttons:
 - **Start with:** the list of results includes all of the components that start with the keyword you enter, in alphabetical order, and includes all other components in the database.
 - **Begin with:** the list of results includes only components that start with the keyword you enter.
 - **Contains:** the list of results includes all of the components that contain the keyword you enter.
5. **Optional:** The default search criteria is card user name. To change the search criteria, on the left of the **Search** field, click the **Index** icon and select which criteria you want to search, for example, card number or email.
6. Click the **Find** icon.
7. From the list of search results, select the card that you want to display.
8. Click **OK**. The card that you select displays in the **Card** window.
 If card information is modified, the updates do not register in the open search window. To see the latest updates in your search results, refresh by pressing **F5**, or by closing and re-opening the **Card** window.
 For more information about searching in EntraPass, see [Finding components](#).

Editing a card

To edit a card in the **Card** window, complete one of the following steps:

- In the **Card user name** field, enter a user name. Existing user names display as you enter a value in this field. Alternatively, use the up and down arrows to browse for a card. Select the card that you want to modify.
- In the **Card number** field, enter the card number and press **Enter**.

The card displays in the **Card** window and you can modify it as required.

Deleting a card

About this task:

If you have the appropriate access rights, you can use the delete feature to remove a card from the cardholder database. If you delete a card from the cardholder database, you must re-issue it to use it.

1. Find the card that you want to delete. To search for cards, see [Finding a card using the toolbar search](#).
2. In the **Card** window, on the toolbar, click the **Delete** icon.
3. In the **Warning** window, click **Yes**.
 Deleting cards removes them from the cardholder database but they remain in the card history. All events involving a deleted card remain in the event messages database. You can generate an event report that includes past events for deleted cards.

Customizing Card Information Fields

1. Select a **card** field from the list on the left.
 2. Edit the **card** captions through the given text box.
 You can enter two different descriptions and use the **Swap** button to swap the first and second captions.
- ❶ **Note:** If you do not see the **Swap** button, you need to enable the second language option in **Options>Select language**.

3. Click **OK** to keep your changes or **cancel** to return.

Cardholder Access Levels Assignment

An access level must be assigned to each card. Access levels determine where and when the card will be valid. The access level allows the cardholder entry to selected locations during specified schedules. For information on defining access levels, see [Access Levels Definition](#).

- ① **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 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 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**.

- ① **Note:** You have to create Access levels (Users > Access Level) to have them displayed in the Access Level drop-down list.

Assigning additional access levels (Multi-site gateway only)

About this task:

When you use a KT-400, KT-400 rev1, KT-1, or KT-2, you can make up to five total access levels for each user or connection.

1. From the Card definition window, select the **Access level** tab. The Access level window appears, it displays the **Gateway/Connection** column and **Access level** 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 appears with the different Gateways and Connections.
3. From the **Additional access levels** window, you can assign additional access levels.

- ① **Note:** If there is a warning exclamation sign in the right column beside the access level, there are controllers associated with the access level which do not support additional access levels, such as the KT-100, KT-200 and the KT-300.

Assigning secondary access levels (Global/KT-NCC Only)

About this task:

You can assign up to six secondary access levels and use an expiration date for each secondary access level to restrict access to certain doors after the date is reached (button displayed on the right).

- ① **Note:** When a KT-400, KT-1, or KT-2 controller operates in stand-alone mode, the primary and secondary access levels remain valid.

When a KT-100, KT-200, or KT-300 controller operates in stand-alone mode, the secondary access levels are no longer valid, only the primary access level remains valid.

1. Click the button on the right that corresponds to the Gateway/connection you want to define in order to access the Secondary access level dialog,
2. Select the **Access Level** from the list to define a secondary access level.
3. If you want to define an expiry date, select the **Use date** option. This opens a calendar where you can select the **Expiration date**. You also need to set the expiration hour (00 to 23) . The default is 00 (midnight). After you select the date, it displays in the **Expiration date** column.


- ① **Note:** The button displays a green indicator when a secondary access level is assigned.

In the **Secondary access level** window, when a secondary access level reaches its **Expiration date**, the date remains in the list, but changes to a red font.

Access exception

About this task:

Use the **Access exception** tab to link a specific schedule to a door.

1. On the left pane, select a door.
2. On the right pane, from the list, select a schedule. Click the  button to add or remove doors from the list on the right.
3. In the **Access** column, choose between **Allow** or **Deny**.

- ① **Note:** Only doors with an associated schedule are saved.

- ⚠ **WARNING:** The user list report does not take access exception into account.

To enable the **Access level exception** feature, see [Credentials Parameters](#).

Card options definition

About this task:

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 calendar. The start date must be the same day or earlier than the current date; else, the **Card state** field (**Miscellaneous** section) is set to **Pending**.
2. Select the **Use end date** box, if applicable. When this box is checked, the system displays a calendar allowing you to select the end date. When the end date is reached, the **Card state** field is set to **Expired**.
3. Select the **Delete when expired** option, if applicable. This option can only be used with the **Use end date** option. When selected, the card information is automatically deleted on the expiry date (using the end date and hour specified), otherwise the **Card state** field is modified to **Expired**.

- ① **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. Select 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.
 - ① **Note:** Selecting the **Wait for keypad** delays 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** list, assign a state to the selected card. By default, a card is valid. The following 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.
 - ① **Note:** You cannot force a card state to **Pending** by selecting this state from the **Card state** list. To do so, you have to change the start date.
7. Select the **Disable passback** option if you want the card to override the passback option when defined.
 - ① **Note:** If you are issuing a card for a cardholder with disabilities, check the Extended door access delay option. To enable this option in the system, you have to define appropriate delays in the Door definition.
8. Set **Supervisor level** according to user privileges.
 - ① **Note:** If required, select the **Privileged** operation option to override any security measures regarding doors.
9. **Allow multiple-swipe (KT-400, KT-1, and KT-2 only):** Enable the multi-swipe action. For more information, see [Card multi-swipe](#).

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

About this task:

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.
 - ① **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.

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.
 - ① **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.
 - ① **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.
 - ① **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

About this task:

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

- ① **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**).
 - ① **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](#).

- ❶ **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

About this task:

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.
- ❶ **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

About this task:

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

About this task:

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.
2. Select **Start selection mode** from the shortcut menu.
3. Once you have selected the part you want to incorporate into the card, right-click the image again. A shortcut menu appears.

❶ **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.

- ① **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.
- From the shortcut menu, select **Edit (picture or signature)**.
 - 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.
 - Click **OK** to close the **Picture** editing window.
 - 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](#).

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.

- ① **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

About this task:

Two patterns are available: the EntraPass (1,2,3) and the WinPass64 model. You can use the template or you can edit it.

- From the **Users** toolbar, select the **Import/Export CSV file** button.
- From the **Select operation** drop-down list, select either **Import** or **Export**.

3. In the **Available Patterns** pane, select the pattern you 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

About this task:

This menu lets you create your own import/export mask to use 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-click the **available fields** or use the **left** and **right hand** button to move 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).
 - ① **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**.
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. The 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. The 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
 - ① **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 exit 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

About this task:

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 that EntraPass saves the card database content in. You can open the CSV file in Excel, NotePad.
5. Once you have selected or 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.
 - ① **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 is not 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.
 - ① **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 displays.
2. In the **Select Operation** drop-down list, select Import.
3. Click the **Available patterns** button to select the pattern that is 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** and you 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.
 - ① **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 or export errors

About this task:

The CSV Import/Export feature imposes a number of rules: each field contains a specific value format that must be followed. For example, the card state field only accepts the following values (0=valid, 1=invalid, 2=stolen/lost). The pattern used must match the pattern used by the source file. The present section assists you in correcting import or 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.
 - ① **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.
 - ① **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

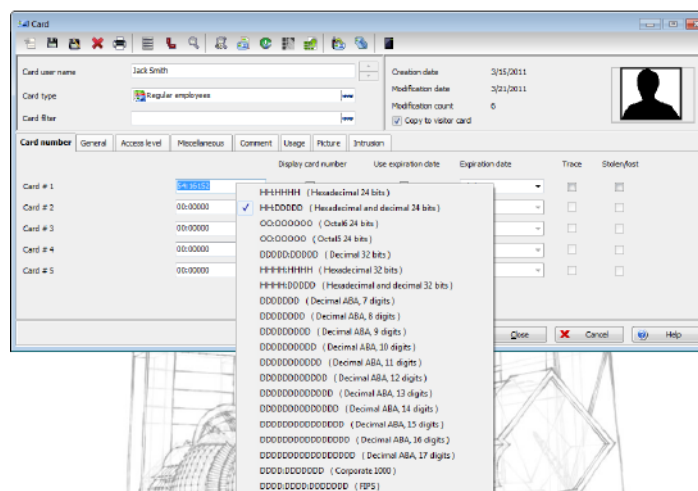
1. Select a **card** field from the list on the left.
2. Edit the **card** captions through the given text box.
You can enter two different descriptions and use the **Swap** button to swap the first and second captions.
 - ① **Note:** If you do not see the **Swap** button, you need to enable the second language option in **Options>Select language**.
3. Click **OK** to keep your changes or **cancel** to return.

Issuing a new card in enhanced user management environment

- ① **Note:** See [Credentials Parameters](#) for more details on how to enable the **Enhanced User Management** environment.
1. Click the **Users** tab, and click **Card**.
 2. In the **Card** window, click the **New** icon. In the **Card user name** field, enter the card holder's name. You can enter up to 50 characters.
 3. Click **Save**.
 4. Double-click 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 actions such as, modifying an existing card group and creating reports. For more information about how to create or modify card types, see [Card Type Definition](#).
 - ① **Note:** In the **Card type** field, you can right-click the **Card type** field, and select **New** to create a new card type, select **Select** to choose an existing card type, or select **Edit** to edit an existing card type.

5. Click the **Card number** tab, and double-click **Card #1** if you want to change the label.
 6. In the **Card number**, 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:DDDD (Hexadecimal and decimal 24 bits).
- ❶ **Note:** The **Access Level** applies to the user which means all 5 cards.
- When the **Multiple Card Format** is selected, a list of all card formats is displayed when you right-click the **Card number** field.
 - When a card format is defined by the system administrator, the card format in use has a check mark next to its description.

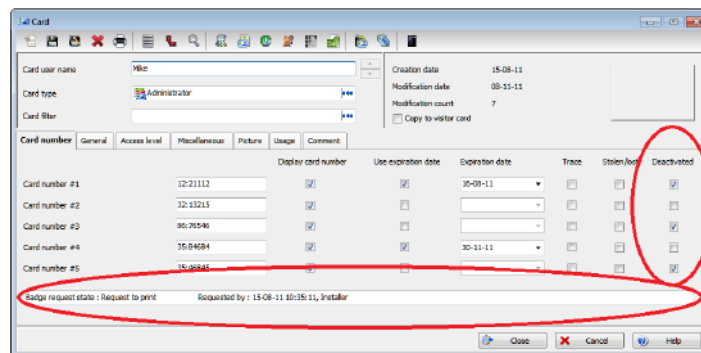
Figure 13: Multiple card formats



7. **Optional:** Assign the **Card number** immediately.
 8. If you have the appropriate access rights, you can select **Display card number** to display the user card number in reports and message lists in the EntraPass workstations .
- ❶ **Note:** The creation date, the modification date, and the modification count information automatically displays in the upper right of the **Card** window.
9. Select **Use expiration date** and select the corresponding date.
 10. Select **Trace** if you want to monitor the use of a particular card. Selecting this option causes the **Card traced** event to generate each time this card is presented to a card reader. For example, you can request and generate a report containing the **Card traced** event to verify user actions.
 11. Select **Stolen/Lost** if the card is stolen or lost. The card will not be functional anymore.
 12. Repeat Steps 5 to 11 for Card #2 to Card #5, if applicable. You can select different options for the 5 cards.
 13. In a hattrix environment, information on the last transaction made on a card displays at the bottom of the **Card** window. Also, use the **Deactivated** checkbox to give a card an activated or deactivated status.

Result

Figure 14: Card deactivated status



① **Note:** These fields display only when the **Badging Credential** option is activated.

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:

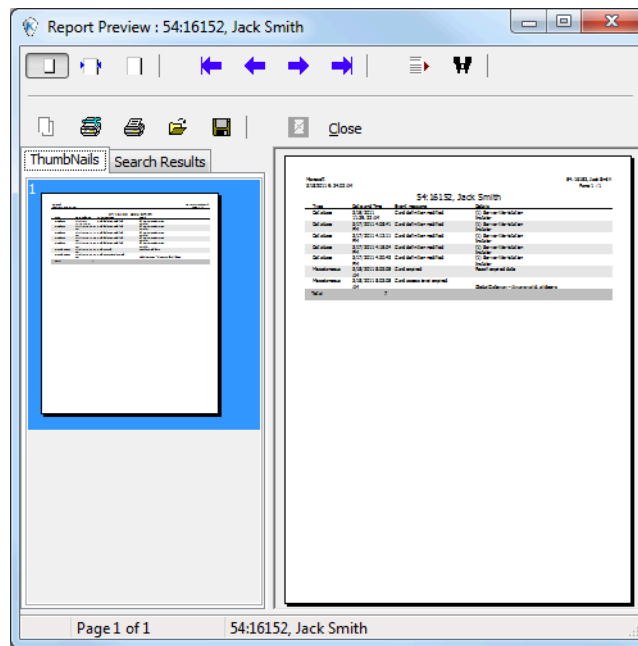
- Access denied events (bad location, bad access level, bad card status, etc.),
- Access granted events,
- Database events (that have affected the database, such as: card definition modified, relay definition modified, etc.),
- Other/Miscellaneous events (these include events that were generated by cardholders),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

① **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

- 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, and 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.

Result



Quick Access to Door List per Card

About this task:

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:

Result



The information is displayed over five columns:

- Gateway/connection button
- Gateway/connection description
- Door description
- Schedule description

① **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

Result

Default value is Hexadecimal 32 bits

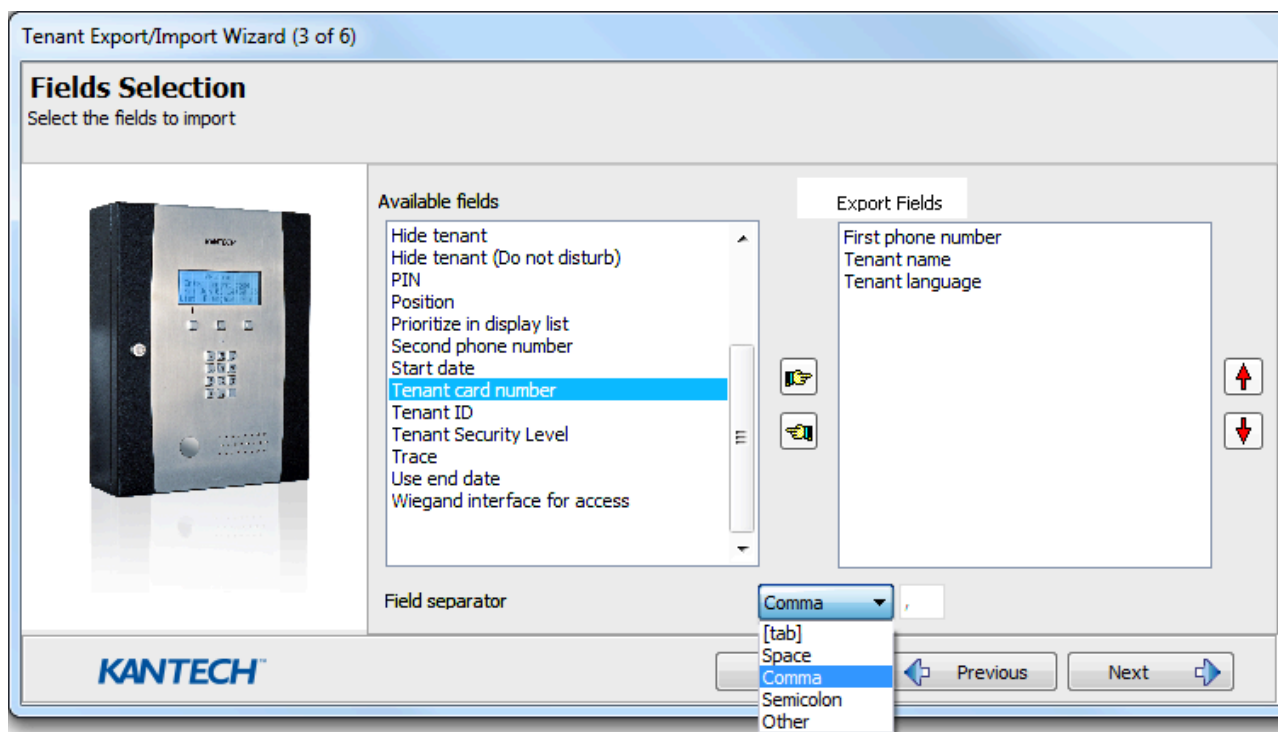
Adding new tenants to the list

1. Click 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). The default value is **New tenant**.
 - **Tenant ID:** Enter the tenant's ID. The tenant's ID is an identification code of 1 to 5 numbers that a visitor can use to call a tenant. The number of digits available for an ID is configured when the list is created. The 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 is not displayed in the KTES directory either (15 digits maximum). The 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). The default value is empty.
 - **PIN:** A Personal Identification Number (PIN) is 4 to 6 numbers configured for each tenant. The number of digits available for a PIN is configured when the list is created. The default value is 0000.
 - **Access schedule:** Enter the access schedule. For security reasons, an access schedule is configured to link a schedule with the tenant access rights. A tenant can access the building according to specific times, days and holidays defined in the system. The default value is always valid. For more information about defining schedules, see [Schedules Definition](#).
 - **Tenant admin level:** Select the administration level for the tenant (installer, owner, maintenance or tenant). The default value is **Tenant**.
 - **Tenant language:** Select the default language used by the KTES for the tenant (System, English, French, Spanish, Custom). The default value is **Default**. For more information about the system language, see [Kantech Telephone Entry System \(KTES\) Configuration](#).
 - **Disabled Tenant:** A disabled tenant status allows the activation of a relay and/or the generation of an alarm. The default value is deselected (enabled).

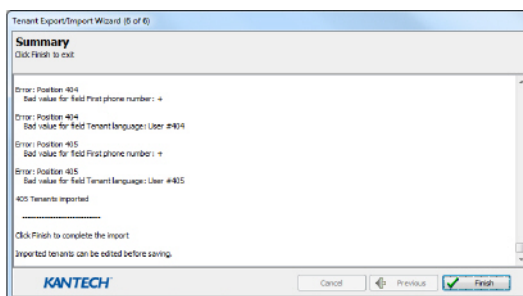
- **Trace:** The trace option allows the activation of a relay and/or the generation of a traceability event. The default value is deselected (not traced).
 - **Hide tenant:** This option is used if you want the current tenant's name to be displayed or hidden. The default value is deselected (displayed).
 - **Extended door access delay:** The extended delays correspond to the additional time lapse a door should stay unlocked and can be kept opened. The default value is deselected (no extended delay).
 - **Extended ring:** The system can allow an extended number of rings to give more time for the tenant to answer. The default value is deselected (no extended ring).
4. Click 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 the **Calendar** button to select a date. The 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 longer valid. Select the checkbox to enable the end date. The default value is deselected (**no end date used**). Enter the date in the field (mm/dd/yyyy) or click the **Calendar** button to select a date. The 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. Select the **Hide tenant** check box if you want 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 want to use the second phone number only when the selected schedule is active, select the **Call second phone number only on schedule** check box.
 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 cardholder's number is the first card number to be used by the tenant to get access from the KTES.

Importing a tenant list

1. Click the **Import** button to run the **Tenant Export/Import Wizard**.
2. Click the **Next** button and select a CSV format source file.
3. Click the **Next** button and choose the field to be imported from the list on the right. Use the left and right buttons to add or remove data fields. The default field separator is comma but you can select a different one.

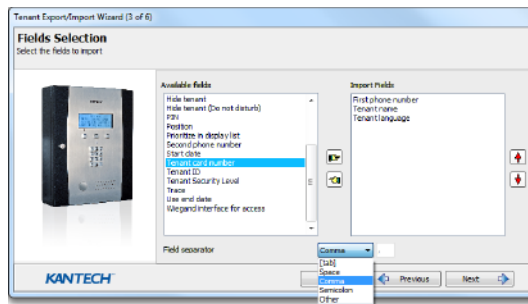


4. Click the **Next** button and select the tenants to be imported.
5. Click the **Next** button and click the **Import** button to complete the operation.
6. Click the **Next** button to see a summary of the imported data.

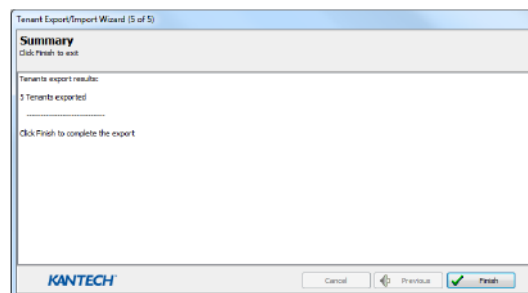


Exporting a tenant list

1. Click the **Export** button to run the **Tenant Export/Import Wizard**.
2. Click the **Next** button and choose the field to be exported from the list on the left. Use the left and right buttons to add or remove data fields. The default field separator is comma but you can select a different one.



3. Click the **Next** button and select the tenants to be exported.
4. Click the **Next** button and select a CSV format destination file. Click the **Export** button.
5. Click the **Next** button to see a summary of the exported data.



Validating card access

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

1. In the **Card** window, select a card.
2. Click the **View and Validate Access** icon. It is the key icon on the toolbar.
3. Select a site/gateway/connection from the **Site/Gateway/Connection** list .
4. In the **Select specific value** area, 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).

Definition

Use this section to define the elements to create a secured area for control and alarm purposes. A schedule indicates when the system executes certain operations, when the system acknowledges events, and when to activate relays controlling different functions, for more information see [Schedules Definition](#).

The alarm system is a group of devices configured in a partition to detect an alarm condition and consequently signal the alarm, for more information see [Alarm Systems Definition \(Global/KT-NCC\)](#).

You can use areas to define anti-passback parameters, for more information see [Area Definition \(Global/KT-NCC Gateways Only\)](#). Anti-passback is a sequencing control to prevent cardholders sharing their badge with another person. You can use [Guard Tour Definition \(Global/KT-NCC Gateways Only\)](#) to define a number of doors that a guard must visit in a certain sequence and verify within a certain schedule.

If you want to assign doors as elevator floors use [Floors Definition](#).

When you want to associate a trigger with a particular event, use [Event Relays Definition \(Global/KT-NCC Gateways\)](#). You can use [Graphics Definition](#) to view a secured area of the system where components are located on a connection. In addition to viewing the status of a component you can perform manual operations including locking or unlocking a door, and moving cards.

You can use [Holiday Definition](#) to assign extra days to a schedule, for example holidays that apply to one site but not another.

Use [Creating a new trigger](#) to define an alarm to an event and create an associated schedule.

If you have a SmartLink application installed, use [Using the task builder](#) to create built-in task commands to SmartLink.

Alarm Systems Definition (Global/KT-NCC)

An alarm partition is a gathering of devices or equipment arranged to signal and detect the presence of an alarm condition requiring immediate attention or operator acknowledgement. The system offers up to 100 virtual alarm partitions per gateway. A virtual alarm partition is an alarm partition that is entirely controlled by the gateway instead of using a hardware device designed to perform the same function. Depending on how virtual alarm partitions are programmed, they can trigger various relays on alarms.

Example of an alarm partition

The system is able to partition the different areas of the building into up to 100 VASP (Virtual Alarm System Partition). Each VASP partition can be set up using any number of readers, door contacts, motion detectors, sirens and user access rights. Monitored points can be used in more than one partition.

Operation

Each area can be delimited by doors equipped with readers and monitored with door contacts. Single reader doors can also be equipped with a T.REX exit detector to provide hands-free door unlock. As required for the security of each area partitioned, the VASP will control a collection of the following devices: readers, door contacts, motion detectors, heating / air conditioning control, exit delay warning device and door locks.

Arming, Postponing and Disarming

Each VASP can be defined with an auto-arming schedule for each day of the week including holidays. At the programmed arming time, the exit delay warning will sound for a minimum of 4 minutes. Any employee in the area who is not allowed to stay later than the arming time will have to leave the area. At the end of the exit delay, the area will arm and will be monitored for intrusion

and, possibly, for turning off or changing the settings of the air conditioning or heating system. During the exit delay, if an authorized employee wants to remain in the secured area later than the arming time, that employee can use his / her card at any of the readers of the area defined as a “postponement reader” in the system. This operation will initiate the postponement of the arming. The postponement delay can be pre-programmed for each area, up to eighteen hours and twelve minutes (18h22). After the postponement period, the system will attempt to arm again and sound the exit delay. The same scenario of postponement will be available to employees wanting to remain in the area unless a maximum number of postponements (if programmed) or a “no disarm” scheduled time has been reached. Each card of the system can be programmed to allow or limit the use of this feature.

When an area is armed, it can be disarmed by authorized cardholders (who share the right to disarm the alarm partition) by presenting their cards at a disarming reader (as defined in the system). If the cardholder is authorized in that area during that specific time, the door will unlock and the partition will be disarmed as soon as the cardholder opens the door. If disarming happens at a time when the system would be normally armed by a schedule, the system will attempt to re-arm automatically after the postponement time described earlier. In addition to those tasks performed by cardholders, an authorized operator (such as a guard) can manually operate the partitions from any of the system's workstations (disarm, arm or modify the postpone delay time).

Alarm System Capabilities

- Up to 100 different independent alarm partitions can be programmed per gateway.
- Each alarm partition can supervise any input or door of the system.
- When defining alarm partitions, elements such as: doors, readers, input zones and output relays can be defined as single or group.
- Each alarm partition can include inputs or doors supervised by one or more alarm partitions as shared elements (common).

Note: If a same input is defined for 2 alarm partitions, and only one system is armed, if this input generates an “alarm”, it will not be reported. Both alarm partitions must be armed for the input to report the alarm condition.

Common Inputs

Input zones or doors, which are shared by multiple alarm partitions, are related according to the following rules:

- An alarm partition will only produce an alarm from an input / door common to other alarm partitions if all the alarm partitions containing that input / door are armed. Inputs or doors which are part of “Alarm Level 1 and 2” can be defined in a different way but have to be part of a group.
- Alarm level 1 and 2 (input groups) are processed together as one large group for the purpose of determining whether an input (zone) is also included in another alarm partition definition.
- Common doors which are defined as “Door to be locked on arming” or “Door disabled on arming” in both alarm partitions will revert to their normal state if one or more of these alarm partitions is disarmed.

Perimeter and Volumetric Detection

The devices of an alarm system are grouped in two categories, perimeter and volumetric detection.

Perimeter (Alarm Level Inputs)

Perimeter detection refers to the detection of access to the outer limits of a detection area by means of physical barriers such as door contacts, glass break detectors, door contacts on uncontrolled doors, etc.

Usually, inputs that are defined as “perimeter” (glass breaks, garage doors, fire doors, door with door contacts not controlled, etc.) are grouped and defined as “alarm level #1 inputs”. When one of these inputs are activated, it will activate the “alarm relay #1” relay which can be connected to an “alarm panel” that will send a warning to the central indicating a parametric intrusion. A perimeter detection is considered more important since it originates from the perimeter of the controlled area. For supervised doors (reader, T.REX, door contact), you can use the field Supervised door when armed to group the doors that will also activate the “alarm relay #1” when a “door forced open” or “door open too long” event is generated for these doors. For example, main entrance doors or back entrance doors can be included in this field.

Volumetric (Alarm Level # 2 Inputs)

Volumetric detection refers to detection of access of the volume, such as an entire room or part of a room by means of volume detectors such as: movement detectors or sensors, controlled doors (readers, etc.). Inputs defined as “volumetric” (PIRs, sensors (heat), etc.) are grouped and defined as “alarm level # 2 inputs”. When one of those inputs is activated, it will activate the “alarm relay #2” relay which can be connected to an “alarm panel” that will send a warning to the central indicating a volumetric intrusion.

Arming Procedure

There are three (3) methods to arm an alarm system:

- **Manual arming:** This is done at the Manual operation window at the workstation by an authorized operator. The alarm system will be armed once the exit delay is over.
 - **Automatic arming (arming schedule):** The alarm partition will initiate the exit delay when the arming schedule becomes valid. The alarm partition will be armed once the exit delay is over.
 - **Arming at a door reader (with or without an arming request button):** There are 3 possible choices:
 - **With a card:** The card is presented at the reader defined as “arming reader”. The exit delay is initiated, once over the alarm partition will be armed.
 - **With a card and an “arming request input”:** The card is presented at the reader defined as “arming reader”. The “arming” delay is initiated. The “arm request input (button)” must be pushed during this delay to confirm arming. Once the arming request input is pushed, the exit delay is initiated and the alarm partition will be armed once the exit delay is over.
 - **With only an “arming request input”:** The “arm request input (button)” must be pushed to confirm arming. Once the arming request input is pushed, the exit delay is initiated and the alarm partition will be armed once the exit delay is over. To only use an “arming request input”, no reader must be defined as “arming reader”.
- ① **Note:** Arming is done by presenting a card at the door reader (or entering a number on the keypad) defined as “arming reader” in the alarm system definition menu. Arming at a door reader is only permitted by a card with the defined arming access level, which must include access to the arming reader in question.

Disarming Procedure

This command disarms the alarm system. Depending on how the partition is programmed, results can be different.

- **Manual disarming:** This is done at the manual operation window at the workstation console by an authorized operator. The alarm partition will disarm right away, unless a “no disarm” schedule is valid, this command will initiate the “postpone” delay.
- **Disarming at a door reader using a card:** Disarming is done at the door reader (or keypad) defined as “disarming reader” in the system.

General Rules:

- Disarming is done by presenting a card at the door reader (or entering a number on the keypad) defined as “disarming reader” in the alarm system definition menu.
- Manual disarming is only permitted by a card with the defined disarming access level, which must include access to the disarming reader in question.
- If there is a door contact defined for the door, then the door must be opened for disarming to take effect. If there is no contact, you don't have to open the door.
- If the arming reader is also defined as “disarming reader”, the door will have to be open to disarm the system. On the other hand, if a “no disarm” schedule is effective, a disarming request will postpone the arming of the system.

Disarming when “No Disarm” Schedule is Valid Procedure

If a “no disarm” schedule is in effect and a user disarms the system, the system will be in the “postpone delay” mode, when this delay expires, the system will be in the “exit delay” mode, when this delay expires, the system will arm again automatically, if the schedule is still valid at that time. In this case the limit on the number of postponement delays is effective only after the initial delay. Arming an alarm partition can be postponed for a pre-set period (maximum 16.5 hours) after which the system will automatically arm only if the “no disarm” schedule is valid at that time.


Postponing arming procedure

A postponement arming can be activated in two ways, depending on the circumstances:

- During the exit delay: when the system is being armed, whether armed manually or by arming schedule, and a “no disarm” schedule is valid.
- While the system is armed, during any interval when the “no disarm” schedule is valid, the normal disarming of the system will automatically initiate a postponed arming, for a number of times not exceeding the maximum number defined in the postpone count field.

Note:

- In both cases, the system will automatically arm itself at the end of the postponement delay (when the postponement delay expires, the exit delay is initiated) only if the “no disarm” schedule is in effect at the time.
- A postponed arming can only be activated at door readers defined as “arming reader” or as “postponing reader”.
- For a door reader defined as “postponing reader”, you can only postpone during the “exit delay”.
- For a door reader defined as “disarming reader”, you can postpone during the “exit delay” or when the system is armed and a “no disarm” schedule is valid.
- A postponed arming can only be activated with a card with the “disarming access level”, which has to include access to the door from which it is to be activated.
- A postponed arming can be activated during the “exit delay” when the system is being armed, during a postponement delay already in progress or when the system is armed and a “no disarm” schedule is valid.
- If a postponement-arming request is done when one is already in progress will reset the postponement delay and decrement the count of consecutive postponement allowed, if the limit has not already been reached. A limit is defined (0-15) for the number of successive postponement delays permitted.

 **WARNING:** An entry of 0 in the “postpone count field” will cause an infinite number of successive postponements to be permitted.

- If a reader is defined as BOTH the arming and disarming reader for a given alarm partition, its function with respect to postponement will be as the postponement reader, i.e. postponement will initiate immediately upon card access.

To Define an Alarm Partition

1. Click the Alarm System button.
2. From the **Select gateway** window, select a gateway associated with the alarm partition.
3. From the **Alarm System** drop-down list, select an existing alarm system or click New to create a new alarm system.
4. From the **Arming Schedule** field, select a schedule according to which the alarm partition will automatically arm at the time that this schedule becomes valid (the exit delay will be initiated before the system actually arms). This schedule is used only to arm the system, do not insert the "All valid" schedule. When this schedule becomes invalid, the system will not disarm, it will remain armed until presentation of a valid card at a disarming reader. You can right-click the selection field to create a custom arming schedule.
5. From the **No Disarm Schedule** field, select a schedule during which a disarming attempt will initiate postponing of the alarm partition. Once the postpone delay is over, the system will automatically initiate the exit delay and arm automatically once expired.
6. Select the **Access and delays** tab to define access level options:
 - **Arming Access Level:** select the access level required to arm the alarm partition. Arming the system requires the arming access level and access to the arming reader(s).
 - **Disarming Access Level:** select the required access level to disarm the alarm partition. Disarming the system requires the disarming access level and access to the disarming reader(s).
7. In the **Delays** (hh:mm:ss) section, specify the entry and exit delays:
 - **Entry:** Specify the entry delay time during which a user will have access to a supervised area to disarm the system.
 - **Exit:** Enter the exit delay. The exit delay is used to warn employees that the system will be armed once this delay is expired following an arming request. The system can be in the "exit delay" mode following:
 - An arming request,
 - or when the "postpone delay" is expired and the "no disarm" schedule is still valid.
 - **Arming:** Enter the arming delay time. This is the delay allowed by the system between the moment that a card is presented at an arming reader and the moment that the "arming request button" is pushed to confirm arming.
 - **Postpone parameters:** Enter the postpone delay time. The postpone delay is a "period" during which the alarm partition is disarmed.
 - If the "no disarm" schedule is still valid, the system will enter in "exit delay" then arm again when the exit delay expires.
 - If a postpone or disarming operation is attempted during this "exit delay" the system will return to the postpone delay.
 - If the "no disarm" schedule is NOT valid, the system will automatically disarm at the end of the postpone delay.
 - The postpone delay can be manually modified through the manual operations section of the system.

- ① **Note:** It is possible to associate a relay that will be triggered when an arming, disarming or postpone delay is initiated. It could for example provide a visual feedback on a status panel to indicate that the system is waiting for a confirmation.
- **Postpone Count:** This option specifies the maximum number of times the alarm system can be postponed. When the maximum count is reached, the system will initiate the exit delay and arm automatically (if a “no disarm “schedule is still valid) or disarm if a normal arming schedule is valid.
- ① **Note:** If set to “0”, the alarm partition can be postponed indefinitely.
- 8. Select the **Door** tab to define the arming and disarming, and postpone options:
 - **Arming reader:** Select a door or door group that will be used to arm the alarm partition. Arming will only work at an arming reader. Arming the system requires the arming access level and access to the arming reader(s).
 - ① **Note:** Usually, arming readers are located near exit doors.
 - If more than one alarm partition can be armed with the same arming reader, use an “arming request input” to confirm arming.
 - **Disarming reader:** Select a door or door group that will be used to disarm the alarm partition. Disarming will only work at a disarming reader. Disarming the system requires the disarming access level and access to the disarming reader(s).
 - ① **Note:** Usually, disarming readers are located within the perimeter of the protected area. For example, a disarming reader could be located at the front door where a video surveillance camera is located for visual recording.
 - **Arming reader no unlock:** Select a door or door group that will be used to arm the system without unlocking the door.
 - **Postpone reader:** Select a door or door group that will be used to postpone the alarm partition from arming. Postponing arming requires the disarming access level and access to the postpone reader. A postpone reader can only be used during the “exit delay”.
 - ① **Note:** Usually, postpone readers are located within the protected area so as to allow employees to postpone the system from any reader located inside.
 - **Reader disabled when armed:** Select a door or door group for which the readers are disabled when the alarm partition is armed. No access is permitted, even for cards with the required disarming access level and at the disarming reader.
 - ① **Note:** For example, this field can be used to select a back door in order for users to use the front door to disarm the system.
 - **Door to be lock on arming:** Select a door or door group that will be locked when the alarm partition is armed. It will override the unlocking schedule (even if valid) and will also override a manual unlocking operation.
 - **Supervised door when armed:** Select a door or a group of doors that will generate an alarm level # 1 (perimeter) and trigger the relay selected in the Alarm # 1 Relay State field (Relay 2 of 2 tab) if the events “door forced open” or “door open too long” are produced by these doors while the system is armed.
- 9. Select the Input tab to define input for arming and disarming:
 - **Alarm level #1:** Select a single input or a group of inputs that will automatically activate the relay selected in the Alarm # 1 Relay State field (Relay 2 of 2 tab) if the system is armed and an alarm is detected from one of the selected inputs.

- **Alarm level #2:** Select a single input or a group of inputs that will automatically activate the relay selected in the Alarm # 2 Relay State field (Relay 2 of 2 tab) if the system is armed and an alarm is detected from one of the selected inputs.
 - **Arming request:** Select a single input or a group of inputs that must be “in alarm” to confirm arming of the alarm partition. An arming request input should be used when more than one alarm partition can be armed with the same arming reader. Usually, a button is used as an arming request input. The card is presented at the reader, the “arming delay” is initiated, the button is pushed, the exit delay is initiated after which the alarm partition will arm.
10. It is possible to associate a relay that will be triggered when the arming delay is initiated. It could for example provide a visual feedback on a status panel to indicate that the system is waiting for a confirmation.
- **Prevent arming:** Select a single input or a group of inputs. If any of these inputs is “in alarm” when arming is attempted, arming will not succeed and will be aborted. Usually inputs from “Alarm Level 1 & 2” are grouped together as one group and selected. This will group all the inputs of the alarm partition. This is only true when an arming request is done at a door reader with an arming request input.
- ❗ **Note:** If the alarm partition is armed automatically with an “arming schedule”, the inputs will be ignored and arming will succeed.
- It is possible to associate a relay that will be triggered when the arming is aborted.
- **Input for entry delay:** Select a single input or a group of inputs used to initiate the entry delay. If any of these inputs is “in alarm” when the system is armed, the entry delay will be initiated and inputs selected in the “Shunted on Disarming” field will be shunted for the duration of the “entry delay”.
 - **Shunted on disarming:** Select a single input or a group of inputs that will be shunted (not monitored) when the “Entry Input” is triggered. These inputs will be shunted for the duration of the entry delay.
11. Select the **Control Relay** tab to define the relays that will be used to indicate or display various status for the alarm system being defined. For each relay, it is possible to determine when the relay will return to its normal condition. There are 2 possible conditions:
- **Temporary:** The relay will remain temporarily activated for the activation time programmed in the relay definition menu. Be careful, if the relay activation time is set to zero in the relay definition menu, the relay will “follow” the condition or device condition even if it is programmed to be temporarily activated.
 - **Follow:** The relay will remain activated until the condition that triggered the relay is over.
- ❗ **Note:** When a relay is activated or deactivated from of an alarm system, EVENTS WILL NOT be generated.
- **System Armed—Relay:** This relay will be triggered when the alarm partition is armed.
 - **System Disarmed—Relay:** This relay will be triggered when the alarm partition is disarmed.
 - **System Status Relay:** This relay will reflect the status of the inputs of “Alarm Level #1 and #2” as well as doors of the “Door supervised when armed” field.
 - **Prevent arming Relay State:** Select the relay that will be triggered when the arming sequence is aborted due to an input in alarm generated during arming. Select, from the pull-down menu, the relay activation.

12. Select the **Status Relay** tab to define the relays that will reflect the various conditions of the alarm system being defined.

- ① **Note:** When a relay is activated or deactivated from an alarm system, EVENTS WILL NOT Postpone Relay—Select the relay that will be triggered when the alarm partition is in “postpone” mode.
- **Entry Relay State:** Select the relay that will be triggered when the “entry delay” is initiated.
- **Exit Relay State:** Select the relay that will be triggered when the “exit delay” is initiated.
- **Arming Delay State:** Select the relay that will be triggered when the “arming delay” is initiated.
- **Alarm #1 Relay State:** Select a relay that will be triggered when the alarm partition detects a valid alarm condition (i.e. input in alarm) from one or more inputs defined in the “Alarm Level #1” field or from one or more doors (i.e. door forced open or door open too long) defined in the Supervised door when armed field.
- **Alarm #2 Relay State:** Select a relay that will be triggered when the alarm partition detects a valid alarm condition (i.e. input in alarm) from one or more inputs defined in the Alarm Level #2 field.
- **Bell-Relay state:** Select a relay that will be triggered when the alarm partition detects a valid alarm condition (i.e. input in alarm) from one or more inputs defined in the Alarm Level #1 field or from one or more doors (i.e. door forced open or door open too long) defined in the Supervised door when armed field. Usually an audible signal is initiated with this relay.

Linked Partitions

Alarm integration, for global gateway and KT-NCC, allows linking existing virtual alarm systems in EntraPass to DSC partitions and Honeywell groups.

Once the panel is created on a gateway, a new **Linked Partition** tab is displayed in the virtual alarm systems menu.

Up to 8 partitions or groups can be linked to a virtual alarm system. The following tasks can then be performed:

- Arm
- Arm no delay (if supported)
- Disarm
- Arm and Disarm
- Arm no delay and Disarm

- ① **Note:** If a partition belongs to more than one virtual alarm system, all these systems will have to be armed first for the partition to be armed.

Comment

- ① **Note:** For more details about the **Comment entry** box, see Comment Field.

Area Definition (Global/KT-NCC Gateways Only)

About this task:

Areas are the basic unit for using anti-passback. They define how to control and monitor cardholder activities within an area of controlled doors. Under a Global and KT-NCC and Gateways, the anti-passback is entirely controlled by the gateway rather than the controllers.

1. Click the **Area** button.

2. Select the **Gateway** associated with the area you want to define, then select an **Area** (to modify one) or click the **New** button to create a new area.
 - ① **Note:** When cards are created in the Card Definition dialog, they are automatically sent to the “unknown area”.
3. Define the **Passback type** applied to the area being defined:
 - **None** : No anti-passback is verified to access the area. If you want to disable the passback for a specific time, use the **Disable passback schedule** field under the **Miscellaneous** tab.
 - **Normal (hard anti-passback)**: The “normal” passback is considered a “Hard Anti-Passback” which means that access is verified and control is done. Usually, doors (or readers) are “shared” between areas, meaning that before accessing a door, a cardholder is considered to be in a certain area (which is called “area before”) and when this cardholder passes the door, he/she is in another area (which is called “area after”).
 - **Supervisor** : Supervisor passback is more like a “controlled passback”. There are various restrictions or controls that can be programmed to use this type of passback. For example, you can indicate that at least 2 supervisors must be inside an area before anybody without a supervisor level can access the area.
 - ① **Note:** The supervisor level of a cardholder is programmed in the Card dialog.
 - **Normal and supervisor** : Both Normal and Supervisor passback types are in effect for the area.
4. Check the **Card position already valid** option if applicable. When selected, the “Card location in bad area” event will not be displayed if the user is no longer permitted in the area since his/her access level (schedule) is expired.
5. Specify the number of cards required to generate the Area open event in the **Card(s) to open area** field. This field will determine the number of valid cards required to consider this area “opened” (an area is considered “closed” or empty when all users have left the area and considered “open” when it is occupied by at least one cardholder). By default, if left to 0, as soon as one user accesses an area, if this area is empty, the system will generate an “Area Opened” event.
 - ① **Note:** If you specify more than 1 card (i.e.: 2 and up), each cardholder will have to pass their card at the reader one after the other (i.e.: the first user passes his/her card, then the second user passes his/her card).
6. If the video feature is enabled in EntraPass, the **Video view** field appears. If this is the case, select the video view in which you want the defined component to appear. For information about defining video views, see [Video Views Definition](#).
7. From the **Graphic** list, you may select the graphic to which the EntraPass applications is assigned, if applicable. For information about defining graphics, see [Graphics Definition](#).
8. Move to the **Miscellaneous** tab to setup the transfer schedules for the area being defined.
 - **Disable passback schedule** : This option sets the schedule during which the Anti-Passback verification (for all types of passback) is disabled. When this schedule is valid, passback will be disabled (not verified).
 - **Supervisor**:
 - **Supervisor level** : Enter the supervisor level required to “open” the area. This field must be used with the “supervisor to open area” field.

- **Supervisor to open area** : Enter the number of supervisors required to “open” the area, meaning that “XX” number of supervisors (having the supervisor level defined in the **supervisor level** field) must be inside the area before anybody else (having a supervisor level lower than defined) can access the area (i.e. 2 supervisors having a supervisor level “9” must be inside before any other cardholder having supervisor levels lower than “9” can access the area). You must specify the supervisor level required in the “supervisor level” field.
 - **Number of supervisor inside** : Enter the number of supervisors that must remain inside the area (having the defined supervisor level) at all time. This field is used when you need to have a supervisor inside the area at all times. When another supervisor comes in (having the defined supervisor level), then the previous supervisor can leave.
 - ① **Note:** You cannot use this field if you are using the **Supervisor must be last on exit** field. This function is disabled when set to zero.
 - **Supervisor must be last on exit** : When selected, a supervisor (having the defined supervisor level) will not be authorized to leave the area if there are any cardholders present within the area without the defined supervisor level.
 - ① **Note:** You cannot use the Number of supervisors inside field if you are using the Supervisor must be last on exit field.
9. Define the **Area transfer** parameters:
- **Area transfer schedule** : This schedule is used to move the cardholders located in an area to another area so as to avoid generating “Access denied - Passback bad location” or “Card in bad location” events. When the transfer schedule becomes valid (or invalid), you can specify an area where cards will be transferred. You can also manually modify the card location using the Manual Operation on Areas menu.
 - **Area on invalid schedule** : This area will receive all cardholders of the area being defined when the transfer schedule becomes invalid.
 - **Area on valid schedule** : This area will receive all cardholders of the area being defined when the transfer schedule becomes valid.
10. Move to the **Relay** tab to define relay activation parameters.
11. From the **Relay will be activated when area is open** field, select a relay or group of relays that will be triggered when the area is opened (Area Open Event) and will remain activated until the area is closed (Area Closed Event).
- From the **Relay activated when area is full** , select a relay or group of relays that will be triggered when the area is full (Area Full Event) and will remain activated until the area is vacated.
 - You can define the **Maximum number allowed** for the area to control the number of people inside an area. This function can be used for parking management as well to control the number of cars on the premises.
 - You can check the **Disable access when area is full** if you want to restrict access to the area when it is full. If you defined the number of entries allowed in the previous parameter, the door(s) or gate(s) will remain closed until someone leaves the area. This parameter can also be used for parking management.
- ① **Note:** For information about the **Comment** entry box, see [Comment Field](#).

Card location

About this task:

You can enable the **Card Location** feature from a graphic.

1. Right-click on an area component.
2. Click **Default double-click** and click **Locate and Move Selected Cards** to enable the feature.

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 pops up on the screen. The system displays the **Open** window. Locate the graphic you want to import and click **Open** . The graphic is then 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 are 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 becomes permanent.
 - Use the **View** menu to define how the graphic is displayed.
- ① **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 position you want. To drag an object across a window, select the object with your mouse and drag, while keeping the button pressed down, to the location in the graphic.
 2. After you have positioned the component and released the mouse button, the **Assign From** dialog displays.
 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.
- ① **Note:** If you do not assign the button to a component, the button is not saved in the graphic. Only components that were not selected in the graphic are 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.

Event Relays Definition (Global/KT-NCC Gateways)

Use this menu to associate events that will trigger relays. You can also specify that the relay be triggered only during a specific schedule and if the relay will be activated, deactivated or temporarily activated. For instance, you can define a relay to be activated when an alarm system is armed. You can for example set the relay to turn off all the lights, etc.

Events are generated for various reasons. They can be generated to report such events as:

- Unauthorized access
- Intrusion
- Defective components
- Modified components
- Guard tour status (for example that a guard has not reached the next station)

Defining Event Relays

1. From the **Definition** tab, click the **Event relay** button.
2. From the **Gateway** list, select a gateway, then select an **event** to which you want to associate a relay. System components associated with the selected event appear in the left-hand pane.
3. Select the component you want to associate with the event, then select the **relay** you want to activate when the selected event occurs.
4. For the selected relay or group of relays, choose the **Relay activation mode** :
 - **Temporarily activated** : The relay will be temporarily activated for the delay defined in the **Temporary activation timer** field of the relay definition.
 - **Activated** : The relay will activate permanently until requested otherwise by the system.
 - **Deactivated** : The relay will deactivate permanently until requested otherwise by the system.
5. Select the **Activation schedule** : The relay will ONLY be triggered when the schedule is VALID. In other words, when the event is generated and the schedule is valid, the event will trigger the relay, if the schedule is not valid, the event will not trigger the relay.

Printing Event Relay

About this task:

This menu is used to print the parameters for a specific event.

1. From the **Event relay** window, click the **Printer** button.
2. Select the **event** for which you want to print the associated parameters.

3. From the **Gateway** drop down list, select the gateway for which you want to print event relay.
4. Select components associated with the selected events: Events are usually associated with a system component, such as a door, controller, alarm partition, workstation, etc. For example, if you select the event "Input in alarm", the component selection will display all the inputs that are defined in your system. Select the input you want to print (you can select all components, use the "check mark" button).

Trigger and Alarm (previously Event Trigger)

Creating a new trigger

1. On the **Definition** toolbar, click the **Alarm and Trigger** button and click the **General** tab.
2. Click **New** and enter a name for the trigger.
3. Select a component from the **Component type** list.
4. Select between **Single component**, **Trigger group** and **All components** as a trigger source. Select between **Single component**, **Trigger group**, **All components** and **All Component selected accounts** as a trigger source.
5. Click the **three-dot** icon to select a door.
6. Click the **three-dot** icon to select a trigger schedule.
7. To use an extended filter, select the **Use extended filter** option.
8. From the **Event category selection** list, select the type of events.
9. In the **Trigger destination** section, click the **three-dot** icon to select the **SmartLink**.
10. Click the **three-dot** icon to select a task. For more information about task creation, see [Task Builder Definition](#).
11. To use a trigger value variable, select the **Use task variable** box and click the **Variable** tab. Select the variable type #1 from the list and the variable type #2 if needed..
12. On 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 **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.

- b. **Acknowledge for all connected workstations.** An acknowledge popup messages is displayed on all online and logged on workstations.
 - c. **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.
 - d. **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.
 - e. **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.
 - f. **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 separated 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).
- ① **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

About this task:

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.

You must enable the **New event operator mode** to receive the thumbnail images e-mail. EntraPass uses the task builder and alarm notifications to send the e-mails.

Floors Definition

About this task:

Use the **Floor** window to create or edit elevator floors. After the floors are created, they are grouped and associated with a schedule that defines when access is permitted.

1. On the **Definition** tab, click the **Floor** button.
2. From the **Site/Gateway/Connection** 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).

- ① **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_GE\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).
 - ① **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.
 - ① **Note:** The **Master Account** and **Accounts** buttons are available only in a **hatrix** environment. See the Accounts section for more information.
 - ① **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.

Card location

- For information on enabling the card location feature, see [Card location](#).

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 is 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 are 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 becomes permanent.
 - Use the **View** menu to define how the graphic will be displayed.
- ❶ **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.
- ❶ **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.

Guard Tour Definition (Global/KT-NCC Gateways Only)

About this task:

A guard tour consists of a number of stations or doors that must be physically verified according to a predefined schedule. The stations can either be door readers or inputs. A delay between stations can be defined; the system will generate an alarm if a station is not visited at a specified time.

- ❶ **Note:** Guard tours can only be initiated and ended by an operator's manual intervention (**Operations > Guard tours**).
1. On the **Definition** tab, click the **Guard tour** button.
 - If you want to create a new guard tour, click the **New** button in the toolbar. The **Select a gateway (Guard tour)** window opens.
 - Select the gateway where the guard tour will take place, then click **OK** to close the window.
 - In the **Guard tour** window, enter a name for the new **Guard tour** and click the **Save** button.
 - If you want to modify an existing guard tour, select it in the **Guard tour** scrolling list.

2. Select a schedule from **Notify schedule** list by clicking the **Select a component** button. If this schedule becomes valid, the system generates the “Guard tour scheduled” event and notify the operator that the guard tour must be started. The operator will then have to start the guard tour physically. He will then present his card to readers related to this specific tour or open/check doors defined in this tour.
3. Specify the **Pre-alarm delay**. After this delay, the system generates the “Guard tour alarm” event.
 - ❗ **Note:** The first late event is issued when the station-to-station time expires; for example, if the guard has 1:00 minute to reach the next station and the 1:00 minute expires, the system will generate the “Guard tour station late” event. Then, the “pre-alarm delay” will be initiated. The “Guard tour alarm” event will be generated when the pre-alarm delay expires.
4. When applicable, enter the **Time adjustment based on Gateway time zone**. For example, if the time difference is 1 hour and 30 minutes, enter 1, 5.
5. Selecting the **Automatically stop guard tour at the end** will not require the guard to manually end the guard tour when it is completed.
6. Select a **Video view**, if applicable, and select a **Graphic view** where the guard tour has been assigned.
7. Select the **Station** tab to define stations for the guard tour.
 - **#** : Indicates the guard tour steps. These must be defined in a way that it will be easy for the guard to go from a station to another. For example, the sequence should be programmed according to the order of stations to be visited.
 - **Delay**: This delay specifies the period (hh:mm:ss) to reach the next station. If this delay expires before the guard reaches the next station, the system generates the “guard tour station late” event. If the guard does not reach the station within the next delay, the system generates the “Guard tour alarm” event.
 - **Door or Input**: The station can either be defined as a door reader or an input. In the description column, select the door or input that will be used for the reporting station.
 - **Unlock door** : When selecting a door as a station, it is possible to specify if the guard must “open” the door (unlock) to complete this tour.
 - **Description**: Select the door or input according to the “door or input” column that will be used as the station for the guard.

Result



- ❗ **Note:** For more information about the **Comment** entry box, see [Comment Field](#).

Holiday Definition

About this task:

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 can be identified by a specific type (Hol 1, 2, 3, 4). The same day can be defined as a holiday at one connection, but as a regular day in another connection. Holidays can also be defined as global holidays or by Gateway.

1. On 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 list.
4. Assign a name to the holiday.

5. From the **Date** menu, select a the holiday date from the calendar.
6. Select the **Recurring** option if this is the case for the holiday you are defining.
 - ❶ **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.
 - ❶ **Note:** The legend is different from the one used to define schedules. For more information, see [Schedules Definition](#).

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) .

- ❶ **Note:** For more information, see [System Parameters Configuration](#).

EntraPass supports three groups of schedules :

- **System schedules** : System schedules for global functions such as operators login schedules and video triggers. These are not loaded in controllers.
- **Global schedules** : Global schedules are grouped by gateway. These are defined per Global Gateway. You can define 99 schedules per Global Gateway for such devices as event relays, secondary access levels, alarm systems, areas, guard tours and elevator controls.
- **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).

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 gateway if you are using a Global Gateway and 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

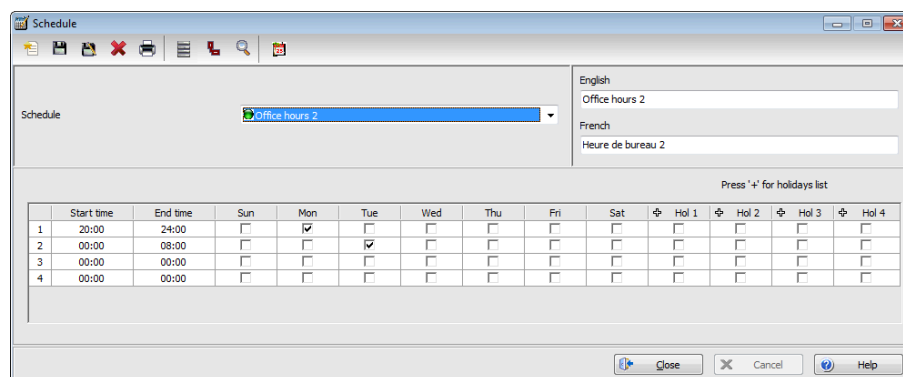
1. From the EntraPass main window, click the **Definition** tab. Then click the **Schedule** button.
 - ① **Note:** If you have checked the Upgrade to advanced schedule capability option (System parameter > Server > Schedule tab), the Gateway/Site drop-down list appears for selection. From the Gateway/site drop-down list, select a Gateway (Global site) or, select a Site (Corporate 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.
 - ① **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.
 - ① **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.
 - ① **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

About this task:

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.

- ① **Note:** Schedules with 20 intervals in stand-alone mode can be used only with KT-400 and KT-400 V1 controllers.

Task builder definition

Minimum requirements

The **Task Builder** and **Event Trigger** buttons only display if the SmartLink component is installed on a workstation and is registered with the EntraPass server.

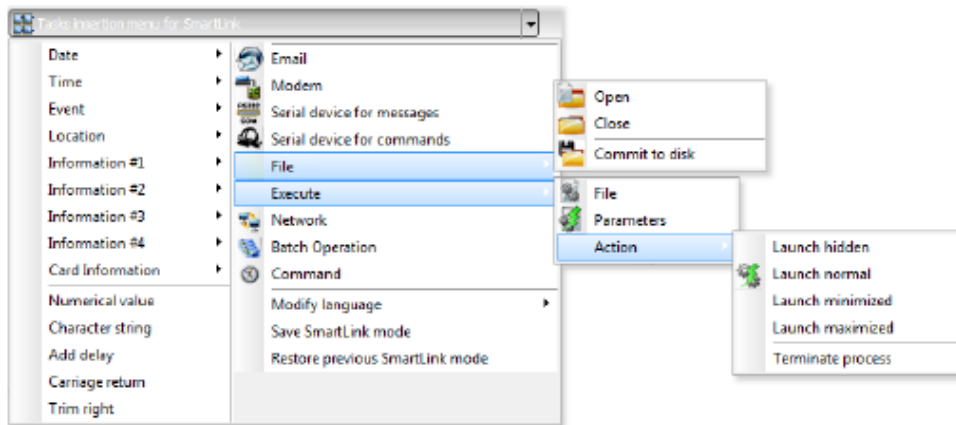
Using the task builder

1. Click the **Definition** tab, and click **Task Builder**.

Use the **Task Builder** menu to create SmartLink tasks. When you install a SmartLink application, the **Task insertion menu for SmartLink** option is activated. This allows operators to send built-in task commands to the SmartLink.

- ① **Note:** The BATCHMODIFY command in SmartLink allows batch modifications to a group of cards. You can change parameters for a group of cards of the same type. Only the data fields indicated in the command are modified.
- 2. Select **Task insertion menu for SmartLink** and a menu displays, or select the options corresponding to the most common insertions.
 - ① **Note:** When creating SmartLink tasks, only commands that are written in the primary language are considered as valid commands.

Figure 15: Task insertion menu for SmartLink



Result

See the following table of task builder parameters.

Table 27: Task builder parameters

Parameter	Description
Date	Insert a date in the task. The options are: Year, Month, Day, YYYY/MM/DD, or MM/DD/YYYY.
Time	Insert a time in the task. The options are: Hour, Minute, Second, HH:MM:SS, or HH:MM.
Event	Insert an 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. The options are: Entrapass Application, Gateway, or connection.
Information #1 to 4	Insert event information. The options in the database are: Index Number, Index Text, Component ID, and Component Text.
User Information	Insert card information in the task. The 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 of 1/10 seconds in the task.
Carriage Return	Insert a carriage return in the task.
Trim Right	Deletes the last character to the right of the task.
Email	Insert an email in the task that sends automatically when the event occurs.
Modem	Insert a message in the task that sends 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.

Table 27: Task builder parameters

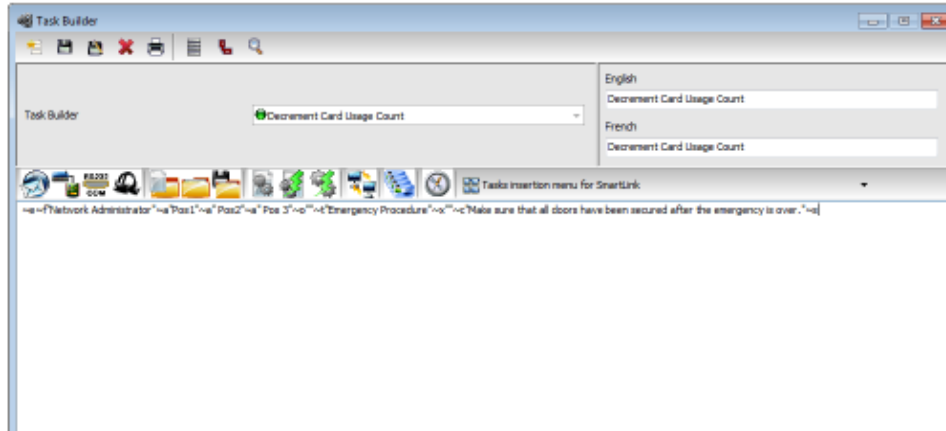
Parameter	Description
File	<ul style="list-style-type: none"> • File opens the Select a file name window that allows you to locate a file, or create a new file where all event information entered in the task is logged when an event occurs. • Close closes the file. • Commit to disk saves the file to disk. This command does not close the file.
Execute	<ul style="list-style-type: none"> • File opens the Select a file name window that allows you to locate the executable file that is used with the task command. • Parameters open the Enter Character Strings window allowing you to type a string of characters that is 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 an email. This command must always be used with Restore Previous SmartLink Mode .
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. Selected an existing task or create a new one, and click the **Mailbox** icon.
2. In the **Email Task Builder** window, in the **From...** field, enter your email address.
3. In the **To...** field, enter the recipient email addresses. Separate each email address with a semi-colon (;).
4. To send a copy of the email to other people, enter their name in the **Cc...** field.
5. In the **Subject** field, enter a subject.
6. To attach a file to the email, enter the entire path to the file in the **Attachment** field. Separate each file with a semi-colon (;).
7. In the **Text** field, enter your message. You can add variables to the email subject and body.
8. Click **OK** to attach the email to the SmartLink task. The message appears in the window.

Result

Figure 16: Task builder window displaying the attached email



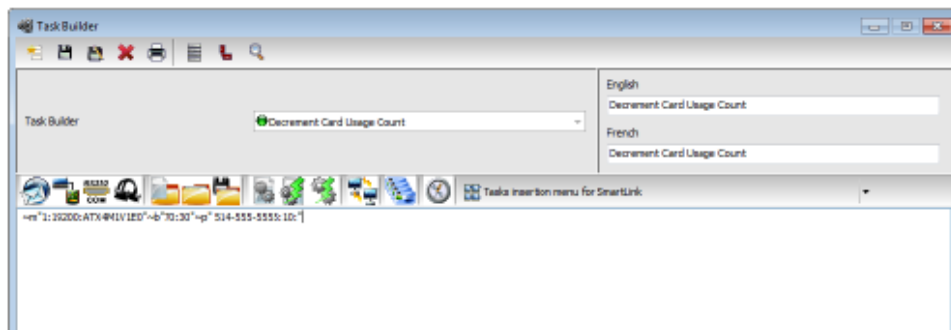
Inserting a pager command in a task

About this task:

When building a task using SmartLink, EntraPass allows you to insert a command that sends a message to a paging system.

1. Click the **Modem** icon. In the **Modem task parameters** window, the **Modem serial port** parameter is already set up.
2. In the **Dial information** fields, enter the relevant information such as the pager phone number.
3. Select the **Pager** options and enter the message that will display on the pager, if the receiving pager has the option to display.
4. In the **Delay before message (seconds)** field, enter a time. The time range value is 00:00 and 09:59 min.
5. Click **OK**. The phone number and message display in the **Task Builder** window.

Figure 17: Task builder window displaying pager message and phone number



Inserting a serial device for messages

1. From the **Task insertion menu for SmartLink** menu, select **Serial device for messages**.
2. In the **Serial com port** window, select the **Port Number** and the **Baud rate**.
3. Click **OK**.

Inserting a serial device for commands

1. From the **Task insertion menu for SmartLink** menu, select **Serial device for commands**.
2. In the **Serial com port** window, select the **Port Number** and the **Baud rate**.

3. Click **OK**.

Inserting a file

1. From the **Task insertion menu for SmartLink** menu, select **File** and **Open**.
2. In the **Select a file name** window, enter the file name or browse to find the file.
3. Click **OK**.

Executing a file

1. From the **Task insertion menu for SmartLink** menu, select **Execute** and **File**.
2. In the **Select a file name** window, enter the file name or browse to find the file.
3. Click **OK**.

Executing parameters

1. From the **Task insertion menu for SmartLink** menu, select **Execute** and **Parameters**. The **Enter character string** window displays.

Entering a network tag

1. From the **Task insertion menu for SmartLink** menu, select **Network**.
2. In the **Enter network tag** window, enter the network tag. The range value is 0 to 999,999.
3. Click **OK**.

Entering commands

1. From the **Task insertion menu for SmartLink** menu, select **Command**.
2. In the **SmartLink Task Builder** window, from the **Component type** list, select a component type.
3. From the **Command** list, select a command.
 - ① **Note:** The **toggle** command is available only with specific component types such as door, input, and relay.
4. From the **Variables list**, select a variable. There are three categories of variable that you can link to a component type and a command:
 - Message value
 - Trigger
 - Card information 1 to 10

Task building examples

The following procedures use each of the three variables that you can link to a component type and a command.

Building a task with a message value variable

1. On the **Definition** tab, click **Task Builder**.
2. Click **New** and enter `Decrement Card Usage Count` as the task name.
3. Click the **Command** button.
4. In the **SmartLink Task Builder** window, from the **Component type** list, select **Card**.
5. From the **Command** list, select **Decrement count usage**.
6. From the **Variable** list, select **Message Value**. The task displays at the bottom of the window.
7. Click **OK**. The SmartLink task now displays in the text field.
8. Click **Save** and close the **Task Builder** window.
9. On the **Definition** tab, click **Event Trigger**.

10. Click **New** and enter `Decrement Card Usage` as the event trigger name.
11. In the **Trigger source** area, from the **Component type** list, select **Door**.
12. Click the **Three dot** icon to select the component.
 - ① **Note:** You can also select a group of components or all of the components as a trigger source.
13. In the **Trigger destination** area, click the **Three dot** icon to select the **SmartLink**.
14. Click the **Three dot** icon to select **Decrement Card Usage Count** as the task.
15. On the **Events** tab, select events.
16. Click **Save** and click **Close**.

Building a task with a trigger value variable

1. On the **Definition** tab, click **Task Builder**.
2. Click **New** and enter `Trigger value` as the task name.
3. Click **Command**.
4. In the **SmartLink Task Builder** window, from the **Component type** list, select **Relay**.
5. From the **Command** list, select **Toggle relay activation**.
6. From the **Variable** list, select **Trigger variable #1**. The task displays at the bottom of the window.
7. Click **OK**. The SmartLink task now displays in the text field.
8. Click **Save** and close the **Task Builder** window.
9. On the **Definition** tab, select **Event Trigger**.
10. Click **New** and enter `Trigger value` as the event trigger name.
11. In the **Trigger source** area, from the **component type** list, select **Door**.
12. Click the **Three dot** icon to select the component.
 - ① **Note:** You can also select a group of components or all of the components as a trigger source.
13. Click the **Three dot** icon to select **Always valid** as the **Trigger schedule**.
14. Select the **Use extended filter** option.
15. In the **Trigger destination** area, click the **Three dot** icon to select the **SmartLink**.
16. Click the **Three dot** icon to select **Trigger value** as the task.
17. Select the **Use task variable** option.
18. On the **Events** tab, select the **Access granted** event.
19. Click **Save**.
20. Click the **Variable** tab.
21. Select **Relay** for both as the variable type.
22. Click the **Extended filter** tab.
23. Select **Card** as the **Filter type**, and select the component filter and both variables.
24. Repeat Step 23 for as many cards as required.
25. Click **Save** and click **Close**.

Building a task with a user information variable

1. On the **Definition** tab, click **Task Builder**.
2. Click **New** and enter `Toggle Relay via User Information` as the task name.
3. Click **Command**.
4. In the **SmartLink Task Builder** window, from the **Component type** list, select **Relay**.

5. From the **Command** list, select **Toggle relay activation**.
6. From the **Variable** list, select **User Information 1** . The task displays at the bottom of the window.
7. Click **OK**. The SmartLink task now displays in the text field.
8. Click **Save** and close the **Task Builder** window.
9. On the **Definition** tab, click **Event Trigger**.
10. Click **New** and enter `User Information` as the event trigger name.
11. In the **Trigger source** area, from the **component type** list, select **Door**.
 - ① **Note:** You can also select a group of components or all of the components as a trigger source.
12. Click the **Three dot** icon to select the component.
13. Click the **Three dot** icon to select **Always valid** as the **Trigger schedule** .
14. In the **Trigger destination** area, click the **Three dot** icon to select the SmartLink.
15. Click the **Three dot** icon to select **Toggle Relay via User Information** as the task.
16. On the **Events** tab, select the **Access granted** event.
 - ① **Note:** Make sure to enter the user information correctly. To see an example, click the **Users** tab, click **Card** and click the **General** tab. Number 1505 is the RELAYID of the relay that will toggle when the task is performed.
17. Click **Save** and close the window.

Groups

To apply an operation to a group of controllers or components instead of individually, use this section. You can use the [Controller group creation](#), [Door group creation](#), [Relay group creation](#), [Access level groups grouping](#), to group a number of controllers, doors, relays, or access levels of the same connection. Use the [Input group creation](#), to group inputs of a controller connection.

You can use [Floor group creation](#) for operations including unlocking schedules and access levels. Use [Trigger group creation](#) to configure trigger elements from a group of sub-components.

Use [Area group creation](#) to monitor specific areas for muster reporting.

Access level groups grouping

About this task:

The Access level group dialog is used to group access levels of the same connection.

1. In the **Group** window, click the **Access level group** button.
2. Click the **View hierarchy** button to display all the sites defined in the system.
3. From the **Gateway/connection** 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. Select the check boxes that correspond to the access level group.

Area group creation

About this task:

Area groups are used to monitor specific areas for muster reporting. Areas must be configured in the Area dialog located under the **Definition** tab, before they can be grouped together.

1. On the **Groups** tab, click the **Area group** button to open the **Area group** window.
2. Click the **View hierarchy** button to display all the gateways defined in the system, and then from the **Gateway** list, select the gateway from which you want to group the areas.
3. From the **Area group** 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 areas, select the boxes corresponding to the areas you want as part of the area group.
5. Click the **Save** button

Trigger group creation

About this task:

Trigger groups are used to configure triggering elements from a group of sub-components.

1. On the **Groups** tab, click the **Trigger group** button to open the **Trigger group** dialog.
2. From the **Trigger group** 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** list, select a component. Select the boxes corresponding to the sub-components you want as part of the trigger group.
4. Click the **Save** button.

Controller group creation

About this task:

Use the Controller group menu to group a number of controllers of the same connection.

1. In the Groups window, click the **Controller** button.
2. Click the **View hierarchy** button to display all the sites defined in the system.
3. From the **Gateway/connection** 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** list, and enter the necessary information in the language section.
5. From the list of controllers connected to the selected connection, select the controllers that are to be assigned to the group.

① **Note:** For more information about controllers, see [Controllers Configuration](#).

Door group creation

About this task:

Use the Door group menu 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. In the **Groups** window, select the **Door** button.
2. Click the **View hierarchy** button to display all the sites defined in the system.
3. From the **Gateway/connection** list, select the connection or gateway from which you want to group doors.
4. From the **Door Group** 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.

① **Note:** For more information about doors, see [Doors Configuration](#).

Floor group creation

About this task:

Use this menu 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) and access levels.

1. On the **Groups** tab, click the **Floor Group** button.
2. Click the **View hierarchy** button to display all the sites defined in the system, and from the **Gateway/connection** list, select the connection or gateway from which you want to group the floors.
3. From the **Floor group** 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, select 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
 - 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 the system scans the schedule column of that group and unlock each floor accordingly. For more information, see [Defining Elevator Doors](#).
 - 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).

Input group creation

About this task:

Use the input group menu 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. In the **Groups** window, click the **Input** button.
2. Click the **View hierarchy** button to display all the sites defined in the system.
3. From the **Gateway/connection** list, select the connection for which you want to group inputs.
4. From the **Inputs group** list, select an existing group to modify it, or click the **New** button to create a new group, and 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 about inputs, see [Input Configuration](#).

Relay group creation

About this task:

Use the Relay group menu 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. In the **Groups** window, click the **Relay** button.
2. Click the **View hierarchy** button to display all the sites defined in the system.
3. From the **Gateway/connection** list, select the connection or gateway from which you want to group relays.
4. From the **Relay group** list, select a relay group or click the **New** button to create a new group, and 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 about relays, see [Relay Configuration](#).

Devices

Use this section to configure EntraPass applications, components, doors, the KTES, and integration panels and components.

You can use [Application Configuration](#) to configure the minimum applications to implement EntraPass. Included in this are procedures to define the general parameters, security parameters, message controls, and alarm control filters. How to configuring a Mirror Database, Redundant Server, SmartLink application, and Video Vault are also included.

Use EntraPass gateways configuration to configure a Multi-site Gateway, Global Gateway, a Redundant Gateway, and a KT-NCC Gateway. The site configuration describes how to configure together controllers communicating over IP to create a virtual site.

Use the [Connection configuration](#) to determine which connection type is suitable for your gateway and how to configure it, how to migrate your KT-1 Standalone backup data to an EntraPass Server, and where to find the KT-1 or KT-2 controller unassigned controller list. The setting up communication timing section explains why you should not alter the system's communication timings.

Use [Configuring controllers](#) to configure any of the Kantech door controllers: KT-100, KT-200, KT-300, KT-400, KT-1, and KT-2. You can define an ioModule, and find a list of modules communicating with a controller but unassigned, and find a list of readers and their compatible controllers. You will also find instructions for configuring general parameters, changing controller types, configuring specific controller parameters and wireless doors. Additional configuration options include anti-passback, duress function, card count, and supervision functions. Depending on the controller type, find out how to configure the controller for use as an elevator, and configuring expansion modules.

To configure the Kantech Telephone Entry System (KTES) see the [Kantech Telephone Entry System \(KTES\) Configuration](#) section. This system is a standalone system, or for larger installations, integrates with EntraPass.

Use [Configuring doors](#) to define general parameters for a door, door keypad options, door contact options, and Request to Exit (REX) options. Find out how to define card multi-swipe, double/triple swipe actions, interlock options, elevator doors, and interlock options (mantrap). Find procedures to describe how to define a door depending on your connection or gateway.

To activate alarms, control lighting, ventilation, and HVAC systems, use [Relay configuration](#).

You can use [Input configuration](#) to define inputs. Door controllers monitor the state of input points, and the number of inputs available depends on the type of controller. To control reader LEDs and buzzer, use [Output device configuration](#).

If you want to share the configuration of an ioSmart reader follow the procedure in [Reader Templates](#). EntraPass integrates with intrusion and fire panels; use the [Integrated panel configuration](#) section to define these. If a [Trigger and alarm tab](#) is available for an application or component, you can define an alarm for an event and an associated trigger, see [Creating a new trigger](#) in the definition section.

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 Global Gateway 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 is a workstation-type application, tabs such as Workstation, Gateway and site, are displayed. If the selected application is a Redundant server, the Redundant server tab appears.
2. From the **Application** 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.
3. The **Dual Gateways** option under the **Global Gateway under Windows** application allows you to simultaneously run a Global and a multi-site Gateway on the same computer. This option adds only one multi-site Gateway and does not require any additional license.
4. 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.
5. Click the **Save** button to activate the new application.

Defining General Parameters

About this task:

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 information about 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 information about 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:
 - b. In the Status window, select the Application button.
 - c. From the root tree menu, right-click the Mirror Database.
 - d. 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

About this task:

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:** If 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.
 - ① **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.

Account Linked

The **Account Linked** tab allows you to link one or more accounts to a workstation. This way, only the accounts linked to the workstation can be used to log in. In an **hatrix** environment:

- Only the events and the components related to that workstation are displayed.
- If no user is logged in the workstation:
 - No event is received or delayed.
 - No alarm is received or delayed.
- The events log is erased each time a user logs out or quits.
- The alarms log is erased each time a user logs out or quits.
- The global alarms are deactivated for this workstation.

From the Application menu, click the **Linked Account Manager and Account:**

- **Use specific account for login and messages:** Check this option to allow only the users of the selected accounts to log on the workstation.
- **Process message according to the user login:** If you check this option, only the events coming from the selected accounts will be displayed on the workstation.

- ① **Note:** The Linked Account Manager and Account tab is only available when the **hatrix** component has been previously registered from the EntraPass Server. It is however not available when Server Workstation is selected from the EntraPass application drop-down list. This option must be properly configured in order to allow the account operator and the account manager to log in to the workstation.

SQL database access

External applications can request information from the EntraPass SQL database.

- ① **Note:** SQL database access must be installed like any other EntraPass application.

Go to **Devices/Application/Database Access**, and enter the **User name** and the **Password** (for Sybase Adssys user only).

- ① **Note:** For more information about the operator parameters to configure, see [Creating or editing an operator](#).

Defining workspaces

- ① **Note:** The Defining Workspaces option is only available when the [Event Operator](#) mode has been enabled.

The **Workspace** tab allows you to select which workspace configuration and event parameters will be applied on a specific workstation therefore making EntraPass geographically relevant. This feature provides the ability to define workstation behaviour.

- **Apply workstation workspace and event parameters:** When checked this enables the workstation workspace definition for event messages display.
 - ① **Note:** Only applies when event parameter is on. Not available in event operator mode.
 - **When logged out :** Applies the selected workspace rules when the no one is logged on the workstation.
 - **When logged in :** Applies the selected workspace rules when an operator is logged in, overriding the operator's workspace definition.
 - **When shutdown :** Will apply the selected workspace rules when the workstation is shutdown.
- **Apply operator workspace to filter messages :** When operator logs on, the workstation applies the operator workspace rules.
- The **Process when both workspaces are selected** section lists the options available when both **Apply workstation workspace and event parameters** and **Apply operator workspace to filter messages** boxes are checked.
 - **Workstation workspace AND Operator workspace :** Events are filtered according to the EntraPass workstation workspace configuration, and filtered again according to the workspace configuration of the operator who is currently logged on the EntraPass workstation.
 - **Workstation workspace OR Operator workspace :** Selects the workspace that has a higher level in the hierarchy.
 - **Operator workspace ONLY :** The operator workspace has priority over the workstation workspace.

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 .

- ① **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.

① **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.).

① **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.

① **Note:** When the **Acknowledge Priority Level** checkbox is selected, the alarm acknowledgement priority level is based on the workstation. The slider is used to modulate the priority level from “Never” to “Always” be the first to acknowledge (see [Alarm Management](#) for more details).

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 desktop**.

❗ **Note:** For more information on EntraPass desktops, see [Alarms Desktop](#).

Configuring an Oracle/MS-SQL Interface (CardGateway)

About this task:

The Oracle/MS-SQL Interface creates a real-time mirror copy of the EntraPass card databases, including 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. Install client 32 bits.

Install the MS-SQL or Oracle client software 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, define the following items:

- 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** list, select **Oracle/MS-SQL Interface**.
 2. Define the application on which you have installed the Oracle/MS-SQL Interface.
 3. Click the **Parameters** tab to define security parameters for the Oracle/MS-SQL Interface. For details, see [Defining Parameters](#).
 4. Click 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** list, select the database server: Oracle 8.0 server, Oracle 7.3 server or SQL server. Ensure that you select the correct server version because the database configuration is different from one version to another.
 - ❗ **Note:** If the wrong version is selected, the Oracle/MS-SQL Interface cannot communicate and cannot 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. Select 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 muster report needs to be printed.
 - Select **Login to EntraPass service application** to activate this option.
 - Enter the Oracle/MS-SQL Interface **Domain name** and **Login name**.
 - Type 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

To integrate Oracle/MS-SQL with EntraPass, create a database.

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

Creating a Kantech operator for an MS-SQL Server

Create an operator for the Oracle/MS-SQL interface to log on to the MS-SQL server.

1. Right-click **Logins** and select **New Login**.
2. In the **Name** field, enter a new name for the operator. The name must be lowercase and cannot contain spaces or special characters.
3. Select **SQL Server Authentication**.
4. In the **Password** field, enter a new password. Create a strong password.
5. Click the **Database Access** tab.
6. Select the name of the database that you created in Step 2. When you select this option, the bottom part of the window displays the following message: **Database Roles - Permit in database role**.
7. To modify the database, select the **Public and db_owner** options and click **OK** to save and exit. You are prompted to confirm the password.
8. Enter the new password and click **OK**.

Creating a Kantech operator for an Oracle Server

1. Log on to the Oracle server as an administrator. Enter a new name for the operator. The name must be lowercase and cannot contain spaces or special characters. Alternatively, use the name you created in [Creating a Kantech operator for an MS-SQL Server](#).
2. Create a database. You can use the default database name **KanCard**.
3. To create a logon profile, use the new operator name and enter a new password. Create a strong password.
4. Assign the kantech operator the permission **Owner**.

Configuring the mirror database and redundant server

About this task:

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.
- Restore parameters.
- Security parameters.
- KT-NCC 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 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.
 - ① **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.
 - ① **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. Move to the **KT-NCC** tab to define a public IP address for the KT-NCC, when applicable.
 - If you want to activate the **Inbound Server Router** address, check the box.
 - You may enter the **Public IP address** or the **Domain name**.
12. Click the **Async updates** tab to define the mirror database synchronization settings. These settings 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**).
 - ① **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**.
13. 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**.

Result

- ① **Note:** For more information about the **Comment** field, see [Comment Field](#).

Configuring the SmartLink application

About this task:

Use the SmartLink application to interface the EntraPass access control software with any intelligent device, for example, video matrix switchers, paging systems, and email applications, using an RS-232 connection between one of the EntraPass workstations and the external device. You can integrate with other systems through software DLLs. Use SmartLink 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.

① **Note:** You do not require an additional license to use the SmartLink feature.

1. From the **Application** list, select **SmartLink**.
2. Define the workstation on which you have installed the SmartLink interface. For more information, see [Defining General Parameters](#).
3. Configure the SmartLink workstation security parameters. For more information, see [Defining Parameters](#).
4. Configure the SmartLink workstation messages. For more information, see [Defining Message Controls](#).
5. Configure the SmartLink workstation email reports.
6. To view and set up the SmartLink connection parameters, click the **SmartLink** tab.
7. From the **Mode enabled** list in the **SmartLink serial connection** section and the **SmartLink network connection** section, select the appropriate mode of transmission:
 - **Messages only:** SmartLink only receives messages.
 - **Commands only:** SmartLink only executes commands (tasks).
 - **Messages and commands:** SmartLink receives messages and execute commands.

① **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 starts to allow a client application to connect to the SmartLink application, either to execute commands or to receive messages sent through the network, or to perform both processes simultaneously.
8. In the **SmartLink tasks** section, you can define **Start up** or **Default** tasks. The tasks you assign are processed automatically when the **SmartLink** application starts. For more information about defining SmartLink tasks, see [Task Builder Definition](#).
9. Click the **SmartLink E-mail** tab to view and set up the SmartLink connection parameters.
10. In the **Email server (SMTP or Exchange server)** field, enter the IP address of the email server to use for sending emails.
11. In the **Email Port** field, enter the number of the port to use for sending emails. This is usually 25.
12. Select the encryption method:
 - Unsecured (No SSL/TLS)
 - Gmail (SSL/TLS)
 - Secured (SSL/TLS)
 - Office 365 (STARTTLS)
13. In the **Email sender** field, enter a valid email address. This email address is used to authenticate the email server.
14. In the **Authentication** area, choose an authentication method.
 - **No authentication:** no authentication is 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. In the **User name** field, enter a user name for the authentication process.
 16. In the **Password** field, enter a password. EntraPass supports SMTP connection passwords with a maximum length of 64 characters.
 17. In the **E-mail server (POP3)** field, enter the POP3 server address for a POP3 authentication.
 18. In the **E-mail port (POP3)** field, enter the POP3 port number for a POP3 authentication.
 19. In the **Delete e-mail(s) when maximum reached** field, enter the number of emails that are kept in the buffer when the feature is active. The maximum number of emails is 9999. The minimum and default number of emails is 1000.
 20. In the **Delete e-mail(s) when older than (hh:mm)** field, enter the amount of time emails are kept in the buffer when the feature is active. The maximum amount of time emails are kept is 24:00. The minimum time is 02:00 and the default time is 05:00.
 21. In the **Send to** field, enter the recipient's email address.
 22. Click the **Test** button to send a test message using the selected parameters. Depending on the test results, different error or success messages display.
 - ❗ **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 the email server settings, contact the network administrator.
 23. To define the EntraPass web parameters, click the **Web Service** tab, and complete the following steps:
 - a. Select the **Use Web Service** check box.
 - b. In the **Connection name** field, enter a name for the connection.
 - c. In the **Web Service Name** field, enter the name of the web service.
 - d. Choose one of the following communication options:
 - Click **IP address**, and enter the IP address of the SmartLink.
 - Click **Domain name**, and enter the domain name.
 - **Optional:** To test the connection, click **Test DNS**.
 - e. In the **Web Service Port** field, enter the port number.
 - f. From the **Web Service Protocol** list, select a protocol. HTTPS is selected by default. If you select **http**, the following warning message appears: **Using a non-HTTPS protocol will make your system less secure. Are you sure?** Click **Yes** to change the protocol to HTTP.
 - ❗ **Note:** To use HTTPS protocol, you require an SSL certificate. For more information, see Step 2 in the [Security hardening guide](#).
 - g. In the **EntraPass web link for welcome email** field, view and edit the EntraPass web link.
 - 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
 - Include go Pass link

24. In the **Connection timeout on idle (mm:ss)** field, enter a timeout time. After the connection timeout time, the operator must log on again to continue. All changes made after the last save are lost. The default connection timeout is 5:00 min. The timeout range is 00:30 to 20:00 min.
 - ❗ **Note:** If you update the EntraPass system, the connection timeout does not modify automatically. Make sure to check its value.
25. Click the **Service** tab to define logon information when the SmartLink server runs as a service and a report needs to be printed.
 - To activate this option, select the **Login to EntraPass service application** check box.
 - In the **Domain name** and **Login name** fields, enter the SmartLink domain and logon names.
 - In the **Password** and **Password confirmation** fields, enter a password.
 - ❗ **Note:** For more information about the **Comment** field, see [Comment field](#).

Configuring the EntraPass Video Vault Application

About this task:

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 run 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 \(KAP\)](#) 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](#).

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:** We do not recommend using a video vault and video server gateway at the same time. If you select the **Use as a Video Server Gateway** check box, all new exacq video server connections connect to any available video vault.
 - 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 required 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:** This configuration is mandatory.

The **Connected Video Servers** field displays the amount of video servers reporting to the 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.
 - ① **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.
 - ① **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.
 - ① **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.
 - ① **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**.

Result

① **Note:** For more details about the **Comment** entry box, see [Comment Field](#).

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.
 - ① **Note:** If you do not see the **Swap** button, you need to enable the second language option in **Options>Select language**.
3. Click **OK** to keep your changes or **Cancel** to return.

Comment field

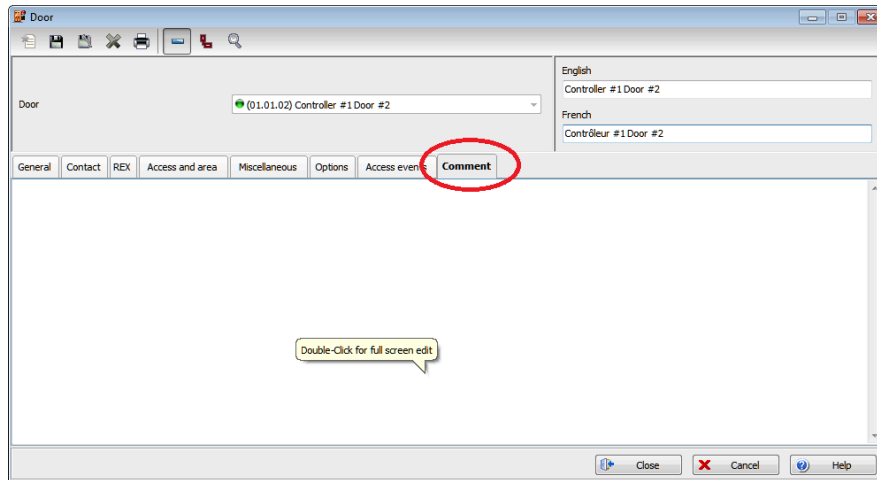
Enter, modify, or delete text in the comment field at any time. There is no character limit. The following table lists the components that include a comment field.

Table 28: Components including a comment field

EntraPass application	Controller	Area
Active Directory	Door	Alarm system
Gateway	Relay	Guard tour
Site	Input	
Connection	Output	

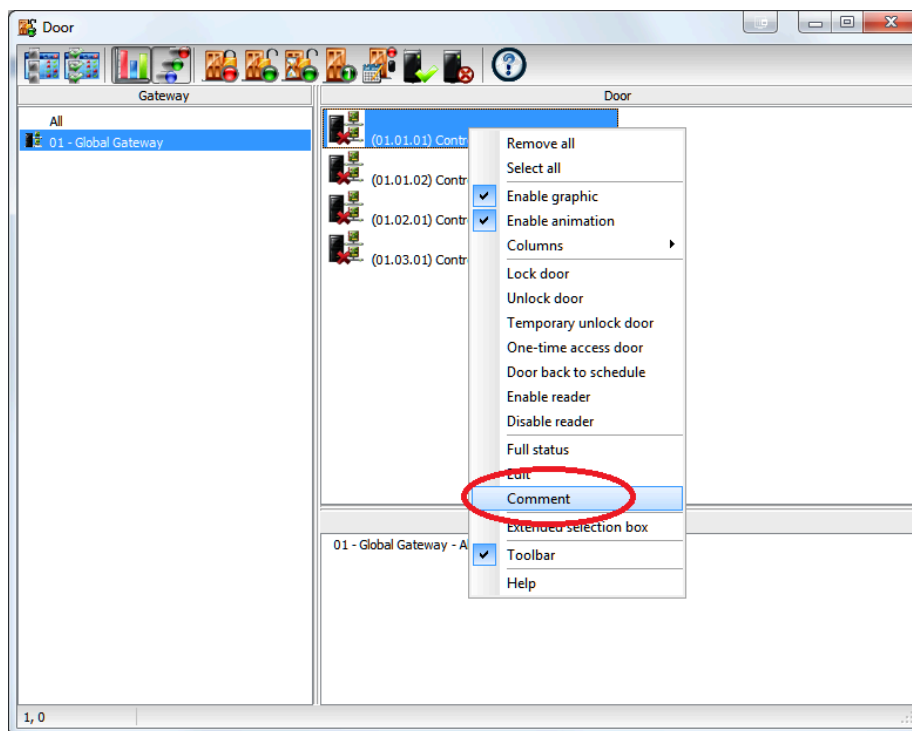
To enter text in the comment field, in the component window, click the **Comment** tab. Double-click in the field to activate edit mode.

Figure 18: Comment field in the door window



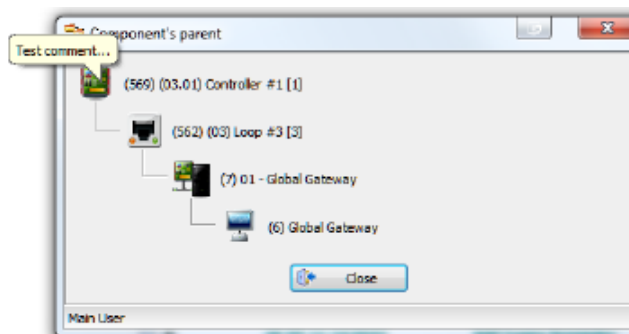
You can view comments in the **Operation** window. Right-click a component and select **Comment**, as the following figure shows.

Figure 19: Accessing comments in the operation window



You can also view comments in the messages list or in the graphic area. Right-click a component and select **View parent/controller**. In the **Component's parent** window, hover over the controller to view the associated comment.

Figure 20: Viewing comments in the component's parent window



Trigger and alarm tab

The trigger and alarm 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
Event	The name of the event. For example "Door locked by an operator". ① Note: This heading is only available when Event Operator mode has been enabled.
Trigger description	The name of the trigger. This is given when the 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 is listed here.

To view, add, edit, or delete a trigger, select a trigger from the list and right-click to open the menu. Deleting a trigger only removes the trigger, it does not remove the application or selected event from the trigger.

Connection configuration

About this task:

A connection is composed of controllers attached to the same communication port. The system can manage up to 32 connections per multi-site Gateway, 3 physical connections per KT-NCC Gateway, and 32 connections per Global Gateway. EntraPass also allows users to add up to 2048

connections per multi-site Gateway. Corporate and Global Gateway connections are composed of KT-100, KT-200, KT-300, KT-400, KT-1, and KT-2 controllers. It is not recommended to use KT-100, KT-200, KT-300, KT-400, KT-1, and KT-2 controllers in the same loop.

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), Secure IP (KT-2), Ethernet (polling) and Dial-Up (RS-232) modem. See the following table for the connection types and the gateways.

Table 29: Connection types and gateways

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-2)	Yes	Yes	Yes
Secure IP (KT-1)	Yes	Yes	Yes
Secure IP (KT-400)	Yes	Yes	Yes
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 to 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 list.
3. Select the **Gateway**.
4. From the **Connection** 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.

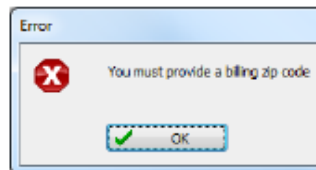
Note: Under Global and KT-NCC gateways, connections are predefined via the gateway.

Note: The **Billing Zip or Postal Code** option is only available when the **hatrix** component has been previously registered at the EntraPass Server. See the Accounts section for more information on the hatrix feature.

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 for each connection. If the number specified is greater than the maximum allowed, the system will set the value to 32.

- ① **Note:** When the connection type is **IP address (KTES)**, the number of KTES is automatically limited to a single KTES per connection.
- Select a **Time zone**: This setting allows events from the remote site to display at local gateway time on EntraPass workstations located in different time zones.
- Enter the **Billing Zip** or **Postal Code**. This field is mandatory. Otherwise, the following warning message displays:

Result



- Select a **Graphic** and **Video view** to which the gateway is assigned, if applicable. The video view is activated only if the video feature is enabled in EntraPass.
- Use the scroll list to select the **Connection type between the computer and the gateway**. This determines which tabs display for the 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 Global Edition for Global and multi-site Gateways, and KT-NCCs to communicate by a RS-232 gateway.

When selecting the **Direct RS-232 connection type** option in the **General** tab, a **RS-232** tab becomes 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

About this task:

Configure this type of connection in a multi-site Gateway with EntraPass Global Edition to communicate using a Kantech IP Link, a KT-400, a KT-1, a KT-2, or a KTES.

- ① **Note:** For more information about configuring the Kantech IP Link, refer to the *Kantech IP Link Installation Guide*, DN1670. For more information about the KT-400, refer to the *KT-400 Ethernet Four-Door Controller Installation Guide*, DN2003. For more information about the KT-1, refer to the *KT-1 One-Door Controller Installation Guide*, DN2186.

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 more information about the KTES, see the *KTES Installation Manual*, DN1769.

1. From the **Connection** list, select a connection type. If you select one of the following devices: **KT-400**, **KT-1**, **KT-2**, **IP Link**, or **KTES**, the following three tabs become available:
 - **IP Device IP configuration**
 - **IP Device Automated Connection**
 - **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:** Select this option when configuring the device with a **Reserved DHCP IP** address.
 - **Use the following IP Address:** Select this option when you want to assign a static IP address to the device. When selected, the following three parameters become available.
 - **IP Address:** The static IP address is provided by the System Administrator.
 - **Subnet Mask:** This address is provided by the System Administrator.
 - **Gateway (Router):** This address is provided by the System Administrator.
 - **DNS server address:** This address is provided by the System Administrator (for Kantech IP Link, KT-400, KT-1, and KT-2 only).
 - **Protocol:** Used to specify the communication protocol, UDP or TCP.
 - **Port:**
 - **For TCP:** 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 on a **WAN**.
 - ① **Note:** Use port 18802 with KT-400, KTES, KT-1, KT-2, and IP Link.
 - The **multi-site Gateway IP address** is 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.
 - ① **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:** Enter the gateway computer IP address.
 - **Domain name:** If you do not have the gateway IP address, you can enter the domain name provided by the System Administrator (for Kantech IP Link, KTES, KT-400, KT-1, and KT-2 only) .
 - ① **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, KT-2, and KT-400 only) .
 - **Test DNS:** After you enter the domain name, click the **Test DNS** button to display the corresponding IP address (for Kantech IP Link, KTES, KT-1, KT-2, 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:** type a 16-digit hexadecimal code to encrypt 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 EntraPass Global Edition for Global and multi-site Gateways, and KT-NCCs to communicate with the gateway by the network (Lantronix). with the gateway by the network (Lantronix).

When selecting the **Ethernet (Polling)** option in the **General** tab, an **IP device** tab becomes available.

- Enter the terminal server **IP address** and **Portnumber**.
- 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

About this task:

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

① **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.

① **Note:** The **Remote Baud rate** must not be changed. If you are uncertain about modem setup parameters, consult your network administrator for the settings that apply to your particular hardware configuration.

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

① **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 defines 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 is allowed to answer on one ring.
 - Set the **Number of retries**. This sets the number of calls the modem attempts 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 priority call type** and **Report events automatically**.
 - Define the delay before the system will **Fail to report after (mm:ss)**.

① **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**. The 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 want 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.
- ① **Note:** Do not click the **Remote modem delays** button. All values are factory-set for optimum performances with the supported US Robotics modems. Settings **MUST NOT** be edited unless recommended by Kantech.

Result

- ① **Note:** For more details about the **Comment** entry box, see [Comment Field](#).

Migrating KT-Standalone backup data to an EntraPass server

About this task:


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

- ① **Note:** The following features are not included in the migration.

- Time zone
- Alarm panel integration
- Multi-swipe settings on exit door.

Table 30: Import KT-Standalone icon

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. Click the **Options** tab, and click **Display Format**.
2. 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.

① **Note:** If card #1 and card #2 use a different display format, EntraPass migrates to card #4 or card #5.
3. In the **Global Card Format** area, choose the appropriate global card format.
4. 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, click **Connection**.

2. Click the **KT-Standalone** icon on toolbar 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: the **Card #1** format to match the **Card #1** format in the standalone controller, repeat for card #2 to card #5.
 - a. Backup date and time
 - b. Controller type
 - c. Controller type
 - d. Controller MAC/Serial number
 - e. Controller firmware version
 - f. Amount of schedules
 - g. Amount of holidays
 - h. Amount of action scheduler
 - i. Amount of doors
 - j. Amount of relays
 - k. Amount of input
4. A window displays 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.

Configuring controllers

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 the following controllers: KT-100, KT-200, KT-300, KT-400, KT-1, and KT-2. 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.

Table 31: Kantech controller components

Type	Doors	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	8	2	5	5
KT-2	2	8	2	8	5

 **Note:** Corporate and Global Gateways support all Kantech products (KT-100, KT-200, KT-300, KT-1, KT-2, and KT-400). Under Global, KT-200 must be used with EP-Entra3 EPROMs.

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. Click the **Devices** tab, click **Controller**, and, from the **Site filter** list, select a site filter.
2. Select the **Gateway**. For information about configuring a gateway, see [Gateway Configuration](#).
3. From the **Connection** list, select the connection where the controller is located. For more information about configuring a connection, see [Connection Configuration](#).
4. From the **Controller** 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** 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, and click the **Save** icon. After you save, the **Controller type** list is disabled.
 - The system prompts you to use the **Express Setup program**. Click **Yes** to continue. If you click **No**, you must manually configure these devices in their respective definition menus (doors, relays, inputs and auxiliary outputs).
6. Select the reader installed on your controller from the **Reader type** lists. Check [Table 32](#) for the reader types and the controller types.


- ① **Note:** The  icon allows you to install a custom driver for a specific controller. Use this icon to add the driver in the Reader+ Driver table, making it available the next time you want to configure a new controller.

Table 32: Reader types

Reader Types	KT-100	KT-200	KT-300	KT-400/ KT-1/KT-2
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	

Table 32: Reader types

Reader Types	KT-100	KT-200	KT-300	KT-400/ KT-1/KT-2
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	
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 Security 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
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	
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

Table 32: Reader types

Reader Types	KT-100	KT-200	KT-300	KT-400/ KT-1/KT-2
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** list. Check [Table 33](#) for the keypad types and the controller types.

Table 33: Keypad types

Keypad Types	KT-100	KT-200	KT-300	KT-400/ KT-1/KT-2
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 is never polled and all status requests from this specific controller send a message that this controller is disabled.
 - ① **Note:** This option can be used when a controller is removed temporarily but must not be deleted. For example, if the controller is under repair. It also allows operators to easily set up the software before the physical installation is completed.
9. Select the **Vital LED** mode (for KT-1 and KT-2 only). For more information, refer to the *KT-1 Installation Guide* or to the *KT-2 Installation Guide*.
10. Select between **On demand** and **Always on** for the **Status LED (for KT-1 or KT-2 only)**. For more information, refer to the *KT-1 Installation Guide* or to the *KT-2 Installation Guide*.
11. Select a **Graphic** and **Video view** to which the gateway is assigned, if applicable. The video view is activated only if the video feature is enabled in EntraPass.

Changing controller type

About this task:

Controller types can be updated to newer controllers without resetting the controller configuration. To change the controller type, complete the following steps:

1. Click the **Devices** tab, click **Controller**, and, from the **Controller** list, select a controller.
2. Select a new controller type from the **KT controller type** list.
3. Click the **Save** icon. A warning message asks if you want to continue. Click **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.

- Click **OK** to complete the process.
- During the process, the option **Disable controller polling** is automatically selected. Ensure that this option is cleared.

Result

This function only supports updating controllers to newer controllers. The rules for updating controller types are summarized in the following table.

Table 34: Updating controller types

Original controller type	Supported update controller types
KT-100	KT-300, KT-1, KT-2, KT-400
KT-200	KT-300, KT-2, KT-400
KT-300	KT-2, KT-400
KT-1	KT-2, KT-400
KT-2	KT-400

Note: When converting from a KT-100 or a KT-1 to a KT-400, exit readers are converted to a second door.

It is not possible to change the controller type if a KT-IP has been used.


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

- Click the **Controller** tab (KT-100, KT-200, KT-300, KT-400 or KT-1/KT-2) from the **Controller** window.
- 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.
- For KT-400 only:
 - To configure SPI modules, see [Expansion Modules Setup](#).
 - To configure the elevator floor associations, see [Defining the KT-400 Elevator Floor Associations](#).
 - To configure OSDP, see [Configuring an OSDP reader to a KT-400 or KT-4 controller](#).
- For KT-300 only:
 - To configure Combus Modules, see [KT-300 Combus Modules](#).
 - To configure the elevator floor associations, see [Defining the KT-300 Elevator Floor Associations](#).
- For KT-200 only:
 - To configure KT-200 Auxiliary devices, see [Configuring KT-200 Auxiliary Devices](#).
 - To define REB-8 relays, see [Defining REB-8 Relays](#).
 - To configure REB-8 elevator controllers, see [Programming REB-8 Elevator Controllers](#).
 - To configure KT-2252 elevator controllers, see [Programming KT-2252 Elevator Controllers](#).
- 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)

Click the **Status relay** tab to program a relay or group of relays that activates 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

① **Note:** Before you begin, install the **Licensed Door** feature. For more information, see [System Registration](#).

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, complete the following steps:

1. Click **Devices**, click **Controller**, and select the controller you want to configure. If the controller supports licensed wireless doors the **Licensed door** icon is available on the **Controller** window toolbar.
2. Click the **Licensed doors** icon.
3. If no integrated panel has previously been linked to that controller, EntraPass automatically creates a new integrated panel.
4. Click **Configuration** to open the **Licensed Doors** window. The number of **Purchased** licences and **Available** (remaining) licenses is displayed.
5. To add a door, click +.
6. 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)*.
7. Select the correct box to indicate whether the door has a **contact** (to indicate open or close) or a **REX** (Request To Exit) functionality.
8. To delete a door, click **Delete** and click **OK**.
9. If an integration panel has previously been linked to the selected controller, the **Licensed Doors** window displays, and you can edit existing wireless doors.
10. To view the status of the wireless lock, select the wireless lock from the **Operation/Integrated Panel**. The icon signifies if the device is operational. To view details, double-click on the device. The possible states are listed in the table.

Table 35: Device states

Parameter	Possible States
Door Number	
Tamper	<ul style="list-style-type: none"> • Tamper in alarm • Tamper in normal condition • [Unknown State: NOTHING DISPLAYED]
Device communication status	<ul style="list-style-type: none"> • Device Online, as per Hub Status • Device Offline, as per Hub Status • [Unknown State: NOTHING DISPLAYED]
Door side	<ul style="list-style-type: none"> • Door side: Inside • Door side: Outside • Door side: Both inside and outside • [Unknown State: NOTHING DISPLAYED]
Handle State	<ul style="list-style-type: none"> • Handle not used • Handle used • [Unknown State: NOTHING DISPLAYED]
Key Cylinder State	<ul style="list-style-type: none"> • Key cylinder not used • Key cylinder used • Key cylinder is in Specific position: 1 (or 2 or 3) • [Unknown State: NOTHING DISPLAYED]
Lock State	<ul style="list-style-type: none"> • Door unlocked • Door locked • Door lock secured • Door lock jammed • [Unknown State: NOTHING DISPLAYED]
Door State	<ul style="list-style-type: none"> • Door opened • Door closed • [Unknown State: NOTHING DISPLAYED]
Protocol version	
Version Number	
Vendor ID	
Mac Address	
Hub Mac Address	
On abnormal behaviour	<ul style="list-style-type: none"> • 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 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 loses power it will not retain the last status of its 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 its 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 the lock. When the dead bolt is engaged the lock state becomes unknown.
- Currently only 26-bit drivers are supported for wireless locks.

① **Note:** If you go to **Devices>Integrated Panel>Print**, you can see the number of licensed doors associated with that integrated panel.

Currently, wireless licensed doors are only supported for KT-1 and KT-400 controllers.

Defining controller options

About this task:


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.

① **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.

① **Note:** For added security, you may select both options. The duress option is available on both Corporate and Global Gateways. 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 (see [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.
 - ① **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.
 - ① **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).
- ① **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-8s 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-2252s can be connected to the controller.
 - Check the **REB-8 ElevatorController** option if REB-8 are used for elevator control. Up to four REB-8s can be used for elevator control.
- ❗ **Note:** When an elevator controller option is checked, an **Elevator** tab appears beside the KT-200 tab.

Programming REB-8 elevator controllers

About this task:

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.

Table 36: REB-8 assigned to floors and elevators

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 information about 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

About this task:

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 onboard 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 are 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, see [Floor Definition](#).

KT-300 combus modules

About this task:

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.

Table 37: 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.
 - ❶ **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**.
 - ❶ **Note:** For more information, see [Connection Configuration](#).

KT-400

Configuring the KT-400 expansion modules

About this task:

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.

- ❶ **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, refer to the *KT-400 Ethernet Four-Door Controller Installation Guide*, DN2003.

There are three expansion module types 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:

Table 38: Expansion module options

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. To prevent redundancy unless it is planned, select the **Relay number assignments** check box. 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 click on **Add**. If there is more than one input module listed, ensure 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** check box 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 are not available for other modules.

Controller inputs 1-16 are reserved to the inputs on the KT-400.

4. Select the inputs numbers in one of two ways; using the list or the **Extended selection box**. Right-click the **Inputs** menu to view the **Extended selection box**. For more information, see [Using the extended selection box](#).

- ❗ **Note:** This is an exclusive condition. You cannot select the same item in the **Inputs** list and in the **Elevator inputs** list 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 is 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 click on **Add**. When you click 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 click on **Add**. When you click 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 **OK** to return to the KT-400 configuration window.

- ❗ **Note:** For more information, see [Connection Configuration](#).

ioModule

About this task:

To define a KT-MOD-IO16 for a KT-400, a KT-1, or a KT-2 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 the 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 elevator 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**, 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.

Defining the KT-400 Controller local areas

About this task:

❗ **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 areatab).

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

About this task:

- ① **Note:** The **Elevator** tab displays only when expansion modules are defined as inputs or outputs for elevators under the **KT-400** tab.

For KT-400 controller, you can choose a pattern to define door and floor numbers that are 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 #1**, 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.
4. Click **Save**.

- ① **Note:** To define floors, see [Floor Definition](#).

Configuring an OSDP reader to a KT-400 or KT-4 controller

1. On the EntraPass workstation, click the **Devices** tab, and click **Controller**.
2. From the **Controller** list, select the controller that the reader is connected to.
3. In the **Controller** window, click the **KT-400** tab.
4. From the **COM2 Protocol** list, select **OSDP**.

Result The **RS-485 baud rate** changes to **9600** and the **Reader template** changes to **Default OSDP reader template**. You can update these items.

5. To add readers, complete one of the following options:
 - Use the following preferred option to manually add readers:
 - i. Click the **KT-400** tab.
 - ii. Click **Add** and, in the **Address** column, select or type the OSDP reader address. Accepted values range from 0 to 126.
 - iii. In the **Door** column, select the door to associate with the reader.
 - iv. Click **Save**.
 - Use the following option to automatically add unassigned readers. This feature only works for addresses 0 to 31 at the default baud rate of 9600:
 - i. On the **Controller** window toolbar, click the **Request unassigned modules** icon.
 - ii. In the **Request unassigned modules** window, right-click the appropriate reader and select **Assign module**.
 - iii. Click **Save**.

Configuring a KT-4 controller

About this task:

You can add a KT-4 controller as a sub-type for the KT-400 controller. When you connect the KT-4 controller to the EntraPass system, the system detects the controller type and updates the information in the Controller window. Or, to manually add the KT-4 controller to the EntraPass system, complete the following steps:

1. On the EntraPass workstation, click **Devices>Controller**.
2. From the **Gateway** drop-down, select the correct gateway.

3. From the **Connection** drop-down, select the KT-4 controller connection.
4. From the **Controller** list, select the KT-4 controller.

Result By default, in the **General** tab the **KT controller type** is KT-400 and the **Controller sub type** is KT-4.

Connecting a KT-4 controller to Wi-Fi

About this task:

If you want to connect a KT-4 controller through Wi-Fi in the EntraPass system, complete the following steps:

1. On the EntraPass workstation, click **Devices>Connection**.
2. From the **Gateway** drop-down, select the correct gateway.
3. From the **Connection** drop-down, select the KT-4 controller connection.
4. From the **Connection type** drop-down, select **Secure IP (KT-400)**.
5. Click the **IP Device IP Configuration** tab.
6. In the **MAC address** field, enter the STA MAC address provided on the KT-4 controller.
7. Close the **Connection** window and click **Controller**.
8. From the **Gateway** drop-down, select the correct gateway.
9. From the **Connection** drop-down, select the KT-4 controller connection.
10. From the **Controller** list, select the KT-4 controller.
11. Click the **KT-400** tab.
12. In the **Override Wi-Fi Configuration** area, enter the **SSID** and **Password** for the Wi-Fi.

KT-1/KT-2

Enrollment Button

About this task:

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 enrollment 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.

① **Note:** For the enrollment process to be allowed for a given operator, it must first be enabled in **System/Security Level/Devices/Connection/Enrollment**.

Result

When an enrollment 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 **Enrollment 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 Enrollment 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 enrollment 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:

- Account Description (if available)
- 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
- Account

① **Note:** The unassigned controller list can have a limited number of 100 entries.

Configuring an OSDP reader to a KT-1 controller

1. On the EntraPass workstation, click the **Devices** tab, and click **Controller**.
2. From the **Controller** list, select the controller that the reader is connected to.
3. In the **Controller** window, click the **KT-1** tab.
4. From the **COM2 Protocol** list, select **OSDP**.

Result The **RS-485 baud rate** changes to **9600** and the **Reader template** changes to **Default OSDP reader template**. You can update these items.

5. To add readers, complete one of the following options:
 - Use the following preferred option to manually add readers:
 - i. Click the **KT-1** tab.
 - ii. Click **Add** and, in the **Address** column, select or type the OSDP reader address. Accepted values range from 0 to 126.
 - iii. In the **Door** column, select the door to associate with the reader.
 - iv. Click **Save**.
 - Use the following option to automatically add unassigned readers. This feature only works for addresses 0 to 31 at the default baud rate of 9600:
 - i. On the **Controller** window toolbar, click the **Request unassigned modules** icon.
 - ii. In the **Request unassigned modules** window, right-click the appropriate reader and select **Assign module**.
 - iii. Click **Save**.

Enabling exit readers

About this task:

This feature allows a user to add exit readers to doors currently controlled by the KT-400 or KT-2 controllers. Each door in effect has two readers, one for entry and one for exit, using the same door terminal port.

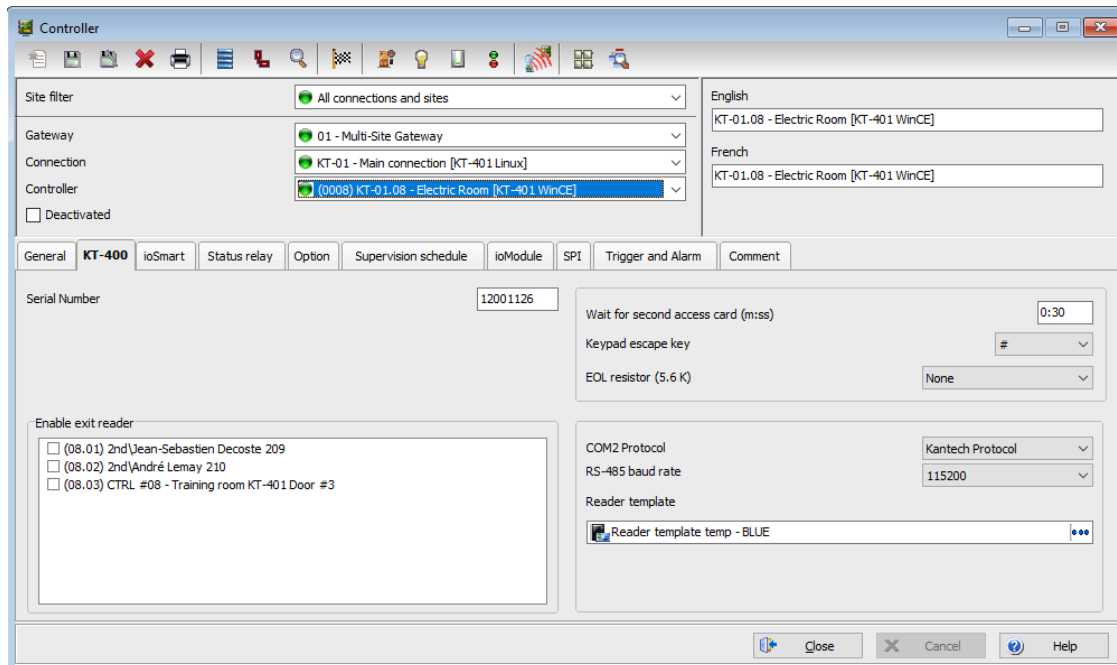
This feature is limited to ioProx XSF, ioSmart SSF, and IoProx UK 31-bit readers. Non-Kantech readers cannot use the Exit Reader feature.

The second reader retains the same values as the first reader for the following configuration settings:

- 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”

Therefore, these fields are not accessible to configure because the values are copied from the Entry Reader. The second Exit door is automatically labelled with the first door name, and the word **EXIT** at the end.

1. Ensure that at least one reader is configured on the controller.
2. From the **Controller Definition** menu, click the **KT-400** or **KT-2** tab. Under **Enable exit reader**, select the doors you want the reader to be enabled for.
3. Click **Save**.



- ❗ **Note:** You cannot delete an exit reader. Deselecting the exit reader under **Controller** disables the exit reader.

Video gateway or video vault enrollment

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 incoming information remains in wait mode, ready for assignment to a hatrix account or a defined Corporate Edition, or Global Edition system. In the workstation, the enrollment pending count displays on the lower right section of the status bar. Double click the **Enrollment pending** label to open the following report:

Table 39: Enrollment report

Column	Description
Request date	Date request received
Account	Identifies if the account is selected or assigned.
Icon	Video server
Model	exacq model
MAC address	MAC address of the DVR unit.
Request received from	IP address of the DVR that sent the request.

When you select an enrollment, double-click the enrollment to bring up the shortcut menu. The following options are available:

Table 40: Enrollment shortcut menu

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.
Assign account	Adds the selected DVR to the enrolment list of a specified account; the operator can use EntraPass workstation or Web to define the DVR.
Delete	Prompts to confirm and remove the unit from the list.

When you define a DVR using enrollment, 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.

 **Note:** For more details about the **Comment** entry box, see [Comment Field](#).


Expansion modules setup

For information about configuring expansion modules, see the following topics:


- [Input module KT-MOD-INP16 configuration](#)
- [Output Module KT-MOD-OUT16 Configuration](#)
- [Output Module KT-MOD-REL8 Configuration](#)
- [Modify an Existing Expansion Module Configuration](#)

Input module KT-MOD-INP16 configuration

1. To add a **KT-MOD-INP16**, click the **Input Module** tab and then click **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** check box 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. For more information, 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 [ioModules](#).
3. When you have finished configuring the expansion modules, click the **OK** button to go back to the KT-400 configuration window.

① **Note:** For more information, see [Connection Configuration](#).

Configuring doors

Use this menu to define the door parameters on which readers and 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.

① **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

About this task:

① **Note:** When you use the KT-300 system, you work with h:mm:ss and the range value is from 00:00:01 to 9:06:07. Each time you use a KT-400 system, you work with hh:mm:ss and the range value is 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. Take this difference into consideration.

1. In the **Devices** window, click the **Door** button.

① **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 list.
3. Select the **Gateway**.
4. From the **Connection** list, select the connection where the controller is located.
5. From the **Controller** list, select the controller you want to define. After it is selected, the language section is enabled. You may rename the selected controller.
6. From the **Door** 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**, go to Step 16.
9. Select 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. The default value is cleared.

10. Specify the **In/Out** type from the list:
 - **None**: The reader is considered as an access reader. An access reader generates only **Access granted/Access denied** events. This option is selected by default.
 - **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. 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, go to Step 14.
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 16.
 - ❗ **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, KT-1, and KT-2. 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, KT-1, and KT-2. 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, KT-1, and KT-2.
 18. **Unlock Schedule** will allow the system to unlock the door for a predetermine period of time that you will select.
 19. **First Person In** option (Not for KT-200): keeps door locked until the first granted card access while an unlock schedule is valid. Default is unselected.
 - For the KT-400, KT-1, and KT-2 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 and a Global 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 controllers with firmware version 1.04 and higher and KT-300 controllers with firmware version 1.16 and higher.

For KT-400 controllers

About this task:

Doors can be defined with relay or relay group activation by pressing any specified key on the keypad.

- ① **Note:** The Keypad tab is only enabled 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 you want to grant access using a reader or a keypad only. A keypad access is less secure than a reader access as the user may share their PIN and cannot permit further use, compared to lending a card and getting it back.
 - **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).

① **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. Default value is deselected. (Multi-site/Global/KT-NCC doors only)
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

About this task:

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).

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.

- ① **Note:** A door contact cannot be assigned to more than 2 readers.

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

About this task:

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 or KT-200)** , 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.
- ① **Note:** The primary and secondary **Rex Bypass message schedule** options will be available upon activation in **System parameters**. See [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.
- ① **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

About this task:

You can use double and triple card swipe actions with the KT-1, KT-2, and KT-400 (firmware KT-400: 1.08; KT-400 V1: 1.11).

1. Click the **General** tab.
2. **Enable Multi-swipe:** Select to enable the multi-swipe function. The **Multi-Swipe** tab appears. Deselecting disables the multi-swipe function but keeps the parameters entered previously for future use.
3. Click 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.

① **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) is triggered and the buzzer on the reader starts to beep.

The pre alarm door open too long delay overrides the default setting for the Open time. For example, if you have an unlock time of 10 seconds and an open time of 2:00 minutes, and tthe **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 triggers a pre alarm door open too long alarm and the buzzer starts to beep on the reader.

This feature is only available on a 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 is automatically checked and disabled
- **Request to arm granted - Alarm interface :** Equivalent to an arm door manual operation including panel partitions arming functionality. When this action is selected on a global or a KT-NCC gateway, it is only performed when the door is configured as an arming reader in one or more alarm systems. The operator needs to use a double or triple swipe to arm an alarm system. The double/triple swipe conditions are first verified and then the arming conditions of the alarm system.
- **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 is 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 is automatically checked and disabled.
- **Toggle relay :** A relay or relay group can be selected.
- **Unlock door :** Relock on access on double/triple swipe is automatically checked and disabled.

Defining interlock options (mantrap)

About this task:

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.

- ① **Note:** The Interlock options do not apply to a KTES door.
1. In the **Door** window, click the **Miscellaneous** tab.
 2. From the **Door** 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. from the **Door** list, select the second door for which the interlock options (mantrap) are being defined and 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.
 - ❶ **Note:** The interlock options (mantrap) are not available on doors controlled by a KT-100.
6. Select **No unlock by input when armed** when applicable. It is cleared by default.
7. 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.
8. 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**.
 - ❶ **Note:** The Shunt input items vary depending on the KT-300 or KT-400 system used.

Defining elevator doors

About this task:

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.

❶ Note:

- 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 about how to program elevator control using REB-8 relays, see [Controllers Configuration](#).

Defining a door under a Global/KT-NCC Gateway

About this task:

This option is only available when selecting a Global Gateway or a KT-NCC in the **Gateway** scroll list.

1. Use the **Access and Area** tab to define dual custody operation, area before/after, and restrictions for the door being defined.
2. Check the **Dual Custody** option to enable this feature. Dual custody is used to add extra security to a door by requesting that 2 cardholders must access the door together.
3. Define the proper access levels for both cardholders:
 - Select **Access Level 1**, the first access level needed to access the door.
 - Select **Access Level 2**, the second access level needed to access the door.
 - Select **Privileged access**. This is the access level selected to override dual custody on a door.

❗ **Note:** With the **Dual custody** feature, cards must be presented in proper order to grant access. Card with Access Level 1 must be presented first then card with Access Level 2 is presented second.
4. Define **Area** for Anti-Passback and muster reporting:
 - **Area before:** Select the area which will be considered as “area before” when a cardholder presents a card at this door. For muster reporting, always select **Unknown** area. To disregard anti-passback for this door, leave this field blank.
 - **Area after:** Select the area which will be considered as “area after” access will be permitted to the cardholder. To disregard anti-passback for this door, leave this field blank.

❗ **Note:** Usually, doors (or readers) are “shared” between areas, meaning that before accessing a door, a cardholder is considered to be in a certain area (which is called “area before”) and when this cardholder passes the door, he/she is in another area (which is called “area after”). For example, a cardholder who is in an “Unknown” area and wants to access “Area A”:

 - The card holder presents his card at the door reader and wants to access area “A”.
 - The system verifies the current location of the cardholder (to verify the current location of cardholder within areas, see [Manual Operations on Areas](#)).
 - The system then looks in the door definition menu where the cardholder presented his card to see which area is defined as “area before” and “area after” for the selected door reader.
 - If area “Unknown” is set as “area before” and “area A” is set as “area after” and the current position of the card holder is “Unknown”, access will be granted.
 - If this card holder’s current position would have been in Area B, access would have been denied, since the reader “area before” (door) was set to “Unknown”.
5. Define **Timed Anti-Passback** by checking the **Restrict Access** box and entering time (mm:ss) for **Restrictive Access Delay**.

❗ **Note:** When cardholders present their cards at this door, they will not be able to present their cards at another reader/door also defined with “restrictive access” until the delay expires.

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 is 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 is not sent to the pager), **Call immediately** (the relay activation for that event is immediately to the pager) or **Call when scheduled** (the relay activation for that event is sent to the pager according to the pager call schedule). Default value is **Do not call**.
 - ① **Note:** To specify pager call types for each events, the **Pager reporting** function must be enabled. See [KTES Configuration](#).
4. Under **modem call type**, assign the call type option that best suits event reporting.
 - ① **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.
5. 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.
 - ① **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. This feature is only available with Corporate and Global Gateways.
6. Select the relay that will be activated locally or the relay group (if you are using KT-400) for each event .
7. **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** .
 - ① **Note:** To specify pager call types for each events, the **Pager reporting** function must be enabled. See [KTES Configuration](#).
8. Under **modem call type**, assign the call type option that best suits event reporting.
 - ① **Note:** To access the **modem call type** feature, the site connection type must be set to **Modem**. For more information, see [Connection Configuration](#).

Defining door options for controllers and the KTES (multi-site gateway only)

The following tab only appears when KT-100, KT-300, KT-400, KT-1, and KT-2 controllers and the KTES have been configured in a multi-site Gateway.

Click the **Options and alarm system** tab (or **Options** for a KTES).

- **Supervised door lock device:** use this feature 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 opens the door before it has been completely secured at the end of unlocking delay. Select the **Supervised door lock device** check box to enable this option.

- **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 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. 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 an ioSmart reader in RS-485.

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.

① **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 function 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](#).
- ① **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)

About this task:

The following option is only available when KT-100, KT-300, KT-400, KT-1, and KT-2 controllers are configured in a multi-site Gateway. KT-100, KT-300, KT-400, KT-1, and KT-2 controllers have 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 increases the system security because cardholders are required to enter a PIN in addition to presenting a card. This 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 the **Schedule** section and select **New**.
- To edit existing schedules, right-click the **Schedule** section and select **Edit**.
- To apply existing schedules to an access level, select from the list beside the schedule.

For more information about access levels, see [Access levels definition](#).

❗ **Note:** For more details about the **Comment** entry box, see [Comment Field](#).

Reader Templates

About this task:

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)**.
9. Select **Visible in all accounts** to make the template accessible for all accounts.

Result

The **Visible in all accounts** checkbox is available in system account. When it is selected, the template is viewable across all accounts, however operators cannot edit or delete the template. When you clear the checkbox, the default reader template is reassigned to the controllers that previously used the assigned template. A confirmation message appears and the option to delete becomes available.

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.

EntraPass Global Edition supports two types of gateways: Corporate and Global. It also supports KT-NCC gateway functionality. All gateways interface the connections and the server. Except for the KT-NCC, the gateways may be installed on a dedicated computer, or integrated with another EntraPass workstation.

- ① **Note:** For a single gateway, limits are 2048 connections, 10,000 doors, 100,000 inputs and 100,000 outputs.

EntraPass Global Edition is shipped with a Global Gateway and KT-NCC Gateway functionality. A single multi-site Gateway can be enabled through the Dual Gateway option without any additional license.

Additional Gateways (Corporate and Global) require additional licenses.

To identify issues with the gateway or check on its status you can run gateway application (**Program Files...EntraPass GE/CE...Gateway**). This user interface displays information about the **Application Status**, **Connection Status** and **Performance** of the gateway.

Table 41: Gateway capacities in EntraPass Global Edition

Capacities	Multi-site Gateway	Global Gateway	KT-NCC
Number of gateways	40	128	128
Local connections	32 sites with serial and USB	32	2 x RS-485 1 x RS-232
On-line remote connections	512 sites with Kantech IP Link*; 32 connections with Lantronix	32	4 x TCP/IP (UDP)
Dial-up modems at host connection	32 per gateway	N/A	N/A
Remote dial-up connections	512 per gateway	N/A	N/A
Controllers per gateway	17,408 total (32 KT per connection)	1,024 per Global Gateway (32 KT per connection)	128 per KT-NCC (32/ COM Port x 3, 8 TCP/IP / connection x4)
Readers/keypads per gateway	34,816	2,048	256

* System requirements may differ according to the size of the connections and the number of events generated each day.

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. EntraPass Global Edition installation package includes one Global Gateway. Global, multi-site Gateways and KT-NCC can be used in EntraPass Global Edition. You may add up to 40 multi-site Gateways, 128 Global Gateways and 128 KT-NCC Gateways to your EntraPass software.

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".

Creating an operator manually in the Oracle/MS-SQL Server

To integrate Oracle/MS-SQL with EntraPass, create a database.

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

Creating a Kantech operator for an MS-SQL Server

Create an operator for the Oracle/MS-SQL interface to log on to the MS-SQL server.

1. Right-click **Logins** and select **New Login**.

2. In the **Name** field, enter a new name for the operator. The name must be lowercase and cannot contain spaces or special characters.
3. Select **SQL Server Authentication**.
4. In the **Password** field, enter a new password. Create a strong password.
5. Click the **Database Access** tab.
6. Select the name of the database that you created in Step 2. When you select this option, the bottom part of the window displays the following message: **Database Roles - Permit in database role**.
7. To modify the database, select the **Public and db_owner** options and click **OK** to save and exit. You are prompted to confirm the password.
8. Enter the new password and click **OK**.

Creating a Kantech operator for an Oracle Server

1. Log on to the Oracle server as an administrator. Enter a new name for the operator. The name must be lowercase and cannot contain spaces or special characters. Alternatively, use the name you created in [Creating a Kantech operator for an MS-SQL Server](#).
2. Create a database. You can use the default database name **KanCard**.
3. To create a logon profile, use the new operator name and enter a new password. Create a strong password.
4. Assign the kantech operator the permission **Owner**.

Configuring a Multi-site Gateway

1. On the **Devices** definition tab, click the **Gateway** button.
2. From the **Gateway** list, select the gateway to be configured.
 - ① **Note:** The **Billing Zip or Postal Code** option is only available when the **hatatrix** component has been previously registered at the EntraPass Server.
 - ① **Note:** If the **Dual Gateway** option was enabled for the Global Gateway application, a **multi-site Gateway** will be listed. See [Configuring an Application](#).
 - ① **Note:** The **Dual Gateway** option is disabled in a **hatatrix** environment.
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.
 - ① **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/KT-2 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.

Table 42: 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 (<i>Note 1</i>)	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 (<i>Note 3</i>)
Valid floor selection	Door open too long	Access denied by tenant (<i>Note 3</i>)
Invalid floor selection	Door alarm on relock	Auxiliary relay activated by tenant (<i>Note 3</i>)
Time-out on floor selection	Door unlocked	Postal lock request granted (<i>Note 3</i>)
Request to exit granted	Reader disabled	Postal lock request denied (<i>Note 3</i>)
Request to exit denied	Door armed	
Arming request granted	Waiting for a second card (<i>Note 2</i>)	

❗ **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.

Result

① **Note:** For more details about the **Comment** entry box, see [Comment Field](#).

Configuring a Global Gateway

1. On the **Peripherals** toolbar, click the **Gateway** button.
2. From the **Gateway** list, select the Global Gateway that you want to configure
3. On the **General** tab:
 - Use the up/down arrows to enter the Number of controller loops. The Global Gateway can accommodate up to eight controller loops.
 - Enter the **zip code**. This is a mandatory field.
 - Select an image and a video sequence to which the Gateway is assigned, if applicable. If the video feature is installed, the **Video sequence** field will be added.
4. Select the **KT-100/KT-200/KT-300 events** tab:
 - Set the **Timer running** and the **Timer stopped** for each event. A Global Gateway is configured to manage events connected to the KT-100, KT-200 or KT-300.
5. Select the **KT-400/KT-1/KT-2 events** tab:
 - Set the **Pulse running** and the **Pulse stopped** for each event. A Global Gateway is configured to manage events connected to the KT-400.

The following table lists the events that can be accessed from a Global Gateway.

Table 43: Events accessed from a Global Gateway

Access authorized	Inactivated time on floor selection	Door unlocked
Access refused	Exit request authorized	Reader deactivated
Inactivated time for authorized access	Exit request refused	Waiting for a second card (<i>Comment 2</i>)
Waiting for a keyboard (<i>Comment 1</i>)	Door open	Inactivated time on waiting for a second card
Inactivated time for the keyboard	Door forced	Access refused - waiting for a second card
Wrong keyboard code	Door open too long pre-alarm	Access refused - reader locked
Floor selection valid	Door open too long	
Floor selection invalid	Door open on relocking	

① **Note:** The activation period for the **Waiting for the keyboard** event is defined in the **Keyboard time limits** tab in **Step 6**.

6. Select the Digital keyboard time limit tab:
 - In the Keyboard time limit section, enter the Time limit between keys (**m:ss**). This time limit is the maximum time allowed between each selection of a keyboard key by a cardholder.
 - Type in the Keyboard inactivated time (**m:ss**). The time is counted in seconds and represents the maximum time permitted for users to start entering their personal identification number using the keyboard.
- ⓘ **Note:** The maximum time allowed between keys and for inactivity is two minutes seven seconds; for the KT-400, it is four minutes fifteen seconds.
- In the **Time limits (KT-100, KT-300, KT-1 and KT-400 only)** section, click on the up/down arrows to set the Number of attempts **before the keyboard is locked**. The maximum number of attempts before the keyboard is locked is set at 255.
- Enter the Keyboard locked time (**h:mm**). The maximum length of time allowed is 4 hours 15 minutes. When the counter reaches the maximum number, the keyboard will be locked for all cards and will be inactivated for the length of time specified in the **Keyboard inactivated time**.
- Type in the Reset counter time (m:ss). When the time specified in the **Reset counter time** has elapsed, the system will attempt to reset the counter to zero. The maximum time is 4 hours 15 minutes. If the value entered is greater than the maximum allowed, the system will use the last correct value.
7. Click **Save**.

Configuring a redundant gateway

About this task:

- ⓘ **Note:** Redundant Gateway is only available for multi-site gateways.
1. From the **Devices** tab, click the **Gateway** button.
2. From the **Gateway** list, select the redundant gateway you want to configure. You can set the name of the redundant gateway here.
3. From the **Devices** tab, click the **Gateway** button.
4. From the **Gateway** list, select the multi-site gateway you want to configure.
5. Under the **Redundant** tab:
 - Use the blue dots icon to select your redundant gateway. You can select up to two Redundant Gateways.
6. The status of the redundant gateway can be viewed by selecting the **Gateway** button from the **Operations** tab. Selecting the multi-site gateway displays the status of the associated redundant gateways.
7. The assigning process automatically reloads the redundant gateways. This causes temporary disconnection of the primary gateways connections.
- ⓘ **Note:** For automatic switching of gateways to work correctly controllers must be configured to communicate with the gateway through a domain name. The dealer is responsible for changing the controllers to point toward the correct DNS for the gateway.

The redundant gateway will automatically become active when the primary gateway fails. To reinstate the primary gateway it must be manually changed. For more details about the configuration of a badge in EntraPass, see [Manual Operations on Gateway](#).

Direct connections, modem connections and Ethernet (Lantronix polling) connections are not supported by redundant gateway.

Configuring a KT-NCC Gateway

Before you start configuring your KT-NCC Gateway, make sure you consult with the Network Administrator to obtain the proper IP address to avoid network conflicts. For complete information on the KT-NCC, see the KT-NCC Installation Manual, DN1611 and the KT-NCC Quick Configuration Guide, DN1656. There are three different network connections you can define and parameters will be setup according to your network architecture.

DHCP with Enterprise Server IP Address:

- Use this type of setup when assigning the company server IP address to communicate between the server and the KT-NCC.

Static IP address:

- Use this type of setup when you have a dedicated IP address for communicating between the EntraPass server and the KT-NCC.

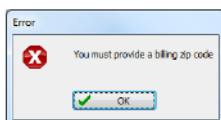
❶ **Note:** The initial configuration is done through a Web page. Please refer to the KT-NCC Installation Manual, DN1611 and the KT-NCC Quick Configuration Guide, DN1656.

WAN

About this task:

Use this type of setup in an environment where remote sites are protected with routers and they communicate with each other through the Internet.

1. In the EntraPass Workstation main window, click the **Devices** tab and click **Gateway**.
2. On the **General** tab:
 - Click the down arrow next to the text box marked **Gateway** and scroll down the selection of gateways until you reach your KT-NCC Gateway. The KT-NCC Gateway will appear along with a number on the right-hand side of the dialog.
 - Select the **Number of controller loops** in the text box under **Loop Configuration**. The KT-NCC can physically support 7 controller loops.
 - Enter the **Billing Zip** or **Postal Code**. This field is mandatory. Otherwise, the following warning message will be displayed:



- In the **KT-NCC Time Zone configuration** area, you must select the appropriate **Time zone setting**.
 - Check the box underneath it if you want the system to **automatically adjust the clock for daylight saving changes**.
 - 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.
3. Move to the **Ethernet #1** tab to setup the KT-NCC network connection.
 - Enter the **KT-NCC MAC address**. The first 6 characters in the MAC address (00-50-F9 in the example above) cannot be modified.
- ❶ **Note:** The MAC address can be found on the KT-NCC board, underneath the Ethernet #1 port. It is a 12-Digit hexadecimal code, with each two digits separated by a hyphen (that is: xx-xx-xx-xx-xx).

Table 44: Parameters to configure depending on your environment

Parameter	DHCP Enterprise	Static IP	WAN
Ethernet Port #1	Checked	Checked	Checked
Obtain an IP Address Automatically	Selected	N/A	Selected
Use the Following IP Address	N/A	Selected	N/A
IP address	Leave empty	KT-NCC IP Address	Leave as is
Subnet Mask	Leave empty	KT-NCC Subnet Mask	Leave as is
Gateway (Router)	Leave empty	KT-NCC Gate-way Address	Leave as is
Port	18710	18710	18710
Enable broadcast assignment	Checked	Checked	Checked
Local IP address LAN	Leave empty	Leave empty	Leave empty
Public IP address (LAN/WAN)	Leave empty	Leave empty	Selected and enter IP public address from Server Parameters dialog.
Domain name (LAN/WAN)	Leave empty	Leave empty	Leave empty
Use inbound server router	Leave empty	Leave empty	Checked

① **Note:** We strongly suggest that you keep the **Port number default value 18710**.

- **Network Response Time** is set to **Average** by default. You can modify it to specify the polling frequency between the EntraPass server and the KT-NCC.
Parameter Communication Timing Very fast Latency period: max 300 ms Fast Latency period: max 800 ms Average Latency period: max 1500 ms Slow Latency period: max 2500 ms Very slow Latency period: max 4000 ms Extremely slow Latency period: max 6000 ms.
- 4. Move to the **Ethernet #2** tab when you need a second **Ethernet port** for setting up IP loops.
 - You will select to **Obtain an IP address automatically** when the server will assign an IP address.
 - You will select to **Use the following IP address** when you want to use a fixed **IP address** and **Subnet Mask**.
- 5. Move to the **Onboard Relays** tab to define the activation event and longevity of any circuit connected to the relay terminals on the KT-NCC board.
- 6. Make sure the **Allow KT-Finder diagnostic access for KT-NCC** option is checked.
 - Select the **Activation on event** for each enabled **Onboard relay**.
 - If the activation is only temporary, make sure that you check the **Temporary activation** box.
 - Enter the related activation period in the **Timer** fields.

7. Click the **KT-100/KT-200/KT-300 Events** tab. Set the **Timer on** and **Timer off** for each event. A KT-NCC Gateway is configured to manage KT-100/KT-200/KT-300 events.
 8. Click the **KT-400/KT-1/KT-2 Events** tab. Set the **LED Pulse on** and **Pulse off** for each event. A KT-NCC Gateway is configured to manage KT-400 events.
- The following table lists all the events that are available in a KT-NCC Gateway.

Table 45: All the events available in a KT-NCC Gateway

Access granted	Time-out on floor selection	Door unlocked
Access denied	Request to exit granted	Reader disabled
Time-out on access granted	Request to exit denied	Waiting for a second card (Note 2)
Waiting for keypad (Note 1)	Door opened	Time-out on waiting for a second card
Time-out on keypad	Door forced open	Access denied - Waiting for a second card
Bad code on keypad	Pre-alarm door opened too long	Access denied - Reader locked
Valid floor selection	Door open too long	
Invalid floor selection	Door alarm on relock	

① **Note:** The activation period for the event **Waiting for keypad** is defined under the **Keypad delays** tab in Step 9.

9. Click the **Keypad delays** tab.
 - 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.
- ① **Note:** The maximum time allowed for both the inter-digit and time-out on keypad delays is 2 minutes and 7 seconds, and, for the KT-400, it 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.

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.

- **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.
 - **KT-100 Controllers:** Input 1 is reserved for door contact while input 2 is reserved for a request to exit device.
 - **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.
 - **KT-400 Controllers:** Reserve input 1 for the contact on door 1. Reserve input 2 for a request to exit device for door 1. Reserve input 5 for the contact on door 2. Reserve input 6 for a request to exit device for door 2. Reserve input 9 for the contact on door 3. Reserve input 10 for a request to exit device for door 3 of the controller. Reserve input 13 for the contact on door 4. Reserve input 14 for a 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.
- **KT-1 controllers:** Reserve input 1 for the contact on door 1. Reserve input 2 for a request to exit device for door 1.
 - **KT-2 controllers:** Reserve input 1 for the contact on door 1. Reserve input 2 for a request to exit device for door 1. Reserve input 5 for the contact on door 2. Reserve input 6 for a request to exit device for door 2.

Defining Input

About this task:

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** .

- ① **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 (Corporate and Global Gateways only). Default is 50 cc.

① **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).
 - ① **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.

① **Note:** To specify pager call types for each events, the **Pager reporting** function must be enabled. See [KTES Configuration](#).
 12. **For a Global Gateway only:** Check the **Transfer to Unknown Area (anti-passback)** option to assign input to a push button which can be used by the system security department to move all cards of all sectors to the "Unknown area" if anti-passback is defined in the system. This button can be used when all the personnel have to leave the building due to a fire, for instance. This option will reset all cards instead of using a manual operation, which can be a long task.

① **Note:** The input's monitoring schedule must be valid.
 13. **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.
 14. 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) are activated or shunted when this input is enabled.

2. From the **Activate relay** list, select a relay or a relay group that is triggered when this input is enabled.
3. **Activate relay temporarily** activates 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. (Corporate or Global Gateway). Default is 0s.
 - ❶ **Note:** Under a Global Gateway, users have the ability to define a delay before shunt. 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 resets the delay. For example, if Input 1 temporary shunts 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 is not 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.
 - ❶ **Note:** When the input is restored or returns to normal condition, the shunted input returns to normal condition. The event "Input shunted by input" is generated by the system. When the input returns to normal condition, the event "Input unshunted by input" is 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 relaylist** (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

About this task:

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.
 - ❶ **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 is triggered when this input is in alarm (activated).
 - ① **Note:** The relay group is available only when you are using KT-400.
3. Under **modem call type**, assign the call type option that best suits event reporting. The default value is **Do not call**.
 - ① **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.

Defining an Input for a Group of Doors

About this task:

This feature allows operators to setup an input that will allow unlocking a group of doors upon an input alarm. This feature can only be setup for groups of doors.

- ① **Note:** If you only have one door that you want to setup to unlock upon an input alarm, create a group that will only include that door. To create groups, see [Door Group Creation](#).

When the input being defined / edited is used for a door contact, a **Door** tab is displayed in the **Input definition** window.

1. In the **Input definition** window, select the **Doortab**.
 2. Select the group of doors that will be unlocked upon input alarm.
 3. Select action to take once the doors are unlocked:
 - **Latch** will keep the doors unlocked until an operator manually relocks them regardless of the input's state.
 - **Follow** will keep the doors unlock until someone physically resets the inputs state. This option is the most appropriate for manual pull stations since they require special tools and/or user intervention to reset the alarm condition.
 - Example: For a door, part of a group, on a schedule; when the input is restored, it will lock the group of doors and return the door back to its original schedule.
 - **Access** will unlock the group of doors for the duration of the unlock time even if the input is back to its normal state.
- ① **Note:** This feature is not operational if communication links between the controllers and the Global Gateway are down.

Result

- ① **Note:** For more details about the **Comment** entry box, see [Comment Field](#).

Integrated component configuration

Use the **Integrated Component** window for any type of panel component, including partition and zone, under any type of panel, including intrusion and temperature control.

1. On the EntraPass workstation, click **Devices** and click **Integrated Component**.
 2. From the **Component** list, select the component.

① **Note:** You can use the list in the toolbar to sort the displayed components by type.
 3. From the **Component type** list, select the component type.
 4. Click **Configuration Form** to display the **DSC Power Series** window.
 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. After the device is granted an address (manually or automatically from IDNet import), the user cannot change it unless the point is deleted and another one is created.
 7. For a **Virtual Zone**, from the **Component type** list, select a component type. You can select door, input, or event.
 - a. For an **Event** component type, select an event. For a list of events based on the selected component type, see [Table 46](#).
 - b. For a **Door** or **Input** component type, indicate the component source (controller).
 - c. Select the appropriate **Component action** to be reported for the virtual zone and click **OK**. The purpose of this feature is to create virtual zones in an alarm panel that receive commands from groups of selected inputs, doors, and other events of a gateway. These commands are then transmitted from the panel to a central station.
- ① **Note:** The DSC PowerSeries Neo 1.1 integrated panel can support 16 or 32 virtual zones: 16 virtual zones for HS2016 and 32 virtual zones for HS2032/3032, HS2064, HS2128/3128, and HS3248.
- ① **Note:** This feature is available only when using KT-400, KT-1, and KT-2 controllers. You require the following firmware: KT-400 v1.16.xx, KT-1 v1.02.xx, or KT-2 all firmware versions.

Table 46: 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		

Table 46: Events sent to the virtual zone

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		

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 information about defining video views, see [Video Views Definition](#).
 9. From the **Graphic** list, select the graphic to which the application is assigned, if applicable (for zones and partitions only). For information about defining graphics, see [Graphics Definition](#).
- ❗ **Note:** The **Details** button is available only for a **User** or a **Virtual Zone** component type.
10. Click **Save**.

What to do next:

To complete the configuration, see [Manual Operations on Integrated Panels](#).

Integrated panel configuration

To view and use the integration buttons, ensure that your system meets the following minimum requirements:

- Load the Integration DLL on the EntraPass Server. If the toolbar does not display the two buttons, see [System Parameters Configuration](#).
- Connect the third party hardware on the serial port of the multi-site gateway or on the serial port of a pass-through KT-400 controller.
- Turn on the third party hardware.

Intrusion panel integration within the global gateway and KT-NCC

You can integrate an intrusion panel through a global gateway, with or without a KT-NCC controller. Global gateways support the following panels:

- DSC MaxSys, Gateway serial connection
- DSC MaxSys, KT-400/KT-1 serial connection
- DSC PowerSeries, Gateway serial connection
- DSC PowerSeries, KT-400/KT-1/KT-2 serial connection
- Honeywell Galaxy, Gateway IP connection (under license)
- DSC PowerSeries Neo HS2016, HS2032, HS2064, and HS2128 serial connection
- DSC PowerSeries Pro HS3032, HS3128, and HS3248 IP connection

KT-NCC gateways support the following panels:

- DSC MaxSys, KT-NCC serial connection
- DSC MaxSys, KT-400/KT-1 serial connection
- DSC PowerSeries, KT-NCC serial connection
- DSC PowerSeries, KT-400/KT-1/KT-2 serial connection
- DSC PowerSeries Neo HS2016, HS2032, HS2064, and HS2128 serial connection
- DSC PowerSeries Pro HS3032, HS3128, and HS3248 IP connection

Note: Before defining an integration panel in EntraPass, ensure that no partition is armed. If a partition is armed, you cannot program the panel.

1. On the EntraPass workstation, click **Devices** and click **Integrated Panel**.
2. Click the **New** icon, and, in both language fields, enter a name for the panel.
3. From the **Panel** list, select a panel.

General tab

1. From the **Connection type** list, select a connection type.
2. From the **Panel model** list, select a panel model.
3. If the **Video feature** is enabled, the **Video view** list appears. If so, select the video view in which you want the defined component to appear. For more information about defining video views, see [Video Views Definition](#).
4. From the **Graphic** list, select the graphic to which the application is assigned, if applicable. For more information about defining graphics, see [Graphics Definition](#).
5. Click **Configuration** to display the **Panel Configuration** window. A different window displays according to the selected connection type.

Table 47: List of panel models and connection types

Callout	Panel model connection type
A	DSC PowerSeries Neo connected to serial or IP controller
B	DSC PowerSeries Neo connected to serial or IP gateway
C	DSC PowerSeries Pro connected to IP controller
D	DSC PowerSeries Pro connected to IP gateway
E	DSC PowersSeries or MaxSys connected to serial controller
F	DSC PowersSeries or MaxSys connected to serial gateway
G	Bentel Kyo320 connected to IP gateway
H	Honeywell Galaxy connected to IP gateway

Table 47: List of panel models and connection types

Callout	Panel model connection type
I	Simplex 4100 & 4007ES connected to serial controller
J	Simplex 4100 & 4007ES connected to serial gateway

Table 48: Panel configuration parameters summary

Parameters	A	B	C	D	E	F	G	H	I	J
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		Yes							
Intrusion model: Select the access management. By partition means that the default user code is used to arm and disarm the system. By users means that the user card is used to arm and disarm the system.	Yes		Yes		Yes					
Controller selection for pass-through: Select the controller to which the panel is connected to establish communication.	Yes		Yes		Yes				Yes	
Integration identification number: Enter the DSC communicator code to establish communication.	Yes	Yes	Yes	Yes						
Integration access code: The DSC communicator code that the user can configure.	Yes	Yes	Yes	Yes						
Number of digits: Enter the number of digits for the master access code.	Yes	Yes	Yes	Yes	Yes	Yes	Yes			
Master access code: Enter a code that is used to program the panel.	Yes	Yes	Yes	Yes	Yes	Yes				
Default user access code: From the list, select a default user access code.	Yes	Yes	Yes	Yes	Yes	Yes				
Communication port COM: From the list, select a port. This port is used for manual operations and when the system uses the managed by partition mode.		Yes				Yes				
Communication type: Select between Serial (RS-232), IP-TCP, and IP-UDP physical connections.	Yes	Yes	Yes	Yes						

Table 48: Panel configuration parameters summary

Parameters	A	B	C	D	E	F	G	H	I	J
Connection filter NEO connected to serial or IP controller: Used to filter controllers on the gateway. Selected controllers are used for virtual zones.	Yes	Yes	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			
IP ports: Select the three IP ports 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			
Select Always validate MAC address upon startup to verify that it is the right panel.							Yes			
For Simplex 4100 panels, select Import IDNet points to automatically import the panel points defined into the IDNet boards located on the fire panel. The information imported is the point addresses includes the slot number, the point value, and the subpoint value with the corresponding point label.									Yes	Yes
For Simplex 4100 panels, select Import panel button points to retrieve the button addresses to generate an EntraPass-specific named event for the following buttons: <ul style="list-style-type: none"> 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:** You cannot use the default integration access code when you program a DSC PowerSeries Pro or Neo panel. For information about retrieving an integration access code from a DSC PowerSeries Pro or Neo panel, refer to the following application notes: *Integrating the DSC PowerSeries Pro panel with KT controllers using type 2 encryption* and *Integrating the DSC PowerSeries Neo panel with KT controllers using a DSC communicator 5.3x with type 2 encryption*.

- ❗ **Note:** If you select **Access managed by user**, on the **Users** tab, in the **Card** window, an **Intrusion** tab becomes available.

For the KT-400 version, an additional list is available to select a controller for pass-through.

Panel component tab (Bentel, DSC Maxsys, PowerSeries Neo and Pro)

This feature depends on the type of intrusion panel. You must create the device in EntraPass for the DLL to download to the corresponding gateway or KT-400. After it downloads, the auto-detection becomes active.

1. Define the **Zone**, **Partition**, **User**, and **Virtual Zone** parameters. The following table lists the parameters' maximum values.

Table 49: Parameter maximum values

Parameter	PC1616	PC1832	PC1864	HS2016	HS2032 /3032	HS2064	HS2128 /3128	HS3248
Zones	32	32	64	16	32	64	128	248
Partitions	2	4	8	2	4	8	8	32
Users	48	72	95	48	72	500	1000	1000
Virtual Zones				16	32	32	32	32

2. Select the number of **Zones**. Click the button in the upper left to display a table that shows all the defined zones. Click **View** or **Edit** to view or edit the selected zone.
3. Select the number of **Partitions**. Click the button in the upper left to display a table that shows all the defined partitions. Click **View** or **Edit** to view or edit the selected partition.
4. Select the number of **Users**. Click the button in the upper left to display a table that shows all the defined users. Click **View** or **Edit** to view or edit the selected user.
5. Select the number of **Virtual Zones**. This is available only for Neo panels connected to a KT-1 or a KT-400. A corresponding number of virtual inputs are added in **Integrated Component** window. Configure virtual zones in the **Integrated Panel** window to view all zones. Configure virtual zones in the **Integrated Component** window to view one zone at a time.

- ❗ **Note:** The default number of **Virtual Zones** is the maximum value shown in [Table 49](#). The purpose of this feature is to create virtual zones in an alarm panel that receives commands from groups of selected inputs, doors, and other events of a gateway. These commands are then transmitted from the panel to a central station.

The DSC PowerSeries Neo 1.1 integrated panel can support 16 or 32 virtual zones: 16 virtual zones for HS2016 and 32 virtual zones for HS2032/3032, HS2064, HS2128/3128, and HS3248.

This feature is available only when using KT-400, KT-1, and KT-2 controllers. You require the following firmware: KT-400 v1.16.xx, KT-401 v1.22.xx, KT-1 v1.02.xx, or KT-2 any firmware versions.

6. Click **Virtual Zone List**. The displayed table allows you to map Kantech components to DSC virtual zones.

① **Note:** The **Physical Zone** column is displayed only with a valid DSC panel communication.

- a. Click the **Door**, **Input** and **Event** tabs, and select a physical zone number and the type of event (**Alarm**, **Trouble** or **Tamper**) to be sent to the central. View the remaining available zones on the counter in the upper right.

Table 50: 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		
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		

- b. Click **Add** to add a new event in the list or click **Remove** to remove the selected event.
- c. Click **Save** or **Cancel** to return to the **Integrated Panel** window.

- d. **Printing:** Use the **Print** button from the **Virtual Zone Summary** section to send the virtual zone configuration parameters to the central.

Figure 21: Virtual zone printing

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. From the lists, select the **Communication port COM** and the **Baud rate**.
2. Click **Save**.

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, see the *KTES Installation Manual, DN1769* and the *KTES Programming Manual, DN1770*.

- ① **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. On the **Devices** toolbar, select the **KTES** button.
 - ① **Note:** You must select a multi-site Gateway when configuring a KTES.
Use the **KTES Setup Wizard** to set up the Kantech Telephone Entry System (KTES) in a few steps. For more information, see [Configuring a KTES using Express Setup](#).
2. Select a **Site filter** from the first list.
3. Select the **Gateway**.
4. From the **Connection** list, select the connection where the controller is located.
5. From the **KTES** list, select the KTES you want to define. When selected, the language section is enabled. You may rename the selected KTES.

- ① **Note:** For more information about configuring connections, see [Connection Configuration](#).
6. On 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**:
 - ① **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.
 - ① **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.
 - ① **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.
 - ① **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**.
- ① **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.
- ① **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 KantechXSF .

- **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: &yy/&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: &Ooooooooo = January
- The complete current date in letters and digits format: &ww &oo &d &yy = thu jan 18 2007

Table 51: Special characters commands

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

Table 51: Special characters commands

Display	Format
Month	&o
Date	&d
Day of the week	&ww to &wwwwwwwwww
Current month in text format	&oo to &oooooooo

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** : TheBacklight 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** : TheNext Character Delayis 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 theFindoption key, the Find user timeout delays 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 delays 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. In the **KTES** window, click the **Status relay** tab.

- ① **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. The 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). The default value is none.
 - **Tamper in alarm:** This is the relay that can be activated when a KTES tamper switch event occurs. The 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. The default value is none.
 - **Lock power trouble:** This parameter defines the relay to be activated in the event of a door lock problem, locking device disconnected or shorted to ground. The default value is none.
 - **Other troubles:** Relay that will be activated when any other trouble on the KTES occurs. The default value is none.
 - **Heater kit activated:** Relay that will be activated when cabinet inside temperature falls below +5°C. The default value is none.
 - **Postal lock:** Relay that will be activated with an entry request from the front door postal lock. The 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). The default value is **No call**.

① **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.

① **Note:** For New Zealand: This equipment is not 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 that events are reported to (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**.

① **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** : TheField 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 theKTES (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 that corresponds 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 that corresponds 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**).

Result

Note: For more details about the **Comment** entry box, see [Comment Field](#).

Output device configuration

Outputs usually control the reader LED and buzzer. There are four outputs available for each 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

About this task:

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.

① **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. A multi-site Gateway supports up to 34 events and a Global Gateway supports up to 22 events.

Result

- ① **Note:** For more details about the **Comment** entry box, see [Comment Field](#).

Relay configuration

Use the output control relays provided on each KT-100, KT-200, KT-300, KT-400 and KTES to activate alarms or other devices such as lighting control, ventilation, and air conditioning. You can activate these relays according to schedules, events reported by the system. You can also activate them to indicate the status of an alarm system or a combination of different logic conditions.

Defining relays

1. Click the **Devices** tab, and click **Relay**.
2. Select a **Site filter** from the list.
3. Select the **Gateway**.
4. From the **Connection** list, select the connection where the controller is located.
5. From the **Relay** list, select the relay you want to define. Once selected, the language section is enabled. You may rename the selected relay.
6. On 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 (Corporate/Global Gateway only) .
 - ① **Note:** Under Global Gateways, EntraPass offers users the ability to force the **Temporary activation timer**. In EntraPass Global Edition, the **Force temporary activation** check box appears in the Relay window (Devices > Relays). Normally, a relay that is manually activated remains in this state until it is manually deactivated. When this option is checked, the relay will be deactivated by an alarm event, a system event or a schedule.
9. Set the **Temporary activation timer** to indicate the delay during which the relay will be temporarily triggered following a temporary activation.
 - ① **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.

Result

For more details about the **Comment** entry box, see [Comment Field](#).

Site configuration

About this task:

A site is composed of one or many physical connections. For more information about connections, see [Connection Configuration](#).

You can link together a large number of controllers, communicating over IP within an EntraPass system, into a common virtual site, regardless of their physical connections.

- ① **Note:** Dial-up connections are not supported by virtual sites.
1. Click the **Devices** tab and click **Site**.
2. If you are defining a new site, click the **New** icon, assign a name to the new site and click the **Save** icon. The bullet next to the site name turns green.
3. Enter or edit the description in both languages.

Video

Use video to define cameras, video servers, and events recorded by cameras. You can also view video recordings. The [EntraPass Video Vault](#) is an archive management tool that organises recordings in a directory style pane that makes retrieval easy, and has large storage capacity. You can use Video Vault to export video files, to find video events, set up recording parameters, link video clips with key frames, and view recordings of up to 16 cameras simultaneously.

To find out how to integrate with the exacq DVR, see [Programming the Exacq DVR using EntraPass](#).

Camera definition

You can 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** .
 - ① **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

About this task:

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 are recorded by the camera being defined and that are 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 the video server uses 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 example, choosing an Always valid schedule sends all the selected events to the EntraPass server. Specifying a limited period of time sends 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 by gateway if you are using a Global Gateway and 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.

Result

① **Note:** For more details about the **Comment** entry box, see [Comment Field](#).

Current recording

Use the current recording feature 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. On the Video toolbar, click the **Current recording** button. The **Current recording** window displays all on-going recordings.

Result

The following table shows the information displayed in the **Current recording** window depending on the source of the recording.

Table 52: Current recording information

Initiated by	Information
Video server alarm	<ul style="list-style-type: none"> Initiated by Event name Start date and time
Video trigger	<ul style="list-style-type: none"> Initiated by Video trigger Recording parameter Event Start date and time Remaining time for the recording
Operator	<ul style="list-style-type: none"> 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.

Viewing exported videos

About this task:

EntraPass enables users to view all exported videos. Use this feature 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. You can preview the exported video segment before viewing it.

1. In the **Video** window, click the **View exported video** button. The Video folder opens automatically and includes 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

About this task:

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 is saved among EntraPass program files: \Kantech\Server-GE\Video. Later you can call this file simply by double-clicking it.
 - ① **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

About this task:

Go to **Video > Video event** list, and click the **Search** button to locate and view video segments. If the **Search** button is not displayed, click the **Menu** button.

- Click the **Video server** tab to search for a video segment on a specific video server.
 - Click the **Events** tab to filter events.
 - Click the **Options** tab 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. In the **Video Events** window, click the **Search** button.
 - ① **Note:** If the **Menu** and **Legend** buttons are not activated, the window will not show the legend or the buttons in the lower part.
 2. In 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.
 - ① **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.

- ① **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.
- Click the **Events** tab to filter events to be included in the report. If you select **All events**, all the specific events are selected.
 - Click the **Options** tab to filter video segments according to their duration.
 - Check the **Video segment duration limit** option, and 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.
 - Click the **Archive State** tab to filter events according to the archive status.
 - Select 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.
 - Click **OK** to go back to the **Video event list** window.
- ① **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.
- Complete one of the options outlined in the following table:

Table 53: Finding video events buttons

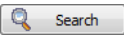
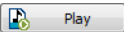

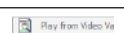
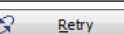


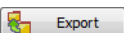
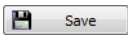

Button	Use description
 Search	Use this Search button to search for events associated with a video segment.
 Play	Use the Play button to view a video event. When you click this button, the Video desktop displays the video event. If only one camera was used, which is most often the case, the system displays 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.
 Copy from Vault	The Copy from Vault button allows operators to retrieve video segments that have been archived on EntraPass Video Vault.
 Play from Video Vault	The Play from Vault button enables operators to view a video event that has been archived on EntraPass Video Vault.
 Retry	The Retry aborted button enables operators to trigger any archiving process that was suspended.
 Menu  Legend	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.
 Export	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.

Table 53: Finding video events buttons

Button	Use description
 Save	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.
 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.

Recording parameters

Use the **Recording Parameters** menu to define parameters that control video recording and to associate recording parameters, such as video source and cameras, 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.

You can associate multiple recording parameters with one trigger. In this case, all recordings are associated with the single event and it is possible to save all record segments as a single event recording.

Setting Up Recording Parameters

About this task:

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.
 - ① **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

About this task:

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 that are configured and connected to the network.

Displaying a video view

1. On the EntraPass workstation, click the **Desktops** tab, and select the desktop dedicated to video.

❗ **Note:** The Video desktop is empty the first time you open it and the message **No video view selected** displays.
2. In the **Video View** window, select **Video view** from the list. You can edit the view (**Video view** > select a specific **View** > **Modify Video view components** button).
3. Perform various tasks using the icons in the lower part of the window. The following table describes the icons.

Table 54: Video view icons






Icons	Description
	Use these icons 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 icons 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. To program these icons, see Security Level Definition .
	Use these icons to Create and Edit video views.

Table 54: Video view icons

Icons	Description
	Use this Show view selector icon to display a mosaic view of all the cameras, or one of the cameras defined in the system.
	Help and Close icons. These are EntraPass standard icons.

- Click the **Show view selector** icon to display the View selector window. This small window allows you to 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 icon blinks until the end of the recording.
- From the displayed view, you can click a dome camera icon to display control icons for this camera (movement, zoom, focus). Available options depend on the Digital Video Management system connected to your system. For more information, refer to your DVMS documentation.
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 information, 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 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 permissions 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

- For information about how to find video events, see [Finding video events](#).

Playing Video Segments

About this task:

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.

❶ **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.
- ❶ **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

About this task:

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

About this task:

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-GE\Video. Later you can call this file simply by double-clicking it.

① **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

About this task:

You can protect exported videos using a password. Users must enter this password to view exported videos.

- ① **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

Use the video playback feature 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 them to 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.
 - ① **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 appear 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.
 - ① **Note:** You can drag the slider at the bottom of the right-hand pane to increase or decrease the speed of the video clip you 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_GE\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.
 - ① **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. To use the video feature in EntraPass, the video server must be identified to EntraPass. To ensure that the video server is identified to EntraPass, complete the following steps:

- 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.
- ① **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. On the EntraPass workstation, click the **Video** tab, and click **Video server**.

2. From the **Video server** list, select the server that you want to configure, or to add a new server, click the **New** icon on the toolbar.
3. In the **English** field, enter a descriptive name for the server. Enter a name in the other language field if the application runs in two languages.
4. On the **General** tab, from the **Video Server type** list, select the digital video recorder (DVR) type for the video server you are configuring.

Note: EntraPass supports the following integrations:

Table 55: American Dynamics models

Name	Model	Maximum number
Intellex	DVMS8000	8 cameras
Intellex	DVMS1600	16 cameras
Intellex IP		16 network video streams
Intellex Ultra		16 channels
Intellex LT-4		4 channels
Intellex LT-8		8 channels
Intellex LT-16		16 channels
AD-TVR-04	ADTVR04050	4 video channels
AD-TVR-04	ADTVR04100	4 video channels
AD-TVR-08	ADTVR08100	8 video channels
AD-TVR-08	ADTVR08200	8 video channels
AD-TVR-16	ADTVR16050	16 video channels
AD-TVR-16	ADTVR16100	16 video channels
AD-TVR-16	ADTVR16200	16 video channels
AD-TVR-16	ADTVR16400	16 video channels
AD-TVR-VS		4 video inputs
AD-HDVR-16		16 cameras
AD-HDVR-32		32 cameras
AD-NVR		128 IP cameras
AD-VideoEdge Hybrid-16		16 cameras
AD-VideoEdge Hybrid-32		32 cameras
AD-VideoEdge Hybrid-64		64 cameras

Table 56: Exacq models

Name	Maximum number of IP cameras
Exacq-8	8
Exacq-16	16
Exacq-32	32
Exacq-48	48
Exacq-64	64
Exacq-256	256

5. To register the video server as online in EntraPass, select the **Online** check box.
 - If the server is offline for long periods, for example for maintenance, clear the **Online** check box. If you do not clear the check box, EntraPass continues to poll the video server and this may cause the system to hang.
6. In the **IP address** field, enter the static IP address of the video server. Ensure that the video server is set to a static IP address. For more information about the video server IP address, contact your network administrator.
7. In the **Domain name** field, enter the video server domain address.
8. In the **Web service port** field, enter a port number for **Video (Intellex only)**, **Communication (Intellex, HDVR and TVR II)**, and **Event (Intellex only)**. Ensure that the port number matches the port used by the DVR.
 - ① **Note:** The video application uses transmission control protocol (TCP) port 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 refer to the documentation provided with your DVR.
9. The **Secure Connection (HTTPS)** check box is selected by default for the primary and alternative IP addresses.
 - If the server cannot support HTTPS protocol, clear the **Secure Connection (HTTPS)** check box. A warning message appears: **Using a non-HTTPS protocol will make your system less secure. Are you sure?**. Click **Yes** to change the protocol to HTTP.
 - ① **Note:** To use HTTPS protocol, you require an SSL certificate. For more information, see Step 2 in the [Security hardening guide](#).
10. On the **Server Parameters** tab, select the **Bypass Ping for identification (Intellex only)** check box if you want to conserve bandwidth usage. If you do not select this option, the workstation continually polls for server identification.
11. If you want users to enter their credentials to access the video server, select the **Specify video server login (Intellex only)** check box. If this option is selected, the **Login** tab appears in the **Video Server** window.
12. To cancel all the messages coming from Intellex, select the **Bypass DVR Messages** check box.
13. In the **Video server parameters** area, complete the following steps:
 - In the **Number of cameras** field, enter the number of cameras that are connected to the video server or click **Import camera details**. If you click the button, EntraPass connects to the video server to retrieve the number of cameras and the default names for the cameras.
 - 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 the **Polls before Communication failure**. This refers to the number of unsuccessful polls before the video server is declared as offline. For example, if you enter 4 in this field, EntraPass attempts to connect to the video server four times before the video server is declared as offline.
 - Click the up and down arrows to 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.

- Select the **Time for clock synchronization (Intellex only)** check box. The time synchronization refers to the time of the day when the video server synchronizes with the Kantech server for date and time. This operation is processed by the Kantech video server interface.
- ❗ **Note:** The EntraPass server is the reference time source. The video server processes the time according to the EntraPass server's time. For example, if the EntraPass server's time is 3:00 and the video server's time is 2:00, the timezone adjustment data is -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 uses Policy Manager, EntraPass operators must use a domain name, a specific login and password to access the video server. On the **General** tab, select the **Specify Video server login** check box.

❗ **Note:** Login name and password are mandatory if a HDVR or a TVR II video server type is used.

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.

The **Video Viewer** option, accessible from the EntraPass installation process, must be used for the RemoteVideoProcess function to work.

Installation of the **Remote Video Connection** will add 128 new video servers.

Defining the EntraPass Video Vault

About this task:

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.
 - ① **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.

Result

① **Note:** For more details about the **Comment** entry box, see [Comment Field](#).

Programming the Exacq DVR using EntraPass

About this task:

To program the Exacq DVR using the EntraPass workstation, complete the following steps:

1. On the EntraPass workstation, click the **Video** tab, and click **Video server**.
2. Click **Import camera details**. The DVR can be local or remote. In the case of a remote DVR, hatrrix 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

About this task:

To use the Exacq DVR to program the IP address of the video vault or video gateway, 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 **Enabled** check box.
4. Enter the IP address of the video vault in the **Address** field.
If you enter a domain name in the Address field, the exacqVision server attaches the system's serial number automatically and identifies the system. When you make a successful connection, the video gateway takes the DVR information and adds it to a list that EntraPass workstation or EntraPass Web accesses, the gateway then assigns the DVR within EntraPass.

Defining exacq DVRs

About this task:

EntraPass can have 512 exacq DVR connections per video vault. Use the video vault as a video gateway to connect to an exacq DVR. On specific event triggers, EntraPass sends an automatic e-mail that contains four thumbnail views of the event; one before, one during, and two after the event.

You can define DVRs by enrollment or in the [Video server configuration](#) section. To define by enrollment, complete the following steps:

1. Click the **System** tab, and select **Security Level** from the menu.
2. Click the **Devices** tab, and in the **Connection** area, click **Enrollment**.
EntraPass provides a report on the full status of the enrollment details.

Activating the Video Gateway for hatrrix license

To define new video servers in the video vault, you must enable the video gateway for hatrrix license, to do this, you need an unlock code. When you enable the license, the video vault option becomes visible.

When you update to the latest version of EntraPass, there is no change to existing defined DVR connections, these maintain connection to the video server. All new defined DVRs connect through a video vault; use any available video vault to connect a new video.

- ❗ **Note:** In EntraPass 7.60 and later, you can only define exacq DVRs. All video servers must be exacq and only connect to a video vault. There are no tokens added to the Kantech Advantage Program (KAP).

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

About this task:

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: alarm systems, areas, guard tours, gateway, connection, controller.

Based on an event that occurred on the selected system component, the trigger starts or stops 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 and the component for the trigger being defined.

3. From the **Component type** drop-down list, select the component that triggers 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 is 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.

A Video view may only includes cameras of the same DVR type (HDVR, Intellex, TVR).

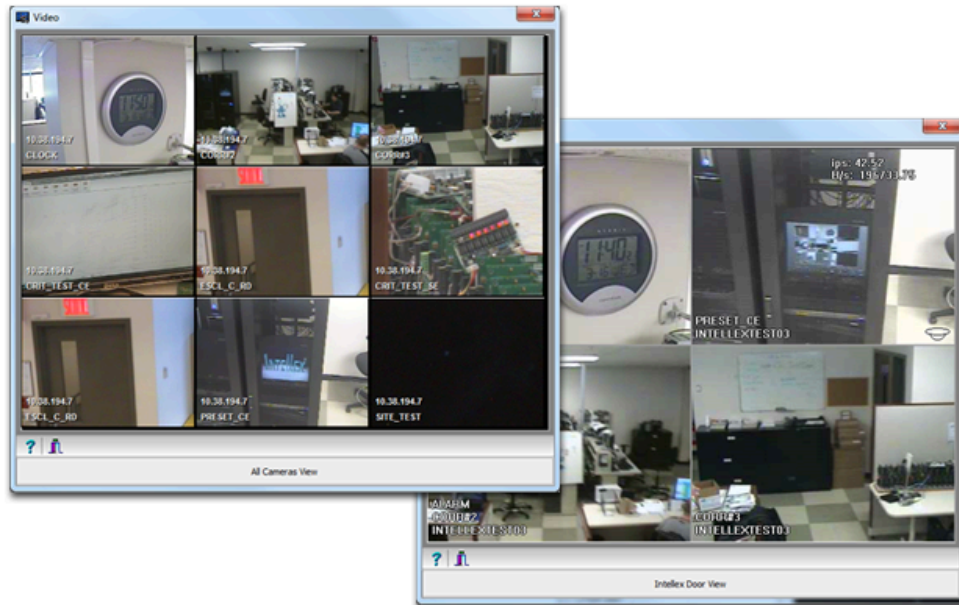
The maximum number of TVR available is 128 .

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.

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).



- ① **Note:** To delete a camera from a cell, right-click it, then select Delete from the shortcut menu.

- Click the **Close** button (bottom left or the "X" top right) to close the Video test window.

Video views definition

After the video server is defined and its cameras are identified, operators can define video views that are displayed in the video desktop for viewing and monitoring purposes. EntraPass operators can 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 to display the component in the video view.

Defining video view general parameters

- Click the **Video** tab and click **Video view**. The Video View window appears with the **General** tab enabled.
- In the **Video view** window, from the **Video view** list, select a video view (or click the **New** icon to create one), and enter a name for the video view. If the system is running in two languages, enter a name in each language.
- From the **Video server** list, select a video server type (Intellex, HDVR or TVR).
- From the **Default size on video** list, select an appropriate size for the image to display. You can 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.
- From the **Default size on graphic** list, select a size for the image to display on the system graphics (Large, Medium, Small, Tiny, Last used).
- Specify the **Refresh rate percentage** using the **Up/down** arrows.

- ① **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. If you set the Refresh Rate to high (> 80), the compression is low. As result, the application uses a larger network bandwidth. This may result in a slower process. The following table shows the recommended options.

Table 57: Image quality 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. Select the **Re-initialize video view delay (mm:ss)** option if you want the system to refresh the displayed image. If you select this option, the displayed image updates automatically when the specified delay elapses. This feature is useful if the defined camera view includes patterns or presets.
8. In the **Video control** section, select the appropriate options:
 - **Show overlay Intellex and HDVR only):** select this option if you want the camera identification (camera name and server) to appear in the video desktop.
 - **Show camera control:** select 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):** select this option to enable 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 you select this option, the system does not display the information related to a camera.
 - **Enable image zoom (Intellex only):** select this option if you want to display the zoom value for the selected camera.
9. Select the **Enable video pattern** check box to alternate video images in the video window. If you have defined a 2X2 view, the video pattern is composed of four images alternating in the video display according to the delay specified in the **Camera display** delay field. If you do not select this option, the video view displays all the cameras simultaneously.

① **Note:** The enable video pattern section is enabled once components are assigned to the video view.
10. Select the **Delay before launching sequence (m:ss)** check 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**.

- ① **Note:** These delays indicate the time interval during which a video or graphic appears in the video display before it is replaced by another. See the following table for the minimum or default delays. The maximum delay is 9:59 seconds.

Table 58: Display delays default times

Delay	Minimum (seconds)
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. Click the **Details** tab to view data about the selected view: video servers, cameras, and when applicable, camera presets and patterns.

Accounts

Use this section to configure and manage hattrix accounts. Functionality includes defining [Account settings](#), and viewing the communication status of accounts in [Account status](#). If you are an installer, see [Account settings](#) for information on applications, components, and usage of various components.

You can use [Account management](#) to manage access control functionality of several accounts centrally. hattrix has four different types of accounts: hosted, managed, credential, hosted-credential, and managed – credential. Use [Account type and status](#) to change from one account server to another and to select badging credentials.


For real-time status updates on cards, see [Card credentials](#), and to switch accounts and master accounts, see [Switching accounts and logon](#).

Account configuration

1. On the EntraPass workstation, click the **Accounts** tab, and click **Account**.
2. From the **Account** list, select an account.
3. On the **Information** tab, in the **Account information** fields (1 to 20), enter the relevant details. Each tab contains 10 editable fields where you can enter account information. You can customize each field label to suit your particular needs. For example, in the **1. Account Information** field, enter the company name, and in the **2. Account Information** field, enter the company address.

Customizing account information fields

1. Select an **account information** field from the list on the left.
2. Edit the **account information** captions through the given text box.
Example: In the **1. Account Information** field, enter the company name, and in the **2. Account Information** field, enter the company address.
You can enter two different descriptions and use the **Swap** button to swap the first and second captions.

 **Note:** If you do not see the **Swap** button, you need to enable the second language option in **Options>Select language**.
3. Click **OK** to keep your changes, or **cancel** to return.

Miscellaneous

1. Click the **Miscellaneous** tab.
2. To prevent a user logging on to this account, select **Deactivate login access**. Only a user that has administration rights can log on using the **Switch account** function.
3. In the **Account subfolder name** field, enter a name for the directory where the account reports are saved.
4. In the **Security Level** field, click the **Three dot** icon, select the security level and click **OK**. This is an additional security level that affects access rights to this account for all operators. The security level that is assigned to an account is added to the operator's current security level. The feature is available only if the operator's security level corresponds to the account's security level.

Badging credential

About this task:

To enable the badge printing feature, in the **Account** window, click the **Badging Credential** tab, and select the **Enable badging credential** checkbox.

1. Click the **Badging Credential** tab. This tab displays only if the badging credential option is activated. To activate the option, on the EntraPass workstation, click **Options**, click **Registration** and select the badging credential option.
2. To enable the badging credential feature, select **Enable badging credential**.
3. When you add a new card number through the badge printing module, you can set an initial state. To choose the default state for a new card number, select one of the following options:
 - Card to be activated by customer.
 - No activation required.
 - Manual card activate state. This option allows the operator to choose the initial card mode.
4. Enable **E-mail triggers**. During the badge treatment process, notification emails can be sent to inform users of their request's status. For each of the eight possible statuses, you can send a notification to one or many email addresses.
5. In the **Email address for notification** field, enter the recipient's email address or email addresses.
6. **Mandatory card number when verified**: The system waits for a card number before changing the status from printed to verified.
7. **Clear upon activation**: When it activates, the card is cleared from the **Card Account State** dialog box. For more information, see [Card credentials](#).

Adding a shipping address

About this task:

When they are printed, badges are sent to their owners. To make the process easier, you can enter different delivery addresses.

To add a shipping address, complete the following steps:

1. Click the **Shipping address** tab.
2. To add a new address, click the **New** icon.
3. Enter the address name.
4. **Optional**: To delete an address, click the **Delete** icon in the first window.

Importing gateways, sites or connections

1. Click the **Import Gateway, Sites or Connections** tab. The gateways and sites that were previously selected during the **Express Setup** will be checked in the list.
2. Select the gateways, connections and sites to assign to this account.

Comment

1. Click the **Comment** tab.
2. Enter comments in the blank space. Double-click anywhere in the blank space to display a full screen edit window.

Login message

1. Click the **Login message** tab.
2. In the **Display Login Message** pane, click one of the following options:
 - **None**

- **Always:** The message always pops up when the operator logs on.
 - **Only once:** The message displays only once for each operator.
 - **Until:** The message displays until the selected date.
 - **Only once until:** The message displays once until the selected date, or until the operator receives the message.
3. In the **Login message** fields, enter a message in the primary and secondary languages.
 4. Click **Save**.
- ❗ **Note:** All login messages display only when the user first logs on.

Account manager

About this task:

You can group a number of accounts under the same account manager. This way, installers can share the same facilities while managing data specific to their accounts. You cannot delete an account manager. However, you can create an unlimited number of account managers.

1. Click **Account Manager** to configure the account manager parameters such as:
 - Account manager description
 - 20 configurable information fields
 - Comments

❗ **Note:** For more information about the **Comment** field, see [Comment field](#).
 2. Double click the field label to display the **Change labels** window. Labels are the same for all account managers in the system.
 - a. To change a label, select the label in the list you want to change. In the text field, enter the new label name and click **OK**.
 3. Click the **Login message** tab.
 4. In the **Display Login Message** pane, click one of the following options:
 - **None.**
 - **Always:** The message always displays when the operator logs on.
 - **Only once:** The message displays only once for each operator.
 - **Until:** The message displays until the selected date.
 - **Only once until:** The message displays once until the selected date, or until the operator receives the message.
 5. In the **Login message** fields, enter a logon message in the primary and secondary languages.
 6. Click **Save**.
- ❗ **Note:** All logon messages only display upon the first logon.

Customizing account manager information fields

1. Select an **account information** field from the list on the left.
2. Edit the **account information** captions in the given text box.

You can enter two different descriptions and use the **Swap** button to swap the first and second captions.

❗ **Note:** If you do not see the **Swap** button, you need to enable the second language option in **Options>Select language**.
3. Click **OK** to keep your changes, or **cancel** to return.

Account settings

1. On the toolbar, click **Settings**.
2. In the **Central Station Name**, enter a name.
3. In the **Billing Zip** or **Postal Code**, enter a billing zip or postal code. This field is mandatory. If you do not enter this information, you see the following error message: **You must provide a billing zip code**.
4. To include the account name in the report, select **Report with account name**.
5. Enter the email addresses to send the report to.
6. Select the billing day of the month and the time, or select **Now** if applicable.
7. To import and export billing settings, click **Import** or **Export**.
8. Enter the header and footer parameters.
9. To add an image header of your choice, click **Add**.

Account statistics

Enabling the account statistics feature

By default, only the installer can access the account statistics feature. To enable the feature for other users, you must change their security level to include account statistics. For more information about changing security levels, see [Creating and modifying operator security levels](#).

To view account statistics, on the EntraPass workstation, click **Accounts**, and click **Account statistics**.

The account you are logged on to determines which statistics you can view.

- Installers can view statistics for all accounts.
- Account managers can view statistics for all of the operators on the account they manage.
- If you log on to a single account, you can view statistics only for that account.

Statistics tab

The statistics tab lists information about all of the accounts that you can access. To show, hide or move columns, click the icon in the first cell in the upper left of the table.

View the following information for each account:

- The account manager
- The account name
- The state of the account. For more information, see [Account type and status](#).
- The account service type. For more information, see [Account type and status](#).
- Number of sites
- Number of connections
- Number of controllers
- Number of doors
- Number of cards
- Number of panels
- Number of operators
- Number of reports
- Number of access levels
- Number of schedules
- Action scheduler. For more information, see [Manual operations on action scheduler](#).

- Number of go Pass credentials that are used
- Video servers
- Number of defined cameras
- Total number of logons since the last server reboot
- Average number of web logons each day
- Total number of events since the last server reboot
- Average number of events each day.

Operator tab

The operator tab lists information about the operators on the system. To view the list of operators, click **Search**. By default, the list does not include the default installer, administrator or operator. To view the default operators, select **Include system defaults** and click **Search**.

View the following information for each operator:

- Account manager
- Account
- Indication if the account operator is a technician
- Name
- Logon name
- Email
- Last logon date and time

To view, edit or delete an operator, right-click on their row in the table.

Report tab

The report tab displays all reports from the system. To view the list of reports, click **Search**. By default, the default reports do not display. To view the default reports, select **Include system defaults** and click **Search**.

View the following information for each report:

- Account manager
- Account name
- Type of report
- Name of report
- The date and time the report was executed last

To view, edit, or delete a report, right-click on their row in the table.

Exporting an account statistics CSV file

1. On the EntraPass workstation, click **Accounts** and click **Account statistics**.
2. In the **Account statistics** window, click the **Statistics** tab, the **Operator** tab, or the **Report** tab.
3. Right-click in the table area, and click **CSV Export**.

Account management

Use the account management feature to manage access control functionality across several clients and accounts through a central station. Companies often use this feature when they take over access control management for smaller companies. In this type of environment, under a multi-site gateway, a central station handles several accounts where clients can access their account information on an individual basis.

An operator's logon name and password defines which accounts they can access in EntraPass and the type of actions they can perform, for example, viewing, editing or deleting accounts. The system administrator assigns accounts to operators. An operator can have access to several accounts.

In order to activate this option in EntraPass, you must register the hattrix component. To register a new component in EntraPass, see [Adding system components](#).

Note: Registering to the hattrix component is not reversible.

After you register the hattrix component in EntraPass, you can create accounts that operators access with a logon name and password. For more information on logging on to an account, see [Accessing an account under hattrix](#).

Accounts tab

Use the accounts tab to configure and manage the accounts. If the accounts tab is not available, see [Adding system components](#).

Note: To switch between accounts, see [Switching Accounts and Login](#).

Creating a new account

1. On the EntraPass workstation, click the **Accounts** tab, and click **Account**.
2. Click the **New** icon to start the Account Express Setup utility:
 - In the **English**
 - **Select an Account Event Parameter Configuration** .
3. Click **Next** and select gateways and sites to associate with the account: field, enter an account name. If you are running EntraPass in two languages, two text fields display so that you can enter the information in both languages.
 - If you need to create a new site, select the gateway where you want to create the new site and click **New**.
 - In the **New site** window, enter the **New site** name.
 - Click **OK**. The new site is listed in the **Gateway/Site** window.
4. Click **Next** and select the card types to associate with the account:
 - If you need to create a new card type, click **New**.
 - In the **New card** window, enter the **New card type** name.
 - Click **OK**. The new card type is listed in the **Card type** window.
5. Click **Next** and select the card filters to use. Use the **New** and **Delete** field, enter an account name. If icons, if needed.

Note: For more information, see [Defining card filters](#).

6. Click **Next** and select the operators:
 - To create new operators to assign to the account, click **New**.
 - In the **New operator** window, enter the **Operator Name** , **Login name** and **Password**.
 - Select the operator's **Security level** .

Note: Only one security level can be assigned for each operator.

- Click **OK** . The new operator is listed in the **Operators** window.

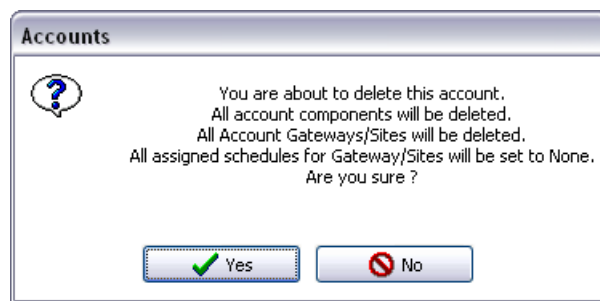
Note: You can create as many operators as you want.

7. After you create all the operators, click **Finish**.

Deleting an account

1. To delete an account, click the **Delete** icon. The following message appears:

Result



① **Note:** You can retrieve a deleted account only by restoring the database.

Moving an account between account managers

About this task:

To move a hattrix account from one master account to another, complete the following steps:

1. On the EntraPass workstation, click the **Accounts** tab, and click **Account**.
2. From the **Account** list, select the account you want to move.
3. Click on the move account icon to start the transfer process.
4. From the **Account Manager** list, select the destination master account. If only two master accounts are available, the system automatically selects the other master account.
5. Click **Yes** to confirm the move. A **Request completed** confirmation message displays.

Account configuration

1. On the EntraPass workstation, click **Accounts** tab, and click **Account**.
2. From the **Account** list, select an account.
3. Enter the relevant details in the **Account information** fields (1 to 20) from the **Information** tab:
 - Each tab contains 10 editable fields where you can enter account information. Each field label can be customized to suit your particular needs. For example, in the **1. Account Information** field, you might enter the company name, and in the **2. Account Information** field, you might enter the company address.

Miscellaneous

1. Click the **Miscellaneous** tab.
2. To prevent a user logging on to this account, select **Deactivate login access**. Only a user that has administration rights can log on using the **Switch account** function.
3. In the **Account subfolder name** field, enter a name for the directory where the account reports are saved.

Badging credential

About this task:

To enable the badge printing feature, in the **Account** window, click the **Badging Credential** tab, and select the **Enable badging credential** checkbox.

1. Click the **Badging Credential** tab. This tab displays only if the badging credential option is activated. To activate the option, on the EntraPass workstation, click **Options**, click **Registration** and select the badging credential option.
2. To enable the badging credential feature, select **Enable badging credential**.

3. When you add a new card number through the badge printing module, you can set an initial state. To choose the default state for a new card number, select one of the following options:
 - Card to be activated by customer.
 - No activation required.
 - Manual card activate state. This option allows the operator to choose the initial card mode.
4. Enable **E-mail triggers**. During the badge treatment process, notification emails can be sent to inform users of their request's status. For each of the eight possible statuses, you can send a notification to one or many email addresses.
5. In the **Email address for notification** field, enter the recipient's email address or email addresses.
6. **Mandatory card number when verified**: The system waits for a card number before changing the status from printed to verified.
7. **Clear upon activation**: When it activates, the card is cleared from the **Card Account State** dialog box. For more information, see [Card credentials](#).

Adding a shipping address

About this task:

When they are printed, badges are sent to their owners. To make the process easier, you can enter different delivery addresses.

To add a shipping address, complete the following steps:

1. Click the **Shipping address** tab.
2. To add a new address, click the **New** icon.
3. Enter the address name.
4. **Optional**: To delete an address, click the **Delete** icon in the first window.

Account gateway and site

Click the **Account Gateway and Site** tab.

- The gateways and sites that were previously selected during the Express Setup will be checked in the list.

Comment

Click the **Comment** tab:

- Enter comments in the blank space.
- Double-click anywhere in the blank space to display a full screen edit window.

Assigning system gateways and sites

1. Click the **System Gateway and Site** tab.
2. Select the gateways and sites to assign to this account.

Account status

About this task:

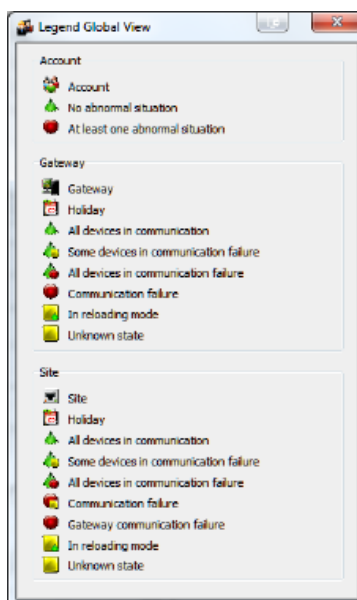
Use the status function to view the status of the accounts in the hattrix environment.

1. On the EntraPass workstation, click **Accounts** and click **Status**.
 - In the **Status** window, the **Account, Gateway / Connection** pane displays a list of all the accounts. Click the **Tree view** to view the associated gateways or sites.

- The gateways and sites have **Status** icons which change color based on their status:
 - **Black:** Dial-up not connected.
 - **Green:** Dial-up or IP or Direct connected.
 - **Yellow:** Connection in trouble, one or more controllers are offline.
 - **Red:** All controllers from a connection are offline.
- ① **Note:** A modem connection with a red dot is considered as normal.
- In the **Account, Gateway / Connection** pane, select an account, gateway or connection. The **Controller** pane displays a list of the controllers associated with the selected account, gateway or connection.
- 2. From the **Device** list, select a device.
 - For each different item that you select in the controller or in the device pane, an appropriate list of menu icons display at the top of the **Status** window.
- 3. Use the menu icons to perform various actions on sites, controllers or components. To view a list of the statuses, in the **Status** window, click the **Legend** icon, or see the following figure.

Result

Figure 22: Legend global view



- ① **Note:** For more information on the different icons in the **Status** window, see [EntraPass icons](#).

Account type and status

Use the accounts tab to change from one type of account service to another, to view the settings associated with an account, and to select badging credentials. The following table lists the account service types.

Table 59: Account service type

Account service type	Description
Hosted	Hosted cloud services
Managed	Managed cloud services

Table 59: Account service type

Account service type	Description
Credential	Badge printing available
Hosted - Credential	Hosted cloud services, badge printing available
Managed - Credential	Managed cloud services, badge printing available
Hosted - Local Printing	Hosted cloud services, local printing available
Managed - Local Printing	Managed cloud services, local printing available

There are no restrictions when you change from one service type to another. When you select **Credential**, **Hosted - Credential**, or **Managed - Credential**, the **Badging Credential** tab appears.

When you update your system and select the **Enable badging credential** check box, the selected service type automatically changes to **Credential**. For **Hosted** and **Managed** accounts, the existing functionality remains the same in relation to alarm management.

Based on the service type that you select in the **Account** window, the **Switch Account** bar displays the service type. The color of the bar indicates the status of the account. The following table outlines the three status types.

Table 60: Account status

Account state	Account color coding: switch account bar, bullet or field
Active	Grey
Deactivated	Red
Pending	Blue

Account color coding is used in the **Account** list, in the **Switch account** window and in the **Operator Account Manager and Account Login** window. When you change the status from **Deactivated** or to **Deactivated**, the account reloads.

Configuring an account

- On the EntraPass workstation, click the **Accounts** tab, and click **Account**.
 - Note:** If you migrated your account, the creation date is not visible. To view the creation date, click **Save**.
- From the **Service Type** list, select the appropriate service type.
- From the **State** list, select the appropriate state.
 - Note:** When you select **Deactivated**, the deactivated date is visible but you are unable to use EntraPass Web to log on, and the **Operation** tab in EntraPass workstation is not available. When you update the system, the selected state determines the migration state. For example, a deactivated account migrates to the deactivated state, and an active account migrates to the active state. The pending state provides a neutral state before deciding whether the account is Active or Deactivated. When you log on or switch accounts and the state is pending, a pop-up window reminds you of the pending state and offers the option to set it to active. To change the account state to active, click **Yes**. Pending accounts display in reports but you cannot create a new operator.

Configuring the default state for a new account

- Click the **Options** tab, and click **System Parameters**.
- On the left pane, click **Workstation**.
- In the **Default state for a new account** area, click **Active**, **Deactivated**, or **Pending**.

Viewing account statistics

To view account statistics, on the EntraPass workstation, click **Accounts** and click **Account statistics**. For more information, see [Enabling the account statistics feature](#).

Viewing accounts status

1. Click the **Accounts** tab, and click **Status**.
2. In the **Account, Connection** pane, from the **States** list and from the **Service types** lists, select the search criteria to filter the list of accounts.

① **Note:** For more information, see [Account status](#).

Switching an account

1. On the EntraPass workstation, click the **Accounts** tab, and click **Account**.
2. In the **Account** window, click the **Instant switch account** icon.

Badging credential

About this task:

To enable the badge printing feature, in the **Account** window, click the **Badging Credential** tab, and select the **Enable badging credential** check box.

1. Click the **Badging Credential** tab. This tab displays only if the badging credential option is activated. To activate the option, on the EntraPass workstation, click **Options**, click **Registration** and select the badging credential option.
2. To enable the badging credential feature, select **Enable badging credential**.
3. When you add a new card number through the badge printing module, you can set an initial state. To choose the default state for a new card number, select one of the following options:
 - Card to be activated by customer.
 - No activation required.
 - Manual card activate state. This option allows the operator to choose the initial card mode.
4. Enable **E-mail triggers**. During the badge treatment process, notification emails can be sent to inform users of their request's status. For each of the eight possible statuses, you can send a notification to one or many email addresses.
5. In the **Email address for notification** field, enter the recipient's email address or email addresses.
6. **Mandatory card number when verified:** The system waits for a card number before changing the status from printed to verified.
7. **Clear upon activation:** When it activates, the card is cleared from the **Card Account State** window. For more information, see [Card credentials](#).

Card credentials

1. To enable the card credentials icon in the **Account** window, on the EntraPass workstation, click the **Options** tab, click **Registration** and select the **Badging Credential** option.
2. On the EntraPass workstation, click **Accounts** and click **Account**.
3. Click **Card Credentials**. During the process, a card can adopt 8 different statuses. Each status corresponds to a step in the process from the request to the activation. Each of the steps has its own distinctive colour.

Status	Description
Badge requested	The card is requested for printing.
Request to print	The card is ready to be printed. All connected workstations that have the badge printing function enabled and a printer configuration associated with it can print the badge.
Printing	The badge printing is in process.
Failed to print	The badge printing process failed.
Badge printed	The badge is printed.
Badge verified	After printing the badge, the operator must verify the badge. During the verification process, the operator edits the card and saves it.
Badge shipped	The card is ready to send to the user.
Badge activated	The badge is activated by the user.

- ❗ **Note:** For more information on configuring badge printers, see [Selecting and Setting Up a Badge Printer](#).

Switching accounts and logon

1. To switch accounts and master accounts, click the green icon. The **Operator Master Account and Account Login** window displays.
2. In the **Operator Account Manager and Account Login** window, from the **Account Manager** list, select a master account, and from the **Account** list, select an account.
3. **Optional:** If you select the **Account event only** check box, only events corresponding to the active account display. If you clear the check box, events display according to the event parameters.

- ❗ **Note:** After switching account managers, system requests adjust accordingly. Events can be restricted based on the selected account or account manager.

System

This section contains information about how to configure applications with EntraPass, in particular, [Active Directory](#) and [Defining Alarm Systems](#).

Use this section to create, define, and modify an operator's security level. For more information, see [Security level definition](#). Before defining operators, a system administrator must grant or deny operators access to system components. For more information, see [Workspace definition](#).

Use associations to logically group devices and use commissioning to perform a series of tests to verify correct installation of each device. To define how EntraPass processes each event, see [Event Parameters Definition](#).

Active Directory

About this task:

Use the Active Directory (AD) feature 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 client's AD. The sync feature eliminates the manual creation and maintenance of AD users in EntraPass and the AD integration permits Single Sign On (SSO) authentication. 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.

- ❶ **Note:** To run the EntraPass LDAP service you need to install the Microsoft .NET Framework. Install .NET version 4.6.1 on the same machine where SmartLink is installed.

You must enter network and AD settings for the server you want to connect with.

1. On the **System** tab, click **Active directory**. The Active Directory window displays with the **General** tab enabled.
2. Click the **New** icon to create a new Active Directory, and enter the necessary information in the language section.
 - ❶ **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.
 - ❶ **Note:** After first installing the LDAP application, EntraPass completes a full sync. After a restart, EntraPass completes a partial sync where SmartLink only updates new or modified entries.
5. Assign a **SmartLink** to the Active Directory because the LDAP application connects to the SmartLink Web service.
 - ❶ **Note:** Several SmartLink connections are possible on the same SmartLink. The maximum number of Active Directories defined in EntraPass is ten.
6. In the **Active directory settings** area, 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.
- ① **Note:** If the connection is successful, synchronization occurs. You can view the LDAP service status in the following locations: **System > Active directory, Status > Application > SmartLink, Windows system tray > LDAP Service Control**, and the **SmartLink application** window.
7. Click **IMPORT AD/LDAP**. If the connection is successful the **Imported fields** box is populated with the number of fields available from the AD server.

① **Note:** The **Import AD\LDAP** option is grayed out if the LDAP Base DN (User) is blank, or if the AD server IP or domain name is blank.
 8. For users, the **User Mapping** tab defines which Active Directory attributes are mapped to which EntraPass database field. Users can customize the fields used in the users synchronization. To view which EntraPass database fields you can map, see the following [Table 61](#).
 9. Click **Sync now** to manually start synchronization with the selected Active Directory server.

① **Note:** The button is grayed if the Active Directory is not connected.
 10. For operators, the **Operator Mapping** tab displays 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. This is because EntraPass does not store passwords in its database. Active Directory fully controls passwords. If you select **Use expiry date** and **Operator expiry date**, Active Directory controls when the account expires. If you clear these fields, the EntraPass settings remain operational. Select **Picture** if you want to store images of the operator; EntraPass can import both jpeg and thumbnail photo types. When you select **E-mail**, you can import and store email addresses for an operator.
 11. For information about the comment tab, see [Comment tab](#).

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

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: <ul style="list-style-type: none"> • integer • numerical string • enumeration
Start Date (date)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • Generalized Time • UTC Coded Time
User End Date (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • integer • enumeration • boolean

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
End Date (date)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • Generalized Time • UTC Coded Time
Card # 1 - Card Number (char)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • integer • enumeration • boolean
Card # 1 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • integer • enumeration • boolean
Card # 1 - Expiration Date and Hour (date)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • Generalized Time • UTC Coded Time
Card # 1 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • integer • enumeration • boolean
Card # 1 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • integer • enumeration • boolean
Card # 2 - Card Number (char)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 2 - Display Card Number (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> integer enumeration boolean
Card # 2 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> integer enumeration boolean
Card # 2 - Expiration Date and Hour (date)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> Generalized Time UTC Coded Time
Card # 2 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> integer enumeration boolean
Card # 2 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> integer enumeration boolean
Card # 3 - Card Number (char)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> integer enumeration boolean
Card # 3- User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> integer enumeration boolean
Card # 3 - Expiration Date and Hour (date)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> Generalized Time UTC Coded Time

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 3 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • integer • enumeration • boolean
Card # 3 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • integer • enumeration • boolean
Card # 4 - Card Number (char)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • integer • enumeration • boolean
Card # 4 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • integer • enumeration • boolean
Card # 4 - Expiration Date and Hour(date)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • Generalized Time • UTC Coded Time
Card # 4 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • integer • enumeration • boolean
Card # 4 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • integer • enumeration • boolean

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 5 - Card Number (char)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• integer• enumeration• boolean
Card # 5 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• integer• enumeration• boolean
Card # 5 - Expiration Date and Hour (date)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• Generalized Time• UTC Coded Time
Card # 5 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• integer• enumeration• boolean
Card # 5 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• integer• enumeration• boolean
Card Information 1 (up to 10 with EP Corporate)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• 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)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 2	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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 3	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 6	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 9	TBD	AD fields drop list returns attributes of types: - <ul style="list-style-type: none"> • 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)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 10	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 12	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 14	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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 15	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 18	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 21	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 22	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 24	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 26	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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 27	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 30	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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 33	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• 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)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 34	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 36	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 38	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• 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 39	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• integer• numerical string• enumeration
Privileged Operation (Global Gateway only) (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• integer• enumeration• • boolean

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Supervisor level (Global/Hattrix only) (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> integer enumeration boolean
Delete when expired (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> integer enumeration boolean
Wait for Keypad (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> integer enumeration boolean
PIN (char)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> integer enumeration boolean
Disable Passback (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> integer enumeration
Extended Door Access	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> integer enumeration
Allow Multi-Swipe (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> integer enumeration
Picture (binary)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none"> replica link (type received from AD as octet string) octet string SID (type received from AD as octet string)

Table 61: EntraPass database fields for user mapping. You can customize the TBD field.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Badge Layout (integer)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• integer• numerical string• enumeration
Bar Code (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• integer• enumeration
Value (char)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• 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)
Enable usage restriction (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• integer• enumeration
Maximum card usage (integer)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• integer• numerical string• enumeration
Manual Operation only (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• integer• enumeration
Card access group (shortint)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• integer• enumeration
Comment (char)	TBD	AD fields drop list returns attributes of types: <ul style="list-style-type: none">• 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

About this task:

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.

① **Note:** A maximum of eight 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.

① **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 list and select the **Delete** button.
7. To modify an association, select the association from the list, make changes and click the **Save** button.

Result

① **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.

Configuring the security level in EntraPass Web

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, see [Security level definition](#).

Creating or editing a field technician

A field technician is an operator that has access to the system only during an appointment. When the appointment is complete, the operator's access is disabled automatically.

- To create a field technician, complete the steps in [Creating or editing an operator](#). Select the **Field Technician** check box to save the new operator as a technician.
- To view previous technician appointments click the **System** tab, and click **Operator**. Select the technician operator from the list. The **Technician log** tab displays all previous appointments for the selected technician.
- To schedule a technician appointment, see [How to schedule a technician appointment](#).

Credential E-mail Notification

About this task:


For each badge status, an e-mail notifications can be sent to recipients email address in order to keep them informed on their badge requests status.

1. From the **System/Operator** menu, select the **Credential E-Mail Notification** tab:
2. Select an e-mail trigger and, in the E-mail Address for Notification edit box, enter the e-mail addresses to be notified.

 **Note:** The **Badging Credential** option must be enabled first.

Filtering Desktop Events

About this task:

 **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 different 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.

Result

Under the **Default value** tab in the **Current selection** section, you can select which event group is assigned to which desktop.

- ① **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, areas, alarm systems, 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.
 - ① **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.
 - ① **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**.
 - ① **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](#).

Defining Alarm Systems

About this task:

Associating alarm systems to a workspace allows you to control the alarm systems that an operator can define or modify.

1. Move to the **Alarm system** tab to select the list of alarm systems that will be available to an operator who is assigned this workspace.
 - Select **All alarm systems** if you want all the alarm systems to be available to the operator assigned this workspace.
 - You can also select individual alarm systems from the displayed list.
2. Save your modifications.


Defining Card Filters

About this task:

Associating card filters to a workspace allows you to control the card filters that an operator can define or modify.

1. Move to the **Card Filter** tab to select the list of card filters that will be available to an operator who is assigned this workspace.
 - Select **All cards filter** if you want all the card filters to be available to the operator assigned this workspace.
 - You can also select individual card filters from the displayed list.
2. Save your modifications.

Event Parameters Definition

 **Note:** You now have the option to migrate from event parameter mode to event operator mode. For more information on how to migrate to event operator mode, see [How to migrate from event parameter to event operator mode](#). If you choose to remain in event parameter mode the following section still applies. If you migrate to event operator mode, see the following sections:

- [Filtering Desktop Events](#)
- [Creating a new trigger](#)
- [Event color and priority](#)

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 alarm systems, 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

About this task:

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 can keep the default settings.

Table 62: Default associations

Default associations		Comments
Component	Workstation	
Default	Default	All events originating from all components are sent to all workstations
Default	(Specific) Workstation 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 set up by the administrator and allow you to send messages to message desktops for specific events. The following table shows the three types of manual associations.

Table 63: 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. Click the **System** tab, and click **Event parameters**.
2. From the **Event category selection** list, choose a category between **Access control events** and **Intrusion events** .
3. From the **Event** list, select an event for which you want to define settings.

- ① **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.
 - ① **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.
 - ① **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** icon 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).
 - ① **Note:** The Save button is enabled only when the selected event/component becomes part of an association.

Viewing Default Parameters

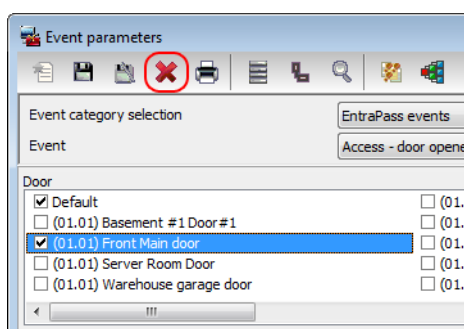
1. From the component pane (on the left) select a component and then select an EntraPass application to which the event message will be sent .
2. Click on the **View default parameters** button in the toolbar to view the default parameters message box. It will show if the event parameters were set by default or manually.
3. Click again on the **View default parameters** button to close the message box.

Deleting and Restoring Associations

About this task:

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. It is recommended to 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

About this task:

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.

① **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 will contain a single directive; the response instructions will be 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.
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.

① **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. For example, you may define specific filters for an operator: a Guard may only view “Guard tour events”. You can then create filters so that only guard tour events are sent to the Guard’s EntraPass workstation. There are many pre-defined filters such as: access events, controller events, etc. These filters can be accessed by all operators. You can select or create filters directly from the “Filtered Messages” desktop or from the Message Filters menu.

① **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.
 - ① **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.
 - ① **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 creating accounts, issuing cards, carrying out manual operations on system components, requesting reports, and arming the system. 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 for the operator to use and operate EntraPass and to receive event messages.

There is one default operator created in the system:

Installer: full access to view, modify, delete, and print components. The default username is `kantech`. You must create a new password. For information about creating passwords, see [Password rules](#).

Note: You can define operators using the default operator or you can create new operators. For information about operators' security levels, see [Security Level Definition](#).

When the [Active directory](#) application is active, a new default operator called **LDAP Interface** is created and available from the **Operator** list.

Creating or editing an operator

1. Click the **System** tab, and click **Operator**.
 - Note:** The upper right-hand corner shows the last EntraPass workstation where the operator logged on and the last login date.
2. In the **Operator** window, enter the operator **Name**. The operator name can have a maximum of 40 alphanumeric characters including spaces. The operator name displays in the desktop message lists and the reports.
3. **Optional:** Enter the operator's **email**.
4. Enter the operator **Login name**. This descriptive name can have 6 to 20 alphanumeric characters including spaces.
 - Note:** On login, operators must enter their login name and password to validate their access. The login name is displayed in the events details when operator events are generated, for example, manual operation, login, and logout.
5. In the **Password** field, enter a new password. For information about creating passwords, see [Password rules](#).
6. In the **Password Confirmation** field, re-enter the new password. If this password is not identical to the one entered in the password field, an error message appears.
7. In the **Language** section, select the display language for this operator. If you change the display language, it is 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 to the application sees 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 is ignored and the operator receives events from all workstations and gateways.

- Select 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 displays automatically. 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 selected, 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 on to. If this option is selected and **Apply operator parameters for messages** and **Apply operator parameters for alarms options of the Workstation definition** are also selected, then the basic configuration is ignored and events are filtered according to the security level of the operator who is currently logged on to the workstation.
 - If required, select **Allow login to EntraPass Web** from the operator. To display this option, the EntraPass Web component must be registered with the EntraPass Server.
 - Select **Filter reports using workspace** to issue all requested custom and in/out reports according to the operator's permissions as defined in their workspace.
 - ❗ **Note:** A selected component in the workspace must have its parent component selected as well, otherwise it does not display in the report even if the **Filter reports using workspace** option is selected.
9. Click the **Security tab** to set operator access parameters.
 10. From the **Login Schedule** list, select the schedule when the operator can log on to the system. You can create a specific schedule for an operator, **Definition > Schedule**, and then assign the schedule to the operator.
 - ❗ **Note:** To allow an operator to log on to different EntraPass applications or to the EntraPass Server, select **Allow login on application** and **Allow login on server** (System > Security Level > Miscellaneous tab).
 11. From the **Security Level** list, select a security level that determines which components an operator has access to. A security level consists of menus through which an operator can perform tasks such as modify the database, create components, and view system components and events.
 - ❗ **Note:** You can define up to 250 custom security levels. EntraPass offers three built-in security levels, Installer, Administrator and Guard. The default configuration for an installer permits access to all system components. The installer must program other security levels to limit operator access to menu commands or options.
 12. From the **Workspace** list, select a workspace that determines which physical components, including desktop display and card fields, the operator can 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 in the lower left of the window is visible only when you activate the [Active directory application](#). When you enter the **Profile** for an operator, it 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 display in the read-only fields underneath.

- ① **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. Users can click the toolbar **Search** icon and 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 is not updated by the synchronization.
 15. Select **Alarm acknowledgement** to enable the alarm acknowledgement priority level for the operator. Use the slider to set a value to the priority level. For more information about alarm management parameters, see [Alarm Management](#).
 16. 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 select this option, the selected operator cannot run the application.
 - **Change password at next login:** use this feature if you want an operator to change their password the next time they log on.
 - **Disable operator on bad password:** use this feature to limit the number of retries on bad password. For example, if you set this number to three, the operator disables after three errors when entering their password.
 - **Days before password is reset:** use this feature to manage operators' passwords. At the end of the number of the days specified in this field, the operator is prompted to change their password.
 - **Use expiration date:** use this feature to manage operators' passwords. If you select this feature, you must select an operator expiration date.
 - **Operator expiration date:** used this feature with the **Use expiration date** feature. Use this feature 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**.
 17. To configure the EntraPass database for external application requests, select **Create login name in external SQL database menu**.
 18. Select the **Web parameters** tab to configure EntraPass Web settings for an operator.
 19. Select **Send an EntraPass Welcome E-mail** to send a welcome email to an operator. Select the links you want to include in the email (EntraPass Web, EntraPass Go, and EntraPass Go Install). Click **Save** to send the email.
 20. **Optional:** To change the links in the welcome email, click **Devices**, click **Application**, and, from the **Application** list, select your **SmartLink**. Click 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.
 21. **Optional:** To configure the Smartlink that is used in the welcome email, click the **Account** tab, click **Account** and select the **Default** tab. Edit the **Preferred Smartlink included in Welcome Email** to include your preferred Smartlink. The default (empty) includes all Smartlinks that are configured on your system.

22. Click the **Save** icon.

- ① **Note:** The EntraPass Web component must have been registered with the EntraPass Server in order to display the option.

Concurrent Logins

About this task:

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.

Table 64: 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	

- ① **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 including desktops and card information, 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 or options on the system menu.

You can customize an operator security level; the system allows you to create up to 250 security levels. Each operator has a separate logon name, password, and a corresponding security level. The password is case sensitive. There is one operator and security level pre-configured in EntraPass.

Installer

- **Logon name:** kantech.
- **Password:** You must create a new password. For information about creating new passwords, see [Password rules](#).
- **Security level:** By default, a user that is defined as an installer has full access to all the system menus, can read and edit system components, and has unrestricted access to the system.

Creating and modifying operator security levels

About this task:

Assigning security levels is critical to the system. If a security level is given full access to a system menu, operators who are assigned this security level are able to modify system parameters. Ensure that each operator is given the security level corresponding to their 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 levels 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 security level by double clicking an item until it changes to the desired colour code.

- Note:** Operators cannot see items that they have not been given access to.
1. On the **System** tab, click **Security level**.
 2. In the **Security level** window, from the list, select the **Security level** you want to modify.
 - To create a new security level, click the **New** icon 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 cannot print components in EntraPass.

Defining Login Options for an Operator

About this task:

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 or without their physical address. The physical address can appear on the left or right of the component name.
1. Select the **Miscellaneous** tab to define 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, 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

About this task:

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 that are visible to the operator who is assigned this security level.

① **Note:** The **Supervisor parameters** card database field is only available with EntraPass Global Edition.

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

About this task:

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.

① **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 are allowed to perform in EntraPass; such as creating and editing items, viewing components, printing lists or reports. 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.

① **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 are displayed according to the item selected in the level above. For example, when selecting a specific site (parent), the system automatically adjusts itself to display only the corresponding controllers (children). If you select a specific controller (parent), the system adjusts itself to display only the corresponding doors (children), and so on.
 - ① **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 remains activated under all tabs.

Selecting accounts

About this task:

This feature allows you to select the accounts that are available to an operator who is assigned this workspace.

1. From the **Workspace** drop-down list, select the workspace you want to define or edit.
 - To create a new workspace, click the **New** button and enter the necessary information in the language section.
 - Select **All accounts** if you want all the displayed accounts to be available to the operator who is assigned the workspace
 - You can also select individual accounts from the displayed list.
2. Save your modifications.

Selecting an account manager

About this task:

This feature allows you to select the account manager that is available to an operator who is assigned this workspace.

1. From the **Workspace** drop-down list, select the workspace you want to define or edit.
 - To create a new workspace, click the **New** button and enter the necessary information in the language section.
 - Select **All Accounts Managers** if you want all the displayed account managers to be available to the operator who is assigned the workspace
 - You can also select individual account managers from the displayed list.
2. Save your modifications.

Selecting EntraPass applications

About this task:

This feature allows you to select the applications that are 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.
 - ① **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 are 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 are 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 are 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.
 - ① **Note:** When you select a controller, you also select all the components defined “under” or related to the controller (such as doors, relays, inputs, outputs). Make sure that you have also selected the gateway (Gateway and Site tab) that the selected controller is defined. If the gateway is not selected, the controller is available even if it is selected in the list.

Defining doors

1. Move to the **Door** tab to select the list of doors that are 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 are 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 are 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

About this task:

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 are 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 alarm systems

About this task:

Associating alarm systems to a workspace allows you to control the alarm systems that an operator can define or modify.

1. Move to the **Alarm system** tab to select the list of alarm systems that are available to an operator who is assigned this workspace.
 - Select **All alarm systems** if you want all the alarm systems to be available to the operator assigned this workspace.
 - You can also select individual alarm systems from the displayed list.
2. Save your modifications.

Defining areas

About this task:

Associating areas to a workspace allows you to control the areas that an operator can define or modify.

1. Move to the **Area** tab to select the list of areas that are available to an operator who is assigned this workspace.
 - Select **All areas** if you want all the areas to be available to the operator assigned this workspace.
 - You can also select individual areas from the displayed list.
2. Save your modifications.

Defining guard tours

About this task:

Associating guard tours to a workspace allows you to control the guard tours that an operator can define or modify.

1. Move to the **Guard tour** tab to select the list of guard tours that are available to an operator who is assigned this workspace.
 - Select **All guard tours** if you want all the guard tours to be available to the operator assigned this workspace.
 - You can also select individual guard tours from the displayed list.
2. Save your modifications.

Defining card types

About this task:

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 are 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 filters

About this task:

Associating card filters to a workspace allows you to control the card filters that an operator can define or modify.

1. Move to the **Card Filter** tab to select the list of card filters that are available to an operator who is assigned this workspace.
 - Select **All cards filter** if you want all the card filters to be available to the operator assigned this workspace.
 - You can also select individual card filters from the displayed list.
2. Save your modifications.

Defining card access group

About this task:

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 are 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

About this task:

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 are 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 are 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

About this task:

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 are 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 is 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

About this task:

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. However, the Guard's Supervisor must have access the information available to all the Guards working in his department. In that case, the list of workspaces for the Supervisor contains all the Guards' workspaces defined in EntraPass.

1. Move to the **Workspace** tab to select the list of workspaces that are 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

About this task:

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

About this task:

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 are 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.

i 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 is not 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 are 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

About this task:

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 are 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

About this task:

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 are 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

About this task:

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 are 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

About this task:

- ① **Note:** If the [Event Operator](#) mode is enabled, this feature is now available in [Creating or editing an operator](#).

Use this feature to define the event messages that display to operators who are assigned the selected workspace.

1. Click the **Events** tab to select the list of events that you want to display on an operator workstation. These events display for operators who are assigned to the 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 can see a list of operators who can be seen by the selected operator in the **Workspace** drop down.

Audit

About this task:

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.
 - **Account column:** indicates, which system account the change occurred.

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 in the upper left table.

- **Data type:** the database data type:
 - **TimeStamp**
 - **Integer**

- **Object**
- **Components**
- **Table name:** the database table name.
- ① **Note:** Define the results based on the amount of records, or by date. For more information, see [Server logs](#).

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.

Reports

Use this section to view, and define reports, their formats, and schedules. You can use [Quick report definition](#) to create a report for a set number of specific events. If you want to configure the system to generate automatically a report on a specific recurring day, see [Custom reports definition](#).

You can choose to customize the report with an event filter, and component filter. To view archived reports saved in the system, use [Archive viewing](#). The [Card Use Report](#) creates reports that lists cardholders who did, or did not generate events for a specific period. To choose an output format, see [defining a report output format](#), and for report schedules, see [Defining automatic report schedules](#).

You can use [Requesting Reports](#) to request pre-defined historical reports, or card use reports that the system created using the [Custom reports definition](#). To view the status of all requested reports that are still pending, see [Report state](#). The [Report Log](#) is a detailed list of all history reports processed by the system. If you need to know the location of all personnel in an emergency, use [Muster reports](#). If you need to know who swiped their card at a reader or group of readers within a certain period, use [Roll Call Reports](#).

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.

- ❶ **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.
 - ❶ **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

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.
 - ❶ **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.

Card Use Report

About this task:

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 events** 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

About this task:

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. Click the **Report** tab, and click **Custom report**. The Custom report window appears.
2. In the **Custom report** window, to create a new report, click the **New** icon and enter the necessary information in the language section. To modify an existing report, select it from the **Report** list.
3. You can use the default **All events** option or select a specific event type from the list. To select particular events, go to [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:** 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.
 - **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. For more information, see [Creating or editing an operator](#).
 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 check box.
 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 selected in the **Origin Filter**, an **Origin** tab is added and this allows 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 are 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)
- ① **Note:** The checkboxes under **Specific Database Event** are displayed only when a database event is selected.

The **Events selection** tab contains events based on the selected filters only.

Origin

From this tab, you can select components from the origins selected in the **General** tab with the **Origin filter**.

Components

About this task:

If you have selected a Step 9, 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.

- ① **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

About this task:

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:

- ① **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.
- ① **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](#).
- ① **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.

Table 65: Database formats and output file types

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.

Table 65: Database formats and output file types

Database	Description
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 includes 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), and the card number (for card-related events).
 - ① **Note:** A database only report is saved in the reports folder in the specified format. It is not printed nor displayed.
2. If you select **Display custom report - Display card last transaction report** (Sybase Only): The report is automatically 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 includes 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.
 - ① **Note:** The printed reports (option three and four) are saved in the reports folder in the specified format. They are 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

About this task:

In/Out reports are 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 and 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 and 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 for each 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

About this task:

In the **Report>Custom Report** window, select the **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 **Languages** area, select the **Description language** and the **User interface language**.
4. In the **Start report** field, enter the time at which the system will start executing the report.
5. 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 automatic reports

1. Click the **More** button to configure additional settings for the automatic scheduled report. When you click the **More** button, the **Automatic report output definition** window appears.
2. From the **Database output type** list, select the output format of the report. You can choose Sybase, CSV, PDF, Excel, RTF, or text formats.
3. From the **Database output process** list, select the output type.

The following table describes the different database formats and their output file formats.

Table 66: Database formats and output file types

Database	Description
SyBase	The EntraPass database
CSV	The report saves in a comma separated values format (yourfile.csv). In this formate, each piece of data is separated by a comma. This is a popular format for transferring data from one application to another because you can import and export comma-delimited data into most database systems.
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 structured as a sequence of lines. It can be opened by a large number of editing tools.

4. You can select the **Automatic file name (...)** option. The default file name is YYYY_MM_DD-HH_MM_SS.X, indicating the year_ month_ day-hours, minutes_second.file extension.
5. Select the report language. For more information about the available languages, see [System Language Selection](#).
6. Select a destination.

In/Out reports definition

Use this feature to define customized In/Out reports with automatic execution parameters.

- ① **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.

Filter Index	Filter mode
Card user name	None
Employee Name	None
Employee Number	Include
Department	Exclude
Card Information 4	None
Card Information 5	None
Card Information 6	None

- ① **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.

① **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

Use the Request In/Out reports feature 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 are 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 the **Date and time** and the **Output parameters**.
4. In the **Languages** tab, select the **Description language** and the **User interface language**.
5. Select the **Queue priority** level. A report with a priority of 1 is processed before a report with a priority of 99.
6. Click **Execute** to trigger the report.

Note: For the Sybase output type, the system displays a report preview window. For other output formats, you have to retrieve the report manually because it is not printed or displayed. To view all the reports that have been generated, use the Archive button in the Report toolbar. For information about reports output formats, see [Defining a Report Output Format](#).

Muster reports

Muster reporting in EntraPass allows roll call reporting that is used mostly in emergency situations where the location of all personnel is required at once. When an input (an emergency alarm, for example) is triggered, a muster report can automatically list all the people currently present in a pre-defined area. Muster reports can be sent through email and directed to up to 32 printers. EntraPass will send the reports to the printers first, then to the pre-configured email addresses. Muster reports come in Sybase format when printed and in a CSV format through email.

Note: If a report cannot be printed or an email cannot reach its destination, a message displays on the workstation where the report was issued from.

Graphic desktops display area groups statuses. Icons indicate when the area is active and when the area is empty.

Certain conditions must be defined to trigger a muster report:

- A muster area must be defined where there is a badging station and where employees gather during the emergency procedure.
- Area groups must be configured to contain the areas that need to be monitored during an emergency situation. If only one area needs to be monitored, an area group must be created to contain that area. For instructions on configuring area groups, see [Area Group Creation](#).

- Doors with anti-passback that are part of muster area groups must have their “Area before” parameter set to “Unknown area” in order for employees to gain access to their working area after the emergency situation is over. For instructions on configuring door anti-passback, see [Defining a door under a Global/KT-NCC Gateway](#).
- An input must be defined to trigger the muster report. For instructions on configuring inputs, see [Input Configuration](#).
- Graphics on graphics desktops may contain the area groups buttons that are monitored during an emergency period.

Muster reports for emergency management

About this task:

Before setting up a report, you must make sure that an area group is already defined. You must also select a new or already defined input that triggers the muster report generation automatically. Each muster report is defined for one area group and one input.

1. Under the **Report** toolbar, click the **Muster report** button.
2. Select the **View hierarchy** button to display all the gateways defined in the system. Then, from the **Gateway** drop-down list, select the gateway from which you want to generate a muster report.
3. From the **Muster Report** drop-down list, select an existing report if you want to modify it; or click the **New** button to create a new muster report. Then, enter the name of the report in the language section.
4. Select the **Area group** you want to assign to this report.
5. Select the **Input to start the report process**. As soon as this input is triggered, a muster report is generated.
6. Select the **Report type** to generate:
 - **Cards in area group**: will list all the cards currently present in the predefined area group.
 - **Supervisor cards in area group**: will only list all the Supervisor cards present in the predefined area group.
 - **Invalid cards in area group**: will only list the cards that are invalid and are present in the predefined area (ex: a card manually transferred in an area without the access level needed for that area).
7. Select the **Sort by** preference.
8. Check the **Automatic report refresh** box if you want EntraPass to generate more than one report automatically. Reports will contain up to date information.
 - Define the **Interval delay (mm:ss)** between each report generation. The time range value is 01:00 to 59:59 minutes.
 - Define the **Number of times (1-4)** you want to regenerate the muster report for a maximum of 5 reports (including one report that is generated automatically when the input is triggered).
9. If EntraPass is running in two languages, select the **Report languages** for generating the muster report.
10. Move to the **Destination** tab.
11. Select the **Report destination** application. This is the application that will manage the muster report generation (server, workstation, etc.).

- ① **Note:** If this application is running in service, you must define the Login parameters for that application or the printer will not generate the muster reports. For instructions on configuring login parameters for EntraPass applications, see [Application Configuration](#). For information on configuring login parameters for the EntraPass Server, see [Service Login Information](#).
- If you are generating muster reports on printers, check the **Output printer** box and select the printers in the list. You can select up to 32 printers. The muster report is generated in Sybase format.
 - If you are sending muster reports through email, check the **Email recipient** box and type each email address separated by a semi-colon (;). The muster report is generated in an Sybase format.

12. Click the **Save** button.

Muster reports for parking management

Creating reports for parking management is similar to creating reports for emergency management. You must select an area group and an input that triggers the automatic action, such as sending a message to a billboard that the parking area is full, locking a gate until someone leaves the premises, or sending a message to a guard station that the area is full. However, an extra step is required when setting up an area for parking management. In the Area dialog, you must make sure that a **Relay activated when area is full** is selected and the **Disable access when area is full** parameter is activated to be able to restrict access to that area. This may consist of locking doors or gates to restrict access to the area, or sending messages to a bulletin board to notify that a parking area is full, depending on the input you setup. For more information on setting up an area, see [Area Definition \(Global/KT-NCC Gateways Only\)](#).

Muster report generation

A first muster report is generated as soon as the corresponding input is triggered. For example, an alarm system.

- A message is displayed on the screen to indicate that a Sybase type report is being printed.
- If e-mail recipients are defined, e-mails are sent automatically after the reports are printed. An CSV containing the report contents is attached to the email.

Sequence	Date and Time	Event message	Event number	Object #1	Description #1	Object #2
1	3/24/2011 8:28:57 AM	Camera video restored	973	42	Camera 08	61
2	3/24/2011 8:28:57 AM	Video server communication failed	970	61	HDVR Video Server	0
3	3/24/2011 8:29:21 AM	Video server communication re	971	61	HDVR Video Server	0
4	3/24/2011 8:07:56 AM	Camera video restored	973	42	Office 2	61
5	3/24/2011 8:19:09 AM	Camera video restored	973	42	Office	61
6	3/24/2011 8:29:21 AM	Camera video lost	972	42	Camera 08	61
7	3/24/2011 8:28:34 AM	Camera motion alarm activated	1501	42	Office	61
8	3/24/2011 8:28:39 AM	Camera motion alarm restored	1502	42	Office	61
9	3/24/2011 8:29:49 AM	Camera motion alarm activated	1501	42	Camera 02	61
10	3/24/2011 8:30:08 AM	Camera motion alarm restored	1502	42	Camera 02	61
11	3/24/2011 8:30:28 AM	Camera motion alarm activated	1501	42	Camera 02	61
12	3/24/2011 8:30:48 AM	Camera motion alarm restored	1502	42	Camera 02	61
13	3/24/2011 8:31:46 AM	Camera motion alarm activated	1501	42	Office	61
14	3/24/2011 8:31:54 AM	Camera motion alarm restored	1502	42	Office	61
15	3/24/2011 8:34:22 AM	Camera motion alarm activated	1501	42	Camera 02	61
16	3/24/2011 8:34:39 AM	Camera motion alarm restored	1502	42	Camera 02	61
17	3/24/2011 8:34:45 AM	Camera motion alarm activated	1501	42	Camera 02	61
18	3/24/2011 8:34:51 AM	Camera motion alarm restored	1502	42	Camera 02	61
19	3/24/2011 8:34:51 AM	Login on workstation	450	44	(1) Server Workstation	45
20	3/24/2011 8:35:09 AM	Camera motion alarm restored	1502	42	Camera 02	61
21	3/24/2011 8:35:09 AM	Browse Video Vault	598	44	(1) Server Workstation	45
22	3/24/2011 8:36:23 AM	Camera motion alarm activated	1501	42	Camera 02	61
23	3/24/2011 8:36:42 AM	Camera motion alarm restored	1502	42	Camera 02	61
24	3/24/2011 8:36:46 AM	Camera motion alarm activated	1501	42	Camera 02	61
25	3/24/2011 8:37:00 AM	Camera motion alarm restored	1502	42	Camera 02	61
26	3/24/2011 8:36:25 AM	Camera motion alarm activated	1501	42	Office	61
27	3/24/2011 8:36:32 AM	Camera motion alarm restored	1502	42	Office	61
28	3/24/2011 8:37:42 AM	Camera motion alarm activated	1501	42	Camera 02	61
29	3/24/2011 8:38:22 AM	Browse Video Vault	598	44	(1) Server Workstation	45

- The muster report contains cardholders' name, card number and area where they are currently located within the monitored area.
- The muster report also indicates if cardholders are a supervisors, their supervisor levels and if cards are invalid.
 - ① **Note:** If the reports cannot be printed or delivered to the recipient, a warning will be issued and the system will try to print the report or send the email again.
- When the **Automatic refresh report** parameter is activated, the system waits for the pre-defined delay period to print the same report with up to date information.

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

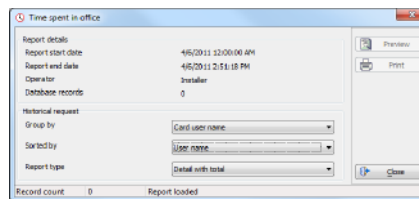
1. Under the **Report** toolbar, click the **In/Out Adjustment** button.
2. Enter the **Card number** for which you want to modify the In/Out transactions, then click the **Load** button. If you do not know the number, use the **Find** button.
 - ① **Note:** The card number field is mandatory to start 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.
 - ① **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 connection to 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 you are inserting an exit transaction, only doors defined as “Exit doors” will be displayed in the list.
11. Click the **Load** button to load the transactions from the server for this cardholder. You have to enter the card number, select the gateway/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. In 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 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 select 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.
- ① **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.
 - ① **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. In the **Languages** tab, select the **Description language** and the **User interface language**.
10. 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.
11. Click on the **Execute** button to launch the report.

Report Log

About this task:

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 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.
 - **Reportname** : 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 view the statuses of all requested reports that are still pending. On the **Report** tab, click **Report state**.

Report state fields

- **Priority**: Priority level for the treatment of messages (1 to 99). A priority of 1 is processed before a priority of 99.
- **CPU**: Level of CPU usage to be used to process the report (Lower, Normal, Higher).
- **Report**: Name of the report in process.
- **Destination**: Displays the workstation or SmartLink name to that the report is 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 and right click 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 of in process reports

Select a report and right click 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.
- ① **Note:** A red dot indicates a pending report In/Out, and a green dot indicates a report in process.

Requesting Reports

About this task:

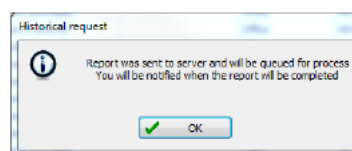
With this feature operators can request pre-defined historical reports or Card use reports that were created using the Custom Report menu. Operators can also email the report to one or multiple recipients.

- ① **Note:** If your report contains automatic settings, these are ignored. You must indicate new settings.
1. In the **Report** window, click the **Report request** button.
 2. In the **Report request** window, from either the **Custom reports** pane on top or the **Card Use reports** on the bottom, select the report that you want to execute.
 3. In the **Languages** tab, select the **Description language** and the **User interface language**.
 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. You can define **output parameters**, including the **database output type** format such as 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](#).

① **Note:** From the **Database output process** list, you can select **Email custom report** if you want this report to be automatically sent to specified recipients. If you choose this option, the email page is launched. EntraPass enables you to protect the report by a password before emailing it.

If a Card use report is selected, the Date and time section is disabled.
 6. 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.

Figure 23: Historical request window



7. Select the **Preview button** to define the report and filter options. This increases the readability of the report by adding, for instance, alternating band colors, framing events, buttons in the reports, or by sorting events in the report by event ID number, alphabetical order, or date and time.
8. Enter the **description** in the **Search description** field. The report is updated in real-time when you enter a filter option.
9. Use **Preview** to preview the report or the **Properties** button to view details about the report. When you click the **Preview** button, the system displays 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	Blayge 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 automatic reports

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** list, select the output format of the report. You can choose Sybase, CSV, PDF, Excel, RTF or text formats.
 3. From the **Database output process** list, select the report template. It will be used with the requested report. For information about the output format, see [Defining a Report Output Format](#).
- ① **Note:** From the **Database output process** list, 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 addresses in the **Send Email to** field. You can protect the report using a password before emailing it.

The following table describes the different database formats and their output file formats.

Table 67: Database formats and output file types

Database	Description
SyBase	The EntraPass database
CSV	The report saves in a comma separated values format (yourfile.csv). In this formate, each piece of data is separated by a comma. This is a popular format for transferring data from one application to another because you can import and export comma-delimited data into most database systems.
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 structured as a sequence of lines. It can be opened by a large number of editing tools.

4. You can select the **Automatic file name (...)** option. The default file name is YYYY_MM_DD-HH_MM_SS.X, indicating the year_ month_ day-hours, minutes_second.file extension.
5. Select the report language and the destination.

Options

Use this section to manage, define, and customize system setting and parameters. To secure against data loss, you can use [Backup Scheduler](#) to make a backup of the system database.

To authenticate EntraPass Workstations to the EntraPass Server, you must define the [Connection password modification](#). If you want to manage users by their user name as well as their card number, use [Card](#) credentials parameters. To customize messages that appear when the system generates an event, use [Custom messages](#). To obtain support for technical issues, enter contact data for the dealer in [About box details](#) dealer information.

EntraPass supports many reader types, use [Defining a card display format](#) to define the system for your particular card reader. You will also find [Changing from a 24-bit to 32-bit global card format](#).

To personalize events, use [Event color and priority](#). To change their appearance, and when you want to integrate EntraPass with a third party device, use [Integration](#) to select the hardware and register the DLL.

To customize the login message for EntraPass and EntraPass go, see [Login messages](#).

See [Configuring multimedia devices](#) to define alarm sounds, videos features, and video and signature capture devices. For printing instructions for event logs, reports and badge printing use [Configuring and selecting printers](#). For new system components, you must register them in the system [Registration](#) section. To run EntraPass Server as a service you must define [Service Login Information](#), EntraPass Server also uses the information entered here to access network resources. Read the [System date and time modification](#) section to find out why you should approach changing the system time with caution and the options available. If you want to change the system language see [System language selection](#), and choose from English, French, Spanish, German, Italian, Portuguese, Dutch, Turkish, Simplified Chinese, Finnish, Czech, Slovak, Danish, Swedish, and Haitian Creole.

Use [System parameters configuration](#) to define the following components and features:

- [Operator auto-deactivate](#)
- [Server logs](#)
- [Disk space](#)
- [Redundant server](#)
- [Logout and idle](#)
- [Schedule](#)
- [Icon status](#)
- [Alarm management](#)
- [Password rules](#)
- [Gateway parameters](#)
- [KT-NCC global features](#)
- [KT-NCC](#)
- [Firmware parameters](#)
- [Image parameters](#)
- [Picture and badging](#)
- [Report parameters](#)
- [Disk space](#)
- [User name format](#)
- [Video parameters](#)
- [Time parameters](#)
- [Card](#)

- [Toolbar buttons](#)
- [Integration](#)
- [User name format](#)

Alarm Management

There are five different ways to manage alarms:

- In compatible mode
- With notification based on event priority
- With notification based on the operator acknowledgement level
- With notification based on the workstation acknowledgement level
- With notification based on the workstation and on the operator acknowledgement level

These different **Alarm Management Models** determine the first to acknowledge the alarm. For each case, the acknowledgement must be completed within the **Acknowledge time-out delay**. Once the delay is expired, every workstation that received the alarm event will also receive an acknowledgement notification.

Compatible mode

When an alarm message is acknowledged on a workstation in compatible mode, every workstation on which it is programmed receives the same alarm message acknowledgment.

The Alarm Management Model is used to establish a priority level among users in regards to acknowledging an alarm. However, the alarm acknowledgement must be completed within the acknowledgement time delay; otherwise, every workstation that receives the event is notified to acknowledge the alarm.

Notification based on event priority

The priority level related to the event is now used to determine which workstation can proceed to the acknowledgment. If more than one workstation is granted the same priority level, they all receive the same request for acknowledgment.

Notification based on the operator acknowledgement level

In this model, the operator's Acknowledge Priority Level determines who has the alarm acknowledgement priority. In the Operator window, the Acknowledge Priority Level was added.

- ① **Note:** For more information about how to set the acknowledgement level for an operator, see [Creating and modifying operator security levels](#).

Notification based on the workstation acknowledgement level

The acknowledgement priority level is based on the workstation. In Devices / Application, the option Acknowledge Priority Level was added.

- ① **Note:** For more information about how to set the acknowledgement level for a workstation, see [Defining Alarm Systems](#).

Notification based on the workstation and on the operator acknowledgement level

This model is a combination of the two previous alarm management models:

The **Alarm acknowledgment** check box status (selected or not) indicated in **Devices/Application/Alarms** (for workstation priority) and **System/Operator/Security** (for operator priority) determines the resulting acknowledgement priority level for a given Operator-Workstation

combination. For more information about the alarm acknowledgement check boxes, see [Creating and modifying operator security levels](#) and [Defining Parameters](#).

		Workstation Alarm Acknowledgement			
		Not selected		Selected	
				Slider left	Slider right
Operator Alarm Acknowledgement	Not selected	Never ackn.		Never ackn.	
	Selected			Never first	Never first
				Never first	Product of both
				Slider left	Slider right

Resulting acknowledgement priority levels:

- **Never ackn.:** The operator and the workstation never receive any alarm acknowledgement notification.
- **Never first:** The operator and the workstation are never the first to receive any alarm acknowledgement notification.
- **Always first:** The operator and the workstation are always the first to receive any alarm acknowledgement notification.
- **Product of both:** The resulting priority level is calculated as a product of the operator priority level and the workstation priority level.

Enter the **Acknowledge time-out delay**. If the delay is exceeded, a new acknowledgement notification is sent.

Note: When [Event Operator](#) mode is enabled, alarm management is defined according to [Trigger and Alarm](#).

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 any of the following options:
 - Menus of the Server/ Backup Tab
 - Backup Scheduler to apply automatic schedules
 - Mirror Database application
 - Other third party software and hardware. Third party software is not recommended.

Note: By default, when you backup or restore files, the Server databases is temporarily 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

About this task:

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**.

- ① **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.
 - ① **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).
 - ① **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).
 - ① **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.
 - **Self-extracting compressed file** : will create an executable file (*.exe) that will compress the information so as to reduce the amount of disk space taken by the backup.
 - Under the **Archive, In/Out** and **Video Event** tabs only:
 - **Separate files (full backup)** : will backup all databases.
 - **Self-extracting compressed file (full backup)** : will create an executable file (*.exe) that will compress the information so as to reduce the amount of disk space taken by the backup.

- **Separate files (incremental)** : will backup all databases. Only the information that was modified since the last backup will be saved.
- **Self-extracting compressed file (incremental)** : will create an executable file (*.exe) that will compress the information so as to reduce the amount of disk space taken by the backup. Only the information that was modified since the last backup will be saved.

① **Note:** Restoring a self-extracting backup after an EntraPass upgrade can only be done from the EntraPass Server where the original self-extracting backup was done.

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.

① **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.

Badge Printer

About this task:

In the **Badge Printer** tab, you can associate a technology to a local printer. The system will then use the printer corresponding to each linked technology. If you have two printing workspaces, you will be able to dispatch your printings to one or the other.

1. From the **Credentials/Badge** printer menu, enter the printer configuration descriptions. To associate a printer configuration description to a printer, see [Printers Selection and Configuration](#).

① **Note:** The Badge printer tab is available only when the **Badging Credential** option is enabled.

Connection password modification

The connection password is used to authenticate EntraPass workstations to the EntraPass server. The connection password window displays automatically when the system is not registered.

⚠ **CAUTION:** You cannot reset the connection password if you forget it.

① **Note:** You must use a specific password. You cannot use the default password.

Changing the connection password

1. On the **Options** tab, click **Connection password**.
2. In the **Old connection password** field, enter the current connection password. Passwords are case sensitive.
3. In the **New connection password** field, enter the new connection password.
4. In the **Verify connection password** field, enter the new connection password to confirm it.
5. Click **OK** to exit. If you receive an error message, make sure that the data you entered in the **New connection password** and in the **Verify connection password** fields are identical.

① **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

On the **Card** tab, system administrators can 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 is handled by user name and has up to 5 different numbers . This allows for creating cards without assigning a card number to the new cards. For more information, see [Issuing a new card in enhanced user management environment](#)

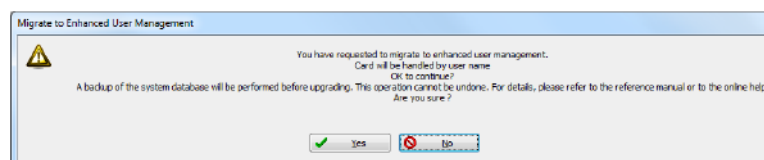
① **Note:** This option is used with EntraPass web for card management.

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:** If you select this option, EntraPass migrates to the enhanced user management. For more information, see [Issuing a new card in enhanced user management environment](#).

After selecting the box and clicking **OK**, a warning displays indicating that the action is irreversible before EntraPass performs a backup of your data.

Figure 24: Migrate to enhanced user management warning



After the process has completed, the option is grayed out on the **Card** tab.

- **Badge credential outside account:** Indicates whether to use the badging system for cards that do not belong to any account as well as the initial state of the added card number.
- **Mandatory card number when verified:** The system waits for a card number before changing the badge status from **Printed** to **Verified**.
- **Clear upon validation:** Clear the account name upon validation from the badge status section in the **Badge Request** window.

① **Note:** These fields are available only when the **Badging Credential** option is activated.

Enable access level exceptions: If selected, access level exceptions can be activated by user for each door. On activation, the user receives a warning message indicating that the controller reload process might slow down. To find out how to link a specific schedule to a door, see [Access Exception](#).

Badge Printer

In the **Badge Printer** tab, you can associate a technology to a local printer. The system will then use the printer corresponding to each linked technology. If you have two printing workspaces, you will be able to dispatch your printings to one or the other.

From the **Credentials / Badge** printer menu, enter the printer configuration descriptions. To associate a printer configuration description to a printer, see [Printers Selection and Configuration](#).

 **Note:** The Badge printer tab is available only when the **Badging Credential** option is enabled.

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 display in the Messages List. Two fields are available for primary and secondary languages.
3. Select a preset schedule that determines when the custom event is 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.

Dealer Information

About box details

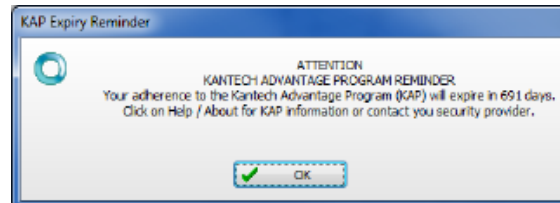
1. Fill in the **Dealer Information** fields:
 - Company name
 - Address
 - Phone number / Fax
 - E-mail
 - Website

 **Note:** The **Company Name** and **Phone number / Fax** fields are mandatory.
2. Optional: Add a picture logo with the **Add** button.
3. Fill in the **Site information** data.
4. Click **OK**.

KAP reminder

A message displays 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:

Figure 25: KAP expiry reminder



Pop-up message

A pop-up message is automatically generated by EntraPass to advise the user that their KAP is expiring. Messages display at the following times:

- 60 days before expiration
- 30 days before expiration
- On expiration
- 30 days past expiration

The user must acknowledge the reminder message. It is logged in the events database, displays in the message list, and appears in reports.

Email

In the **Dealer Information** window, you can configure the email reminder. You can add up to 4 recipients. Click the **Send reminder now** button to save the information and send a reminder immediately.

A new event is logged in the desktop events list.

Each workstation also receives a 60-second notification pop-up message. See the following figure.

Figure 26: KAP expiration 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: hhdhdpxdew93in3d390d
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

① **Note:** You can also access the KAP reminder feature in the **About** window.

Defining a card display format

About this task:

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 will be setup automatically when creating a new card.

1. Under the **Options** toolbar, click on the **Display format** button.

① **Note:** The Card #2, Card #3, Card #4, Card # 5 sections will not appear unless the **Enhanced User Management** option is activated.

2. Select 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. For more information, see [Card options definition](#).
 - ① **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.
 - ① **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

About this task:

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.

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.

Result

EntraPass converts all 24-bit card numbers to 32-bit card numbers using the proper family code.

In the workstation, EntraPass backs up the system before conversion.

hatrix does not perform a backup when switching from 24-bit to 32-bit card format.

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 card accounts 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.

① **Note:** The Auto conversion feature is available when running the redundant server.

Event color and priority

About this task:

You can change the color and priority of any event.

1. In the **Options** window, 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 an 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

About this task:

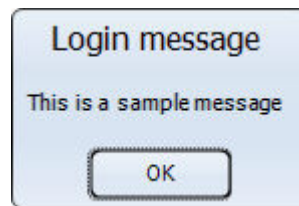
Use this feature to enter a text message that displays to other operators when they log into any workstation.

1. From the **Options** menu, select **Login message**.

Figure 27: Login message

2. Set the recurrence:
 - **None.**
 - **Always:** The message always displays after login.
 - **Only once:** The message displays only once for each operator.
 - **Until:** The message displays until the selected date.
 - **Only once until:** The message displays once until the selected date or until the operator receives the message.
3. In the **Login Message** text boxes for the primary and secondary languages, type a message.
4. Click the **OK** button.

Login message 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.
5. To write a message to an operator to notify them of a field technician's appointment, click the **Appointment message** tab.

Configuring multimedia devices

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.

- ① **Note:** The Priority level refers to the order in which alarm messages are displayed in the Alarm desktop. In EntraPass, 0 is associated with the highest priority, and 9 to the lowest. For more information, see Options > Event color and priority.
- 5. Click the **Play** button to listen to the selected sound. The system plays 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.
- ① **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. Select 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 from the Card definition window.
 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.
- ① **Note:** The video bandwidth control value cannot **exceed** the EntraPass Server value (see page 476).

Configuring and selecting printers

The **Printer options** window is accessed under the **Options** toolbar and allows users to select a log printer to use when printing events, and to select a report or a badge printer.

Selecting and setting up a log printer

About this task:

When you define events (in the **Events parameters** definition menu), it is possible to determine how and when events are 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 send alarms to a remote terminal at a specific moment.

❶ **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 is 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 are buffered and printed when a full page is ready to be printed. Events are 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 are printed one-by-one and one under the other, or it prints one event per page, depending on your printer type. Select the printer port that is used in the “printer” field. Specify if messages and alarms are 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 are 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 are printed.
4. From the **Printer** drop-down list, select the specific printer that is 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

About this task:

The **Report printer** is defined to print reports.

1. From the **Printer options** window, select the **Report printer** tab.

Registration

Use this menu to register new system components, including the KTES, Workstation, Gateway, SmartLink, to register and use the system's database and to establish communication with the Server. For more information, see [System Registration](#).

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 and time modification

About this task:

Use the **Change system** option with caution and only when necessary; this function may affect logical components of the access system (for example schedules). If, for any reason, you want to adjust the system time and date, use 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 calendar. Connected components of this application will also receive the date change notification.
3. Enter the time in the **Time** field. Connected components of this application will also receive the time change notification.
4. Click **OK** to exit.

❗ **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 more information, see [Time parameters](#).

➤ **Important:** Do 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, Portuguese, German, Italian, Dutch, Turkish, Simplified Chinese, Norwegian, Finnish, Swedish, Danish, Czech, Slovak, and Haitian Creole. Use the vocabulary editor utility to add other custom languages.

Changing the system language

1. From the EntraPass main window, select the **Options toolbar**, then click the **System language** button. Or for accounts within a master account in hattrib systems, click the **Account language** button.

❗ **Note:** When you modify the primary language, the database operation is 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. If an operator needs a different system language than the defined primary or secondary language in the account, see [Changing the system language for an operator](#).
3. Log out of EntraPass and log on again.

Changing the system language for an operator

About this task:

You can change the system language for a specific operator to be different than the defined primary or secondary language. In this case, the database language remains as the defined primary or secondary language, but the user interface for the operator or account changes to the new selection.

1. From the EntraPass main window, select **System>Operator**.
2. In the **Operator** drop-down, select the type of operator.
3. In the Languages section, from the **User interface language** drop-down, select the language.
4. Log out of EntraPass and log on again.

System parameters configuration

The system parameters window allows the system administrator to modify parameters that define the EntraPass system. This window may be accessed from a workstation or a server. Parameters have been grouped together under different labels such as Server, 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

On the **Server** tab, you can define server logs capacity, diagnostic capabilities, security parameters, disk free space threshold, alarm management, network alarms and button status.

E-mail server

About this task:

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.

① **Note:** SSL connections are not supported.

1. In the **Email server (SMTP or Exchange server)** field, enter the IP address of the Email server that is used for sending emails.
2. In the **Email Port** field, enter the number of the port that is 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 is used for authenticating the email server.
5. Authentication: These options can be used to configure the authentication method.
 - **No authentication:** No authentication is applied.

- **SMTP authentication:** An authentication, sent on the SMTP port, must be validated before the message is released.
 - ❗ **Note:** SMTP authentication is discontinued from xyz date (need info for discontinued date & new type of authentication)
- **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

About this task:

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. These records are kept with the date and 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

① **Note:** The Redundant Server component is only available 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.

① **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 buffers 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-enter 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.

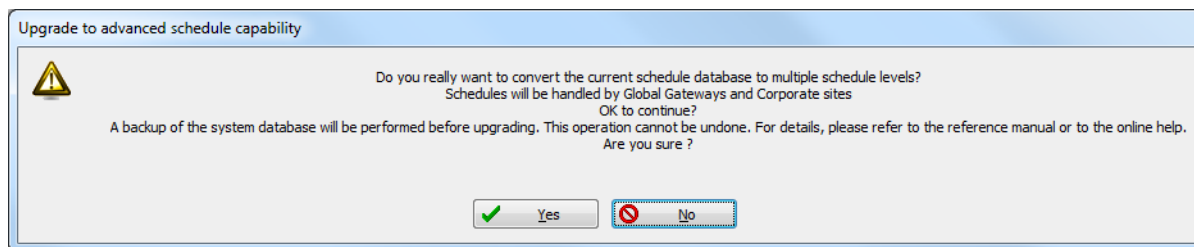
Schedule

The **Schedule** tab is where you are able to upgrade to advanced schedule capability. 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 logon schedules, video triggers. 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.
- **Global schedules:** Global schedules are grouped by gateway. These are defined for each Global Gateway. You can define 100 schedules per Global Gateway for such devices as event relays, secondary access levels, alarm systems, areas, guard tours, elevator controls. You can program 100 schedules per gateway.
- **Multi-site schedules:** These are defined for each connection. You can define 100 schedules for each Multi-site for such purposes as power supervision (controllers), door unlocking, REX trigger (doors), activation mode (relay), input monitoring.
- After checking the box and clicking **OK**, a warning appears on the 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, the **Schedule** tab disappears 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 is, 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.

1. To enable the feature, select the **Login Server Service Application** box.
2. Enter the server **Domain name or Computer name**, the **Login name**, and the **Password** twice for confirmation.

① **Note:** When there is no domain name or workgroup configured, enter the **Computer Name** instead, in the **Domain Name** field.

Call home

About this task:

The **Call home gateway** field allows you to assign a Multi-site Gateway that is used to register all the system's IP sites. This way, all the IP devices can be pre-programmed using the same information with no regards to the gateway they are connected to. The **Call home** feature is not related to the firmware version.

1. From the **Option** toolbar, click **System Parameters**, then select the **Call home** tab.

① **Note:** The **Call Home** function is only available when the **hattrix** option has been previously registered. See the Accounts section for more information on the hattrix feature.

Alarm management

- For information on alarm management, see [Alarm Management](#).

Password rules

The purpose of this feature is to add more parameters to the operator's password.

1. On the **Options** tab, click **System parameters** and click **Server**.
2. Click the **Password rules** tab and select **Specific password rules**. To create strong passwords, for each field, select the following values:
 - A minimum of 8 and a maximum of 20 characters.
 - A minimum of 1 numerical character.
 - A minimum of 1 special character.
 - A minimum of 1 uppercase letter.

① **Note:** Also, when you create passwords, remember the following rules:

- Passwords are case sensitive.
- Passwords cannot contain the word `Kantech`.

Result

After you select this option, all newly created or modified operators must comply with the password rules.

Gateway parameters

The Gateway section is only available in EntraPass Global Edition to setup parameters for your NCC Global, KT-NCC and Multi-Site gateways.

The Multi-Site gateway parameters include a **Failsoft event interval delay** option. This defines the time between successive fail-soft messages. This option is used to reduce the impact of controllers, following a communication error, on the network.

KT-NCC global features

These parameters are defined for a Global gateway.

- **Report input in alarm when the alarm system is armed:** check this box if you want the system to generate the “input in alarm” messages only if the alarm system is armed. If there is a monitoring schedule on an input, and if this box is not checked, the system generates the input in alarm event even if the alarm system is not armed.
- **Enable card already busy feature:** If this feature is checked, a cardholder is not able to open another door before the door open delay is expired on the first door. Check this feature to prevent cardholders from opening a door for example for someone else and then attempting to open another door during the first door open delay.
- **Multiple messages on prevent arming:** an input or group of inputs can be used to prevent arming (**Definition > Alarm System > Input**). If arming is attempted while a group of inputs is in alarm, the system will not arm and generates an “aborted arming event”. If this option is not checked, only one message is generated even if arming was prevented by more than one component.

KT-NCC

To facilitate a situation where the EntraPass server site is distant from the KT-NCC site, configure the KT-NCC site to communicate through the Internet, complete the following steps:

1. Select the **Inbound server router** check box.
2. Choose one of the following options:
 - Select **IP address**, and type the new address in the IP address field.
 - Select **Domain name**, and type the domain name.

If the EntraPass server site is on the same LAN as the KT-NCC site, complete one of the following fields:

- In the **Default Domain Name** field, type the domain name of the server.
- In the **DNS server address** field, type the server IP address.

To prevent any firmware applications download, select the **Firmware reload control** check box.

To select, which firmware applications download to the controller, select the controller type check boxes.

Firmware parameters

This section contains all the information pertaining to controllers, gateways and IP communication module, and the section to update you firmware.

- ❗ **Note:** The KTES tab is only available if a KTES controller is 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 uses 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 uses 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 uses 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.
 - ① **Note:** The automatic firmware update function applies only to KT-400s that support it.
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/KT-2

The **KT-1/KT-2** tab specifies the location of the folder containing the firmware for KT-1 and KT-2 controllers. The system uses this data to update the installed controllers.

- Select the **Enable TFTP KT-1/KT-2 updater** option to allow operators to upgrade the controller firmware using the **Update firmware** button from the **Operation > Site** dialog in EntraPass.
- **Enable automatic firmware update:** Select to make an update of each controller with a different firmware version.
 - ① **Note:** The automatic firmware update function applies only to controllers that support it.
Restart the multi-site Gateway 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 uses 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 uses this data to update the installed firmware .

- When checked, the **Enable TFTP IP Link updater** option allows operators to upgrade the IP Link firmware from the **Update firmware** button from the **Operation > Site** dialog in EntraPass.
 - ① **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.

KT-NCC

The **KT-NCC** tab specifies the location of the folder containing the firmware for KT-NCC. Unlike the other firmware, KT-NCC is updated automatically when a version of EntraPass Global Edition is upgraded.

- ❗ **Note:** There are two generations of the KT-NCC: Gen 1 and Gen 2. You can check the controller's label to see which generation the controller is.
- When checked, the **Enable TFTP KT-NCC updater** option will allow operators to upgrade the KT-NCC firmware from the **Update firmware** button from the **Operation > Site** dialog in EntraPass.
 - ❗ **Note:** The EntraPass Server computer must be restarted in order to enable the TFTP KT-NCC 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 uses this data to update the installed readers.
 - ❗ **Note:** There are two generations of ioSmart readers: Gen 1 and Gen 2. You can check the reader's label or the full status to see which generation the reader is.
 - ❗ **Note:** The ioSmart Gen 2 is not supported by the KT-400 WINCE. Ensure that you update the controller firmware before you update the reader firmware.

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 uses this data to update the installed controllers.

- When checked, the **Enable TFTP KT-401 updater** option allows 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.
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 define parameters for the badging features. You can define image quality for picture, signature, and background images.

- If you are using the badging feature, 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 can reduce the jpeg quality of your images so that they do not occupy a large space in the database. However, 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 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 is 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.
 - ① **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 is 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 creates **Picture** and **Signature** directories under C:\Program Files\Kantech\Server_GE\Data where all pictures and signatures will be saved instead of directly in the database.
- ① **Note:** When modifying an existing picture or signature, EntraPass saves 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.
 - ① **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_GE\Data where all graphics will be saved instead of directly in the database.
 - ① **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.

- When CSV (comma separated values) is selected as the output process for your reports, the system includes the date and the time in a single field. It is recommended to check the **Date and time on separate fields** option . When you select this option, the system separates 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 aborts 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 by 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 are not included in the report. This creates the event **Report event quota exceeded**. This is displayed in the desktop Messages and is added to the report.

User name format

Specifying the user name format tells the system how card holder's names are displayed in EntraPass.

- **Parse user name** must 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 is used to parse the user name fields. Options are: Comma, Period, Equal, Semicolon, Colon, Space.
 - **Strict search on card field** must be empty unless you want 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 displays all user names that start with an A just by entering A as a lower and upper boundary.

Video parameters

The **Video** section only displays if the Video integration option is enabled in the EntraPass system. You can 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** keeps 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 are 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 processes 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** allows 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** allows 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 allows 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_GE\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 generates as many log files as there are control applications running concurrently (RVPControl_LOG_05 to 08). The number of error log files are 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 displays in the video thumbnails.

- The **Video image snap** indicates the quality of the image that is saved as a thumbnail for each video. If you choose 10, the saved image quality is 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** disables 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 uses 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 applies 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 is 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** disables the option.
- **By Gateway** automatically synchronizes the time of all computers with the Gateway selected in the scrolling list.
- **By Server** automatically synchronizes 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

On the **Card** tab, System Administrators can 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 is handled by user name and can have up to 5 different numbers. This allows for creating cards without assigning a card number to the new cards, see Issuing a New Card in Enhanced User Management Environment This option is used with the EntraPass web for card management. For more information about EntraPass web, refer to the *EntraPass web User Manual*.

- ❗ **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. For more information, see [Issuing a new card in enhanced user management environment](#).
- **Badge credential outside account:** Indicates whether to use the badging system for cards that do not belong to any account as well as the initial state of the added card number.

- **Mandatory card number when verified:** The system waits for a card number before changing the badge status from **Printed** to **Verified**.
- **Clear upon validation:** Clear the account name upon validation from the badge status section in the **Badge Request** window.

① **Note:** These fields are available only when the **Badging Credential** option is enabled.

Badge printer

In the **Badge Printer** tab, you can associate a technology to a local printer. The system then uses the printer corresponding to each linked technology. If you have two printing workspaces, you are able to dispatch your printings to one or the other.

From the **Credentials/Badge** printer menu, enter the printer configuration descriptions. To associate a printer configuration description to a printer, see [Printers Selection and Configuration](#).

① **Note:** The Badge printer tab is only available when the **Badging Credential** option is enabled.

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 on to apply the change to the toolbar.

Assign a new connection to a site

① **Note:** 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)

① **Note:** No reference will be made virtual sites unless at least one has been created previously (see [Site Configuration](#) for details). This is also valid for each account.

① **Note:** Same options (Prompt, Mandatory, Disable) exist under **Accounts>Miscellaneous**.

① **Note:** When creating an account in EntraPass using the **Mandatory** option, a connected site will be created automatically.

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.

① **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

About this task:

There are five free go Pass licenses included with EntraPass. The free licenses are in addition to any purchased licenses.

Use go Pass with a smartphone or an Apple watch to lock or unlock a door from a remote location. For a higher level of security, use an ioSmart reader with the door. ioSmart readers use BLE technology. Select an option from the **Proximity Restriction** list to cater for a range of security levels.

1. To display a cardholder's encrypted personal profile on notification e-mails, select the **Display viable notification information** check box. Cardholders use their personal profile details or a link on 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 card holders** button.
3. To control how and when SmartLink responds to invalid go Pass commands, define all three settings in the **Security** area:
 - To set how many invalid requests occur before SmartLink responds, enter a number in the **Notification debounce on wrong request** field.
 - To set the time to pass before SmartLink responds, enter a number in the **Debounce delay (ss)** field.
 - To prevent SmartLink responding to any go Pass requests 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 requests + "Too many goPass failed request" event displays.
4. In the **Direct BLE** section, you can use the ioSmart credential features to add extra security or allow users to access doors when they are offline by configuring the **Key Cycle** and **Key Lifespan** fields:

- **Important:** The **Use Key Cycle** check box is selected by default to enable both the **Key Cycle** and **Key Lifespan** configurations. These features provide optimal security. Do not disable them unless required.
- a. **Key Cycle** is an hourly interval of time for which a new key for Bluetooth Low Energy (BLE) authentication is generated. For example, if you enter **4**, then a new key is generated every four hours. You can enter a Key Cycle value between 1 and 72 hours. A low Key Cycle number results in a higher level of security because a new key generates more often.
 - ❗ **Note:** If you make a change to the Key Cycle timing, then the KT-NCC and Global Gateway reload.
 - b. **Key Lifespan** is how long a BLE key is valid. For example, if you enter **8**, then the key is valid for eight hours. The minimum value for Key Lifespan is the same as the Key Cycle value, and the maximum value is twice the Key Cycle value, up to 120 hours. For example, if the Key Cycle is 20 hours, then you can enter a Key Lifespan value between 20 and 40 hours. Enter a high Key Lifespan number for users with inconsistent internet access, such as in remote areas, to allow the user to access a door while offline for up to five days (120 hours).
 - ❗ **Note:** For optimal security results, use a short Key Cycle and Key Lifespan. The Key Cycle default value is 12 and the Key Lifespan default value is 24.
 - To edit the Key Cycle and Key Lifespan values at an account level, click **Account>Options** and the go Pass settings appear.
 - To edit the Key Cycle and Key Lifespan values at a user level, click **Card>Card number** and the go Pass settings appear.
 - ❗ **Note:** To use the ioSmart Mobile Credential feature, you must have the following specifications:
 - go Pass version 2.20 or later
 - ioSmart firmware version 1.09 or later
 - KT-1 version 3.07 or later
 - KT-400 version 3.01 or later
5. 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.

Using the SmartTap feature

About this task:

Go Pass users connected to a hattrix system can use the SmartTap feature. The SmartTap feature uses a BLE scan to unlock the door for users with valid access.

Table 68: SmartTap software and firmware requirements

Component	Version
ioSmart Gen 1	1.10.11 and later
ioSmart Gen 2	2.02.12 and later
go Pass application	2.23 and later
iOS	9 and later
Android	6 and later

The SmartTap feature is turned on by default and cannot be turned off. To configure and use the SmartTap feature with your mobile device, complete the following steps:

1. Configure the SmartTap permissions in your mobile device:
 - For iOS devices, enable the following permissions:
 - Location
 - Notifications for SmartTap
 - Bluetooth access
 - Access to discover devices in the local network
 - For Android devices, enable the following permissions:
 - Location
 - Background location, only applicable for Android versions 10 and later
 - Bluetooth permission, only applicable for Android versions 12 and later
2. To unlock the door, bring your mobile device within one foot of a reader.
3. To adjust the BLE filter strength in the go Pass app, use one of the following options:
 - For iOS devices:
 - i. In the **Settings** tab, triple-tap the **Settings** label.
 - ii. In the **Scan filter options** drop-down, select the RSSI and tap **Set RSSI Value**.
 - For Android devices:
 - i. In the **Settings** tab, long-press the **Settings** label.
 - ii. In the **Scan filter options** drop-down, select the RSSI and tap **Set RSSI Value**.

Configuring the BLE mode in EntraPass for the SmartTap feature

In EntraPass, there are three BLE modes that affect how the SmartTap feature works in the go Pass app:

- **None:** SmartTap does not work. You can see a list of doors in the Sites and Doors tab and can unlock any door remotely without BLE technology.
- **Hybrid:** You can see the list of doors in the Sites and Doors tab and unlock BLE doors when your mobile device is near the reader. To unlock non-BLE doors, tap the door name. For BLE doors, SmartTap is enabled.
- **Strict:** You only use SmartTap, and the Sites and Doors tab does not display a list of doors.
 - The app displays the nearest locked door as a red icon, which changes to green when unlocked.
 - If no door is in range, then a grey icon with a **No doors in range** message displays.

To change the BLE mode, complete the following steps:

1. in the EntraPass hatrix system, navigate to **Account>Account menu>Menu**.

2. From the **Proximity restriction** drop-down list, select the BLE mode.

EntraPass Server

Use server to define capacity, diagnostic capabilities, and security parameters specific to the EntraPass Server. To obtain information that relates to EntraPass Workstation and EntraPass Server section see .

Use [Application](#) to view the current operational status between the EntraPass Server and the Workstations connected to it. The [Error Log](#) displays system errors identifying the Workstation, the date and time, the code number, and a description. To view the login and logout events for all Workstations, use the [Log](#) window, and use [Restores](#) to restore data previously backed up.

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

About this task:

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

About this task:

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, such as Kantech, and the system only displays 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.
 - **Account:** The account name.
 - **Code :** When selected, all columns are sorted according to the **Code** column in alphabetical order.
 - **Workstation :** When selected, all columns are sorted according to the **Workstation** column in alphabetical order.
 - **Error Code :** When selected, all columns are sorted according to the **Error Code** column in alphabetical order.
 - **Description :** When selected, all columns are 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.

- ① **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

About this task:

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. In the **Text filter** window, enter the text string, for example *Kantech*, and the system will only display logs containing the specified string text. To return to normal display, click **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.
 - **Account:** The account name.
 - **Workstation:** When selected, all columns are sorted according to the **Workstation** column in alphabetical order.
 - **Operator name:** When selected, all columns are sorted according to the **Operator** name column in alphabetical order.
 - **Transaction:** When selected, all columns are sorted according to the **Transaction** column in alphabetical order.
4. To change the **background color**, right-click in the window and select **Background color** from the displayed shortcut list. Pick a color from the standard Windows dialog.
5. To clear the window, right-click in the window and select **Delete All** from the shortcut menu.
6. **Optional:** To export the logs to a CSV file, right-click in the window and, from the shortcut menu, select **CSV Export**.

Registration

Use this menu to register new system components, including the KTES, Workstation, Gateway, SmartLink, to register and use the system's database and to establish communication with the Server. For more information, see [System Registration](#).

Report Log

About this task:

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 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.
 - **Reportname** : 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 can restore a backup copy onto another computer, that has the EntraPass server 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.

Use the following safeguarding 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 and keep them in different locations.
- To backup your files, use any of the following options:
 - The menu of the EntraPass backup utility.
 - The EntraPass backup scheduler to apply automatic schedules parameters.
 - Other third party software and hardware.

- ❗ **Note:** By default, when you backup or restore files, the EntraPass database is temporarily disabled. In the EntraPass application main window, the second colored square at the bottom left of the screen turns red when the database is unavailable. Modifications made on the workstations are not 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_GE \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

About this task:

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.

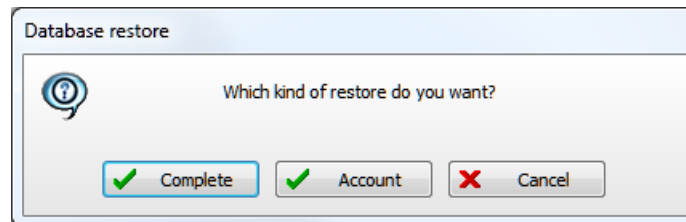
1. Select the item you want to backup:
 - **Backup Data**
 - **Backup Archive**
 - **Backup In/Out**
 - **Backup Video Events**
- ❗ **Note:** By default, EntraPass backs up all the information originating from the following directory: C:\Program Files\Kantech\Server_GE\Data or Archive or In/Out to C: \ProgramFiles\Kantech\Server_GE\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

About this task:

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 appropriate 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** list. Click **OK** to launch the restore process.
3. If the **hatrix** option has previously been registered, EntraPass will ask for the kind of restore to apply:



4. If you click the **Complete** button, the system restores all the information from the selected directory.
 - ① **Note:** By default, the system restores all the information originating from the following directory: C:\ProgramFiles\Kantech\Server_GE\Backup\ X_YYYY_MM_DD-h_mm_ss to C:\Program Files\Kantech\Server_GE\Data or Archive or In/Out.

We recommend to reload the Gateway after restoring the data (Operation > Reload data).

If a **Clean Database** command is executed, it will be impossible to restore the deleted account.

Options

Connection password modification

The connection password is used to authenticate EntraPass workstations to the EntraPass server. The connection password window displays automatically when the system is not registered.

⚠ CAUTION: You cannot reset the connection password if you forget it.

① **Note:** You must use a specific password. You cannot use the default password.

Changing the connection password

1. On the **Options** tab, click **Connection password**.
 2. In the **Old connection password** field, enter the current connection password. Passwords are case sensitive.
 3. In the **New connection password** field, enter the new connection password.
 4. In the **Verify connection password** field, enter the new connection password to confirm it.
 5. Click **OK** to exit. If you receive an error message, make sure that the data you entered in the **New connection password** and in the **Verify connection password** fields are identical.
- ① **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, Portuguese, German, Italian, Dutch, Turkish, Simplified Chinese, Norwegian, Finnish, Swedish, Danish, Czech, Slovak, and Haitian Creole. Use the vocabulary editor utility to add other custom languages.

Changing the system language

1. From the EntraPass main window, select the **Options toolbar**, then click the **System language** button. Or for accounts within a master account in hattrix systems, click the **Account language** button.

① **Note:** When you modify the primary language, the database operation is 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. If an operator needs a different system language than the defined primary or secondary language in the account, see [Changing the system language for an operator](#).
3. Log out of EntraPass and log on again.

System date and time modification

About this task:

Use the **Change system** option with caution and only when necessary; this function may affect logical components of the access system (for example schedules). If, for any reason, you want to adjust the system time and date, use 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.

① **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 more information, see [Time parameters](#).

➤ **Important:** Do not change the time using Windows settings. It is strongly recommended to change the system time through the server parameter settings.

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 any of the following options:
 - Menus of the Server/ Backup Tab
 - Backup Scheduler to apply automatic schedules
 - Mirror Database application
 - Other third party software and hardware. Third party software is not recommended.
- ❗ **Note:** By default, when you backup or restore files, the Server databases is temporarily 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

About this task:

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.
 - **Self-extracting compressed file** : will create an executable file (*.exe) that will compress the information so as to reduce the amount of disk space taken by the backup.
 - Under the **Archive, In/Out** and **Video Event** tabs only:
 - **Separate files (full backup)** : will backup all databases.
 - **Self-extracting compressed file (full backup)** : will create an executable file (*.exe) that will compress the information so as to reduce the amount of disk space taken by the backup.
 - **Separate files (incremental)** : will backup all databases. Only the information that was modified since the last backup will be saved.
 - **Self-extracting compressed file (incremental)** : will create an executable file (*.exe) that will compress the information so as to reduce the amount of disk space taken by the backup. Only the information that was modified since the last backup will be saved.

❗ **Note:** Restoring a self-extracting backup after an EntraPass upgrade can only be done from the EntraPass Server where the original self-extracting backup was done.

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.

Utilities

Use utilities to manage, maintain and optimize EntraPass. The express setup feature provides a quick and simple way to configure all the components of a new connection, use [Express setup program](#) when configuring a KTES, system gateway, or controller. If you want to define operation modes and schedules for relays, see [Defining relays](#). For input response times and monitoring schedules, see [Defining Inputs](#). To establish which, auxiliary output to use for your controller, see [Defining auxiliary outputs \(LED and buzzer\)](#).

Use the [Database utility](#) program to verify manually the integrity of the database tables. Features include verifying database index, links, and hierarchy, as well as updating database fields and cleaning the database.

The [EntraPass Video Vault](#) is a video data storage and archive management tool. Use this section to install and launch Video Vault, and to manage archived video segments. Use [PING Diagnostic](#) to troubleshoot Internet connection problems to a specific component or computer. To view EntraPass reports without starting EntraPass use [Quick report viewer](#) from Windows Start menu.

If you want to communicate with an external device, for example a video matrix switcher, or paging system without special drivers, install the [The SmartLink interface](#) application. Use the SmartLink interface to define a message and format type that EntraPass sends using the second COM port or a disk file.

Use the [Vocabulary editor](#) to change the Graphical User Interface (GUI) language, choose from English, French, Spanish, Portuguese, German, Italian, Dutch, Turkish, Simplified Chinese, Norwegian, Finnish, Swedish, Danish, Czech, Slovak, and Haitian Creole.

Database utility

The database utility program verifies the integrity of the database tables that are used to store events, alarms, network alarms, and graphics. 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, they can 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: You must shut down the EntraPass Server 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 Global 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

About this task:

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.
 - ① **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.

- ① **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 is assigned to a functionality and this schedule is deleted, the system initializes the field where it is assigned in the primary database. It also removes the records that point to deleted components. For example, if an access level is assigned to a gateway and this access level is deleted, it deletes 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 is deleted. For example, if a schedule is deleted, the system uses the link list to initialize all the database fields that contains this schedule.

- ① **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. This 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 considerably reduces the space required by your database. It also improves system performance relating to searches for card information. It does not affect the table Registry, nor does it have an impact on historical reports.

-  **Note:** You must back-up the database before performing this operation. Cleaning the database suspends 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. Video recordings have a limited life span depending on the video server setting and capability. Because 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 processes 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
- ① **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

About this task:

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 the 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, connection, number of connections, connection name, number of controllers on a connection, etc. For example, users can modify a door's name by automatically applying default settings to all relays and inputs of controllers connected to the selected door.

Configuring a global connection using Express Setup

1. From Windows Start menu: **Start > All Programs > EntraPass Global Edition > Server > Express Setup NCC**. The system displays the Express setup window with a progress of the startup. Then Operator logon window appears.
2. Enter your operator name and password to log on, and click **OK**. The Express Setup window displays on the screen.
3. Select the **Gateway** and **Reader type** that is used in conjunction with the doors configured under this gateway.

4. Click **Next** to continue.
5. You can modify the **Gateway name**.
 - Specify the **NCC connection** type between the NCC and the gateway:
 - **RS-232**: Select if the NCC is installed on a separate computer than the gateway.
 - **Integrated with gateway**: Select if the NCC computer is the same as the gateway computer.
 - Specify the **Number of controller loops (max: 8)** on this gateway.
6. Click **Next** to continue. The system displays the next window. Depending on the number of controller loops you have entered in the previous window, the system may display the next window more than once.
7. Specify the **connection name** and the **Number of controllers** on this connection.
8. Click on **Next** to continue. The system displays the next window. Depending on the number of controllers on the connection you have entered in the previous window, the system may display the next window more than once.
9. Specify the **Controller Name**.
 - Specify if the **Door configuration** by defining if readers are located on the same door or on separate doors.
 - Select the appropriate **Reader and Keypad** option.
 - Select the "define all relays and inputs" boxes if you want the system to automatically label (address) them.
10. Click **Next** to continue.
11. Specify the door names (primary and secondary language) and click "**Finish**" to end.
 - ① **Note:** If you have more than one controller connection on the gateway, the system displays the last three windows until all of the controllers connections are defined.

Configuring a multi-site gateway connection using express setup

1. From the Windows® Start menu: Start > **All Programs > EntraPass Global/Corporate/ Special 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.
 - ① **Note:** The Operator login window appears only when starting Express setup in stand-alone mode.
2. Enter your Operator user name and password, then click **OK**. The **OK** button is enabled when the **Password** field contains data.
3. Select the gateway for which you want to configure a connection, then click the **New connection** button.
4. Enter the connection name in the **connection description** field, then select the reader type.
5. Select the **Controller type** for this connection.
 - ① **Note:** The KTES option is available for a Multi-site Gateway only.
There is no **reader type** or **number of controllers** to select when the controller type is a KTES.
6. Select the **Reader type**.
7. Set the **Number of controllers**.

8. 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 **IP address (KT-400)** if applicable. Complete the associated tabs.
 - Select **IP address (KTES)** if applicable. Complete the associated tabs.
 - Select **IP address (IP Link)** if applicable. Complete the associated tabs.
 9. Click **OK** .
 10. 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.
 11. For a new site with a **KTES**, go to [Step 14](#).
 12. 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.
 13. 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.
 14. Go to [Step 16](#).
 15. Check the **Door contact** option.
 16. Check the **Postal lock** option, if applicable, for a KTES only.
 17. Enter the **Serial number** , if this column is displayed. The serial number (**S/N**) is on a sticker and generally starts with **Axxxxxxx** .
 18. 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.

Result

The following are default values assigned to controllers by the Express Setup program.

Table 69: Express Setup controller default values

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
KT-2	2	2	8	5

The following table summarizes how input zones are used by the system for controllers.

Table 70: How the system uses input zones for controllers

Input zone	System use	Controllers
1	Door 1 contact	KT-100, KT-200, KT-300, KT-400, KT-1, and KT-2
2	Door 1 Rex	
3	Door 2 contact	KT-300
4	Door 2 Rex	
5	Door 2 contact	KT-400 and KT-2
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 table summarizes how input zones are used by the system for the KTES.

Table 71: How the system uses input zones 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.

Table 72: How the system uses output zones

Auxiliary output	Use	Controllers
1	LED (Door 1)	KT-100, KT-200, KT-300 and KTES
2	Buzzer (Door 1)	

Table 72: How the system uses output zones

Auxiliary output	Use	Controllers
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)	
1	OUT1 (Door 1)	KT-1
2	OUT2 (Door 1)	
3	LED (Door 1)	
4	Buzzer (Door 1)	
5	Unassignable	
1	LED (Door 1)	KT-2
2	Buzzer (Door 1)	
3	LED (Door 2)	
4	Buzzer (Door 2)	
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

About this task:

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 can 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 **Save** and a message box displays the following message: 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 return to the express setup by clicking **Express Setup**.
- ❗ **Note:** The KT-300 is a 2-door system and the KT-400 is a four-door system.
4. Click **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 can later modify any component description in its definition menu (**Devices>Controller/Door/Relay/Input/Output**).

Configuring a KTES using Express Setup

About this task:

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** button in the **KTES** dialog.

1. From the **Site** window, click **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 **Save** and a message box displays the following: 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 **No**, you can return to the express setup by clicking **Express Setup**.
4. Select the **Door contact** and the **REX contact** options.
5. Select 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

About this task:

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

About this task:

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)

About this task:

When you define a controller or a KTES, you can also change the assignment of auxiliary outputs. On the EntraPass workstation, click **Devices** and click **Output**.

1. Select the first undefined output; its check box is not gray. Select it to enable the language fields, and then assign names to it.
2. Choose the **Operating mode** option.
3. Assign a door to the output from the **Selected doors** list.

Result

The following table summarizes how output zones are used by the system.

Table 73: How the system uses output zones

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

About this task:

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.

1. From the Windows® Start menu, click Start > **All Programs** > **EntraPass Global 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 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

About this task:

The **Quick Report Viewer** program allows operators to view previously saved reports without having to start EntraPass. It is used to view, display and load reports that were previously saved (in a.QRP format) during a print preview or Quick reports. For more information about 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, browse to the folder to select the report.
4. Click **Open** to preview the report.
5. Use the toolbar buttons to preview the report.

Table 74: Report toolbar icons







Icon	Description
	Use the Zoom out icon to zoom out the report view.
	Use the Zoom In icon to display details.
	Use Previous Page and Next Page icons to change pages.
	Use the Open icon to open a report located in any folder on your computer.

Table 74: Report toolbar icons

Icon	Description
	Use the Print icon to print the report. There is no printer setup dialog box, the report prints automatically. To cancel the printing, click Cancel .
	Use the Quit icon to quit the application.

The SmartLink interface

The SmartLink interface allows users to define a message and format type that may be sent on the second COM port or to a disk file. The following section explains how to build a character string that can be sent through the SmartLink. Using the SmartLink feature, you can interface to most intelligent devices such as video matrix switchers and paging systems. To do this, a RS-232 link is cabled between one of the EntraPass workstations and the external device. The necessary command strings and protocols can be easily edited on connection to fit most jobs.

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

To use the SmartLink application, you require the following items:

- A computer that meets the same requirements as an EntraPass Workstation. For more information, see [Minimum System Requirements](#).
- Installation CD-ROM for the SmartLink application including the serial number.

Installing the SmartLink application

1. From the **Workstation Registration** menu, create the new application. For more information about how to create new applications, see [Minimum System Requirements](#).
2. Install the SmartLink application on the computer. For more information, see [System Installation](#).

❗ **Note:** EntraPass web installs with **SmartLink** automatically.

3. After you install the SmartLink application, you must configure the SmartLink application.
4. If you are using the message mode, you must create tasks. For more information about how to create tasks using the task builder, see [Task Builder Definition](#).

Configuring the SmartLink application

Configure SmartLink on an ordinary EntraPass workstation or on any EntraPass workstation for configuration that is found on the same computer as the Server software. Depending on the modes that you want to use for the SmartLink, messages or commands, you must program the workstation accordingly. For more information, see [Configuring the SmartLink application](#).

Starting the SmartLink application

- On the computer where you installed the SmartLink application, on the Windows taskbar, go to: **Start > All Programs > EntraPass > SmartLink > SmartLink**. The SmartLink application starts. The application user interface includes status information about the SmartLink application. This information allows installers to quickly identify any issues with the system.

- ① **Note:** Limited support is provided on the SmartLink interface.

Vocabulary editor

Use the vocabulary editor to translate the display text of the software into the language of your 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, Spanish, Portuguese, German, Italian, Dutch, Turkish, Simplified Chinese, Norwegian, Finnish, Swedish, Danish, Czech, Slovak, and Haitian Creole, 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:

1. Translating the source text
2. Integrating the newly created language to the EntraPass dictionary in the Server
3. Distributing the new custom language to all EntraPass application

- ① **Note:** 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, contact 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.

- ① **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

About this task:

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 assists you if you want to translate the software in a language, other than English, French, Spanish, Portuguese, German, Italian, Dutch, Turkish, Simplified Chinese, Norwegian, Finnish, Swedish, Danish, Czech, Slovak, and Haitian Creole.

1. Start the Vocabulary editor from the Windows® **Start** menu: click **Start > All Programs > EntraPass Global 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.

- ① **Note:** You must make sure that the Customdictionary directories are regularly backed up (C:\ProgramFiles\Kantech\Vocabulary Editor\CustomDictionary\files.xxx.ath) or C:\ProgramFiles\Kantech\“Application type”\CustomDictionary\files.xxx.0

Result

The following table shows the value of the Vocabulary Editor color codes.

Table 75: Vocabulary editor color codes

Vocabulary editor color codes	Value
Green	Valid text string.
Blue/Green	New text string.
Red	Obsolete text string.





- The “Source language” column contains text based on the basic language that was selected during the creation of the vocabulary. This column will serve as a “source” for the translation. Software language columns cannot be modified by the user.
- Use the right-click to enable a contextual sub-menu or use the **Language editor** toolbar. A hint appears when you position the mouse over a button.

Integrating the custom language in EntraPass

About this task:

After the translation is finished, integrate the new dictionary into the system dictionary so that system operators can use it. The following table describes the icons in the vocabulary editor window. You can also select these options from the **Actions** menu.

Table 76: Vocabulary editor icons

Icon	Description
	Apply changes to operational dictionary: Select this option when you want to test your changes before you update other workstations.
	Restore operational vocabulary: Select this option to restore the default languages. It creates a self-extracting file which restores the original dictionary.
	Scan dictionary for new entries: Select this option when the software was updated.
	Create self-extracting file for update: Select this option if you decide to implement the new vocabulary. The system creates an <code>Updatedictionary.exe</code> 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.
 - ❶ **Note:** The Graphic User Interface appears only in one of fifteen languages: English, French, Spanish, Portuguese, German, Italian, Dutch, Turkish, Simplified Chinese, Norwegian, Finnish, Swedish, Danish, Czech, Slovak, and Haitian Creole.
2. Select a newly translated vocabulary.
 - You can 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, click the **Actions** menu and select **Create self-extracting file for update**. 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)`.

- ① **Note:** 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 and click **Update dictionary**.
5. Add the `Updatedictionary.exe` to every computer where EntraPass is installed, and double-click it to launch the language update. Exit all EntraPass applications before you run the self-extracting file.
6. Select the applications you want to update, one at a time, and click **Update dictionary**. The system automatically copies the vocabulary to the **Custom Dictionary** directory, and merges the custom directory with the application dictionary.

- ① **Note:** You must update all the applications in the system.

To restore the dictionary to original default values, follow the same procedures as for updating the dictionary.

7. After you finish updating the dictionary database for the Primary Server, the Mirror Database and the Redundant Server, start the Primary server.
8. Click **Options** and click **Select language**.
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 cannot use it.


① **Note:** For example, if your primary language is English and your secondary language is French, and you select the new language, for example Russian as primary, all operators who have English as their display language in the **Operator menu** now see the Russian language. However, if you change the secondary language to Russian, operators must manually select Russian in the **Operator definition** menu to use it. 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, log on to the server and verify the display language. If it correct, update the system.

① **Note:** The computer display and keyboard must support the language.

① **Note:** For every language you install, 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

There are over 90 animated icons in EntraPass that indicate the status of a physical or logical component.

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 is 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.

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. When this delay is over, the system initiates 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 is in 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 is in AC failure and Tamper Switch in alarm

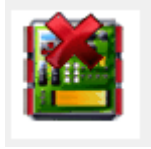


Appears when the controller is in AC failure and the tamper switch is in alarm. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)

- the Operation > Controller Reset

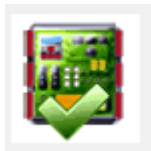
Controller is not communicating



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.

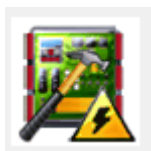
Controller is in Reset and AC failure



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 Switch is 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 Switch in alarm



Appears when the controller is in “reset mode” and the tamper switch is in alarm. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Controller Reset.

Controller tamper switch in alarm



Appears when the controller tamper switch 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

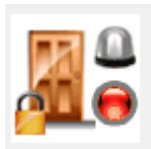
Door forced open (reader disabled)



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 disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door.

Door pre-alarm on open too long



This animated icon appears when the door is opened more than half the time permitted delay set in "open time". It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door.

Door pre-alarm on open too long (reader disabled)



This animated icon appears when the door is opened more than half the time permitted delay set in "open time" and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door.

Door still opened schedule invalid



This animated icon appears when the door is opened and the unlock schedule is invalid. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door.

Door still opened schedule invalid (reader disabled)



This animated icon appears when the door is opened and the unlock schedule is invalid and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/ Elevator door.

Door unlocked by an operator



This animated icon appears when the door is unlocked by an operator (manually). It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door > Elevator door.

Door unlocked by an operator (reader disabled)



This animated icon appears when the door is unlocked by an operator (manually) and the reader is disabled. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door.

Door unlocked by a schedule



This animated icon appears when the door is unlocked by a schedule. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door.

Door unlocked by a schedule (reader disabled)



This animated icon appears when the door is unlocked by a schedule and the reader is disabled.

It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door.

Elevator door unlocked and closed



This animated icon appears when the elevator door is closed and unlocked. It is displayed in:

- the Graphic desktop (Desktop > Graphic desktop window)
- the Operation > Door/Elevator door.

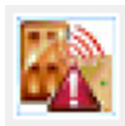
Wireless lock connected



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 alarm system in alarm



This animated icon appears in:

- the “Graphic” window (desktop—graphic) for a relay triggered by an alarm system in alarm.
- the Operation > Relay when the relay is triggered by an alarm system in alarm.

Relay activated by alarm system function



This animated icon appears in:

- the “Graphic” window (desktop—graphic) for a relay triggered by a function of an alarm system.
- the Operation > Relay when the relay is triggered by a function of an alarm system.

Relay activated by alarm system delay



This animated icon appears in:

- the “Graphic” window (desktop—graphic) for a relay triggered by the delay of an alarm system.
- the Operation > Relay when the relay is triggered by the delay of an alarm system.

Relay activated by an event



This animated icon appears in the following:

- 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—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.

Gateway—reload KT-NCC firmware



This animated icon appears in

- the “Graphic” window (desktop—graphic) when the system is performing an automatic upgrade of the KT-NCC firmware.
- the “Operation” when the system is performing an automatic upgrade of the KT-NCC firmware.

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.

End-User License Agreement

Software Terms

Use of this software that is in (or constitutes) this product, or access to the cloud, or hosted services applicable to this product, if any, is subject to applicable end-user license, open-source software information, and other terms set forth at <http://johnsoncontrols.com/techterms>. Your use of this product constitutes an agreement to such terms.